Comput. complex. **7** (1998), 291 – 324
1016-3328/98/040291–34 \$ 1.50+0.20/0

computational complexity

LOWER BOUNDS FOR THE POLYNOMIAL CALCULUS

Alexander A. Razborov

Abstract. We show that polynomial calculus proofs (sometimes also called Groebner proofs) of the pigeonhole principle PHP_n^m must have degree at least $(n/2)+1$ over any field. This is the first non-trivial lower bound on the degree of polynomial calculus proofs obtained without using unproved complexity assumptions. We also show that for some modifications of PHP_n^m, expressible by polynomials of at most logarithmic degree, our bound can be improved to linear in the number of variables. Finally, we show that for any Boolean function f_n in n variables, every polynomial calculus proof of the statement "f_n cannot be computed by any circuit of size t," must have degree $\Omega(t/n)$. Loosely speaking, this means that low degree polynomial calculus proofs do not prove $\mathbf{NP} \not\subseteq \mathbf{P}/poly$.

Subject classifications. 68Q25, 13P10.
Key words. Proof complexity; polynomial calculus; pigeonhole principle.

1. Introduction

Complexity of propositional proofs is rapidly assuming as important a role in the theory of feasible proofs as the role played by the complexity of Boolean circuits in the theory of efficient computations. In many cases it provides a very elegant and combinatorially clean framework for studying the provability of Σ_0^b-formulae in first-order theories of feasible arithmetic, which bears essentially the same message as the original framework of first-order ("uniform") provability.

After Ajtai (1988), Bellantoni *et al.* (1992), Krajíček (1994), Krajíček *et al.* (1995), Pitassi *et al.* (1993) established exponential lower bounds for the bounded depth Frege system F_d, the next logical system to attack was its extension $F_d(MOD_p)$ with MOD_p gates, where p is a prime. Some hope and direction for this research was given by Razborov (1987), Smolensky (1987), where an analogous problem was successfully solved in the context of Boolean complexity.

Along these lines, Ajtai (1994a), Beame *et al.* (1994), Riis (1997) proved (barely) super-polynomial lower bounds for the weaker system $F_d + Count_a$ in which counting modulo a is allowed only implicitly in the form of additional axioms, $Count_a$ expressing some natural combinatorial principle; on the optimistic side, these proofs are suitable for arbitrary integers a, not only for primes. Of special interest to us here is the paper by Beame *et al.* (1994) which contains a reduction from $F_d + Count_a$ to some natural *algebraic* proof system, suggested by Hilbert's Nullstellensatz and named accordingly the *Nullstellensatz proof system.*

More generally, Beame *et al.* (1994) initiated the study of propositional proof systems which simulates the most basic algebraic facts and constructions. Beame *et al.* (1994) itself established a (barely) super-constant lower bound on the degree of every Nullstellensatz proof of $Count_q$ over any ring $\mathbf{Z}_a$, where q is a prime not dividing a (which, along with their reduction, implied super-polynomial lower bounds on the size of proofs of $Count_q$ in the system $F_d + Count_a$).

Beame *et al.* (1995) proved an $\Omega(\sqrt{n})$ lower bound on the degree of Nullstellensatz proofs of the *pigeonhole principle* PHP^m_n. Buss *et al.* (1996) improved the bound from Beame *et al.* (1994) to $n^{\Omega(1)}$ with exponential lower bounds on the proof size of $Count_q$ in $F_d + Count_a$ as a straightforward application. Buss & Pitassi (1996a) proved an $\Omega(\log n)$ bound on the degree of Nullstellensatz proofs for some form of the induction principle. Beame & Riis (1997) showed that every proof of the *onto* version of PHP^m_n in $F_d + Count_a$ must have exponential size by first extending the reduction from Beame *et al.* (1994) to work with this combinatorial principle, and then by proving an $n^{\Omega(1)}$ lower bound on the degree of Nullstellensatz proofs for this onto version.

Clegg *et al.* (1996) introduced an even more natural algebraic proof system that directly simulates the process of generating an ideal from a finite set of generators. They called it the *Groebner proof system*; we, however, prefer to use the term "polynomial calculus," suggested in Buss *et al.* (1996). This is because the reasoning based upon the Groebner basis indeed turned out to be very useful in Clegg *et al.* (1996), as well as in the current paper for *studying* this system, but there is nothing in its *description* that would justify using "Groebner" in the *name.*

Polynomial calculus is stronger than the Nullstellensatz proof system. In fact, Clegg *et al.* (1996) proved an exponential separation between these two by the so-called house-sitting principle. On the other hand, Buss *et al.* (1996)

showed that the Nullstellensatz proof system is essentially equivalent to the *tree-like* polynomial calculus.

In another direction, polynomial calculus over a finite field $\mathbf{F}_p$ clearly makes a subsystem of $F_2(MOD_p)$. Thus, polynomial calculus can be viewed as the next logical step in the program of proving lower bounds for $F_d(MOD_p)$. Pitassi (1996) observed that lower bounds for polynomial calculus proofs of either the onto version of $PHP_n^{n+p^\ell}$ ($p^\ell \ll n$) or $Count_a$ would imply lower bounds for the fragment of $F_d(MOD_p)$ in which formulae are allowed to contain MOD_p only as the output gate.

The Groebner basis algorithm from Clegg *et al.* (1996) gives rise, in a fairly straightforward way, to the interpolation theorem for the polynomial calculus over any finite field. Hence, due to the general theory (see, e.g., Krajíček 1997a, Razborov 1994), lower bounds for this calculus follow from respectable complexity assumptions such as $\mathbf{NP} \cap co - \mathbf{NP} \not\subseteq \mathbf{P}/poly$ or $\mathbf{UP} \not\subseteq \mathbf{P}/poly$.

In this paper we establish almost optimal *unconditional* lower bounds for the polynomial calculus over any ground field. Our central result (Theorem 3.1) states that every polynomial calculus proof of PHP_n^m must have degree $\geq (n/2)+1$. This improves upon the Nullstellensatz $\Omega(\sqrt{n})$ bound from Beame *et al.* (1995) both qualitatively and quantitatively. The proof is fairly straightforward: for the lexicographic ordering of variables we manage to construct explicitly the Groebner basis (in the dual form) and prove its necessary properties.

We also present some variations of this result. In particular, we show how to improve the bound to linear *in the number of variables* at the expense of introducing some generalizations of PHP_n^m, whose degree is at most logarithmic (Theorems 4.2, 4.5).

We also give one application of our bound within the framework for studying the provability of central open problems in computational complexity that was proposed in Razborov (1995a) (see also Razborov (1996) for a more updated account). Recall that we take as our primary length measure the number of input *strings* 2^n (rather than the number of input bits n) and ask if there are short propositional proofs (or proofs in certain fragments of bounded arithmetic as in Razborov 1995a) of the tautology $\neg Circuit^*_{t(n),n}(f_n, \vec{p})$ which expresses that no propositional vector $\vec{p}$ encodes a $t(n)$-sized circuit in the class specified by the formula $Circuit^*$ that computes the function f_n in n variables. We prove that, for any $f_n, t(n)$ and any ground field, every polynomial calculus proof of $\neg PDNF^*_{t(n),n}(f_n, \vec{p})$ must have degree at least $(t/2)+1$, where $PDNF^*$ corresponds to the class of all perfect disjunctive normal forms, and the size $t(n)$ of a PDNF is the number of its elementary conjunctions (Theorem 5.1).

This implies an $\Omega(t/n)$ lower bound on the degree of polynomial calculus proofs of the tautologies $\neg Circuit_{t(n),n}(f_n, \vec{p})$, corresponding to ordinary circuits over a complete basis (Corollary 5.2).

2. Notation and preliminaries

Fix an arbitrary field k. We will be working in the k-algebra $S_n(k)$ which results from factoring the polynomial ring $k[x_1, \ldots, x_n]$ by the ideal generated by the relations $x_i^2 - x_i$ $(1 \leq i \leq n)$.[1] Every element $f \in S_n(k)$ has a unique representation as a multilinear polynomial (which determines its *degree* $\deg(f)$), and a unique representation as a k-valued function on $\{0,1\}^n$. We will be alternately exploiting both representations.

Definition 2.1 (Clegg *et al.* 1996). A *polynomial calculus proof* is a directed acyclic graph in which every line is an element of $S_n(k)$. The rules of inference (called *addition* and *multiplication*, respectively) are

$$\frac{f \qquad g}{\alpha f + \beta g} \tag{2.1}$$

and

$$\frac{f}{f \cdot x}, \tag{2.2}$$

where $f, g \in S_n(k)$; $\alpha, \beta \in k$, and x is a variable. For $f_1, \ldots, f_m, g \in S_n(k)$, a *polynomial calculus proof of g from $f_1, \ldots, f_m$* is a proof in which initial polynomials are among $f_1, \ldots, f_m$, and the final polynomial is g. A *polynomial calculus refutation of $f_1, \ldots, f_m$* is a polynomial calculus proof of 1 from $f_1, \ldots, f_m$.

Clearly, g has a polynomial calculus proof from $f_1, \ldots, f_m$, if and only if g belongs to the ideal generated in $S_n(k)$ by $f_1, \ldots, f_m$. In particular, $(f_1, \ldots, f_m)$ is refutable if and only if the ideal generated by $f_1, \ldots, f_m$ contains 1, and if and only if (see, e.g., Buss *et al.* 1996, Theorem 5.2) the system $f_1 = f_2 = \ldots = f_m = 0$ has no 0–1 solutions.

The *degree of the addition inference* (2.1) is $\max\{\deg(f),\ \deg(g)\}$, and the *degree of the multiplication inference* (2.2) is $\deg(f) + 1$. The *degree of a proof* is the maximum of the degrees of all its inferences.

[1] S stands for Smolensky who was the first to exhibit the importance of this ring for complexity theory (Smolensky 1987).

Remark 2.2. One important subclass of polynomial calculus proofs is made by *Nullstellensatz proofs* which are simply representations of the form

$$g = \sum_{i=1}^{m} P_i f_i,$$

and the *degree* of this proof is $\max_{1\leq i\leq m}(\deg(P_i) + \deg(f_i))$. In the opposite direction, Buss *et al.* (1996) considered a stronger version of the polynomial calculus in which the multiplication rule has the form

$$\frac{f}{f \cdot g}$$

for an *arbitrary* $g \in S_n(k)$, and the degree of this inference is $\max\{\deg(f), \deg(fg)\}$ so that the degree of a proof is simply the maximum of the degrees of the polynomials appearing in it. However, for the most important case when k is a fixed finite field, this change in the definition affects the minimal possible degree of a proof of g from $f_1, \ldots, f_m$ by at most a constant multiplicative factor for any $f_1, \ldots, f_m, g \in S_n(k)$.

Now we recall some material in Clegg *et al.* (1996) which has been modified for our purposes.

Denote by T_n the set of all *multilinear terms*, i.e., products of the form $x_{i_1} x_{i_2} \ldots x_{i_d}$ with $1 \leq i_1 < i_2 < \ldots < i_d \leq n$. As we noted above, $S_n(k) \approx kT_n$. The *degree* $\deg(t)$ *of a term* t is the number of variables occurring in it. Let $T_{n,d} \rightleftharpoons \{t \in T_n \mid \deg(t) \leq d\}$, and $S_{n,d}(k) \rightleftharpoons kT_{n,d}$ be the linear space of all multilinear polynomials of degree at most d.

Definition 2.3. An ordering $\preceq$ of T_n is *admissible* if:

1. $\forall t_1, t_2 \in T_n(\deg(t_1) < \deg(t_2) \Rightarrow t_1 \prec t_2)$.

2. If $t_1 \preceq t_2$ and $t \in T_n$ does not contain any variables from t_1, t_2, then $tt_1 \preceq tt_2$.

Fix an admissible order $\preceq$ on T_n, and let $\subseteq$ be the partial ordering on T_n w.r.t. divisibility: $t_1 \subseteq t_2$ iff $t_2 = tt_1$ for some $t \in T_n$. Part 1 of Definition 2.3 implies in particular that any admissible ordering $\preceq$ extends the partial ordering $\subseteq$.

For $f \in S_n(k)$, $LT(f) \in T_n$ is the *leading term* of (the multilinear representation of) f w.r.t. $\preceq$. Part 1 of Definition 2.3 also implies that $\deg(LT(f)) = \deg(f)$.

For $f_1, \ldots, f_m \in S_{n,d}(k)$, denote by $V_{n,d}(f_1, \ldots, f_m)$ the set of all $g \in S_{n,d}(k)$ that are provable from $f_1, \ldots, f_m$ by a polynomial calculus proof of degree at most d. Due to the presence of the addition rule, $V_{n,d}(f_1, \ldots, f_m)$ is a linear subspace in $S_{n,d}(k)$. A term $t \in T_{n,d}$ is called *reducible* if $t = LT(f)$ for some $f \in V_{n,d}(f_1, \ldots, f_m)$, and *irreducible* otherwise. Denote by $\Delta_{n,d}(f_1, \ldots, f_m)$ the set of all irreducible terms in $T_{n,d}$. Definition 2.3, along with the closure of $V_{n,d}(f_1, \ldots, f_m)$ under the multiplication rule, ensures that if $t, t' \in T_{n,d}$, $t \subseteq t'$ and t is reducible, then so is t'. Hence, $\Delta_{n,d}(f_1, \ldots, f_m)$ is closed downward w.r.t. the partial ordering $\subseteq$.

Clegg *et al.* (1996) were mostly concerned with the structure of minimal elements in $T_{n,d} \setminus \Delta_{n,d}(f_1, \ldots, f_m)$ which are called the *Groebner basis.* Since in this paper we are interested in lower bounds, our target is the structure of $\Delta_{n,d}(f_1, \ldots, f_m)$ itself.

Terms from $\Delta_{n,d}(f_1, \ldots, f_m)$ are linearly independent modulo $V_{n,d}(f_1, \ldots, f_m)$, and the *reduction process* finds, for every $f \in S_{n,d}(k)$, the unique $f' \in k\Delta_{n,d}(f_1, \ldots, f_m)$ for which $f - f' \in V_{n,d}(f_1, \ldots, f_m)$. Algebraically, this means that we have the representation

$$S_{n,d}(k) = k\Delta_{n,d}(f_1, \ldots, f_m) \oplus V_{n,d}(f_1, \ldots, f_m) \tag{2.3}$$

of $S_{n,d}(k)$ as the direct sum. We will denote the result of the reduction process by $R_{n,d,f_1,\ldots,f_m}(f)$; in terms of the representation (2.3), this is simply the projection onto the first coordinate.

We abbreviate $\{1, 2, \ldots, a\}$ to $[a]$.

Definition 2.4. ($\neg\mathcal{PHP}_n^m$) is the following system of elements in $S_{mn}(k)$; the variables are indexed x_{ij} with $i \in [m]$ and $j \in [n]$:

$$\begin{aligned} Q_i \ &\rightleftharpoons\ 1 - \sum_{j\in[n]} x_{ij}\ (i \in [m]); \\ Q_{i_1,i_2;j} \ &\rightleftharpoons\ x_{i_1j}x_{i_2j}\ (i_1, i_2 \in [m],\ i_1 \neq i_2;\ j \in [n]); \\ Q_{i;j_1,j_2} \ &\rightleftharpoons\ x_{ij_1}x_{ij_2}\ (i \in [m];\ j_1, j_2 \in [n],\ j_1 \neq j_2). \end{aligned}$$

Clearly, for $m > n$ the system of equations $\{Q_i = 0\}$, $\{Q_{i_1,i_2;j} = 0\}$ does not yet have solutions in any field; therefore ($\neg\mathcal{PHP}_n^m$) is refutable. Let m, n be such that $m > n$. For $I \subseteq [n]$, let X_I be the set of all variables x_{ij} with $i \in I$. By $\mathrm{dom}(t), \mathrm{dom}(f)$ we denote the set of all $i \in [m]$, such that at least one variable of the form x_{ij} appears in the term t (in the polynomial f, respectively). Let $T_I, T_{I,d}$ be the set of all terms t (terms of degree at most d, respectively) with $\mathrm{dom}(t) \subseteq I$, and let $S_I(k) \rightleftharpoons kT_I$; $S_{I,d}(k) \rightleftharpoons kT_{I,d}$. M_I is the set of all assignments to variables from X_I that correspond to *total* mappings from I to $[n]$. $M_I \neq \emptyset$ if and only if $|I| \leq n$.

3. Main result

In this section we prove the following theorem.

THEOREM 3.1. *For any $m > n$ and any ground field k, every polynomial calculus refutation of $(\neg\mathcal{PHP}^m_n)$ over k must have degree at least $(n/2) + 1$.*

The strategy of the proof is simple: for $d < (n/2)+1$ we manage to describe $\Delta_{mn,d}(\neg\mathcal{PHP}^m_n)$, $R_{mn,d,(\neg\mathcal{PHP}^m_n)}$ and $V_{mn,d}(\neg\mathcal{PHP}^m_n)$ quite explicitly. We begin with the axiomatic description of $\Delta_{n,d}(\vec{f})$, $R_{n,d,\vec{f}}$ and $V_{n,d}(\vec{f})$ in the general situation; and later we will construct Δ_d, V_d, R_d, satisfying these axioms for the specific case $\vec{f} = (\neg\mathcal{PHP}^m_n)$.

LEMMA 3.2. *Let $f_1, \ldots, f_m \in S_{n,d}(k)$, and $R : S_{n,d}(k) \longrightarrow S_{n,d}(k)$ be some linear operator.*

1. *Assume that*
$$R(f_1) = \ldots = R(f_m) = 0, \tag{3.4}$$
$$\forall f \in S_{n,d}(k)(\deg(R(f)) \leq \deg(f)) \tag{3.5}$$
and
$$\forall f \in S_{n,d-1}(k)\forall i \in [n](R(fx_i) = R(R(f)x_i)) \tag{3.6}$$
(*the latter equation makes sense since* $\deg(R(f)) \leq d-1$, *due to* (3.5)). *Then*
$$V_{n,d}(f_1, \ldots, f_m) \subseteq \mathrm{Ker}(R).$$
In particular, if $R \neq 0$, then $(f_1, \ldots, f_m)$ has no polynomial calculus refutation over k of degree $\leq d$.

2. *Assume additionally that*
$$\forall f \in S_{n,d}(k)(f - R(f) \in V_{n,d}(f_1, \ldots, f_m)). \tag{3.7}$$
Then
$$V_{n,d}(f_1, \ldots, f_m) = \mathrm{Ker}(R). \tag{3.8}$$

3. Suppose now that R satisfies the equality (3.8)*,* $\mathrm{im}(R) = k\Delta$ *for some* $\Delta \subseteq T_{n,d}$*, and that R is a* **retraction***, i.e.,*

$$\forall f \in k\Delta(R(f) = f). \tag{3.9}$$

Suppose also that for some admissible ordering $\preceq$, we have

$$\forall f \in S_{n,d}(k)(LT(R(f)) \preceq LT(f)). \tag{3.10}$$

Then $\Delta_{n,d}(f_1, \ldots, f_m) = \Delta$ and $R_{n,d,f_1,\ldots,f_m} = R$ w.r.t. this ordering $\preceq$.

PROOF. 1. We show by induction on the number of lines in a degree d polynomial calculus proof from $f_1, \ldots, f_m$ that $R(g) = 0$, where g is the last line in the proof. Axioms correspond to (3.4), and (3.6) implies an inductive step for the multiplication rule.

2. (3.7) clearly implies the converse inclusion $\mathrm{Ker}(R) \subseteq V_{n,d}(f_1, \ldots, f_m)$.

3. Let t be a reducible term w.r.t. $\preceq$, and let $f \in V_{n,d}(f_1, \ldots, f_m)$ be such that $LT(f) = t$. Let $f = \alpha t + f'$, where $\alpha \in k^*$ and $LT(f') \prec t$. Since $R(f) = 0$, we have $\alpha R(t) + R(f') = 0$. Hence $LT(R(t)) = LT(R(f')) \preceq LT(f') \prec t$ (we used (3.10) here). In particular, $R(t) \neq t$, which, by (3.9), implies that $t \notin \Delta$. This shows that $\Delta \subseteq \Delta_{n,d}(f_1, \ldots, f_m)$.

If t is irreducible, the difference $t - R(t) \in \mathrm{Ker}(R) = V_{n,d}(f_1, \ldots, f_m)$ cannot have t as the leading term. Along with (3.10), this means that $R(t) = t + f$, where $LT(f) \prec t$. But $R(t) \in k\Delta$, hence the term t appearing in $R(t)$ must be in Δ. This shows the converse inclusion $\Delta_{n,d}(f_1, \ldots, f_m) \subseteq \Delta$.

Since R is a retraction onto $k\Delta$, it is actually the projection onto the first coordinate in the representation

$$S_{n,d}(k) = k\Delta \oplus V_{n,d}(f_1, \ldots, f_m).$$

But we already know that $\Delta = \Delta_{n,d}(f_1, \ldots, f_m)$, therefore this representation coincides with (2.3). Hence $R = R_{n,d}(f_1, \ldots, f_m)$, and this concludes the proof of Lemma 3.2. □

REMARK 3.3. In fact, part 1 of Lemma 3.2 alone already suffices for the purpose of lower bounds. However, properties from more advanced parts of this lemma are needed for our proof anyway; hence giving a complete description of the Groebner basis in our situation requires no more work than merely proving the bound of Theorem 3.1.

From now on we fix $m > n$ and some field k. We order the variables

$$\{x_{ij} \mid i \in [m],\ j \in [n]\}$$

lexicographically:

$$x_{11} \prec x_{12} \prec \ldots \prec x_{1n} \prec x_{21} \prec \ldots \prec x_{mn}.$$

This induces a natural ordering $\preceq$ on T_{mn}. Namely, if $\deg(t_1) < \deg(t_2)$, we always let $t_1 \prec t_2$. Terms of the same degree are also ordered lexicographically: if $t \neq t'$, $t = y_1 y_2 \ldots y_d$ and $t' = y'_1 y'_2 \ldots y'_d$, where $y_1, \ldots, y_d, y'_1, \ldots, y'_d$ are variables and $y_1 \prec y_2 \prec \ldots \prec y_d$; $y'_1 \prec y'_2 \prec \ldots \prec y'_d$, then we let $t \prec t'$, if for the largest ν with the property $y_\nu \neq y'_\nu$, we have $y_\nu \prec y'_\nu$. It is easy to see that $\preceq$ is admissible. We abbreviate $S_{mn,d}(k), T_{mn,d}, V_{mn,d}(\neg\mathcal{PHP}^m_n), \Delta_{mn,d}(\neg\mathcal{PHP}^m_n)$ and $R_{mn,d,(\neg\mathcal{PHP}^m_n)}$ (w.r.t. this $\preceq$) to $S_d(k), T_d, V_d, \Delta_d$ and R_d, respectively.

Now we give two alternative descriptions of the operator R_d: one of them, R^{sem}_d is semantic, and the other, R^{syn}_d, is syntactic. The hard part (which is the essence of the proof) will be to show that $d \leq \frac{n+1}{2}$ implies $R^{\text{sem}}_d = R^{\text{syn}}_d$. Both R^{sem}_d and R^{syn}_d are first defined on T_d and then extended to $S_d(k)$ by linearity.

3.1. Semantic description. Let $I \subseteq [m]$ be such that $|I| \leq n$. Using the set of assignments M_I to variables from X_I, we define the local notion of reducibility on T_I. Namely, let V_I be the (ordinary!) ideal in $S_I(k)$ consisting of all polynomials that are identically zero on M_I. We simply set $\Delta^{\text{sem}}_I \rightleftharpoons \Delta_{|I|\cdot n,\, |I|\cdot n}(V_I)$ and $R^{\text{sem}}_I \rightleftharpoons R_{|I|\cdot n,\, |I|\cdot n, V_I}$ (w.r.t. the restriction of $\preceq$ on T_I). In other words, we apply the ordinary construction of the Groebner basis for true ideals when we do not care about proofs and their degrees.

Now we let $\Delta^{\text{sem}}_d \rightleftharpoons \bigcup_{|I|\leq d} \Delta^{\text{sem}}_I$, and we would like to glue together the local mappings R^{sem}_I in order to get a global mapping $R^{\text{sem}}_d : T_d \longrightarrow k\Delta^{\text{sem}}_d$. Formally we do it as

$$R^{\text{sem}}_d(t) \rightleftharpoons R^{\text{sem}}_{\text{dom}(t)}(t)\ (t \in T_d);$$

our eventual goal is to show that $R^{\text{sem}}_d = R_d$ for $d \leq (n+1)/2$ by checking that R^{sem}_d satisfies all properties in Lemma 3.2. Even with this naive definition, we have (3.7), (3.9) and (3.10) (the latter also implies (3.5)).

Indeed, these three properties can be checked locally, i.e., for the case when $f = t$ is a term. With this remark in mind, (3.10) immediately follows from the corresponding local property for $R^{\text{sem}}_{\text{dom}(t)}(t)$.

Similarly, $t - R^{\text{sem}}_{\text{dom}(t)} \in V_{\text{dom}(t)}$. But it is easy to see that $V_I \cap S_{|I|}(k) \subseteq V_{|I|}$: indeed, $M_I \subseteq \{0,1\}^{I\times[n]}$ is the variety of zeros of the system of polynomials

$$\{Q \in (\neg\mathcal{PHP}^m_n) \mid \text{dom}(Q) \subseteq I\}.$$

Hence, every $f \in V_I$ belongs to the ideal generated by these polynomials and can be easily seen (cf. Buss *et al.* 1996, Lemma 3.1) to have a Nullstellensatz proof from them of degree at most $\max\{\deg(f), |I|\}$. This gives us (3.7).

In order to see (3.9), note that V_I is monotone in I. Hence, $I \supseteq \mathrm{dom}(t)$ and $t \in \Delta_I^{\mathrm{sem}}$ imply $t \in \Delta_{\mathrm{dom}(t)}^{\mathrm{sem}}$ which, in turn, implies $R_d^{\mathrm{sem}}(t) = t$.

In order to go further, however, i.e., to prove the remaining crucial properties (3.4) and (3.6), we have to show that the operators R_I^{sem} glue together "nicely," i.e., they are consistent with each other at intersections of their domains. In other words, we want to show that

$$R_I^{\mathrm{sem}}(t) = R_{\mathrm{dom}(t)}^{\mathrm{sem}}(t) \tag{3.11}$$

for any t, I such that $\mathrm{dom}(t) \subseteq I$ and $|I| \leq (n+1)/2$.

The good news is that (3.11) would already suffice to check the remaining properties in Lemma 3.2, and thus to finish the proof of Theorem 3.1. Indeed, if $Q \in (\neg\mathcal{PHP}_n^m)$, then $Q \in V_{\mathrm{dom}(Q)}$, hence $R_d^{\mathrm{sem}}(Q) = R_{\mathrm{dom}(Q)}^{\mathrm{sem}}(Q) = 0$. This gives us (3.4). The most crucial property (3.6) is almost equally simple, modulo (3.11). Namely, by linearity, we only have to prove that $R_d^{\mathrm{sem}}((t - R_d^{\mathrm{sem}}(t)) \cdot x_{ij}) = 0$ for any $t \in T_{d-1}$ and any variable x_{ij}. But this becomes clear after replacing R_d^{sem} with R_I^{sem}, where $I = \mathrm{dom}(t) \cup \{i\}$: $t - R_I^{\mathrm{sem}}(t)$ is identically zero on M_I; hence the same is true for $(t - R_I^{\mathrm{sem}}(t)) \cdot x_{ij}$ which, in turn, implies that $R_I^{\mathrm{sem}}((t - R_I^{\mathrm{sem}}(t)) \cdot x_{ij}) = 0$. It is worth noting that all the reasoning has been very general so far and is not much deeper than the most basic constructions in algebraic geometry or topology.

The bad news is that in order to prove the innocent-looking property (3.11) we should give a very explicit (and not so easy to justify) description of the operators R_I^{sem} so that the independence of I becomes visible.

3.2. Syntactic description. Fix some $I \subseteq [m]$, $|I| \leq (n+1)/2$. Our goal is to define a mapping $R_I^{\mathrm{syn}} : T_I \longrightarrow S_I(k)$ such that $R_I^{\mathrm{syn}}(t)$ obviously does not depend on I (as long as $\mathrm{dom}(t) \subseteq I$), and gradually to prove that $R_I^{\mathrm{syn}} = R_I^{\mathrm{sem}}$. This will give us (3.11).

Denote the set of all elements of T_I that correspond to *partial* one-to-one mappings from I to $[n]$ by $\widetilde{T}_I$. Suppose that $t \in \widetilde{T}_I$ and $t = x_{i_1j_1}x_{i_2j_2}\ldots x_{i_dj_d}$, where $i_1 < i_2 < \ldots < i_d$. It is convenient to visualize t as the arrangement of d pigeons, tagged $i_1, \ldots, i_d$, to d holes with numbers $j_1, j_2, \ldots, j_d$, where ν's pigeon i_ν sits in the hole j_ν. Both pigeons and holes are sorted from the left to the right in increasing order.

Using these terms we define the following (non-deterministic) process which we call the *pigeon dance*. The first pigeon i_1 flies to some free hole of his choice to the right of him. Then pigeon i_2 does the same, etc. The dance is *aborted* if some pigeon does not have any hole to fly to[2], and is *completed* if all d pigeons safely move to new homes. The pigeons' goal is to complete their dance (actually, Claim 3.7 below will imply that the best strategy for them is to be lazy and always fly to the *closest* free hole). Let Δ_I^{syn} be the set of all $t \in \widetilde{T}_I$ for which pigeons can achieve their goal. Note for the record that the fact "$t \in \Delta_I^{\mathrm{syn}}$" does *not* depend on I, since the pigeons missing in t have absolutely no effect on the performance.

CLAIM 3.4. *For every $t \in T_I \setminus \Delta_I^{\mathrm{syn}}$, there exists $f \in S_I(k)$ such that $t = f \bmod V_I$, and either $f = 0$ or $LT(f) \prec t$.*

PROOF. If $t \notin \widetilde{T}_I$, we simply let $f = 0$. Suppose that $t \in \widetilde{T}_I \setminus \Delta_I^{\mathrm{syn}}$;

$$t = x_{i_1j_1}x_{i_2j_2}\ldots x_{i_dj_d} \ (i_1 < i_2 < \ldots < i_d).$$

We imitate the pigeon dance by an algebraic expansion. More specifically, applying the relation Q_{i_1}, we have:

$$\left.\begin{array}{rcl} t & = & x_{i_2j_2}\ldots x_{i_dj_d} - \sum\limits_{j_1^*<j_1} x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d} \\ & - & \sum\limits_{j_1^*>j_1} x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d} \bmod V_I, \end{array}\right\} \quad (3.12)$$

and we can immediately cross out all $x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d}$ with $j_1^* \in \{j_2,\ldots,j_d\}$. All remaining terms in the first two summands of the right-hand side are already smaller than t, and we leave them alone. Terms of the third summand correspond to all possible arrangements in the pigeon dance after the first pigeon's move. We apply to every individual term $x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d}$ the same expansion w.r.t. the second pigeon, i_2, and once more we get some terms smaller than t (when the second pigeon moves left) and terms corresponding to arrangements in the pigeon dance after two moves. Continuing this way, we finally kill all terms larger than t (since $t \notin \Delta_I^{\mathrm{syn}}$, the dance is eventually aborted for any strategy by the pigeons). □

[2] it might be instructive to imagine the cat sitting in the virtual hole $(n+1)$; see, e.g., the proof of Claim 3.7 below.

Claim 3.5. *For any $t \in T_I$, there exists $f \in k\Delta_I^{\mathrm{syn}}$ such that $LT(f) \preceq t$ and $(t-f) \in V_I$.*

Proof. Apply iteratively Claim 3.4 until we get rid of all terms not in Δ_I^{syn}. $\square$

Define now $R_I^{\mathrm{syn}}(t)$ in accordance with the last claim to be some polynomial from $k\Delta_I^{\mathrm{syn}}$ such that $LT(R_I^{\mathrm{syn}}(t)) \preceq t$ and $(t - R_I^{\mathrm{syn}}(t)) \in V_I$. The polynomial with these two properties will be shown later to be unique; the only thing we require at the moment is that $R_I^{\mathrm{syn}}(t) = t$ for $t \in \Delta_I^{\mathrm{syn}}$.

Extend R_I^{syn} to $S_I(k)$ by linearity. Then $\mathrm{Ker}(R_I^{\mathrm{syn}}) \subseteq V_I$, and R_I^{syn} is a retraction onto $k\Delta_I^{\mathrm{syn}}$. Thus, in order to complete the proof of $\Delta_I^{\mathrm{syn}} = \Delta_I^{\mathrm{sem}}$, $R_I^{\mathrm{syn}} = R_I^{\mathrm{sem}}$ by Lemma 3.2 (3) with

$$d := |I| \cdot n,\ \vec{f} := \{ Q \in (\neg\mathcal{PHP}_n^m) \mid \mathrm{dom}(Q) \subseteq I \},$$

we only have to show the opposite inclusion $V_I \subseteq \mathrm{Ker}(R_I^{\mathrm{syn}})$. Since $S_I(k) = k\Delta_I^{\mathrm{syn}} \oplus \mathrm{Ker}(R_I^{\mathrm{syn}})$, and we already know that $\mathrm{Ker}(R_I^{\mathrm{syn}}) \subseteq V_I$, this is tantamount to showing that terms in Δ_I^{syn} are linearly independent as functions on M_I. This requires some more work.

For $t \in \widetilde{T}_I$, $t \neq 1$, let $Kill(t)$ be the result of eliminating the left-most pigeon and moving the hole occupied by him to the very left. Formally, if $t = x_{i_1j_1}x_{i_2j_2}\ldots x_{i_dj_d}$ with $i_1 < i_2 < \ldots < i_d$, then $Kill(t) \rightleftharpoons x_{i_2j'_2}\ldots x_{i_dj'_d}$, where

$$j'_\nu \rightleftharpoons \begin{cases} j_\nu \text{ if } j_1 < j_\nu \\ j_\nu + 1 \text{ if } j_1 > j_\nu. \end{cases}$$

We extend this operator to T_I by letting $Kill(t) = 0$ for $t \notin \widetilde{T}_I$.

Claim 3.6. *Let $t \in \widetilde{T}_I$; $t = x_{i_1j_1}x_{i_2j_2}\ldots x_{i_dj_d}$, $i_1 < i_2 < \ldots < i_d$. Then $t \in \Delta_I^{\mathrm{syn}}$ if and only if there exists $j_1^* > j_1$ such that $Kill(x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d}) \in \Delta_I^{\mathrm{syn}}$.*

Proof. Immediately follows from definitions: $t \in \Delta_I^{\mathrm{syn}}$ if and only if there exists $j_1^* > j_1$ (corresponding to the first pigeon's move) such that $j_1^* \notin \{j_2, \ldots, j_d\}$, and in the arrangement corresponding to $x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d}$, the pigeons can complete the part of their dance beginning with pigeon i_2. But since the first pigeon participates in the rest of the performance only by locking j_1^*'s hole, the same effect can be achieved by removing him completely, and moving this hole to the very left so that it cannot be used by anyone else. This is exactly what the operator $Kill$ does. $\square$

We define one more partial ordering $\sqsubseteq$ on $\widetilde{T}_I$, which is intermediate between $\subseteq$ and $\preceq$. Namely, $t' \sqsubseteq t$ if the following three conditions hold:

1. $\mathrm{dom}(t') \subseteq \mathrm{dom}(t)$;
2. for every $x_{i_1 j'_1} x_{i_2 j'_2} \subseteq t'$ and $x_{i_1 j_1} x_{i_2 j_2} \subseteq t$ with $i_1 \neq i_2$, we have that $j'_1 < j'_2 \Leftrightarrow j_1 < j_2$;
3. for every $x_{ij'} \in t'$ and $x_{ij} \in t$, we have that $j' \leq j$.

Informally, all pigeons in t' must be also present in t, sit in the same order as in t, and occupy either the same hole as in t, or move to the left of it.

Claim 3.7. *Δ_I^{syn} is closed downward w.r.t. $\sqsubseteq$, i.e., $t' \sqsubseteq t$ and $t \in \Delta_I^{\mathrm{syn}}$ imply $t' \in \Delta_I^{\mathrm{syn}}$.*

Proof. By induction on $\deg(t)$.

Base $\deg(t) = 0$ is obvious.

Inductive step. Let $t = x_{i_1 j_1} x_{i_2 j_2} \ldots x_{i_d j_d} \in \Delta_I^{\mathrm{syn}}$ $(i_1 < i_2 < \ldots < i_d,\ d > 0)$, $t' \sqsubseteq t$, $t' = \prod_{i_\nu \in \mathrm{dom}(t')} x_{i_\nu j'_\nu}$, and assume that Claim 3.7 is already proved for any t of degree $(d-1)$ (and any t'). By Claim 3.6, there exists $j_1^* > j_1$ such that $Kill(t^*) \in \Delta_I^{\mathrm{syn}}$, where $t^* = x_{i_1 j_1^*} x_{i_2 j_2} \ldots x_{i_d j_d}$.

Case 1. $i_1 \notin \mathrm{dom}(t')$.
Then clearly $t' \sqsubseteq Kill(t^*)$, since the $Kill$ operator can move the surviving pigeons only to the right and does not change their order, and we can apply the inductive assumption.

Case 2. $i_1 \in \mathrm{dom}(t')$.
Let $j_1'^* > j'_1$ be the first free hole to the right of j'_1 in the arrangement t'. We will show later that such a hole really exists, but for the time being let us put $j_1'^* \rightleftharpoons n+1$ if this is not the case.

Case 2.1. $j_1'^* \leq j_1^*$.
This in particular implies that $j_1'^* \neq n+1$, and pigeon i_1 in the arrangement t' can really fly to $j_1'^*$. Let t'^* be the resulting arrangement. We wish to show that

$$Kill(t'^*) \sqsubseteq Kill(t^*). \tag{3.13}$$

By examination, the only reason for violating it might be caused by some pigeon $i_\nu \in \mathrm{dom}(t')$, $\nu > 1$ which occupies the same hole in t' and t: $j'_\nu = j_\nu$, and such that, after moving the first pigeon's hole to the left, j'_ν gets incremented by one in t'^* whereas in t^* this does not happen. But this is impossible:

since $j_1'^* \le j_1^*$, (re)moving j_1^*'s hole results in at least as much incrementing as (re)moving $j_1'^*$'s hole.

When we have (3.13), we conclude by inductive assumption that $Kill(t'^*) \in \Delta_I^{\mathrm{syn}}$, and then $t' \in \Delta_I^{\mathrm{syn}}$, by Claim 3.6.

Case 2.2. $j_1'^* > j_1^*$.
Since $j_1^* > j_1 \ge j_1'$ and $j_1'^*$ is the first free hole to the right of j_1' in t', all holes $j_1^*, j_1^*+1, \ldots, j_1'^*-1$ are occupied by pigeons in t'. On the other hand, j_1^* is free in t, which means that when we change our arrangement from t' to t, the pigeon sitting in j_1^* pushes the whole flock sitting in the adjacent holes $j_1^*+1, \ldots, j_1'^*-1$ to the right, and none of them can stay home (remember that in the definition of $\sqsubseteq$ we required that pigeons be arranged in the same order in t' and t). This in particular implies that $j_1'^* \ne n+1$, so we can define t'^* as in Case 2.1.

By the same argument as above, (3.13) can be violated only due to some pigeon i_ν sitting between j_1^* and $j_1'^*$. But as we have just seen, for these pigeons j_ν is *strictly* larger than j_ν', so no violation occurs for them either.

When we have (3.13), we conclude the proof with the same argument as in Case 2.1. □

Corollary 3.8. *Δ_I^{syn} is closed downward w.r.t. $\subseteq$.*

Corollary 3.9. *Δ_I^{syn} is closed under the $Kill$ operator.*

Proof. Let $t = x_{i_1j_1}x_{i_2j_2}\ldots x_{i_dj_d} \in \Delta_I^{\mathrm{syn}}$; $i_1 < i_2 < \ldots < i_d$. By Claim 3.6, there exists $j_1^* > j_1$ such that $Kill(x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d}) \in \Delta_I^{\mathrm{syn}}$. Since $Kill(t) \sqsubseteq Kill(x_{i_1j_1^*}x_{i_2j_2}\ldots x_{i_dj_d})$, this implies $Kill(t) \in \Delta_I^{\mathrm{syn}}$ by Claim 3.7. □

The following claim is the only place where we use the condition $|I| \le \frac{(n+1)}{2}$.

Claim 3.10. *Let $t \in \Delta_I^{\mathrm{syn}}$, and assume that the minimal element i of I is not in* $\mathrm{dom}(t)$. *Then there exists $j \in [n]$ such that $Kill(x_{ij}t) \in \Delta_I^{\mathrm{syn}}$.*

Proof. Since $i \notin \mathrm{dom}(t)$, $\deg(t) \le |I| - 1 \le \frac{(n-1)}{2}$. Hence, during the whole successful performance of the pigeon dance on t, at most $2\deg(t) \le n-1$ holes can be used (2 holes per capita) and there exists at least one hole not used at all. Take as the required j any such hole. Then $Kill(x_{ij}t)$ is obtained from t by moving the hole j to the very left. Now, since j was not used in the successful performance on t, the pigeons can use the same strategy for certifying $Kill(x_{ij}t) \in \Delta_I^{\mathrm{syn}}$. □

Now we are ready to put things together.

Claim 3.11. *For $|I| \leq \frac{(n+1)}{2}$, terms in Δ_I^{syn} are linearly independent as functions on M_I.*

Proof. By induction on $|I|$.

Base case $|I| = 0$ is obvious.

Inductive step. Let i_1 be the minimal element of I, and suppose that the claim is already proved for $I := I \setminus \{i_1\}$ and $n := (n-1)$. Take any non-trivial linear combination from $k\Delta_I^{\mathrm{syn}}$, and decompose it as follows:

$$\sum_{t\in\Gamma} tA_t, \tag{3.14}$$

where $\Gamma \subseteq \widetilde{T}_{I\setminus\{i_1\}}$, and $A_t \in k\widetilde{T}_{\{i_1\}} \setminus \{0\}$ are non-zero affine forms in variables $X_{\{i_1\}}$. Since Δ_I^{syn} is closed downward w.r.t. $\subseteq$ by Corollary 3.8, we actually have $\Gamma \subseteq \Delta^{\mathrm{syn}}_{I\setminus\{i_1\}}$. Let t_1 be the largest term in Γ (w.r.t. $\preceq$), and let $A_{t_1} = \alpha_0 + \sum_j \alpha_j x_{i_1 j}$.

Case 1. $\alpha_0 = 0$.

Choose j_1 such that $\alpha_{j_1} \neq 0$. Apply to the sum (3.14) the restriction $\rho_{i_1 j_1}$, which sends $x_{i_1 j_1}$ to 1, and sends all x_{ij_1} $(i \neq i_1)$ and $x_{i_1 j}$ $(j \neq j_1)$ to zeros. Note that the effect of this restriction on $\widetilde{T}_{I\setminus\{i_1\}}$ is essentially the same as the effect of the operator $t \mapsto Kill(x_{i_1 j_1} t)$. The only (cosmetic) difference is that we destroy j_1's hole instead of moving it to the left.

In particular, since the sum (3.14) contains the term $t_1 x_{i_1 j_1}$ with the non-zero coefficient α_{j_1}, $t_1 x_{i_1 j_1} \in \Delta_I^{\mathrm{syn}}$, and therefore $\rho_{i_1 j_1}(t_1) \in \Delta^{\mathrm{syn}}_{I\setminus\{i_1\}}$ by Corollary 3.9 (here we slightly abused the notation and denoted by $\Delta^{\mathrm{syn}}_{I\setminus\{i_1\}}$ its analogue for $(n-1)$ holes). Therefore, if we apply $\rho_{i_1 j_1}$ to the sum (3.14), we will obtain $\alpha_{j_1}\rho_{i_1 j_1}(t_1) + f$, where $LT(f) \prec t_1$. Then (with the same abuse of notation) $\alpha_{j_1}\rho_{i_1 j_1}(t_1) + R^{\mathrm{syn}}_{I\setminus\{i_1\}}(f)$ is a non-trivial linear combination from $k\Delta^{\mathrm{syn}}_{I\setminus\{i_1\}}$. Hence, by inductive assumption, there exists some assignment $a \in M_{I\setminus\{i_1\}}$ evaluating this linear combination to some non-zero element. Extending this a in accordance with $\rho_{i_1 j_1}$ by letting $a_{i_1 j_1} = 1$ and $a_{i_1 j} = a_{ij_1} = 0$ for all $i \neq i_1$, $j \neq j_1$, we will find some assignment from M_I that evaluates the sum (3.14) to the same non-zero element. This completes the analysis of Case 1.

Case 2. $\alpha_0 \neq 0$.

Similar to Case 1, we only have to find some $j_1 \in [n]$, such that $\rho_{i_1 j_1}(A_{t_1}) \neq 0$ and $Kill(x_{i_1 j_1} t_1) \in \Delta_I^{\mathrm{syn}}$. By Claim 3.10, there are js satisfying the second condition, and let j_1 be the *largest* of them. Then $x_{i_1 j_1} t_1 \notin \Delta_I^{\mathrm{syn}}$ by Claim

3.6; hence this term may not appear in (3.14), which implies $\alpha_{j_1} = 0$ and $\rho_{i_1 j_1}(A_{t_1}) = \alpha_0 \neq 0$.

This completes the proof of Claim 3.11. $\square$

As we already noticed, Theorem 3.1 follows from Claim 3.11. To repeat the argument in the reverse order, this claim implies the missing inclusion $V_I \subseteq \mathrm{Ker}(R_I^{\mathrm{syn}})$ which, in turn, implies by Lemma 3.2 (3) that the operators R_I^{syn} coincide with their semantic versions R_I^{sem} introduced in Section 3.1. But (3.11) is fairly straightforward for R_I^{syn}: pigeons missing in a term t have been of no importance for the analysis of the reduction process throughout this section. With (3.11) in our hands, the proof of Theorem 3.1 is completed by noticing that all conditions in Lemma 3.2 are local (i.e., by linearity it suffices to check them for terms) and are easy to prove for true "semantic" ideals.

Remark 3.12. An easy analysis of the explicit construction of the operator R_d ($d \leq \frac{n+1}{2}$), given in the proof of Claim 3.4, implies that every polynomial $f \in V_d$ has actually a *Nullstellensatz* proof from $(\neg\mathcal{PHP}_n^m)$ of degree at most $\deg(f)$. This makes a structural refinement of our main result: not only is 1 not provable from $(\neg\mathcal{PHP}_n^m)$ in degree $d \leq \frac{n+1}{2}$, but moreover all polynomials provable in this degree possess a "plain" Nullstellensatz proof.

4. Improved lower bounds

Let us denote by $D_k(n,d)$ the minimal D such that any refutable (in the polynomial calculus over k) system of polynomials $f_1, \ldots, f_m \in S_{n,d}(k)$ has a refutation of degree at most D. Clearly, $d \leq D_k(n,d) \leq n$, and this function is monotone in both arguments. Theorem 3.1 provides the lower bound

$$D_k(n,2) \geq \Omega(\sqrt{n}). \tag{4.15}$$

In this section we will show improved lower bounds on $D_k(n,d)$ for logarithmically small d.

$[m]^d$ will denote the family of all d-element subsets of $[m]$. For $I \subseteq [m]$ and $j \in [n]$, we abbreviate the term $\prod_{i\in I} x_{ij}$ to t_{Ij}.

Definition 4.1. $(\neg\mathcal{PHP}_n^{m,d})$ is the following system of elements in $S_{mn}(k)$:

$$\begin{aligned} Q_I &\rightleftharpoons 1 - \sum_{j\in[n]} t_{Ij} \ (I \in [m]^d); \\ & \ t_{Ij} \ (I \in [m]^{d+1}, \ j \in [n]); \\ Q_{I;j_1,j_2} &\rightleftharpoons t_{Ij_1} t_{Ij_2} \ (I \in [m]^d; \ j_1, j_2 \in [n], \ j_1 \neq j_2). \end{aligned}$$

Clearly, $(\neg\mathcal{PHP}_n^m) = (\neg\mathcal{PHP}_n^{m,1})$, so this is a generalization of Definition 2.4. On the other hand, consider the polynomial system $(\neg\mathcal{PHP}_n^M)$, where $M = \binom{m}{d}$, and identify, in an arbitrary way, $[M]$ with $[m]^d$. Then the *Veronese mapping* that takes the variable x_{Ij} to the term t_{Ij} transforms $(\neg\mathcal{PHP}_n^M)$ into essentially the same system as $(\neg\mathcal{PHP}_n^{m,d})$; the only difference is that $Q_{I_1,I_2;j}$ gets transformed into $t_{I_1\cup I_2,j}$, and the cardinality of $I_1 \cup I_2$ can be in general larger than $(d+1)$. In particular, if $\binom{m}{d} > n$, then the system of polynomials $Q_I\,(I \in [m]^d)$, $t_{Ij}\,(I \in [m]^{d+1}, j \in [n])$ is refutable, and every degree D polynomial calculus refutation of $(\neg\mathcal{PHP}_n^M)$ can be transformed into a degree (dD) refutation of $(\neg\mathcal{PHP}_n^{m,d})$. If we only knew that the degree-optimal refutation of $(\neg\mathcal{PHP}_n^{m,d})$ is induced in this way from a refutation of $(\neg\mathcal{PHP}_n^M)$, we would immediately arrive, via Theorem 3.1, at the very strong lower bound $\Omega(dn)$ for the principle $(\neg\mathcal{PHP}_n^{m,d})$, with the truly linear lower bound

$$D_k(n, \lfloor\log_2 n\rfloor) \geq \Omega(n) \tag{4.16}$$

as a direct consequence.

This, however, might be not as simple: for example, if we multiply Q_{I_1} by $x_{i_1 1}x_{i_1 2}\dots x_{i_1 n}$ where $i_1 \notin I_1$, then, with the help of the axioms t_{Ij} ($|I| = d+1$), we infer $x_{i_1 1}x_{i_1 2}\dots x_{i_1 n}$ in degree $(n+d)$. It is not clear how to explain the fact that this term is reducible working exclusively in the subalgebra generated by terms t_{Ij}, $I \in [m]^d$, as do the induced refutations.

We will show later how to circumvent difficulties of this sort at the expense of introducing more intricate tautologies (Theorem 4.5) which will still lead us to the linear bound (4.16) on $D_k(n, \log n)$. The proof of Theorem 4.5, however, is rather technically involved, so we present first a straightforward reduction argument that, however simple, still allows us to obtain an *almost* linear lower bound on $D_k(n, \log n)$:

THEOREM 4.2. *For any m, d, n such that $\binom{m}{d} > n$ and any ground field k, every polynomial calculus refutation of $(\neg\mathcal{PHP}_n^{m,d})$ must have degree at least $(n/2)+1$.*

Before proving this theorem, let us note that the polynomial system $(\neg\mathcal{PHP}_n^{m,d})$ has only (mn) variables which can be made very close to n and still preserve the crucial condition

$$\binom{m}{d} > n. \tag{4.17}$$

More specifically, since the system of polynomials Q_I, t_{Ij} in Definition 4.1 is already refutable, and every polynomial in this system has degree at most

$(d+1)$, Theorem 4.2 implies the bound $D_k(mn, d+1) \geq \Omega(n)$, as long as (4.17) is true. Substituting here $d := d-1$, $m := \lfloor d \cdot n^{1/d} \rfloor$, $n := \lfloor n^{1-1/d}/d \rfloor$, we obtain the following generalization of the bound (4.15):

$$D_k(n,d) \geq \Omega\left(\frac{n^{1-1/d}}{d}\right). \tag{4.18}$$

In particular, this becomes $\Omega(n/\log n)$ for $d = \theta(\log n)$.

Proof of Theorem 4.2. We define the *linear* transformation

$$\begin{aligned} \pi : S_{mn}(k) &\longrightarrow S_{Mn}(k) \\ x_{ij} &\longmapsto \sum_{I \ni i} x_{Ij} \end{aligned}$$

with the intention of providing a sort of inverse to the above Veronese mapping. For our purposes this indeed works; namely, it is easy to check that $\pi(t_{Ij}) - x_{Ij}$ $(I \in [m]^d)$ and $\pi(t_{Ij})$ $(I \in [m]^{d+1})$ belong to the ideal generated by $x_{I_1 j} x_{I_2 j}$ with $I_1 \neq I_2$, and hence are provable from $(\neg\mathcal{PHP}_n^M)$ in degrees d and $(d+1)$, respectively. With this observation, it is transparent that any polynomial $\pi(Q)$, $Q \in (\neg\mathcal{PHP}_n^{m,d})$ has a degree $\deg(Q)$ proof from $(\neg\mathcal{PHP}_n^M)$.

Hence every degree D refutation of $(\neg\mathcal{PHP}_n^{m,d})$ gets transformed into a degree D refutation of $(\neg\mathcal{PHP}_n^M)$, and we can apply Theorem 3.1 to finish the proof. □

It seems that no direct reduction from $(\neg\mathcal{PHP}_n^M)$ can prove the truly linear degree bound (4.16), and in order to achieve this goal we have to develop a new technique of reductions that *improve* bounds.

Definition 4.3. Let $M > n$ be an arbitrary integer, and $\mathcal{I}_1, \ldots, \mathcal{I}_M \subseteq [m]^d$ disjoint families of sets. $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$ is the following system of elements in $S_{mn}(k)$:

$$Q_\nu \rightleftharpoons 1 - \sum_{I \in \mathcal{I}_\nu} \sum_{j \in [n]} t_{Ij} \ (\nu \in [M]);$$

$$t_{I_1 \cup I_2, j} \ \left(I_1, I_2 \in \bigcup_{\nu=1}^M \mathcal{I}_\nu,\ I_1 \neq I_2;\ j \in [n]\right); \tag{4.19}$$

$$\left.\begin{aligned} Q_{I_1,I_2;j_1,j_2} \ \rightleftharpoons \ & t_{I_1 j_1} t_{I_2 j_2} \ (I_1, I_2 \in \mathcal{I}_\nu \text{ for some } \nu \in [M]; \\ & j_1, j_2 \in [n],\ j_1 \neq j_2) \end{aligned}\right\} \tag{4.20}$$

(note that we do *not* require I_1 to be different from I_2 in (4.20)).

If $M = \binom{m}{d}$ and $\mathcal{I}_\nu$ are all singletons, we obtain $(\neg\mathcal{PHP}_n^{m,d})$ as a partial case. On the other hand, the transformation

$$\pi : x_{\nu j} \mapsto \sum_{I \in \mathcal{I}_\nu} t_{Ij} \tag{4.21}$$

clearly takes default axioms $x_{\nu j}^2 = x_{\nu j}$, and the polynomial system $(\neg\mathcal{PHP}_n^M)$ into easy consequences of $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$. Thus, the best way to think of $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$ (at least, at the intuitive level) is as of the image of $(\neg\mathcal{PHP}_n^M)$ under the transformation (4.21). And now we are going to realize the idea already outlined above: if the set system $\mathcal{I}_1,\ldots,\mathcal{I}_M$ is "generic enough," then every refutation of $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$ can be in a certain sense induced from a refutation of $(\neg\mathcal{PHP}_n^M)$ via the mapping (4.21).

The notion of genericity employed for this purpose is formalized in the following definition:

Definition 4.4. A system $\mathcal{I}_1,\ldots,\mathcal{I}_M \subseteq [m]^d$ of disjoint families of sets is ℓ-*generic*, if for any $I \in [m]^\ell$ and any $\nu \in [M]$, there exists $I' \in I_\nu$ such that $I \cap I' = \emptyset$ and I' is the only set in $\bigcup_{\nu=1}^M \mathcal{I}_\nu$ which is a subset of $I \cup I'$.

We defer a simple probabilistic argument showing the existence of sufficiently generic systems until the end of this section (Lemma 4.7), and proceed immediately to its main technical contribution.

Theorem 4.5. *Suppose that $M > n$, $\mathcal{I}_1,\ldots,\mathcal{I}_M \subseteq [m]^d$ is an ℓ-generic system, and k is an arbitrary field. Then every polynomial calculus refutation of $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$ over k must have degree larger than* $\min\{\ell+1, d/2\}\cdot(n-1)+d$.

Proof. Let V be the ideal in $S_{mn}(k)$ generated by all terms (4.19), (4.20), and let Λ be the factor-ring $S_{mn}(k)/V$. Every element from Λ has the unique canonical representation in which every t contains neither terms (4.19) nor terms (4.20) as subterms. In particular, this canonical form induces the notion of degree on Λ. The statement of Theorem 4.5 is easily implied by the following claim:

Claim 4.6. *Let $P_1,\ldots,P_M$ be polynomials of degree at most D, where $D \leq \min\{\ell+1, d/2\}\cdot(n-1)$. Assume that* $\deg\left(\sum_{\nu=1}^M P_\nu Q_\nu\right) < D + d$. *Then there exist polynomials $P'_1,\ldots,P'_M$ of degree at most $(D-1)$ each, and such that $\sum_{\nu=1}^M P_\nu Q_\nu = \sum_{\nu=1}^M P'_\nu Q_\nu$ (in Λ).*

Proof of Theorem 4.5 from Claim 4.6. By induction on the number of inferences in a polynomial calculus proof of degree $\min\{\ell+1, d/2\}\cdot(n-1)+d$ from $\left(\neg\mathcal{PHP}_n^{\mathcal{I}_1,\ldots,\mathcal{I}_M}\right)$, we show that if f is the final polynomial of this proof, then

$$f = \sum_{\nu=1}^{M} P_\nu Q_\nu \text{ (in } \Lambda), \tag{4.22}$$

where $\deg(P_\nu) \leq \deg(f) - d$. For the inductive step, note that if f is the conclusion of the final inference rule, then the inductive assumption implies a Nullstellensatz representation of the form (4.22) with $\deg(P_\nu) \leq \min\{\ell+1, d/2\}\cdot(n-1)$. If actually $\deg(f) < \min\{\ell+1, d/2\}\cdot(n-1)+d$, we reduce the degrees of P_ν in (4.22) to $\deg(f)-d$ by consecutively applying Claim 4.6 for $D := \min\{\ell+1, d/2\}\cdot(n-1), \ldots, \deg(f)-d+1$. □

Proof of Claim 4.6. Let us say that a term δ is *minor* if it does not contain any subterm of the form t_{Ij} with $I \in \bigcup_{\nu=1}^M \mathcal{I}_\nu$. Then every term t that is not equal to zero in Λ has the unique representation

$$t = \delta(t)\cdot t_{I_1 j_1}\cdot\ldots\cdot t_{I_d j_d},$$

where $\delta(t)$ is a minor term, every I_k belongs to $\bigcup_{\nu=1}^M \mathcal{I}_\nu$ (different I_k's belonging to different members of this union), and no two terms displayed here have common variables. Accordingly, P_ν can be decomposed as

$$P_\nu = \sum_\delta \delta\cdot P_{\nu\delta}, \tag{4.23}$$

where the sum is taken over all minor terms δ, $P_{\nu\delta}$ has degree at most $D-\deg(\delta)$ and belongs to the subalgebra generated by those t_{Ij} for which $I \in \bigcup_{\nu=1}^M \mathcal{I}_\nu$, $\delta\cdot t_{Ij} \neq 0$ and δ, t_{Ij} do not have any variables in common. Let t be any non-zero term t *of degree* $(D+d)$ appearing in $\delta\cdot P_{\nu\delta}Q_\nu$, and let $t = \delta\cdot t'\cdot t''$, where t' appears in $P_{\nu\delta}$, and t'' appears in Q_ν. Since $\deg(\delta)+\deg(t')+\deg(t'') \leq (D+d)$, t'' may not have common variables with δ, t' which implies $\delta(t) = \delta$.

Hence degree $(D+d)$ terms in $\sum_{\nu=1}^M P_\nu Q_\nu$ may result only from those members of the sum (4.23) for which $D-\deg(\delta)$ is divisible by d, and cancellations among them may occur only when the terms being cancelled belong to the same member of this sum. On the other hand, since $\deg\left(\sum_{\nu=1}^M P_\nu Q_\nu\right) < D+d$, all degree $(D+d)$ terms get eventually cancelled, and this implies

$$\deg\left(\delta\cdot\sum_{\nu=1}^M P_{\nu\delta}Q_\nu\right) < D+d \tag{4.24}$$

for every individual δ. Thus, we can also treat different δ's individually.

So, let us fix some minor term δ of degree $(D - dd_0)$ for an integer d_0. Let J be the set of all $j \in [n]$ for which δ contains at most ℓ variables among $\{x_{1j}, \dots, x_{mj}\}$. Since $D \leq \min\{\ell+1, d/2\}\cdot(n-1) \leq (\ell+1)(n-|J|)+\frac{d}{2}(|J|-1) \leq \deg(\delta) + \frac{d}{2}(|J|-1)$, we have

$$d_0 \leq \frac{|J|-1}{2}. \tag{4.25}$$

Since $(\mathcal{I}_1, \dots, \mathcal{I}_M)$ is ℓ-generic, for every $j \in J$ and $\nu \in [M]$, we can fix some $I_{\nu j} \in \mathcal{I}_\nu$, such that δ and $t_{I_{\nu j}j}$ do not have any common variables and $\delta \cdot t_{I_{\nu j}j} \neq 0$ in Λ. Let us replace all occurrences of $t_{I_{\nu j}j}$ in $P_{\nu\delta}, Q_\nu$ by new variables $y_{\nu j}$. We will treat $y_{\nu j}$ as the generators of the "pigeonhole ring" $S_{M\cdot|J|}(k[\vec{t}\,])$ with M pigeons and $|J|$ holes, whereas all other t_{Ij} are treated as coefficients. Variables $y_{\nu j}$ are assumed to be lexicographically ordered in the same way as in the previous section.

Since $P_{\nu\delta}$ have y-degree at most $d_0 \leq \frac{|J|-1}{2}$, we can reduce them in accordance with the general theory developed in that section. This time, however, we want to be more careful and write down the single reduction step (3.12) in the more elaborate form

$$\begin{aligned} y_{\nu_1 j_1} \cdots y_{\nu_\ell j_\ell} &= \left(1 - Q_{\nu_1} - \sum_{\substack{I \in \mathcal{I}_{\nu_1},\ j \in [n] \\ I \neq I_{\nu_1 j}}} t_{Ij}\right) y_{\nu_2 j_2} \cdots y_{\nu_\ell j_\ell} \\ &\quad - \sum_{j_1^* < j_1} y_{\nu_1 j_1^*} y_{\nu_2 j_2} \cdots y_{\nu_\ell j_\ell} - \sum_{j_1^* > j_1} y_{\nu_1 j_1^*} y_{\nu_2 j_2} \cdots y_{\nu_\ell j_\ell} \end{aligned}$$

which holds *in the ring* Λ. As in the proofs of Claims 3.4, 3.5, we eventually find degree d_0 polynomials $\bar{P}_{\nu\delta}(\vec{t}, q_1, \dots, q_M, \vec{y})$, such that $\bar{P}_{\nu\delta}(\vec{t}, Q_1, \dots, Q_M, \vec{y}) = P_{\nu\delta}$, and every term in y-variables appearing in $\bar{P}_{\nu\delta}$ is irreducible, i.e., belongs to the set of irreducible terms Δ_{d_0} described in the previous section.

Let us now consider the sum $\sum_{\nu=1}^M \bar{P}_{\nu\delta}(\vec{t}, \vec{q}, \vec{y}) q_\nu$ and further reduce it modulo relations

$$t_{Ij} = 0 \ (\delta \cdot t_{Ij} = 0 \text{ in } \Lambda),\ q_\nu^2 = q_\nu,\ y_{\nu j} q_\nu = 0. \tag{4.26}$$

Denote the result of this reduction by $S_\delta(\vec{t}, \vec{q}, \vec{y})$. Since the relations of the last two types in (4.26) hold in Λ for $q_\nu = Q_\nu$, we have $\delta \cdot S_\delta(\vec{t}, \vec{Q}, \vec{y}) = \delta \cdot \sum_{\nu=1}^M P_{\nu\delta} Q_\nu$. In particular,

$$\deg(\delta \cdot S_\delta(\vec{t}, \vec{Q}, \vec{y})) < D + d \tag{4.27}$$

by (4.24). We wish to show that this deficit in degree can be caused only for the trivial reason that $\deg(S_\delta(\vec{t},\vec{q},\vec{y})) \leq d_0$ (in this degree bound $\vec{t},\vec{q},\vec{y}$ are counted as single letters).

For a term $T = t_{I_1j_1}\dots t_{I_aj_a}q_{\nu_1}\dots q_{\nu_b}y_{\nu'_1j'_1}\dots y_{\nu'_cj'_c}$, let

$$\gamma(T) \rightleftharpoons t_{I_1j_1}\dots t_{I_aj_a}$$

and

$$\mathrm{dom}(T) \rightleftharpoons \{\nu_1,\dots,\nu_b,\nu'_1,\dots,\nu'_c\}.$$

One important observation is that since $S_\delta(\vec{t},\vec{q},\vec{y})$ is reduced modulo relations (4.26), for every term T appearing in S_δ, we actually have $\delta\cdot\gamma(T) \neq 0$ and all $\nu_1,\dots,\nu_b,\nu'_1,\dots,\nu'_c$ are pairwise distinct. This observation allows us to decompose S_δ as

$$S_\delta(\vec{t},\vec{q},\vec{y}) = S'_\delta(\vec{t},\vec{q},\vec{y}) + \sum_{\substack{\delta\gamma\neq 0,\ \Gamma\subseteq[M]\\ \deg(\gamma)+|\Gamma|=d_0+1}} \gamma(\vec{t})\cdot S_{\delta\gamma\Gamma}(\vec{q},\vec{y}),$$

where $\deg(S'_\delta) \leq d_0$ and $S_{\delta\gamma\Gamma}(\vec{q},\vec{y})$ are degree $|\Gamma|$ forms such that $\mathrm{dom}(T) = \Gamma$ for all terms T appearing in $S_{\delta\gamma\Gamma}$. We wish to prove that, in fact, $S_{\delta\gamma\Gamma} = 0$ for all γ,Γ.

Suppose the contrary, and choose γ,Γ such that $S_{\delta\gamma\Gamma}\neq 0$ and $\deg(\gamma)$ has the minimal possible value among all pairs (γ,Γ) with this property. Convert the form $S_{\delta\gamma\Gamma}(\vec{q},\vec{y})$ into the non-zero polynomial $S_{\delta\gamma\Gamma}(1,\dots,1,\vec{y})$ by substituting ones for all q_ν's. Due to the construction of $\bar{P}_{\nu\delta}$, this polynomial contains only irreducible terms, i.e., belongs to $k\Delta_\Gamma$ in the notation of Section 3 (note that $|\Gamma| \leq d_0+1 \leq \frac{|J|+1}{2}$ by (4.25)). Hence we can apply to this polynomial Claim 3.11 and find some assignment $a\in M_\Gamma$ such that $S_{\delta\gamma\Gamma}(1,\dots,1,\vec{y})(a)\neq 0$. Alternatively, we can interpret this assignment as a y-term T_a with $\mathrm{dom}(T_a) = \Gamma$, and it is easy to see that the *coefficient* of $S_{\delta\gamma\Gamma}(Q_1,\dots,Q_M,\vec{y})$ in front of T_a (this expression is considered as a polynomial in letters $\vec{t},\vec{y}$) is equal exactly to $S_{\delta\gamma\Gamma}(1,\dots,1,\vec{y})(a)\neq 0$. But this is also the coefficient of $S_\delta(\vec{t},\vec{Q},\vec{y})$ in front of $\gamma(\vec{t})\cdot T_a(\vec{y})$. Indeed, this term of degree (d_0+1) may appear neither in $S'_\delta(\vec{t},\vec{Q},\vec{y})$ (since $\deg(S'_\delta)\leq d_0$) nor in $\gamma'(\vec{t})\cdot S_{\delta\gamma'\Gamma'}$ for any other pair $(\gamma',\Gamma')\neq(\gamma,\Gamma)$ (since, due to our choice of (γ,Γ), $S_{\delta\gamma'\Gamma'}\neq 0$ implies that $\deg(\gamma')\geq\deg(\gamma)$). This contradicts (4.27).

We have proved that all $S_{\delta\gamma\Gamma}$ are equal to zero, i.e., $\deg(S_\delta(\vec{t},\vec{q},\vec{y}))\leq d_0$. The rest is easy. Since $S_\delta(\vec{t},\vec{q},\vec{y})$ belongs to the ideal generated by $q_1,\dots,q_M$, we can represent it as $S_\delta(\vec{t},\vec{q},\vec{y}) = \sum_{\nu=1}^M S_{\nu\delta}(\vec{t},\vec{q},\vec{y})q_\nu$, where $\deg(S_{\nu\delta})\leq d_0-1$.

Then $\delta \cdot \sum_{\nu=1}^{M} S_{\nu\delta}(\vec{t}, \vec{Q}, \vec{y}) Q_\nu = \delta \cdot S_\delta(\vec{t}, \vec{Q}, \vec{y}) = \delta \cdot \sum_{\nu=1}^{M} P_{\nu\delta} Q_\nu$. Hence if we let

$$P'_{\nu\delta} \rightleftharpoons \begin{cases} S_{\nu\delta}(\vec{t}, \vec{Q}, \vec{y}) \text{ if } D - \deg(\delta) \text{ is divisible by } d \\ P_{\nu\delta} \text{ for all other } \delta \end{cases}$$

then the sums $P'_\nu \rightleftharpoons \sum_\delta \delta \cdot P'_{\nu\delta}$ will have all the properties required in Claim 4.6. □

As we already noted above, Claim 4.6 implies Theorem 4.5 (and, moreover, it implies this theorem in the stronger form analogous to Remark 3.12). □

LEMMA 4.7. *For $d \leq m/2$, there exists an $\Omega(d)$-generic system $\mathcal{I}_1, \ldots, \mathcal{I}_M \subseteq [m]^d$ with $M \geq (m/d)^{d/6}$.*

PROOF. Let us randomly choose $\mathcal{I} \subseteq [m]^d$ of cardinality $2 \cdot \lceil (m/d)^{d/3} \rceil$. Then the standard probabilistic argument shows that with probability $1 - o(1)$, $\mathcal{I}$ is an $(0.08d+1)$-code, i.e., the symmetric difference between any two different members of $\mathcal{I}$ contains more than $(0.08d)$ elements. Divide $\mathcal{I}$ into $M = \lceil (m/d)^{d/6} \rceil$ groups $\mathcal{I}_1, \ldots, \mathcal{I}_M$ of size $\geq M$ each. Then with probability $1 - o(1)$, for every $I \in [m]^{\lfloor 0.04d \rfloor}$ and $\nu \in M$, there exists $I' \in \mathcal{I}_\nu$ such that $I \cap I' = \emptyset$. But these two properties imply $(0.04d)$-genericity: $I \cup I'$ may not contain any set in $\mathcal{I}$ other than I simply because $\mathcal{I}$ is an $(0.08d+1)$-code. □

Theorem 4.5 and Lemma 4.7 imply $D_k(mn, 2d) \geq \Omega(dn)$ as long as $d \leq m/2$ and $n < (m/d)^{d/6}$. Substituting here $d := \lfloor d/2 \rfloor$, $m := \lfloor dn^{13/d} \rfloor$ and $n := \lfloor \frac{n^{1-13/d}}{d} \rfloor$, we get the bound

$$D_k(n,d) \geq \Omega\left(n^{1-O(1/d)}\right)$$

which improves upon (4.18) when d is in the range between $\frac{\log n}{\log \log n}$ and $\log n$. In particular, when d is logarithmic in n, this gives the truly linear lower bound (4.16).

REMARK 4.8. We do not know of any explicit construction of ℓ-generic systems. But at least they certainly can be constructed in time $(m/d)^{O(d)}$ by (a variation of) the greedy algorithm. In the above application, this grows polynomially in n; hence we have polynomial time computable examples of polynomial systems for which the linear bound (4.16) is attained.

5. Unprovability of circuit lower bounds by low degree polynomial calculus proofs

Razborov (1995a) proposed studying the provability of the $\mathbf{NP} \overset{?}{\subseteq} \mathbf{P}/poly$ question (and its weakened variants for restricted circuit classes) in the somewhat controversial framework when proofs are allowed to operate with objects whose bit size is polynomial or quasipolynomial *in* 2^n, n being the number of variables. The main motivation for introducing this restriction was that it is exactly what *really existing* lower bounds proofs do at the moment (see Razborov & Rudich (1997) for a matching *computational* framework). Then Krajíček (1997a), Razborov (1994) observed that as in the computational complexity itself, things become much more transparent in the non-uniform context, of propositional calculus in this case.

Namely, for $t \leq 2^n$, let $Circuit_{t,n}(f_n, \vec{p})$ be a CNF of size $2^{O(n)}$ and of bounded fan-in at the bottom level, which expresses the fact "$\vec{p}$ encodes a t-sized Boolean circuit that computes the Boolean function f_n in n variables." Exact details of the encoding are actually unimportant at this level. But since they become important for restricted circuit classes (one example is given below), we prefer to fix one possible encoding explicitly. This encoding, however, will not be used until the proof of Corollary 5.2, so the reader interested in the rest of the material in this section may safely skip its somewhat tedious details.

First, we list all variables from the vector $\vec{p}$ (some of them have peculiar long names like $InputType'_\nu(v)$), along with their intended meaning:

p_{av} $(a \in \{0,1\}^n,\ v \in [t])$	–	the Boolean value computed at the node v on the input string a;
$p_{a\nu v}$ $(a \in \{0,1\}^n,\ \nu \in \{1,2\},\ v \in [t])$	–	the value brought to v by ν's wire on a;
$Fanin(v)$	–	this is 0 if v is NOT-gate and 1 if v is AND-gate or OR-gate;
$Type(v)$	–	when $Fanin(v) = 1$, this is 0 if v is AND-gate and 1 if v is OR-gate;
$InputType_\nu(v)$	–	this is 0 if ν's input to v is a constant or a variable and 1 if it is one of the previous gates;
$InputType'_\nu(v)$	–	when $InputType_\nu(v) = 0$, this is 0 if ν's input to v is a constant,

		and 1 if it is a variable;
$InputType''_\nu(v)$	–	when $InputType_\nu(v) = InputType'_\nu = 0$, this equals the ν's input to v;
$InputVar_\nu(v,i)$ $(i \in [n])$	–	when $InputType_\nu(v) = 0$, $InputType'_\nu(v) = 1$, this is 1 iff ν's input to v is x_i
$INPUTVAR_\nu(v,i)$	–	equals $\bigvee_{i' \le i} InputVar(v,i')$, introduced to keep bottom fan-in bounded;
$InputNode_\nu(v,v')$ $(v' < v)$	–	when $InputType_\nu(v) = 1$, this is 1 iff ν's input to v is the previous gate v';
$INPUTNODE_\nu(v,v')$	–	analogously to $INPUTVAR_\nu(v,i)$.

$Circuit_{t,n}(f_n, \vec{p})$ is the conjunction of (conjunctive normal forms equivalent to) the following axioms:

$$\neg InputType_\nu(v) \wedge \neg InputType'_\nu(v) \longrightarrow (p_{a\nu v} \equiv InputType''_\nu(v));$$
$$\neg InputType_\nu(v) \wedge InputType'_\nu(v) \longrightarrow \neg(InputVar_\nu(v,i) \wedge InputVar_\nu(v,i'))\ (i \neq i');$$
$$\neg InputType_\nu(v) \wedge InputType'_\nu(v) \longrightarrow (INPUTVAR_\nu(v,i) \equiv (INPUTVAR_\nu(v,i-1) \vee InputVar_\nu(v,i)))$$
$$(INPUTVAR_\nu(v,0) \rightleftharpoons 0);$$
$$\neg InputType_\nu(v) \wedge InputType'_\nu(v) \longrightarrow INPUTVAR_\nu(v,n);$$
$$\neg InputType_\nu(v) \wedge InputType'_\nu(v) \wedge InputVar_\nu(v,i) \longrightarrow (p_{a\nu v} \equiv a_i);$$

the analogous group of axioms for $InputNode$;

$$\neg Fanin(v) \longrightarrow (p_{av} \equiv \neg p_{a1v});$$
$$Fanin(v) \wedge \neg Type(v) \longrightarrow (p_{av} \equiv (p_{a1v} \wedge p_{a2v}));$$
$$Fanin(v) \wedge Type(v) \longrightarrow (p_{av} \equiv (p_{a1v} \vee p_{a2v}));$$
$$p_{at} \equiv f(a).$$

In this section we will show that for any $t \le 2^n$, any Boolean function f_n whose circuit size is larger than t, and any ground field k, every polynomial calculus refutation of (the polynomial system representing) $Circuit_{t,n}(f_n, \vec{p})$

must have degree $\Omega(t/n)$ (Corollary 5.2). This bound, however, holds even for (an inessential generalization of) the extremely restricted circuit class called (at least in the Russian literature) *perfect disjunctive normal forms* (PDNF). This is simply the class of representations of the form

$$K_1 \vee \ldots \vee K_t, \tag{5.28}$$

where K_j's are conjunctions of literals (*elementary conjunctions*) in which all n variables must occur.

Let $PDNF_{t,n}(f_n, \vec{p})$ be a natural 3-CNF, expressing the fact that $\vec{p}$ encodes a PDNF for f_n with t elementary conjunctions. Thus, $PDNF_{t,n}(f_n, \vec{p})$ is refutable if and only if $w(f_n) > t$, where $w(f_n)$ is the *weight* of f_n, defined as the number of ones in its truth-table. Since the natural method of obtaining lower bounds for perfect disjunctive normal forms consists simply in calculating $w(f_n)$, i.e., is essentially a counting argument, we might expect the tautologies $\neg PDNF_{t,n}(f_n, \vec{p})$ to be hard for any proof system for which counting is hard, e.g., for the polynomial calculus. Unfortunately, we cannot currently prove any lower bounds for polynomial calculus refutations of $PDNF_{t,n}(f_n, \vec{p})$; these would follow from lower bounds for the *onto* version of PHP, which we do not have yet.

Thus we consider the modified version $PDNF^*_{t,n}(f_n, \vec{p})$ of this 3-CNF corresponding to the slightly wider class of representations (5.28) in which K_j's are also allowed to be *identically zero functions*. Note that the complexity (measured by the number of elementary conjunctions t) of every Boolean function with respect to this extended class of circuits is still $w(f_n)$; hence from the complexity point of view this change in the definition is inessential. It, however, becomes esential if we are interested in the efficient provability.

Formally, $PDNF^*_{t,n}(f_n, \vec{p})$ is defined as follows. The vector $\vec{p}$ consists of the variables p_{ajk} ($a \in \{0,1\}^n,\ j \in [t],\ k \in [n]$) with the intended meaning that "$K_j \neq 0$ and a is consistent with the first k literals $x_1^{\epsilon_1}, \ldots, x_k^{\epsilon_k}$ in K_j"; the variables p_{aj} mean "$K_1(a) \vee \ldots \vee K_j(a) = 1$"; q_j expresses the fact "$K_j \neq 0$"; and q_{jk} expresses the sign with which x_k occurs in K_j (if $K_j = 0$, q_{jk} can be arbitrary). The axioms in $PDNF^*_{t,n}(f_n, \vec{p})$ are (3-CNF resulting from)

$$\begin{aligned} p_{ajk} &\equiv \left(p_{aj,k-1} \wedge q_{jk}^{a_k}\right) \ \text{(with } p_{aj0} \rightleftharpoons q_j\text{)};\\ p_{aj} &\equiv (p_{a,j-1} \vee p_{ajn}) \ \text{(with } p_{a,0} \rightleftharpoons 0\text{)};\\ p_{at} &\equiv f(a). \end{aligned}$$

Every tautology of the form $\neg PDNF^*_{t,n}(f_n, \vec{p})$ can be easily proved from the pigeonhole principle $PHP_t^{w(f_n)}$ (on an informal level this was already observed above). Hence, $\neg PDNF^*_{t,n}(f_n,\vec{p})$ have polynomial size Frege proofs by Buss (1987). If, moreover, $w(f_n) \geq 2t$, then $\neg PDNF^*_{t,n}(f_n,\vec{p})$ have constant-depth quasi-polynomial size Frege proofs by Paris *et al.* (1988). What we called above the "natural" 3-CNF $PDNF_{t,n}(f_n,\vec{p})$ is in fact the substitution instance of $PDNF^*_{t,n}(f_n,\vec{p})$ resulting from the substitution $q_j := 1$. Therefore, these upper bounds hold for tautologies of the form $\neg PDNF^*_{t,n}(f_n,\vec{p})$ as well.

Define $\mathcal{PDNF}^*_{t,n}(f_n,\vec{p})$ to be the polynomial system in variables

$$x_{ajk}, x_{aj}, y_j, y_{jk}$$

corresponding to $p_{ajk}, p_{aj}, q_j, q_{jk}$, respectively, which is obtained by replacing in $PDNF^*_{t,n}(f_n,\vec{p})$ every elementary disjunction $\bigvee_{\nu=1}^{\ell} r_\nu^{\epsilon_\nu}$ by $\prod_{\nu=1}^{\ell}(r^*_\nu - \epsilon_\nu)$, where r^*_ν is the variable corresponding to the propositional atom r_ν.

THEOREM 5.1. *For any Boolean function f_n in n variables, any t smaller than $w(f_n)$ and any ground field k, every polynomial calculus refutation of $\mathcal{PDNF}^*_{t,n}(f_n,\vec{p})$ must have degree at least $(t/2)+1$.*

PROOF. Similar to the proof of Theorem 4.2, we exhibit a linear transformation that defines an inverse reduction from $(\neg\mathcal{PHP}_t^{w(f_n)})$ to $\mathcal{PDNF}^*_{t,n}(f_n,\vec{p})$. Intuitively, we assume that we possess an injective mapping $\alpha : [w(f_n)] \longrightarrow [t]$, and we want to construct a PDNF for f_n with t elementary conjunctions. Denote $f_n^{-1}(1)$ by A. All we have to do is to identify $[w(f_n)]$ with A in an arbitrary way, and let K_j compute the singleton function outputting 1 on the only assignment $\alpha^{-1}(j)$ ($K_j = 0$, if j is not in the range of α).

Formally, variables $x_{ajk}, x_{aj}, y_j, y_{jk}$ are transformed to linear forms in the pigeonhole variables z_{aj} ($a \in A$, $j \in [t]$) as follows:

$$\begin{aligned}
x_{ajk}, x_{aj} &\mapsto 0 \ (a \notin A);\\
x_{ajk} &\mapsto \sum_{\substack{b\in A\\ b_1=a_1,\dots,b_k=a_k}} z_{bj} \ (a \in A;\ \text{in particular, } x_{ajn} \mapsto z_{aj});\\
x_{aj} &\mapsto \sum_{j'\leq j} z_{aj'} \ (a \in A);\\
y_j &\mapsto \sum_{a\in A} z_{aj};\\
y_{jk} &\mapsto \sum_{\substack{a\in A\\ a_k=1}} z_{aj}.
\end{aligned}$$

It is straightforward to check that this transformation takes every axiom Q in $\mathcal{PDNF}^*_{t,n}(f_n,\vec{p})$ to a polynomial that has a degree $\deg(Q)$ proof from $(\neg\mathcal{PHP}_t^{w(f_n)})$. Hence the required bound follows from Theorem 3.1. $\square$

Corollary 5.2. *For any Boolean function f_n in n variables, any t smaller than the circuit size of f_n and any ground field k, every polynomial calculus refutation of (the polynomial transformation of) $Circuit_{t,n}(f_n, \vec{p})$ must have degree $\Omega(t/n)$.*

Proof. We may represent the PDNF (5.28) (possibly with zero terms) as the $2n(t-1)$-sized circuit

$$\bigvee_{j=1}^{t}\left(\epsilon_j \wedge \bigwedge_{k=1}^{n} x_k^{\epsilon_{jk}}\right)$$

with the *fixed topology* and (unknown) constant functions $\epsilon_j, \epsilon_{jk}$ describing the structure of the conjunctions K_j's. Hence, if we let $t' := \lceil \frac{t}{2n} \rceil$, then $\mathcal{PDNF}^*_{t',n}(f_n, \vec{p})$ becomes a substitutional instance of $Circuit_{t,n}(f_n, \vec{p})$ (structural variables

$$Fanin(v), Type(v), InputType_\nu(v), InputType'_\nu(v), InputVar_\nu(v,i),$$
$$INPUTVAR_\nu(v,i), InputNode_\nu(v,v'), INPUTNODE_\nu(v,v')$$

get transformed into logical constants describing the topology of this circuit, and $InputType''_\nu(v)$ are taken to the corresponding variables q_j, q_{jk}). Now the bound follows from Theorem 5.1. □

6. Conclusion and open problems

The system $F_d(MOD_p)$ of bounded depth Frege proofs with modular gates is the most notable example of a propositional proof system for which we have no lower bounds, whereas exponential bounds are known for their computational counterpart. The approximation technique used for these computational bounds was formalized in Buss *et al.* (1996), and $F_d(MOD_p)$-proofs were reduced to Nullstellensatz proofs with some additional *extension polynomials*. The characteristic feature of these extension polynomials is that they are zero almost everywhere.

It might well be that lower bounds for the polynomial calculus established in this paper make the next step toward the goal of proving lower bounds for the system $F_d(MOD_p)$. Namely, if we apply the reduction operator R to any Nullstellensatz refutation with extension polynomials of $(\neg\mathcal{PHP}^m_n)$, then we kill all original pigeonhole axioms. The only problem is to show that R preserves the property of extension polynomials to be zero almost everywhere in any reasonable sense. Some hope that this might be doable is, perhaps, provided by the fact that R is described quite explicitly, both from the semantic and syntactic point of view.

Recall that every single *group* of extension polynomials can be eliminated from any Nullstellensatz proof with only a polynomial increase in degree (Buss *et al.* 1996, Theorem 6.13). On the other hand, polynomial calculus proofs (over a finite field) can be simulated by Nullstellensatz proofs with a single *level* of extension polynomials. Apparently, this makes the latter model an attractive goal that might be more accessible than the general case of arbitrarily many levels.

And, as always, there is a lot of structural and refining work to be done after some lower bounds are proved by some method. Here are some immediate questions raised already by the material in this paper.

The explicit description of the reduction operator R given in Section 3.2 is probably interesting in its own right, and the effort we spent on developing the necessary combinatorial machinery should not be considered as a waste of time anyway. Still, the necessity to have all this machinery as an essential ingredient of our proof is somewhat humiliating, especially since the only purpose it serves is to prove something as natural and innocent-looking as (3.11). Can we prove this property by some reasonably general semantic argument?

Can we prove lower bounds for other important counting principles extensively studied in the literature, such as $Count_a$ or the onto version of PHP_n^m? There is one obvious difficulty with extending our proof to these principles. Namely, this proof (as apparently all other proofs in the area) tends to neglect monomial axioms: w.l.o.g. we can factor our ring by them from the very beginning, as we did explicitly in the proof of Theorem 4.5. In the case of PHP_n^m, the remaining "essential" axioms Q_i are totally disconnected (i.e., do not have any variables in common), and this seems to be important for the crucial property (3.11). It is not clear what to do when they are totally connected, and there necessarily must be an essential axiom with support X such that (in the notation of (3.11)) $X \subseteq X_I$ and $X, X_{\mathrm{dom}(t)}$ are in common position.

This is actually the main reason why we preferred to work with the specific case of PHP_n^m rather than to formulate a general lower bound criterion: it seems that at the moment PHP_n^m is the only interesting combinatorial principle to which our argument applies. But if the difficulties sketched in the previous paragraph are somehow overcome, it would be extremely interesting to see such a criterion applicable simultaneously to at least several principles in this area.

We already asked above if one can get lower bounds for Nullstellensatz proofs with a single level of extension polynomials, which is apparently the weakest natural system extending the polynomial calculus. An equally natural question to ask is whether this extension is proper or not. Note that since PHP_n^{2n} has quasi-polynomial size F_3-proofs by Paris *et al.* (1988), $(\neg\mathcal{PHP}_n^{2n})$ has a Nullstellensatz refutation of degree $(\log n)^{O(1)}$ with *four* levels of extension polynomials by Buss *et al.* (1996), Theorem 6.12(1). Hence for the case of several (i.e., at least four) levels of extension polynomials, the answer to this question is positive.

The bound (4.16) completely resolves the question of determining the order of magnitude of the function $D_k(n,d)$ when d is at least logarithmic in n. This leaves open the natural question as to what is happening when d is a constant. More specifically, is it true that for any constant $d > 0$ (and any field k) we have $D_k(n,d) \leq n^{1-\Omega(1)}$?

Do there exist "explicit" examples of ℓ-generic systems with parameters allowing us to prove the bound (4.16)? More generally, can this bound be attained for more explicit tautologies, not necessarily based upon Theorem 4.5?

What is the minimal possible degree D of a polynomial calculus refutation of $(\neg\mathcal{PHP}_n^{m,d})$? We proved that $\Omega(n) \leq D \leq O(nd)$, and if in fact $D = \theta(nd)$, this would give us a quite satisfactory answer to the previous question.

One very interesting open question is about the size of resolution proofs of PHP_n^m when $m \gg n^2$. Some partial results toward it, both in terms of upper and lower bounds were proved in Buss & Pitassi (1996b), Razborov *et al.* (1997). Clegg *et al.* (1996) found some simulations of resolution proofs by polynomial calculus proofs. In particular, our Theorem 3.1 combined with Clegg *et al.* (1996), Theorem 10 gives another proof of the exponential lower bound on the size of *tree-like* resolution proofs for PHP_n^m from Buss & Pitassi (1996b), m arbitrarily large. Can we get some new bounds for resolutions using algebraic methods? Clegg *et al.* (1996) also contains some simulation of *non-treelike* resolutions (Theorem 11) but it seems that our bounds do not give any non-trivial corollaries via this reduction.

Finally, we briefly comment on results in Section 5 where we showed that there is no low degree polynomial calculus proof of $\mathbf{NP} \not\subseteq \mathbf{P}/poly$. Given our proof method (applicable to an extremely weak class of circuits), Corollary 5.2 can be hardly taken as a serious additional evidence that $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ does not possess any feasible proof. But this is a very good illustration to another important thesis, that the tautologies $\neg Circuit_{t,n}(f_n, \vec{p})$ are of "universal" nature and have a lot of useful structure hidden inside. Razborov & Rudich (1997), Razborov (1995b), Krajíček (1997a), Razborov (1994) showed how to extract from them disjoint **NP**-pairs supposedly not separated by a simple set. In

Section 5 we basically exhibited how to extract the counting principle PHP_n^m in its purest form. This gives us the hope that when (and if) the methods for proving really strong lower bounds in proof complexity finally come to the scene (most likely, modulo some equally strong complexity or cryptographic assumptions), the chances are high that these methods can be either directly applied or at least easily adapted to the formulae $\neg Circuit_{t,n}(f_n, \vec{p})$ expressing one of the central open problems of modern mathematics, the $\mathbf{NP} \overset{?}{\subseteq} \mathbf{P}/poly$ question.

7. Recent developments

Based upon the previous work of Ajtai (1994b), Krajíček (1997c) established an $\omega(1)$ lower bound on the degree of polynomial calculus proofs of $Count_a$ over $\mathbf{F}_p$, p does not divide a. Generalizing Pitassi (1996), Krajíček (1997b) noticed that polynomial calculus lower bounds for either onto-$PHP_n^{n+p^\ell}$ ($p^\ell \ll n$) or $Count_a$ imply proportionally strong lower bounds for the proof system $F_d^c(MOD_p)$ in which lines can be obtained by substituting constant-depth De Morgan formulae into constant depth formulae in the language $\{\neg, \wedge, \vee, MOD_p\}$, $\wedge$ and $\vee$ being this time binary. Thus, the combination of Krajíček (1997b) and Krajíček (1997c) implies barely super-polynomial lower bounds for $F_d^c(MOD_p)$.

Impagliazzo *et al.* (1997) gave a simpler proof of Theorem 3.1 that involves only syntactic arguments and does not appeal to assignments from M_I at all. Our crucial Claim 3.11 is replaced in that paper by constructing quite an explicit basis B_I of $k\widetilde{T_I}$ with the property $B_I \supseteq \Delta_I^{\mathrm{syn}}$.

Acknowledgements

I am grateful to Paul Beame for his useful remarks, in particular for his observation that the bound on $|I|$ needed for Claim 3.10 can be loosened by one. I am also indebted to both anonymous referees for many useful comments and results. This work was supported by Russian Basic Research Foundation grant 96-01-01222.

References

M. Ajtai, The complexity of the pigeonhole principle. In *Proceedings of the 29th IEEE Symposium on Foundations of Computer Science*, 1988, 346–355.

M. Ajtai, The independence of the modulo p counting principle. In *Proceedings of the 26th ACM STOC*, 1994a, 402–411.

M. Ajtai, Symmetric systems of linear equations modulo p. Technical Report TR94-015, Electronic Colloquium on Computational Complexity, 1994b.

P. Beame, S. Cook, J. Edmonds, R. Impagliazzo, and T. Pitassi, The relative complexity of NP search problems. In *Proceedings of the* 27*th ACM STOC*, 1995, 303–314.

P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák, Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *Proceedings of the* 35*th IEEE FOCS*, 1994, 794–806. Journal version to appear in *Proc. of the London Math. Soc.*

P. Beame and S. Riis, More on the relative strength of counting principles. In *Proof Complexity and Feasible Arithmetics: DIMACS workshop, April* 21-24, 1996, *DIMACS Series in Dicrete Mathematics and Theoretical Computer Science, vol.* 39, ed. P. Beame and S. Buss. American Math. Soc., 1997.

S. Bellantoni, T. Pitassi, and A. Urquhart, Approximation of small depth Frege proofs. *SIAM Journal on Computing* **21**(6) (1992), 1161–1179.

S. R. Buss, Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic* **52** (1987), 916–927.

S. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. Razborov, and J. Sgall, Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *computational complexity* **6**(3) (1996/1997), 256–298.

S. Buss and T. Pitassi, Good degree lower bounds on Nullstellensatz refutations of the induction principle. In *Proceedings of the* 11*th Annual Conference on Structure in Complexity Theory*, 1996a. Journal version submitted to *Journal of Computer and System Sciences.*

S. Buss and T. Pitassi, Resolution and the weak pigeonhole principle. Manuscript, 1996b.

M. Clegg, J. Edmonds, and R. Impagliazzo, Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the* 28*th ACM STOC*, 1996, 174–183.

R. Impagliazzo, P. Pudlák, and J. Sgall, Simplified lower bounds for the polynomial calculus. Submitted to *computational complexity*, 1997.

J. Krajíček, Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic* **59**(1) (1994), 73–86.

J. Krajíček, Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic* **62**(2) (1997a), 457–486.

J. Krajíček, Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus. Manuscript, 1997b.

J. Krajíček, On the degree of ideal membership proofs from uniform families of polynomials over a finite field. Manuscript, 1997c.

J. Krajíček, P. Pudlák, and A. R. Woods, Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms* **7**(1) (1995), 15–39.

J. B. Paris, A. J. Wilkie, and A. R. Woods, Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic* **53**(4) (1988), 1235–1244.

T. Pitassi, 1996. Personal communication.

T. Pitassi, P. Beame, and R. Impagliazzo, Exponential lower bounds for the pigeonhole principle. *computational complexity* **3** (1993), 97–140.

А. А. Разборов, Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения. *Матем. Зам.* **41**(4) (1987), 598–607. A. A. Razborov, Lower bounds on the size of bounded-depth networks over a complete basis with logical addition, *Mathem. Notes of the Academy of Sci. of the USSR*, 41(4):333-338, 1987.

A. Razborov, On provably disjoint **NP**-pairs. Technical Report RS-94-36, Basic Research in Computer Science Center, Aarhus, Denmark, 1994. Available at http://www.brics.aau.dk/BRICS/RS/94/36/BRICS-RS-94-36/BRICS-RS-94-36.html.

A. Razborov, Bounded Arithmetic and lower bounds in Boolean complexity. In *Feasible Mathematics II. Progress in Computer Science and Applied Logic, vol.* 13, ed. P. Clote and J. Remmel, 344–386. Birkhäuser, 1995a.

A. Razborov, Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic. *Изв. АН СССР, сер. матем.* (Izvestiya of the RAN) **59**(1) (1995b), 201–222. See also *Izvestiya: Mathematics* **59**(1), 205–227.

A. Razborov, Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In *Proceedings of the* 23rd *ICALP, Lecture Notes in Computer Science,* 1099, ed. F. Meyer auf der Heide and B. Monien, New York/Berlin, 1996, Springer-Verlag, 48–62.

A. Razborov and S. Rudich, Natural proofs. *Journal of Computer and System Sciences* **55**(1) (1997), 24–35.

A. Razborov, A. Wigderson, and A. Yao, Read-once branching programs, rectangular proofs of the pigeonhole principle and the transversal calculus. In *Proceedings of the 29th ACM Symposium on Theory of Computing*, 1997, 739–748.

S. Riis, Count(q) does not imply Count(p). *Annals of Pure and Applied Logic* **90** (1997), 1–56.

R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the 19th ACM Symposium on Theory of Computing*, 1987, 77–82.

Manuscript received January 15, 1997

Alexander A. Razborov
Department of Mathematical Logics
Steklov Mathematical Institute
Gubkina 8, 117966, GSP-1
Moscow, RUSSIA
razborov@genesis.mi.ras.ru