Electronic Colloquium on Computational Complexity, Report No. 55 (2001)

ECCC

Improved Resolution Lower Bounds for the Weak Pigeonhole Principle

Alexander A. Razborov *

July 26, 2001

Abstract

Recently, Raz [Raz01] established exponential lower bounds on the size of resolution proofs of the weak pigeonhole principle. We give another proof of this result which leads to better numerical bounds. Specifically, we show that every resolution proof of PHP_n^m must have size $\exp\left(\Omega(n/\log m)^{1/2}\right)$ which implies an $\exp\left(\Omega(n^{1/3})\right)$ bound when the number of pigeons m is arbitrary.

As a step toward extending this bound to the *functional* version of PHP_n^m (in which one pigeon may not split between several holes), we introduce one intermediate version (in the form of a PHP-oriented calculus) which, roughly speaking, allows arbitrary "monotone reasoning" about the location of an individual pigeon. For this version we prove an $\exp\left(\Omega(n/\log^2 m)^{1/2}\right)$ lower bound ($\exp\left(\Omega(n^{1/4})\right)$ for arbitrary m).

1. Introduction

Propositional proof complexity is an area of study that has seen a rapid development over the last decade. It plays 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. Propositional proof complexity is

*Institute for Advanced Study, Princeton, US and Steklov Mathematical Institute, Moscow, Russia, razborov@math.ias.edu. Supported by the State of New Jersey and NSF grant CCR-9987077.

ISSN 1433-8092

in a sense complementary to the (non-uniform) computational complexity; moreover, there exist extremely rich and productive relations between the two areas (see e.g. [Raz96, BP98]).

Much of the research in proof complexity is centered around the resolution proof system that was introduced in [Bla37] and further developed in [DP60, Rob65]. In fact, it was for a subsystem of this system (nowadays called *regular Resolution*) that Tseitin proved the first non-trivial lower bounds in his seminal paper of more than 30 years ago [Tse68].

Despite its apparent (and deluding) simplicity, the first exponential lower bounds for general Resolution were proven only in 1985 by Haken [Hak85]. These bounds were achieved for the pigeonhole principle PHP_n^{n+1} (which asserts that $(n+1)$ pigeons cannot sit in n holes so that every pigeon is alone in its hole), and they were followed by many other strong results on the complexity of resolution proofs (see e.g. [Urq87, CS88, BT88, BP96a, Juk97]).

Ben-Sasson and Wigderson [BW99] established a very general trade-off between the minimal width $w_R(\tau)$ and the minimal size $S_R(\tau)$ of resolution proofs for *any* tautology τ. Their inequality (strengthening a previous result for Polynomial Calculus from [CEI96]) says that

$$w_R(\tau) \leq O\left(\sqrt{n(\tau) \cdot \log S_R(\tau)}\right), \tag{1}$$

where $n(\tau)$ is the number of variables. It is much easier to bound the width $w_R(\tau)$ than the size $S_R(\tau)$ and, remarkably, Ben-Sasson and Wigderson pointed out that (apparently) *all* lower bounds on $S_R(\tau)$ known at that time can be viewed as lower bounds on $w_R(\tau)$ followed by applying the inequality (1) (although, sometimes with some extra work).

This "width method" seemed to fail bitterly for tautologies τ with a huge number of variables $n(\tau)$. There are two prominent examples of such tautologies. The first example is the weak pigeonhole principle PHP_n^m, where the word "weak" refers to the fact that the number of pigeons m may be much larger (potentially infinite) than the number of holes n. The second example is made by the tautologies expressing the hardness of the Nisan-Wigderson generator for propositional proof systems [ABRW00].

Accordingly, other methods were developed for handling the weak pigeonhole principle PHP_n^m (as long as the resolution size is concerned, the case of generator tautologies is still completely open). [RWY97] proved exponential

lower bounds for a subsystem of regular resolution (so-called *rectangular calculus*), [PR00] proved such bounds for unrestricted regular resolution, and recently Raz [Raz01] completely solved the case of general resolution proofs for the version of the weak pigeonhole principle in which the axioms forbidding pigeons to split between several holes are missing.

The main goal of this paper is to present another (and, probably, simpler) proof of the latter result; we also get a stronger bound $\exp\left(\Omega(n^{1/3})\right)$ (Theorem 2.2 below; the bound resulting from [Raz01] would be something like $\exp\left(\Omega(n^{1/10})\right)$). This is already quite close to the best known upper bound $\exp(O(n\log n)^{1/2})$ [BP96b]. What is, however, more important is that we essentially show how to match some basic ideas from [RWY97, PR00, Raz01] with the width-bounding argument from [BW99]. More specifically, our main technical tool (Lemma 3.1, essentially borrowed from [RWY97, PR00, Raz01]) allows us to prove some analogue of the relation (1) (Lemma 3.3, Claim 4.2) even in certain situations when the number of variables is huge.

Neither the methods from [Raz01] nor our methods apply directly to the functional version $FPHP_n^m$ in which one pigeon may not split between several holes. This version of the weak pigeonhole principle appears to be at least as natural and traditional as the "ordinary" one, and some more reasons to be interested in it can be found in the concluding section 5. As a step toward the goal of getting resolution lower bounds for $FPHP_n^m$, we introduce an intermediate version (in terms of the so-called *monotone functional calculus*) which essentially allows arbitrary "monotone reasoning" about the locations of any individual pigeon. For this stronger version we prove a slightly weaker bound $\exp\left(\Omega(n^{1/4})\right)$ (Theorem 2.7).

The paper is organized as follows. In Section 2 we give necessary definitions and preliminaries. In Section 3 we prove our "base result" (which is an $\exp\left(\Omega(n^{1/4})\right)$ lower bound for the *ordinary* version): the proof is simpler than for the better bound $\exp\left(\Omega(n^{1/4})\right)$, but nonetheless illustrates all basic ideas of our approach. The two improvements of this result already mentioned above (Theorems 2.2, 2.7) are presented in Section 4. The paper is concluded with a brief discussion in Section 5 that also includes several open problems.

2. Preliminaries

Let x be a Boolean variable, i.e. a variable that ranges over the set $\{0,1\}$. A *literal* of x is either x (denoted sometimes as x^1) or $\bar{x}$ (denoted sometimes as x^0). A *clause* is a disjunction of literals. The empty clause will be denoted by 0. A clause is *positive* if it contains only positive literals x^1. For two clauses C', C, let $C' \leq C$ mean that every literal appearing in C' also appears in C.

A *CNF* is a conjunction of pairwise different clauses. For a CNF τ, let $n(\tau)$ be the overall number of distinct variables appearing in it.

An *assignment to the variables* $\{x_1, \ldots, x_n\}$ is a mapping $\alpha : \{x_1, \ldots, x_n\} \to \{0,1\}$. A *restriction* of these variables is a mapping $\rho : \{x_1, \ldots, x_n\} \to \{0,1,\star\}$. The *restriction of a Boolean function* $f(x_1, \ldots, x_n)$ *by* ρ, denoted by $f|_\rho$ is the function obtained from f by setting the value of each $x \in \rho^{-1}(\{0,1\})$ to $\rho(x)$, and leaving each $x \in \rho^{-1}(\star)$ as a variable.

One of the simplest and the most widely studied propositional proof systems is *Resolution* which operates with clauses and has one rule of inference called *resolution rule*:

$$\frac{C_0 \vee x \qquad C_1 \vee \bar{x}}{C} \ (C_0 \vee C_1 \leq C).$$

A *resolution refutation* of a CNF τ is a resolution proof of the empty clause 0 from the clauses appearing in τ. The *size* $S_R(P)$ of a resolution proof P is the overall number of clauses in it. For an unsatisfiable CNF τ, $S_R(\tau)$ is the minimal size of its resolution refutation.

For n, a non-negative integer let $[n] \stackrel{\text{def}}{=} \{1, 2, \ldots, n\}$, and for $\ell \leq n$ let $[n]^\ell \stackrel{\text{def}}{=} \{I \subseteq [n] \mid |I| = \ell\}$.

Definition 2.1 $(\neg PHP_n^m)$ is the unsatisfiable CNF in the variables $\{x_{ij} \mid i \in [m],\ j \in [n]\}$ that is the conjunction of the following clauses:

$$Q_i \stackrel{\text{def}}{=} \bigvee_{j=1}^{n} x_{ij} \ (i \in [m]);$$

$$Q_{i_1,i_2;j} \stackrel{\text{def}}{=} (\bar{x}_{i_1 j} \vee \bar{x}_{i_2 j}) \ (i_1 \neq i_2 \in [m],\ j \in [n]).$$

The first main result of this paper is the following

Theorem 2.2 $S_R(\neg PHP_n^m) \geq \exp\left(\Omega(n/\log m)^{1/2}\right)$.

Corollary 2.3 *For every m, $S_R(\neg PHP_n^m) \geq \exp\left(\Omega(n^{1/3})\right)$.*

Proof of Corollary 2.3 from Theorem 2.2. Let $S_R(\neg PHP_n^m) = S$. Since a resolution proof of size S can use at most S axioms from $(\neg PHP_n^m)$, and these axioms involve at most $2S$ pigeons $i \in [m]$, we also have

$$S_R(\neg PHP_n^{2S}) \leq S.$$

Now the required bound $S \geq \exp\left(\Omega(n^{1/3})\right)$ immediately follows from Theorem 2.2.■

The following normal form for resolution refutations of the pigeonhole principle was proposed in [BP96b] (they used for it the longer name "monotone resolution proof system" which we abbreviate to "monotone calculus"). For $I \subseteq [m]$, $J \subseteq [n]$ let

$$X_{IJ} \stackrel{\text{def}}{=} \bigvee_{i \in I} \bigvee_{j \in J} x_{ij}$$

(these are exactly "rectangular clauses" from [RWY97]), and we will also naturally abbreviate $X_{I,\{j\}}$ to X_{Ij} and $X_{\{i\},J}$ to X_{iJ}.

Definition 2.4 ([BP96b]) Fix $m > n$. The *monotone calculus* operates with **positive** clauses in the variables $\{x_{ij} \mid i \in [m],\ j \in [n]\}$, and has one inference rule which is the following *monotone rule*:

$$\frac{C_0 \vee X_{I_0,j} \qquad C_1 \vee X_{I_1,j}}{C} \ (C_0 \vee C_1 \leq C;\ I_0 \cap I_1 = \emptyset). \tag{2}$$

A *monotone calculus refutation* of a set of positive clauses $\mathcal{A}$ is a monotone calculus proof of 0 from $\mathcal{A}$, and the *size* $S(P)$ of a monotone calculus proof is the overall number of clauses in it.

Proposition 2.5 ([BP96b]) *$S_R(\neg PHP_n^m)$ coincides, up to a polynomial, with the minimal possible size of a monotone calculus refutation of the set of axioms $\{Q_1, Q_2, \ldots, Q_m\}$ from Definition 2.1.*

In the rest of this section we will be discussing some modifications of the base principle PHP_n^m. The reader interested only in the original formulation may skip this and proceed directly to Section 3.

The (negation of the) *functional pigeonhole principle* ($\neg FPHP_n^m$) is obtained from ($\neg PHP_n^m$) by adding new clauses

$$Q_{i;j_1,j_2} \stackrel{\text{def}}{=} (\bar{x}_{ij_1} \vee \bar{x}_{ij_2}) \ (i \in [m];\ j_1 \neq j_2 \in [n]).$$

[BW99] also introduced the *extended pigeonhole principle* ($\neg EPHP_n^m$) by allowing abbreviations for arbitrary Boolean functions that depend on a single pigeon $i \in [m]$. $EPHP_n^m$ is obviously reducible to PHP_n^m (in the sense that every resolution proof of PHP_n^m leads to a resolution proof of $EPHP_n^m$ that is roughly of the same size). The reduction from $FPHP_n^m$ to $EPHP_n^m$ may seem somewhat counter-intuitive but it is actually not hard (see e.g. Section 5). Thus, $EPHP_n^m$ is intermediate between PHP_n^m and $FPHP_n^m$.

The following monotone version of $EPHP_n^m$, formulated as a natural extension of the monotone calculus, is in turn intermediate between PHP_n^m and $EPHP_n^m$.

Let F_n^{mon} be the set of monotone Boolean functions in the auxiliary variables $\{x_1, \ldots, x_n\}$, and let $Vars_{\text{mon}}(m,n) \stackrel{\text{def}}{=} \{x_{if} \mid f \in F_n^{\text{mon}}\}$. Denote by ρ_j the restriction of the variables $\{x_1, \ldots, x_n\}$ that assigns x_j to 0 and leaves all other variables unassigned. For $I \subseteq [m]$ and $j \in [n]$, let ρ_{Ij} be the restriction of the variables $Vars_{\text{mon}}(m,n)$ defined by

$$\rho_{Ij} \stackrel{\text{def}}{=} \begin{cases} x_{i,\rho_j(f)}, & i \in I \\ x_{if}, & i \notin I. \end{cases}$$

ρ_{Ij} also naturally acts on clauses in the variables $Vars_{\text{mon}}(m,n)$.

Definition 2.6 The *monotone functional calculus* operates with positive clauses in the variables $Vars_{\text{mon}}(m,n)$ and has the following two inference rules:

$$\frac{C_0 \vee x_{i,f_1} \vee \ldots \vee x_{i,f_r} \qquad C_1 \vee x_{i,g_1} \vee \ldots \vee x_{i,g_s}}{C \vee x_{i,h_1} \vee \ldots \vee x_{i,h_t}}$$

$$(C_0 \vee C_1 \leq C;\ i \in [m];\ (f_1 \vee \ldots \vee f_r) \wedge (g_1 \vee \ldots \vee g_s) \leq (h_1 \vee \ldots \vee h_t))$$

and

$$\frac{C_0 \qquad C_1}{C}$$

$(\rho_{I_0,j}(C_0) \vee \rho_{I_1,j}(C_1) \leq C$ for some I_0, I_1 such that $I_0 \cap I_1 = \emptyset$ and $j \in [n])$.

As always, a *refutation* in this calculus is a proof of 0, and the *size* is measured by the number of clauses.

Our second main result is this:

Theorem 2.7 *Every monotone functional calculus refutation of* $\{Q_1, \ldots, Q_m\}$ *must have size* $\exp\left(\Omega(n/\log^2 m)^{1/2}\right)$.

By the same trick as before, we get

Corollary 2.8 *For every* m*, every monotone functional calculus refutation of* $\{Q_1, \ldots, Q_m\}$ *must have size* $\exp\left(\Omega(n^{1/4})\right)$.

Remark 1 The choice of inference rules for the monotone functional calculus may seem somewhat arbitrary. It is worth noting in this respect that Theorem 2.7 holds for the semantical version as well. Namely, we may allow arbitrary binary rules that are sound w.r.t. the set of assignments satisfying the axioms $Q_{i_1,i_2;j}$.

3. Proof of the base result

We begin with the bound $S_R(\neg PHP_n^m) \geq \exp\left(\Omega(n^{1/4})\right)$. It is weaker than both Corollary 2.3 and Corollary 2.8, but the proof is simpler and already illustrates all the major ideas.

Fix $m > n$. Given Proposition 2.5, we may assume that we have a monotone calculus refutation P of $\{Q_1, \ldots, Q_m\}$, and we should lower bound its size $S(P)$. For analyzing the refutation P we are going to allow stronger axioms of the form X_{iJ} (note that $Q_i = X_{i,[n]}$). X_{iJ} will be allowed as an axiom if $|J|$ exceeds a certain threshold d_i *depending on the pigeon* i. In this way we will be able to simplify the refutation P by "filtering out" of it all clauses C containing at least one such axiom. Our first task (Section 3.1) will be to show that if the thresholds d_i are chosen cleverly, then *in every clause* C *passing this filter, almost all pigeons pass it safely*, i.e. their degree in C is *well* below the corresponding threshold d_i. This part in a sense replaces the inequality (1), and it is inspired by the papers [RWY97, PR00, Raz01].

The *pseudo-width* of a clause C will be defined as the number of pigeons that *narrowly* pass the filter $(d_1, \ldots, d_m)$. The second task (Section 3.2) will be to get lower bounds on the pseudo-width, and this will be accomplished by an easy adaptation of the standard argument from [BW99].

3.1. Pseudo-width and its reduction

For a positive clause C in the variables $\{x_{ij} \mid i \in [m],\ j \in [n]\}$, let

$$J_i(C) \stackrel{\text{def}}{=} \{j \in [n] \mid x_{ij} \text{ occurs in } C\}$$

and

$$d_i(C) \stackrel{\text{def}}{=} |J_i(C)|.$$

Suppose that we are given a vector $d = (d_1, \ldots, d_m)$ of elements from $[n]$ ("pigeon filter"), and let δ be another parameter. We let

$$I_{d,\delta}(C) \stackrel{\text{def}}{=} \{i \in [m] \mid d_i(C) \geq d_i - \delta\} \tag{3}$$

and we define the *pseudo-width* $w_{d,\delta}(C)$ *of a clause* C as

$$w_{d,\delta}(C) \stackrel{\text{def}}{=} |I_{d,\delta}(C)|\,.$$

The *pseudo-width* $w_{d,\delta}(P)$ *of a monotone calculus refutation* P is naturally defined as $\max\{w_{d,\delta}(C) \mid C \in P\}$.

Our main tool for reducing the pseudo-width of a monotone calculus proof is the following "pigeon filter" lemma which is in fact a rather general combinatorial statement (in particular, we will use it in the same form in Section 4).

Lemma 3.1 *Suppose that we are given* S *integer vectors* $r^1, r^2, \ldots, r^S$ *of length* m *each:* $r^\nu = (r_1^\nu, \ldots, r_m^\nu)$. *Then there exists an integer vector* $(r_1, \ldots, r_m)$ *such that* $r_i < \lfloor \log_2 m \rfloor$ *for all* $i \in [m]$ *and for every* $\nu \in [S]$ *at least one of the following two events happen:*

1. $\exists i \in [m](r_i^\nu \leq r_i)$;
2. $|\{i \in [m] \mid r_i^\nu \leq r_i + 1\}| \leq O(\log S)$.

We postpone the proof and first show how to use this lemma for reducing the pseudo-width.

Definition 3.2 Given a vector $d = (d_1, \ldots, d_m)$, a *d-axiom* is an arbitrary clause of the form X_{iJ}, where $|J| \geq d_i$.

Lemma 3.3 *Suppose that there exists a monotone calculus refutation P of $\{Q_1, \ldots, Q_m\}$ that has size $\leq S$. Then there exists an integer vector $d = (d_1, \ldots, d_m)$ with $n/(2\log_2 m) < d_i \leq n/2$ for all $i \in [m]$ and a monotone calculus refutation P' of a set of d-axioms which also has size $\leq S$ and such that*[1]

$$w_{d,n/(2\log_2 m)}(P') \leq O(\log S).$$

Proof of Lemma 3.3 from Lemma 3.1. Fix a monotone calculus refutation P of $\{Q_1, \ldots, Q_m\}$ with $S(P) \leq S$. Let $\delta \stackrel{\text{def}}{=} n/(2\log_2 m)$, and for $C \in P$ define

$$r_i(C) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } d_i(C) \geq n/2 \\ \lfloor \frac{(n/2)-d_i(C)}{\delta} \rfloor + 1 \text{ otherwise.} \end{cases}$$

We apply Lemma 3.1 to the vectors $\left\{ r(C) \stackrel{\text{def}}{=} (r_1(C), \ldots, r_m(C)) \mid C \in P \right\}$, and let $(r_1, \ldots, r_m)$ satisfy the conclusion of that lemma.

Set $d_i \stackrel{\text{def}}{=} \lfloor \frac{n}{2} - \delta r_i \rfloor + 1$ (so that d_i is the minimal integer with the property $\lfloor \frac{(n/2)-d_i}{\delta} \rfloor + 1 \leq r_i$). Note that since $r_i < \lfloor \log_2 m \rfloor$, we have $d_i > \delta$.

Consider now an arbitrary $C \in P$. If for the vector $r(C)$ the first case in Lemma 3.1 takes place, then $\lfloor \frac{(n/2)-d_i(C)}{\delta} \rfloor + 1 \leq r_i$ for some $i \in [m]$. This implies $d_i(C) \geq d_i$; thus, C contains a subclause which is a d-axiom. We may replace C by this axiom which will reduce its pseudo-width $w_{d,\delta}(C)$ to 1.

In the second case, $\left| \left\{ i \in [m] \mid \lfloor \frac{(n/2)-d_i(C)}{\delta} \rfloor \leq r_i \right\} \right| \leq O(\log S)$. Since $i \in I_{d,\delta}(C)$ implies the inequality $\lfloor \frac{(n/2)-d_i(C)}{\delta} \rfloor \leq r_i$, for all such C we have $w_{d,\delta}(C) \leq O(\log S)$.

This completes the proof of Lemma 3.3■

Proof of Lemma 3.1. This lemma is proved by an easy probabilistic argument. For $r = (r_1, \ldots, r_m)$, let $W(r) \stackrel{\text{def}}{=} \sum_{i=1}^{m} 2^{-r_i}$. It suffices to prove the existence of a vector r such that for every $\nu \in [S]$ we have:

$$W(r^\nu) \geq 2\ln S \implies \exists i \in [m](r_i^\nu \leq r_i); \tag{4}$$

$$W(r^\nu) \leq 2\ln S \implies |\{i \in [m] \mid r_i^\nu \leq r_i + 1\}| \leq O(\log S). \tag{5}$$

[1]The condition $d_i \leq n/2$ will not be needed in Section 3. Also, we will not need there the upper bound on the size of the whole refutation P', only its consequence that P' actually employs at most S d-axioms. Both these conditions, however, will be essential for the improvements in Section 4.

Let $t \stackrel{\text{def}}{=} \lfloor \log_2 m \rfloor - 1$ and R be the distribution on $[t]$ given by $p_r \stackrel{\text{def}}{=} 2^{-r}$ $(1 \le r \le t-1)$, $p_t \stackrel{\text{def}}{=} 2^{1-t}$. Pick independent random variables $\boldsymbol{r_1}, \ldots, \boldsymbol{r_m}$ according to this distribution. Let us check that for any individual $\nu \in [S]$ the related condition (4), (5) is satisfied with high probability.

Case 1. $W(r^\nu) \ge 2 \ln S$.
Note that $\sum_{r_i^\nu > t} 2^{-r_i^\nu} \le m \cdot 2^{-t-1} \le 2$, therefore $\sum_{r_i^\nu \le t} 2^{-r_i^\nu} \ge 2 \ln S - 2$. On the other hand, for every i with $r_i^\nu \le t$ we have $\mathbf{P}[r_i^\nu \le \boldsymbol{r_i}] \ge 2^{-r_i^\nu}$ and these events are independent. Therefore,

$$\mathbf{P}[\forall i \in [m] (r_i^\nu > \boldsymbol{r_i})] \le \prod_{r_i^\nu \le t} \left(1 - 2^{-r_i^\nu}\right) \le \exp\left(-\sum_{r_i^\nu \le t} 2^{-r_i^\nu}\right) \le O(S^{-2}).$$

Case 2. $W(r^\nu) \le 2 \ln S$.
In this case $\mathbf{P}[r_i^\nu \le \boldsymbol{r_i} + 1] \le 2^{2-r_i^\nu}$ and, therefore,

$$\mathbf{E}[\,|\,\{\, i \in [m] \mid r_i^\nu \le \boldsymbol{r_i} + 1 \,\}\,|\,] \le 4W(r^\nu) \le 8 \ln S.$$

Since these events are independent, we may apply Chernoff's bound and conclude that $\mathbf{P}[\,|\,\{\, i \in [m] \mid r_i^\nu \le \boldsymbol{r_i} + 1 \,\}\,| \ge C \log S] \le S^{-2}$ for any sufficiently large constant C.

So, for every individual $\nu \in [S]$ the probability that the related property (4), (5) fails is at most $O(S^{-2})$. Therefore, for at least one choice of $\boldsymbol{r_1}, \ldots, \boldsymbol{r_m}$ they will be satisfied for all $\nu \in [S]$. This completes the proof of Lemma 3.1.■

3.2. Lower bounds on pseudo-width

Lemma 3.4 *Let $(d_1, \ldots, d_m)$ be an integer vector, δ be any parameter such that $\delta < d_i$ for all $i \in [m]$ and $\mathcal{A}$ be an arbitrary set of d-axioms. Then every monotone calculus refutation P of $\mathcal{A}$ must satisfy $w_{d,\delta}(P) \ge \Omega(\delta^2/(n \log |\mathcal{A}|))$.*

Proof. Let $w_0 \stackrel{\text{def}}{=} \frac{\epsilon \delta^2}{n \log_2 |\mathcal{A}|}$, where ϵ is a sufficiently small constant. We will show that every refutation of $\mathcal{A}$ must have pseudo-width $> w_0$.

For an assignment a to the variables $\{\, x_{ij} \mid i \in [m],\ j \in [n] \,\}$, let

$$J_i(a) \stackrel{\text{def}}{=} \{\, j \mid a_{ij} = 1 \,\}.$$

Set $\ell \stackrel{\text{def}}{=} \lfloor \delta/(4w_0) \rfloor$, and let D be the set of those assignments a for which:

1. a satisfies all axioms $Q_{i_1,i_2;j}$, i.e., $J_{i_1}(a) \cap J_{i_2}(a) = \emptyset$ for $i_1 \neq i_2$;

2. $|J_i(a)| \leq \ell$ for all $i \in [m]$.

For a set of positive clauses Γ and another positive clause C, let $\Gamma \models C$ mean that every assignment $a \in D$ satisfying all clauses from Γ also satisfies C.

Fix now any proof P from the set of axioms $\mathcal{A}$ with $w_{d,\delta}(P) \leq w_0$. Our goal is to show that $0 \notin P$. Let $\mathcal{A}_i$ consist of those axioms in $\mathcal{A}$ that have the form X_{iJ}, $\mathcal{A}_I \stackrel{\text{def}}{=} \bigcup_{i \in I} \mathcal{A}_i$ and $\mathcal{A}_C \stackrel{\text{def}}{=} \mathcal{A}_{I_{d,\delta}(C)}$ (recall that $I_{d,\delta}(C)$ is given by (3)). For $C \in P$ we will show by induction on the number of steps in the derivation of C that $\mathcal{A}_C \models C$.

Base case $C \in \mathcal{A}$ is obvious since $C \in \mathcal{A}_C$.

Inductive step. *$\mathcal{A}_{C_0} \models C_0$, $\mathcal{A}_{C_1} \models C_1$ and C is obtained from C_0, C_1 by a single application of the rule* (2).
Since the rule (2) is sound on D, $\mathcal{A}_{I_{d,\delta}(C_0) \cup I_{d,\delta}(C_1)} \models C$, and also

$$|I_{d,\delta}(C_0) \cup I_{d,\delta}(C_1)| \leq 2w_0.$$

Let us choose the minimal $I \subseteq [m]$ such that $\mathcal{A}_I \models C$; then still $|I| \leq 2w_0$. We will show that in fact $I \subseteq I_{d,\delta}(C)$, and this will obviously imply $\mathcal{A}_C \models C$.

Assume the contrary, and pick up an arbitrary $i_0 \in I \setminus I_{d,\delta}(C)$. Since I is minimal, $\mathcal{A}_{I \setminus \{i_0\}} \not\models C$, and let $a \in D$ satisfy all clauses in $\mathcal{A}_{I \setminus \{i_0\}}$ and falsify C. Re-assigning in a all values a_{ij} with $i \notin I \setminus \{i_0\}$ to 0 will preserve these properties (remember that C is positive!), therefore we may assume from the beginning that $a_{ij} = 0$ for all $i \notin I \setminus \{i_0\}$ and $j \in [n]$.

Let now

$$J_0 \stackrel{\text{def}}{=} \bigcup_{i \in I \setminus \{i_0\}} J_i(a) \cup J_{i_0}(C) \tag{6}$$

and $J_1 \stackrel{\text{def}}{=} [n] \setminus J_0$. Note that

$$|J_1| \geq n - (2w_0\ell + (d_{i_0} - \delta)) \geq n - d_{i_0} + \delta/2. \tag{7}$$

J_1 is the set of holes "permissible" for the pigeon i_0: if we change a by picking an arbitrary ℓ-subset J of J_1 and letting $a_{i_0,j} = 1$ for $j \in J$, then we will get yet another assignment from D which will still falsify C. We want to show that J can be chosen in such a way that this assignment will also satisfy

all axioms in $\mathcal{A}_{i_0}$, and for that purpose we pick $\boldsymbol{J}$ uniformly and at random among all ℓ-subsets of J_1. Let $\boldsymbol{a}$ be the (random) assignment resulting from a by re-assigning all $a_{i_0,j}$ ($j \in \boldsymbol{J}$) to 1.

Take an arbitrary $A \in \mathcal{A}_{i_0}$. Since $|J_{i_0}(A)| \geq d_{i_0}$, by (7) we have

$$|J_{i_0}(A) \cap J_1| \geq \delta/2. \tag{8}$$

Now we can apply Chernoff's bound and conclude that

$$\mathbf{P}[A(\boldsymbol{a}) = 1] = \mathbf{P}[J_{i_0}(A) \cap \boldsymbol{J} \neq \emptyset] \geq 1 - \exp\left(-\Omega\left(\delta\ell/n\right)\right) \geq 1 - |\mathcal{A}|^{-2}$$

if the constant ϵ in the definition of w_0 is small enough.

Hence, for at least one choice of $\boldsymbol{a}$ all axioms in $\mathcal{A}_{i_0}$ will be satisfied. This contradicts our assumption $\mathcal{A}_I \models C$, and this contradiction completes the inductive step.

We have shown that $\mathcal{A}_C \models C$ for every $C \in P$. Finally, since $\delta < d_i$ for all $i \in [m]$, we have $I_{d,\delta}(0) = \emptyset$ and $\mathcal{A}_0 = \emptyset$. Therfore, $\mathcal{A}_0 \not\models 0$, $0 \notin P$ and Lemma 3.4 is completely proved.■

Combining Lemma 3.4 with Lemma 3.3 (and observing that, as always, we may assume $m \leq 2S$), we get

Theorem 3.5 *For every m, $S_R(\neg PHP_n^m) \geq \exp\left(\Omega(n^{1/4})\right)$.*

4. Improvements

In this section we prove Theorems 2.2 and 2.7. Each of these two improvements is achieved by letting one more ingredient of the basic proof from the previous section to depend on the candidate refutation P. To get the numerical improvement (Theorem 2.2), we will pre-process the set of legitimate assignments D according to the content of P. In proving lower bounds for the monotone functional calculus (Theorem 2.7), the ranking function $r_i(C)$ (cf. the proof of Lemma 3.3) will depend on P and will be constructed dynamically.

For Theorem 2.2 we will show improved lower bounds on the pseudo-width $w_{d,\delta}(P)$. Now we do need the bound $d_i \leq n/2$ promised in Lemma 3.3. Also, we need to know an upper bound on the *size of the whole proof* (as opposed to Lemma 3.4 for which we only needed a bound on the *number of d-axioms*).

Lemma 4.1 *Let $(d_1, \ldots, d_m)$ be an integer vector and δ be a parameter such that $\delta < d_i \leq n/2$ for all $i \in [m]$. Then for every monotone calculus refutation P of any set of d-axioms we have the trade-off $w_{d,\delta}(P) \cdot \log S(P) \geq \Omega(\delta)$.*

Proof. Fix an arbitrary proof P from a set of d-axioms $\mathcal{A}$. Set $w_0 \stackrel{\text{def}}{=} \frac{\epsilon\delta}{\log S(P)}$, where ϵ is a sufficiently small constant; we will show that $w_{d,\delta}(P) > w_0$.

Let $\ell \stackrel{\text{def}}{=} \lfloor \frac{n}{20w_0} \rfloor$. Analyzing the proof of Lemma 3.4, we see that it almost goes through with this new value of ℓ. The only problem is that now the set of forbidden holes $\bigcup_{i \in I \setminus \{i_0\}} J_i(a)$ in (6) may have as many as $\Omega(n)$ elements. Thus, if we are unlucky, it may have a huge intersection with the set

$$J' \stackrel{\text{def}}{=} J_{i_0}(A) \setminus J_{i_0}(C) \tag{9}$$

for some $C \in P$, $i_0 \notin I_{d,\delta}(C)$, $A \in \mathcal{A}_{i_0}$, or even completely cover it. All this means that we do not have any useful analogue of (8).

We take care of this by pre-processing the set D. Namely, we are going to remove from it *in advance* all trouble-making assignments that may *eventually* contribute to the unpleasant situation described above.

Formally, let us call any set of the form (9), where $C \in P$, $i_0 \notin I_{d,\delta}(C)$ and $A \in \mathcal{A}_{i_0}$ a *difference set*. Notice for the record that every difference set has size at least δ, and altogether there are at most $S(P)^2$ of them.

Next, let us call $J \subseteq [n]$ *good* if its intersection with every difference set J' has size at most $|J'|/(4w_0)$. We will call an assignment $a \in D$ *good* if $J_i(a)$ is good for all $i \in [m]$.

Now, we define the main relation $\Gamma \models C$ as the semantical implication with respect to *good* assignments $a \in D$, and literally repeat the argument from the proof of Lemma 3.4 up to and including the definition (6) of J_0, J_1. We no longer have (7) but, using the premise $d_i \leq n/2$, we can at least observe a weaker bound

$$|J_1| \geq n - \left((2w_0) \cdot \frac{n}{20w_0} + (d_i - \delta)\right) \geq \frac{9n}{10} - d_i \geq \frac{2n}{5}. \tag{10}$$

The most crucial observation for our improvement is that the bound (8) still holds for any $A \in \mathcal{A}_{i_0}$, although for a different reason. Indeed, $J_{i_0}(A) \cap J_1 = J' \setminus \bigcup_{i \in I \setminus \{i_0\}} J_i(a)$, where J' is given by (9). Since every one of $J_i(a)$ is good and J' is a difference set, $|J' \cap J_i(a)| \leq |J'|/(4w_0)$. This implies $|J_{i_0}(A) \cap J_1| \geq |J'|/2 \geq \delta/2$, i.e., exactly (8).

Similarly to the proof of Lemma 3.4, we now chose $\boldsymbol{J}$ as a random ℓ-subset of J_1 and denote by $\boldsymbol{a}$ the resulting variation of the original assignment a. Given (8), the same calculation based on Chernoff's bound as before shows that with probability $1 - o(1)$ $\boldsymbol{a}$ satisfies all axioms in $\mathcal{A}_{i_0}$. In order to complete the proof in our case, we, however, still need to make sure that there exists a *good* J with this property.

For this purpose notice that for any fixed difference set J' we have

$$\mathbf{P}[|\boldsymbol{J} \cap J'| > |J'|/(4w_0)] = \mathbf{P}[|\boldsymbol{J} \cap (J' \cap J_1)| > |J'|/(4w_0)]\,.$$

By (10),

$$\frac{|\boldsymbol{J}| \cdot |J' \cap J_1|}{|J_1|} \leq \frac{\ell \cdot |J'|}{(2n/5)} \leq \frac{|J'|}{8w_0}.$$

Therefore, we may apply Chernoff's bound and conclude that (as long as the constant ϵ in the definition of w_0 is small enough), $\mathbf{P}[|\boldsymbol{J} \cap J'| > |J'|/(4w_0)] \leq S(P)^{-3}$.

Thus, $\boldsymbol{J}$ is good with probability $1 - o(1)$. Fixing it in such a way that it is at the same time good and satisfies all axioms from $\mathcal{A}_{i_0}$, we complete the inductive step in the proof of $\mathcal{A}_C \models C$.

Finally, good assignments do exist (see the above argument or simply take the identically zero assignment). Therefore, $\mathcal{A}_0 \not\models 0$, and this completes the proof of Lemma 4.1.■

Theorem 2.2 now straightforwardly follows from Lemma 3.3 and Lemma 4.1.

Finally we prove Theorem 2.7. For a positive clause C in the variables $Vars_{\mathrm{mon}}(m,n)$ denote by $f_i(C)$ the following monotone function in the variables $x_1, \ldots, x_n$: $f_i(C) \stackrel{\mathrm{def}}{=} \bigvee \{ f \mid x_{if} \in C \}$. The vector $f(C) \stackrel{\mathrm{def}}{=} (f_1(C), \ldots, f_m(C))$ bears all the information about C necessary for our proof. Its overall strategy once more naturally generalizes the proof of Theorem 3.5. Namely, we are going to construct an appropriate ranking function $\mathrm{rk} : F_n^{\mathrm{mon}} \longrightarrow \mathbb{N}$, form (similarly to the proof of Lemma 3.3) the family of integer vectors $\{(\mathrm{rk}(f_1(C)), \ldots, \mathrm{rk}(f_m(C))) \mid C \in P\}$, apply to this family Lemma 3.1, define the corresponding notion of pseudo-width, cross our fingers and hope that the proof of Lemma 3.4 also goes through. And indeed there exists a particular combinatorial choice of the ranking function rk for which this plain strategy gives a lower bound $\exp\left(\Omega\left(n^{1/6}\right)\right)$. We, however,

skip this and proceed immediately to the better bound $\exp\left(\Omega\left(n^{1/4}\right)\right)$ whose proof does involve some new and potentially useful ideas.

Fix a monotone functional calculus refutation P of $\{Q_1, \ldots, Q_m\}$ that has size S, and let

$$\mathfrak{M}_i \stackrel{\text{def}}{=} \{ f_i(C) \mid C \in P \} \cup \{0, \bigvee_{j=1}^{n} x_j\}.$$

Our ranking function rk will essentially depend on $\{\mathfrak{M}_i\}$. It is also natural (although, not absolutely necessary) to let it depend on i, so that we will actually have individual ranking functions $\mathrm{rk}_1, \ldots, \mathrm{rk}_m$ for every pigeon. Moreover, rk_i will be defined only on $\mathfrak{M}_i$.

Instead of trying to guess in advance what might be good ranking functions, we will take the opposite approach and *define* them as "universal" (w.r.t. $\mathfrak{M}_1, \ldots, \mathfrak{M}_m$) functions, by which we roughly mean "the best possible ranking function for which the inductive step in the proof of Lemma 3.4 goes through". *After* that it will turn out that these universal functions in fact possess a clean combinatorial meaning (implicit in the proof of Lemma 4.3).

Formally, let $w_0 = C \log S$, where C is the constant assumed in the right-hand side of the second case in Lemma 3.1. Let ℓ be an arbitrary parameter (to be specified later). Similarly to the proof of Lemma 3.4, define D as the set of all assignments satisfying the axioms $Q_{i_1,i_2;j}$ and such that $|J_i(a)| \leq \ell$ for all $i \in [m]$. For every $i \in [m]$ we recursively construct an increasing chain $\mathfrak{R}_{i1} \subseteq \mathfrak{R}_{i2} \subseteq \ldots \subseteq \mathfrak{R}_{ir} \subseteq \ldots \subseteq \mathfrak{M}_i$ ($\mathfrak{R}_{ir}$ will be the set of all functions $f \in \mathfrak{M}_i$ with $\mathrm{rk}_i(f) \leq r$, and, in sharp contrast with the proof of Lemma 4.1, these constructions will be totally independent for different i).

Base. $\mathfrak{R}_{i1} \stackrel{\text{def}}{=} \{\bigvee_{j=1}^{n} x_j\}$.

Recursive step. Suppose that $\mathfrak{R}_{ir}$ is already constructed and $f \in \mathfrak{M}_i$. Then $f \in \mathfrak{R}_{i,r+1}$ if and only if there exists $J_0 \in [n]^{(2w_0\ell)}$ such that every assignment $b \in \{0,1\}^n$ that contains $\leq \ell$ ones, satisfies all functions in $\mathfrak{R}_{ir}$ and, moreover, has the property $\forall j \in J_0 (b_j = 0)$, also satisfies f.

It is important (and easy to see) that indeed $\mathfrak{R}_{ir} \subseteq \mathfrak{R}_{i,r+1}$.

Claim 4.2 *For any $\ell > 0$ there exists $i \in [m]$ such that in the above construction we have $0 \in \mathfrak{R}_{i,\lfloor \log_2 m \rfloor}$.*

Proof. For $i \in [m]$ and $f \in \mathfrak{M}_i$ define $\mathrm{rk}_i(f) \stackrel{\mathrm{def}}{=} \min\{r \mid f \in \mathfrak{R}_{ir}\}$ ($\mathrm{rk}_i(f) \stackrel{\mathrm{def}}{=} \infty$ if no such r exists). For $C \in P$, let $r_i(C) \stackrel{\mathrm{def}}{=} \mathrm{rk}_i(f_i(C))$, and let us apply Lemma 3.1 to the set of vectors $\{(r_1(C), \ldots, r_m(C)) \mid C \in P\}$. Let $r = (r_1, \ldots, r_m)$ be the resulting pigeon filter. Define an *r-axiom* as an arbitrary clause C of the form $x_{i,f_1} \vee \ldots \vee x_{i,f_s}$ with $\mathrm{rk}_i(f_1 \vee \ldots \vee f_s) \leq r_i$. Let $I_r(C) \stackrel{\mathrm{def}}{=} \{i \in [m] \mid \mathrm{rk}_i(f_i) \leq r_i + 1\}$, let $w_r(C) \stackrel{\mathrm{def}}{=} |I_r(C)|$ and let $w_r(P) \stackrel{\mathrm{def}}{=} \max\{w_r(C) \mid C \in P\}$.

Arguing as in the proof of Lemma 3.3, we come up with a monotone functional calculus refutation P' from a set of r-axioms $\mathcal{A}$ which has the same size S and satisfies the additional property $w_r(P) \leq w_0$. What is important to us (and can be easily checked) is that still $f_i(C) \in \mathfrak{M}_i$ for all $C \in P'$.

Now we only have to go through the proof of Lemma 3.4 and check that it applies in the current situation. This is quite straightforward up to the definition (6) of J_0, J_1. Essentially the only thing to be checked up to that point is that the rules of the monotone functional calculus are sound on D, and this is easy.

The rest of the proof does not make sense now since there does not appear to exist any reasonable way to define $J_{i_0}(C)$. What we, however, know is that $\forall A \in \mathcal{A}_{i_0}(f_{i_0}(A) \in \mathfrak{R}_{i_0,r})$, where $r \stackrel{\mathrm{def}}{=} r_{i_0}$. On the other hand, $f_{i_0}(C) \notin \mathfrak{R}_{i_0,r+1}$ since $i_0 \notin I_r(C)$. According to the definition of $\mathfrak{R}_{ir}$, this implies that for every $J_0 \in [n]^{(2w_0\ell)}$ there exists an assignment $b \in \{0,1\}^n$ that contains $\leq \ell$ ones, has the property $\forall j \in J_0(b_j = 0)$, satisfies all $f_{i_0}(A)$ ($A \in \mathcal{A}_{i_0}$) and falsifies $f_{i_0}(C)$. In particular, an assignment b with these properties exists for $J_0 \stackrel{\mathrm{def}}{=} \bigcup_{i \in I \setminus \{i_0\}} J_i(a)$. Re-assigning the values $a_{i_0,j}$ to b_j for all $j \in [n]$, we complete the inductive step in proving $\mathcal{A}_{I_r(C)} \models C$.

Since $0 \in P$, we in particular have $\mathcal{A}_{I_r(0)} \models 0$ which implies $I_r(0) \neq \emptyset$. But $i \in I_r(0)$ in turn implies $0 \in \mathfrak{R}_{i,\lfloor \log_2 m \rfloor}$ since $r_i < \lfloor \log_2 m \rfloor$. Claim 4.2 is proved.■

Thus, we are only left to show a lower bound on $\mathrm{rk}_i(0)$, and this turns out to be (relatively) easy.

Lemma 4.3 *Let $\{0, \bigvee_{j=1}^n x_j\} \subseteq \mathfrak{M} \subseteq F_n^{\mathrm{mon}}$ and L, ℓ be parameters such that*

$$|\mathfrak{M}| \leq \exp\left(\frac{\epsilon L \ell}{n}\right), \tag{11}$$

where ϵ is a sufficiently small constant. Define the sets $\mathfrak{R}_1 \subseteq \mathfrak{R}_2 \subseteq \ldots \subseteq \mathfrak{R}_r \subseteq \ldots \subseteq \mathfrak{M}$ by the following recursion:

Base. $\mathfrak{R}_1 \stackrel{\text{def}}{=} \{\bigvee_{j=1}^{n} x_j\}$.

Recursive step. *$f \in \mathfrak{R}_{r+1}$ if and only if there exists $J_0 \in [n]^L$ such that every assignment $b \in \{0,1\}^n$ that contains $\leq \ell$ ones, satisfies all functions in $\mathfrak{R}_r$ and, moreover, has the property $\forall j \in J_0(b_j = 0)$, also satisfies f.*

Then $0 \notin \mathfrak{R}_{\lfloor n/(2L) \rfloor}$.

Proof. Given $f \in \mathfrak{M}$, let $\mathrm{rk}(f) \stackrel{\text{def}}{=} \min\{r \mid f \in \mathfrak{R}_r\}$. For every $f \in \mathfrak{M}$ with $\mathrm{rk}(f) < \infty$ fix once and for all some $J_0 = J_0(f) \in [n]^L$ witnessing the fact $f \in \mathfrak{R}_{\mathrm{rk}(f)}$. Pick $\boldsymbol{b}$ at random among all assignments in $\{0,1\}^n$ that contain exactly ℓ ones. Given (11), we may apply Chernoff's bound and conclude that

$$\mathbf{P}\left[\forall f \in \mathfrak{M}(\mathrm{rk}(f) < \infty)\left(\left|\{j \in J_0(f) \mid \boldsymbol{b_j} = 1\}\right| \leq \frac{2L\ell}{n}\right)\right] > 0. \qquad (12)$$

Fix an arbitrary $b \in \{0,1\}^n$ with this property.

We claim that $f(c) = 1$ for every $f \in \mathfrak{R}_r$ and every $c \leq b$ that contains at least $1 + (r-1)\frac{2L\ell}{n}$ ones. The base $r = 1$ is obvious.

Suppose that $f \in \mathfrak{R}_{r+1}$, $c \leq b$ and c has at least $1 + r\frac{2L\ell}{n}$ ones. Let $d \leq c$ be obtained from c by re-assigning all positions in $J_0(f)$ to 0. Since b satisfies the condition in (12), d still has at least $1 + (r-1)\frac{2L\ell}{n}$ ones. Therefore, by the inductive assumption, d satisfies all functions in $\mathfrak{R}_r$. By the definition of $\mathfrak{R}_{r+1}$, d satisfies f and, since f is monotone, c satisfies it, too. This completes the inductive step.

In particular, $f(b) = 1$ for every $f \in \mathfrak{R}_{\lfloor n/(2L) \rfloor}$. Lemma 4.3 follows.■

Theorem 2.7 is immediately implied by Claim 4.2 and Lemma 4.3. Indeed, let $\ell \stackrel{\text{def}}{=} Cn^{1/2}$, where $C > 0$ is a sufficiently large constant. Then by Claim 4.2, $0 \in \mathfrak{R}_{i,\lfloor \log_2 m \rfloor}$ for some $i \in [m]$. On the other hand, letting in Lemma 4.3 $\mathfrak{M} \stackrel{\text{def}}{=} \mathfrak{M}_i$ and $L \stackrel{\text{def}}{=} (2\ell w_0)$, we observe that the bound (11) is satisfied (if the constant C is large enough). Therefore, $\log_2 m \geq \frac{n}{4\ell w_0} = \Omega\left(\frac{n^{1/2}}{\log S}\right)$. Theorem 2.7 follows.

5. Conclusion and open problems

Neither techniques from [Raz01] nor our techniques can be directly applied to the functional version $FPHP_n^m$ of the pigeonhole principle (in which one pigeon may not split between several holes). Another problem of a very similar nature which still remains open is to construct a pseudo-random generator $G : \{0,1\}^m \longrightarrow \{0,1\}^n$ with $m \geq n^2$ that would be hard for Resolution (see [ABRW00]). Lower bounds for tautologies from either of these two classes would unconditionally imply that Resolution does not possess a poly-size proof of $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ (as formalized e.g. in [Raz98, Section 5]). At the moment we only know that this independence result follows from the existence of one-way functions, and exponential lower bounds for the *ordinary* pigeonhole principle only imply that Resolution can not efficiently prove the stronger variant "**NP** is not doable by poly-size circuits *of unbounded fan-in*".

Let us clarify some connections that might be useful in this respect. As we noted in Section 2, [BW99] defined so-called extended pigeonhole principle $EPHP_n^m$. In the terminology of our paper, its equivalent formulation can be described as the result of removing in the definition of the monotone functional calculus all references to the monotonicity. That is, the set of variables will be $Vars(m,n) \stackrel{\text{def}}{=} \{ x_{if} \mid i \in [m],\ f \text{ is an } \textit{arbitrary} \text{ function in } n \text{ variables} \}$, the clauses C are no longer required to be positive, and we also restore the resolution rule.

Somewhat counter-intuitively, $EPHP_n^m$ is *stronger* than $FPHP_n^m$: if we have a refutation of $\neg(EPHP_n^m)$, then the substitution

$$x_{if}^{\epsilon} \mapsto \bigvee \{ x_{ij} \mid f(\chi_j) = \epsilon \}$$

will (essentially) take it to a resolution refutation of $\neg(FPHP_n^m)$. On the other hand, it is easy to see that the reduction from $FPHP_n^m$ to the propositional statement expressing $\mathbf{NP} \not\subseteq \mathbf{P}/poly$ given in [Raz98, Section 5] already works with $EPHP_n^m$. Moreover, it needs only the rectangular extension variables X_{iJ}. Unfortunately, in order to prove lower bounds even for this weakest possible form of extension the methods from both [Raz01] and the current paper yet have to be enhanced with some new ideas.

The best known upper bound on $S_R(\neg PHP_n^m)$ is $\exp(O(n \log n)^{1/2})$ [BP96b], and we have shown the lower bound $S_R(\neg PHP_n^m) \geq \exp(\Omega(n^{1/3}))$. That would be interesting to further narrow this gap. Specifically, what is the value of $\limsup_{n\to\infty} \frac{\log_2 \log_2 S_R(\neg PHP_n^\infty)}{\log_2 n}$?

Finally, in Section 4 we saw two separate improvements of our basic technique from Section 3 that nonetheless have a similar flavour. Namely, in the proof of Lemma 4.1 we made the set of legitimate assignments D depend on the candidate refutation P, and in the proof of Theorem 2.7 a somewhat similar construction is applied to the ranking function rk. Are these two really different or we can interpret them as two partial case of a single construction? Can one get better results (specifically, can it be useful for solving open problems posed above) if *both* D and rk are constructed dynamically?

6. Acknowledgements

I am grateful to Stasys Jukna and Toni Pitassi for catching several misprints.

References

[ABRW00] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Pseudorandom generators in propositional complexity. In *Proceedings of the* 41*st IEEE FOCS*, 2000.

[Bla37] A. Blake. *Canonical expressions in Boolean algebra.* PhD thesis, University of Chicago, 1937.

[BP96a] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *Proceedings of the* 37*th IEEE FOCS*, pages 274–282, 1996.

[BP96b] S. Buss and T. Pitassi. Resolution and the weak pigeonhole principle. Manuscript, 1996.

[BP98] P. Beame and T. Pitassi. Propositional proof complexity: Past, present and future. Technical Report TR98-067, Electronic Colloquium on Computational Complexity, 1998.

[BW99] E. Ben-Sasson and A. Wigderson. Short proofs are narrow - resolution made simple. In *Proceedings of the* 31*st ACM STOC*, pages 517–526, 1999.

[BT88] S. Buss and G. Turán. Resolution proofs of generalized pigeonhole principle. *Theoretical Computer Science*, 62:311–317, 1988.

[CEI96] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the 28th ACM STOC*, pages 174–183, 1996.

[CS88] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35(4):759–768, 1988.

[DP60] M. Davis and H. Putnam. A computing procedure for quantification theory. *Journal of the ACM*, 7(3):210–215, 1960.

[Hak85] A. Haken. The intractability or resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Juk97] S. Jukna. Exponential lower bounds for semantic resolution. In P. Beame and S. Buss, editors, *Proof Complexity and Feasible Arithmetics: DIMACS workshop, April* 21-24, 1996*, DIMACS Series in Dicrete Mathematics and Theoretical Computer Science, vol.* 39, pages 163–172. American Math. Soc., 1997.

[PR00] T. Pitassi and R. Raz. Exponential lower bound for the weak pigeonhole principle in regular resolution. Manuscript, 2000.

[Raz96] A. Razborov. Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In F. Meyer auf der Heide and B. Monien, editors, *Proceedings of the* 23*rd ICALP, Lecture Notes in Computer Science,* 1099, pages 48–62, New York/Berlin, 1996. Springer-Verlag.

[Raz98] A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7:291–324, 1998.

[Raz01] R. Raz. Resolution lower bounds for the weak pigeonhole principle. Manuscript, 2001.

[Rob65] J. A. Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, 1965.

[RWY97] 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*, pages 739–748, 1997.

[Tse68] G. C. Tseitin. On the complexity of derivations in propositional calculus. In *Studies in constructive mathematics and mathematical logic, Part II*. Consultants Bureau, New-York-London, 1968.

[Urq87] A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34(1):209–219, 1987.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'