Resolution Lower Bounds for the Weak Functional Pigeonhole Principle

Alexander A. Razborov [1]

Abstract

We show that every resolution proof of the *functional* version $FPHP_n^m$ of the pigeonhole principle (in which one pigeon may not split between several holes) must have size $\exp\left(\Omega\left(\frac{n}{(\log m)^2}\right)\right)$. This implies an $\exp\left(\Omega(n^{1/3})\right)$ bound when the number of pigeons m is arbitrary.

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 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. [15,3]).

Much of the research in proof complexity is centered around the resolution proof system that was introduced in [5] and further developed in [10,19]. 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 [20].

Despite its apparent (and deluding) simplicity, the first exponential lower bounds for general Resolution were proven only in 1985 by Haken [11]. 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

Email address: `razborov@mi.ras.ru` (Alexander A. Razborov).
[1] Steklov Mathematical Institute, Moscow, Russia and Institute for Advanced Study, Princeton, US

hole), and they were followed by many other strong results on the complexity of resolution proofs (see e.g. [21,8,7,2,12]).

Ben-Sasson and Wigderson [4] 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 [9]) 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 [1].

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 open). [18] proved exponential lower bounds for a subsystem of regular resolution (so-called *rectangular calculus*). [13] proved such bounds for unrestricted regular resolution. Finally, Raz [14] completely solved the case of general resolution proofs, and Razborov [16] presented a simpler proof of this result that also led to the better bound $\exp\left(\Omega(n^{1/3})\right)$.

In the *functional version* $FPHP_n^m$ of the pigeonhole principle 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" PHP_n^m. Moreover, apparently all lower bounds for the pigeonhole principle (for various proof systems) prior to [14,16] (including their predecessors [18,13]) worked perfectly well for its functional version. On the contrary, the methods from [14,16] essentially use "multi-valued" matchings and, as a consequence, they do not directly apply to the functional version in which such matchings are wiped out by the new axioms.

In this paper we eliminate this peculiar usage of multi-valued matchings which allows us to extend the $\exp\left(\Omega(n^{1/3})\right)$ bound from [16] to the functional version

$FPHP^m_n$. Like in [16], we show how to match some basic ideas from [18,13,14] with the width-bounding argument from [4], and the resulting analogue of the relation (1) (Lemma 8 below) is actually quite a straightforward generalization of the corresponding statement in [16]. Lower bounds on the analogue of $w_R(\tau)$ ("pseudo-width") are, however, much less straightforward in the case of $FPHP^m_n$. These bounds contained in Lemma 9 make the real (in fact, the only) novelty of the current paper, and we use a somewhat unexpected algebraic technique for deriving them.

The paper is organized as follows. In Section 2 we give necessary definitions and preliminaries. In Section 3 we prove our main result (Theorem 2, Corollary 3) which is an $\exp\left(\Omega(n^{1/3})\right)$ lower bound for the functional version of the pigeonhole principle. The paper is concluded with several open problems in Section 5.

The proof of Theorem 2 is completely self-contained, although some familiarity with [16] may turn out to be helpful for understanding it.

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.

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*:

$$\frac{C_0 \vee x \qquad C_1 \vee \bar{x}}{C} \ (C_0 \vee C_1 \leq C). \tag{2}$$

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 1 *For $m > n$, $(\neg FPHP^m_n)$ is the unsatisfiable CNF in the variables $\{x_{ij} \mid i \in [m],\ j \in [n]\}$ that is the conjunction of the following clauses:*

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

$$Q_{i_1,i_2;j} \stackrel{\rm def}{=} (\bar{x}_{i_1j} \vee \bar{x}_{i_2j}) \;\; (i_1 \neq i_2 \in [m],\; j \in [n]);$$

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

(*let us remark that the ordinary pigeonhole principle* $(\neg PHP^m_n)$ *consists of the clauses* $Q_i,\ Q_{i_1,i_2;j}$).

The main result of this paper is the following

Theorem 2 $S_R(\neg FPHP^m_n) \geq \exp\left(\Omega\left(\frac{n}{(\log m)^2}\right)\right)$.

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

Proof of Corollary 3 from Theorem 2. Let $S_R(\neg FPHP^m_n) = S$. Since a resolution proof of size S can use at most S axioms from $(\neg FPHP^m_n)$, and these axioms involve at most $2S$ pigeons $i \in [m]$, we also have

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

Now the required bound $S \geq \exp\left(\Omega(n^{1/3})\right)$ immediately follows from Theorem 2.■

It will be convenient (although less necessary than in [16]) to get rid of negations once and for all by using the following normal form for refutations of $(\neg FPHP^m_n)$ from [18] (a dual construction proposed earlier in [6] does a similar job for the *ordinary* pigeonhole principle, i.e., in the absence of the axioms $Q_{i;j_1,j_2}$). For $I \subseteq [m],\ J \subseteq [n]$ let

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

(these are exactly "rectangular clauses" from [18]); we will also naturally abbreviate $X_{\{i\},J}$ to X_{iJ}. Note that $Q_i = X_{i,[n]}$.

Definition 4 ([18]) *Fix* $m > n$. *The* positive 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* positive rule*:*

$$\frac{C_0 \vee X_{i,J_0} \qquad C_1 \vee X_{i,J_1}}{C} \;\; (C_0 \vee C_1 \leq C;\;\; J_0 \cap J_1 = \emptyset). \tag{3}$$

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

Proposition 5 ([18]) *$S_R(\neg FPHP_n^m)$ coincides, up to a factor $n^{O(1)}$, with the minimal possible size of a positive calculus refutation of the set of axioms* $\{Q_1, Q_2, \ldots, Q_m\} \cup \left\{ X_{\{i_1,i_2\},[n]-\{j\}} \mid i_1 \neq i_2 \in [m],\ j \in [n] \right\}$.

Proof. Suppose that we have a refutation of $(\neg FPHP_n^m)$. Apply to every line in it the transformation θ that replaces every negated literal $\bar{x}_{ij}$ by the positive clause $X_{i,[n]-\{j\}}$. Clearly, $\theta(Q_i) = \theta(Q_{i;j_1,j_2}) = Q_i$ and $\theta(Q_{i_1,i_2;j}) = X_{\{i_1,i_2\},[n]-\{j\}}$. It is also easy to see that θ takes an instance of the resolution rule (2) to an instance of the positive rule; therefore, θ maps P to a positive calculus refutation of the same size.

In the opposite direction, it is straightforward to check that the axiom $X_{\{i_1,i_2\},[n]-\{j\}}$ has a constant size resolution proof from $Q_{i_1}, Q_{i_2}, Q_{i_1,i_2;j}$, and that in the presence of the axioms $Q_{i;j_1,j_2}$ the positive rule is simulated by an $O(n^2)$-sized resolution proof.■

3 Proof of the main result

Fix $m > n$ and let

$$\mathcal{A}_0 \stackrel{\text{def}}{=} \{Q_1, Q_2, \ldots, Q_m\} \cup \left\{ X_{\{i_1,i_2\},[n]-\{j\}} \mid i_1 \neq i_2 \in [m],\ j \in [n] \right\}.$$

Given Proposition 5, we may assume that we have a positive calculus refutation P of $\mathcal{A}_0$, and we should lower bound its size $S(P)$. For analyzing the refutation P we are going to allow stronger axioms of the form $X_{i(1)J(1)} \vee X_{i(2)J(2)} \vee \ldots \vee X_{i(w_0)J(w_0)}$, where w_0 will be a sufficiently large parameter and $i(1), \ldots, i(w_0)$ are pairwise distinct pigeons. Such a clause will be allowed as an axiom if every $|J(i_\nu)|$ exceeds a certain threshold $d_{i(\nu)}$ determined by a fixed sequence of integers $(d_1, \ldots, d_m)$, d_i in general *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 is a rather straightforward generalization of [16, Lemma 3.3] (the latter in fact exactly corresponds to the case $w_0 = 1$).

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 require an entirely new idea of evaluating propositional proofs in a (linear) matroid.

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

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

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 positive 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 positive calculus proof is the following "pigeon filter" lemma which is in fact a rather general combinatorial statement.

Lemma 6 *Suppose that we are given S integer vectors $r^1, r^2, \ldots, r^S$ of length m each: $r^\nu = (r_1^\nu, \ldots, r_m^\nu)$, and let w_0 be an arbitrary integer parameter. 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) $|\{ i \in [m] \mid r_i^\nu \leq r_i \}| \geq w_0$*;*
(2) $|\{ i \in [m] \mid r_i^\nu \leq r_i + 1 \}| \leq O(w_0 + \log S)$*.*

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

Definition 7 *Given a vector $d = (d_1, \ldots, d_m)$ and an integer w_0, a (w_0, d)-*axiom *is an arbitrary clause of the form $X_{i(1)J(1)} \vee X_{i(2)J(2)} \vee \ldots \vee X_{i(w_0)J(w_0)}$, where $i(1) < \ldots < i(w_0)$ and $|J(\nu)| \geq d_{i(\nu)}$ for all $\nu \in [w_0]$.*

Lemma 8 *Suppose that there exists a positive calculus refutation P of $\mathcal{A}_0$, and let w_0 be an arbitrary integer parameter. Then there exists an integer* *vector $d = (d_1, \ldots, d_m)$ with $n/(\log_2 m) < d_i \leq n$ for all $i \in [m]$, a set of (w_0, d)-axioms $\mathcal{A}$ with $|\mathcal{A}| \leq S(P)$ and a positive calculus refutation P' of $\mathcal{A}_0 \cup \mathcal{A}$ such that*

$$w_{d,n/(\log_2 m)}(P') \leq O(w_0 + \log S(P)).$$

Proof of Lemma 8 from Lemma 6. Fix a positive calculus refutation P of $\mathcal{A}_0$, and let $S \stackrel{\mathrm{def}}{=} S(P)$. Let $\delta \stackrel{\mathrm{def}}{=} n/(\log_2 m)$, and for $C \in P$ define

$$r_i(C) \stackrel{\mathrm{def}}{=} \lfloor \frac{n - d_i(C)}{\delta} \rfloor + 1.$$

We apply Lemma 6 to the vectors $\left\{ r(C) \stackrel{\mathrm{def}}{=} (r_1(C), \ldots, r_m(C)) \,|\, C \in P \right\}$, and let $(r_1, \ldots, r_m)$ satisfy the conclusion of that lemma.

Set $d_i \stackrel{\mathrm{def}}{=} \lfloor n - \delta r_i \rfloor + 1$ (so that d_i is the minimal integer with the property $\lfloor \frac{n-d_i}{\delta} \rfloor + 1 \leq r_i$). 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 6 takes place, then $\lfloor \frac{n-d_i(C)}{\delta} \rfloor + 1 \leq r_i$ for at least w_0 different pigeons $i \in [m]$. For every such pigeon, this inequality implies $d_i(C) \geq d_i$; thus, C contains a subclause which is a (w_0, d)-axiom. We may replace C by this axiom which will reduce its pseudo-width $w_{d,\delta}(C)$ to w_0.

In the second case, $\left| \left\{ i \in [m] \,\middle|\, \lfloor \frac{n-d_i(C)}{\delta} \rfloor \leq r_i \right\} \right| \leq O(w_0 + \log S)$. Since $i \in I_{d,\delta}(C)$ implies the inequality $\lfloor \frac{n-d_i(C)}{\delta} \rfloor \leq r_i$, for all such C we have $w_{d,\delta}(C) \leq O(w_0 + \log S)$.

This completes the proof of Lemma 8.∎

Proof of Lemma 6. This lemma is proved by an easy probabilistic argument. For $r = (r_1, \ldots, r_m)$, let $W(r) \stackrel{\mathrm{def}}{=} \sum_{i=1}^m 2^{-r_i}$, and let $C > 0$ be a sufficiently large constant. It suffices to prove the existence of a vector r such that for every $\nu \in [S]$ we have:

$$W(r^\nu) \geq C(w_0 + \log_2 S) \Longrightarrow |\{ i \in [m] \,|\, r_i \geq r_i^\nu \}| \geq w_0; \tag{4}$$

$$W(r^\nu) \leq C(w_0 + \log_2 S) \Longrightarrow |\{ i \in [m] \,|\, r_i \geq r_i^\nu - 1 \}| \leq O(w_0 + \log S). \tag{5}$$

Let $t \stackrel{\mathrm{def}}{=} \lfloor \log_2 m \rfloor - 1$ and R be the distribution on $[t]$ given by $p_r \stackrel{\mathrm{def}}{=} 2^{-r}$ $(1 \leq r \leq t-1)$, $p_t \stackrel{\mathrm{def}}{=} 2^{1-t}$. 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. $W(r^\nu) \geq C(w_0 + \log_2 S)$.
Note that $\sum_{r_i^\nu > t} 2^{-r_i^\nu} \leq m \cdot 2^{-t-1} \leq 2$, therefore $\sum_{r_i^\nu \leq t} 2^{-r_i^\nu} \geq C(w_0 + \log_2 S) - 2$.
On the other hand, for every i with $r_i^\nu \leq t$ we have $\mathbf{P}[\boldsymbol{r_i} \geq r_i^\nu] \geq 2^{-r_i^\nu}$, hence $\mathbf{E}[|\{i \in [m] \mid r_i^\nu \leq t \wedge \boldsymbol{r_i} \geq r_i^\nu\}|] \geq C(w_0 + \log_2 S) - 2$. Since the events $\boldsymbol{r}_i \geq r_i^\nu$ are independent, we may apply Chernoff's bound and conclude that $\mathbf{P}[|\{i \in [m] \mid r_i^\nu \leq t \wedge \boldsymbol{r}_i \geq r_i^\nu\}| < w_0] \leq S^{-2}$ if the constant C is large enough.

Case 2. $W(r^\nu) \leq C(w_0 + \log_2 S)$.
In this case $\mathbf{P}[\boldsymbol{r_i} \geq r_i^\nu - 1] \leq 2^{2-r_i^\nu}$ and, therefore,

$$\mathbf{E}[|\{i \in [m] \mid \boldsymbol{r_i} \geq r_i^\nu - 1\}|] \leq 4W(r^\nu) \leq 4C(w_0 + \log_2 S).$$

Applying once more Chernoff's bound, we conclude that

$$\mathbf{P}[|\{i \in [m] \mid \boldsymbol{r_i} \geq r_i^\nu - 1\}| \geq C'(w_0 + \log S)] \leq S^{-2}$$

for any sufficiently large constant $C' \gg C$.

So, for every individual $\nu \in [S]$ the probability that the related property (4), (5) fails is at most 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 6.■

3.2 Lower bounds on pseudo-width

Lemma 9 *Let $(d_1, \ldots, d_m)$ be an integer vector, where $d_i \leq n$, w_0, δ be arbitrary parameters such that $\delta < d_i$ for all $i \in [m]$ and $\mathcal{A}$ be an arbitrary set of (w_0, d)-axioms with*

$$|\mathcal{A}| \leq \left(1 + \frac{\delta}{2n}\right)^{w_0}. \tag{6}$$

Then every positive calculus refutation P of $\mathcal{A}_0 \cup \mathcal{A}$ must satisfy $w_{d,\delta}(P) \geq \delta/4$.

Proof. Let us fix an arbitrary infinite field k, let L_i be an $(n - d_i + \delta/2)$-dimensional linear space over k and $L \stackrel{\text{def}}{=} \bigotimes_{i=1}^m L_i$. The idea of the proof is to systematically evaluate in L objects associated with a positive calculus refutation P (and its assumed semantics) until we find an invariant preserved during the progress of P as long as $w_{d,\delta}(P) \leq \delta/4$.

First of all, fix arbitrary generic embeddings $\phi_i : [n] \longrightarrow L_i$ with the property that for every $J \in [n]^{(n-d_i+\delta/2)}$ the elements $\{\phi_i(j) \mid j \in J\}$ are linearly independent and form a basis of L_i. Let $\phi : [n]^{[m]} \longrightarrow L$ be the tensor product of these mappings, i.e., $\phi(a_1, \ldots, a_m) \stackrel{\rm def}{=} \phi_1(a_1) \otimes \ldots \otimes \phi_m(a_m)$. For a *partial* function $a : [m] \longrightarrow [n]$ we denote by $\phi(a)$ the *subspace* in L defined as

$$\phi(a) \stackrel{\rm def}{=} \bigotimes_{i \notin \mathrm{dom}(a)} L_i \otimes \bigotimes_{i \in \mathrm{dom}(a)} \phi_i(a_i).$$

Note that since $\mathrm{im}(\phi_i)$ spans L_i for all i, $\phi(a)$ can be alternatively described as the subspace $\mathrm{Span}(\phi(b) | b \in [n]^{[m]} \wedge b \supseteq a)$ spanned by the elements of the form $\phi(b)$, where b runs over all total extensions of a.

Let now D be the set of all partial matchings, i.e., *partial injective* functions $a : [m] \longrightarrow [n]$. We will freely identify elements of D with their graphs and with the corresponding Boolean assignments to the variables $\{ x_{ij} \mid i \in [m],\ j \in [n] \}$. For a positive clause C let

$$Z(C) \stackrel{\rm def}{=} \{ a \in D \mid \mathrm{dom}(a) = I_{d,\delta}(C) \wedge C(a) = 0 \},$$

and finally let us put

$$\phi(C) \stackrel{\rm def}{=} \mathrm{Span}(\phi(a) | a \in Z(C)).$$

It turns out that $\phi(C)$ is a valid invariant for positive calculus proofs of small pseudo-width: when such a proof P develops, it never generates new vectors in $\mathrm{Span}(\phi(C) | C \in P)$. More precisely, we have the following claim which is the heart of the entire argument.

Claim 10 *Suppose that C is obtained from C_0, C_1 via a single application of the positive rule, and assume that $w_{d,\delta}(C_0)$ and $w_{d,\delta}(C_1)$ do not exceed $\delta/4$. Then $\phi(C) \subseteq \mathrm{Span}(\phi(C_0), \phi(C_1))$.*

Proof of Claim 10. Fix an arbitrary $a \in Z(C)$; we only need to show that $\phi(a) \subseteq \mathrm{Span}(\phi(C_0), \phi(C_1))$. Let $I \stackrel{\rm def}{=} I_{d,\delta}(C_0) \cup I_{d,\delta}(C_1)$, and denote by a' the restriction of a onto $I_{d,\delta}(C) \cap I$. Since the mapping ϕ is anti-monotone w.r.t. inclusion, it is sufficient to show that

$$\phi(a') \subseteq \mathrm{Span}(\phi(C_0), \phi(C_1)). \tag{7}$$

Since C is positive, $C(a') = 0$. $\mathrm{dom}(a') = I_{d,\delta}(C) \cap I$ may be a proper subset of I; let us consider an arbitrary extension $b \in D$ of a' with $\mathrm{dom}(b) = I$ such that $C(b) = 0$. Since the positive rule is sound on D, the latter fact implies $C_\epsilon(b) = 0$ for some $\epsilon \in \{0, 1\}$. Then the restriction b' of b onto $I_{d,\delta}(C_\epsilon)$ belongs to $Z(C_\epsilon)$ which implies $\phi(b) \subseteq \phi(b') \subseteq \phi(C_\epsilon)$. We have proved so far that

$$\mathrm{Span}(\phi(b) | b \in D \wedge b \supseteq a' \wedge \mathrm{dom}(b) = I \wedge C(b) = 0) \subseteq \mathrm{Span}(\phi(C_0), \phi(C_1)), \tag{8}$$

and, in order to get (7), we are going to show

$$\phi(a') \subseteq \mathrm{Span}(\phi(b) | b \in D \wedge b \supseteq a' \wedge \mathrm{dom}(b) = I \wedge C(b) = 0). \qquad (9)$$

For doing this we show by induction on $h = 0, 1, \ldots, |I| - |\mathrm{dom}(a')|$ that the right-hand side $\mathrm{Span}(\phi(b) \mid b \in D \ \wedge \ b \supseteq a' \ \wedge \ \mathrm{dom}(b) = I \ \wedge \ C(b) = 0)$ contains $\phi(a'')$ for every $a'' \in D$ such that $a'' \supseteq a$, $\mathrm{dom}(a'') \subseteq I$, $|a''| = |I| - h$ and $C(a'') = 0$.

Base $h = 0$ is obvious.

Inductive step. Let $h > 0$ and $a'' \in D$ be such that $a'' \supseteq a$, $\mathrm{dom}(a'') \subset I$, $|a''| = |I| - h$ and $C(a'') = 0$. Pick up an arbitrary $i \in I \setminus \mathrm{dom}(a'')$, and let us estimate the number of those $j \in [n]$ for which $a'' \cup \{(i,j)\} \in D$ and $C(a'' \cup \{(i,j)\}) = 0$.

The first condition $a'' \cup \{(i,j)\} \in D$ rules out $|a''| \leq |I| \leq |I_{d,\delta}(C_0)| + |I_{d,\delta}(C_1)| \leq \delta/2$ different holes j. Since $i \notin I_{d,\delta(C)}$, we have $d_i(C) \leq d_i - \delta$ and this is how many j are forbidden by the second condition $C(a'' \cup \{(i,j)\}) = 0$. Altogether we have at most $(d_i - \delta/2)$ forbidden holes j; therefore, if we denote

$$J \stackrel{\mathrm{def}}{=} \{ j \in [n] \mid a'' \cup \{(i,j)\} \in D \wedge C(a'' \cup \{(i,j)\}) = 0 \}$$

then $|J| \geq (n - d_i + \delta/2)$. Finally, since $\{ \phi_i(j) \mid j \in J \}$ spans L_i (recall that the embedding ϕ_i is generic!), we obtain $\phi(a'') = \mathrm{Span}(\phi(a'' \cup \{(i,j)\}) \mid j \in J)$. Since all such $\phi(a'' \cup \{(i,j)\})$ are contained in $\mathrm{Span}(\phi(b) | b \in D \wedge b \supseteq a' \wedge \mathrm{dom}(b) = I \wedge C(b) = 0)$ by the inductive assumption, this completes the inductive step.

In particular, for $h = |I| - \mathrm{dom}(a')$ we get (9) which, along with (8) implies (7) and completes the proof of Claim 10.■

Iterating Claim 10, we see that if there exists a positive calculus proof P of a clause C from $\mathcal{A}_0 \cup \mathcal{A}$ such that $w_{d,\delta}(P) \leq \delta/4$ then $\phi(C) \subseteq \mathrm{Span}(\phi(A) | A \in \mathcal{A}_0 \cup \mathcal{A})$. Let us estimate dimensions.

Note that $I_{d,\delta}(Q_i) = \{i\}$ and $I_{d,\delta}(X_{\{i_1,i_2\},[n]-\{j\}}) = \{i_1, i_2\}$ which implies $Z(Q_i) = Z(X_{\{i_1,i_2\},[n]-\{j\}}) = \emptyset$. Thus, $\phi(A) = 0$ for every $A \in \mathcal{A}_0$.

Next, if $A = X_{i(1)J(1)} \vee X_{i(2)J(2)} \vee \ldots \vee X_{i(w_0)J(w_0)}$ is an (w_0, d)-axiom then

$$
\begin{aligned}
\dim(\phi(A)) &\le \prod_{i\notin \mathrm{dom}(a)} (n-d_i+\delta/2)\cdot |Z(A)| \\
&\le \prod_{i\notin \mathrm{dom}(a)} (n-d_i+\delta/2)\cdot \prod_{i\in \mathrm{dom}(a)} (n-|J_i|) \\
&\le \prod_{i\notin \mathrm{dom}(a)} (n-d_i+\delta/2)\cdot \prod_{i\in \mathrm{dom}(a)} (n-d_i).
\end{aligned}
$$

Thus,

$$
\frac{\dim(\phi(A))}{\dim(L)} \le \prod_{i\in \mathrm{dom}(a)} \left(\frac{n-d_i}{n-d_i+\delta/2}\right) \le \left(1-\frac{\delta}{2n}\right)^{w_0},
$$

and, along with (6) this implies that the set of linear spaces $\{\phi(A) \mid A \in \mathcal{A}\}$ does not span L. Since $\phi(0) = L$, there can be no positive calculus refutation P of $\mathcal{A}_0 \cup \mathcal{A}$ with $w_{d,\delta}(P) \le \delta/4$. Lemma 9 is completely proved.■

Proof of Theorem 2. Suppose that there exists a positive calculus refutation P of the set $\mathcal{A}_0$ that has size $S(P) = S$. Set $\delta \stackrel{\mathrm{def}}{=} n/(\log_2 m)$ and $w_0 \stackrel{\mathrm{def}}{=} \epsilon\delta$, where $\epsilon > 0$ is a sufficiently small constant. Applying Lemma 8, we find an integer vector $(d_1, \ldots, d_m)$, a set of (w_0, d)-axioms $\mathcal{A}$ with $|\mathcal{A}| \le S$ and a positive calculus refutation P' of $\mathcal{A}_0 \cup \mathcal{A}$ such that $w_{d,\delta}(P') \le \delta/8 + O(\log S)$. Lemma 9 now implies that either $w_{d,\delta}(P') \ge \delta/4$ (and, hence, $\log S \ge \Omega(\delta)$) or $|\mathcal{A}| \ge \left(1+\frac{\delta}{2n}\right)^{w_0} \ge \exp\left(\Omega(n/(\log m)^2)\right)$. In every one of these two cases $S \ge \exp\left(\Omega(n/(\log m)^2)\right)$, and the proof of Theorem 2 is now completed by applying Proposition 5.■

4 Latest developments

Since this paper was submitted, the author was able to generalize the main result of this paper to the case of the *functional onto* version of the pigeonhole principle obtained from $FPHP_n^m$ by adding the axioms $Q_j \stackrel{\mathrm{def}}{=} \bigvee_{i=1}^m x_{ij}$ $(j \in [n])$ [17]. This result is actually a direct corollary of a much more general bound on the resolution proof complexity of the perfect matching principle in an arbitrary hypergraph, also proved in [17].

5 Open problems

Can the methods developed in [16] and in this paper be applied to the tautologies $\tau(A, \vec{g}), \tau_{\oplus}(A, b)$ introduced in [1] that express the hardness of the Nisan-Wigderson generator in the context of propositional proof complexity?

The best known upper bound on $S_R(\neg FPHP_n^m)$ is $\exp(O(n\log n)^{1/2})$ [6], and we have shown the lower bound $S_R(\neg FPHP_n^m) \geq \exp(\Omega(n^{1/3}))$. That would be interesting to further narrow this gap. Specifically, what is the value of $\limsup_{n\to\infty} \frac{\log_2\log_2 S_R(\neg FPHP_n^\infty)}{\log_2 n}$?

References

[1] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Pseudorandom generators in propositional complexity. In *Proceedings of the* 41*st IEEE FOCS*, pages 43–53, 2000.

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

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

[4] E. Ben-Sasson and A. Wigderson. Short proofs are narrow - resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

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

[6] S. Buss and T. Pitassi. Resolution and the weak pigeonhole principle. In *Proceedings of the CSL97, Lecture Notes in Computer Science,* 1414, pages 149–156, New York/Berlin, 1997. Springer-Verlag.

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

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

[9] 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*, pages 174–183, 1996.

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

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

[12] 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.

[13] T. Pitassi and R. Raz. Regular resolution lower bounds for the weak pigeonhole principle. In *Proceedings of the 33rd ACM Symposium on the Theory of Computing*, pages 347–355, 2001.

[14] R. Raz. Resolution lower bounds for the weak pigeonhole principle. Technical Report TR01-021, Electronic Colloquium on Computational Complexity, 2001.

[15] 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 23rd ICALP, Lecture Notes in Computer Science,* 1099, pages 48–62, New York/Berlin, 1996. Springer-Verlag.

[16] A. Razborov. Improved resolution lower bounds for the weak pigeonhole principle. Technical Report TR01-055, Electronic Colloquium on Computational Complexity, 2001. Available at ftp://ftp.eccc.uni-trier.de/pub/eccc/reports/2001/TR01-055/index.html.

[17] A. Razborov. Resolution lower bounds for perfect matching principles. Manuscript, available at http://www.mi.ras.ru/~razborov/matching.ps, 2001.

[18] 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.

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

[20] 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.

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