Lower Bounds for the Weak Pigeonhole Principle Beyond Resolution

Albert Atserias*, María Luisa Bonet**, and Juan Luis Esteban***

Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya, Barcelona
{atserias,bonet,esteban}@lsi.upc.es†

Abstract. We work with an extension of Resolution, called Res(2), that allows clauses with conjunctions of two literals. In this system there are rules to introduce and eliminate such conjunctions. We prove that the weak pigeonhole principle PHP_n^{cn} and random unsatisfiable CNF formulas require exponential-size proofs in this system. This is the strongest system beyond Resolution for which such lower bounds are known. As a consequence to the result about the weak pigeonhole principle, Res(log) is exponentially more powerful than Res(2). Also we prove that Resolution cannot polynomially simulate Res(2), and that Res(2) does not have feasible monotone interpolation solving an open problem posed by Krajíček.

1 Introduction

The pigeonhole principle, PHP_n^{n+1}, expresses that it is not possible to have a one-to-one mapping from $n+1$ pigeons to n holes. This simple principle is central to many mathematical arguments. Since it can be formalized in propositional logic, it is natural to ask in which propositional proof systems such a principle can be proved in polynomial-size, with respect to the size of the encoding.

A fair amount of information is known about sizes of proofs of PHP_n^{n+1} in various proof systems. Haken [12] proved that this principle requires exponential-size proofs in Resolution. His proof techniques were later extended and simplified [4, 5]. Also Beame et al. [2] proved that PHP_n^{n+1} requires exponential-size proofs in bounded-depth Frege systems. Regarding upper bounds, Buss [8] gave polynomial-size proofs of PHP_n^{n+1} in unrestricted Frege systems.

The pigeonhole principle can be formulated in more general terms, allowing the number of pigeons to be greater than $n+1$. We call this principle weak pigeonhole principle, or PHP_n^m, when the number of pigeons m is at least $2n$. The proof techniques of Haken where extended in [9] to prove that $\mathrm{PHP}_n^{n^{2-\epsilon}}$ requires exponential-size proofs in Resolution. A very intriguing and often studied

* Supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532.
** Partially supported by MEC through grant PB98-0937-C04 (FRESCO project) and CICYT TIC 98-0410-C02-01.
*** Partially supported by MEC through grant PB98-0937-C04 (FRESCO project)
† Partially supported by ALCOM-FT, IST-99-14186.

open problem is to prove exponential-size lower bounds for Resolution proofs of $\mathrm{PHP}_n^{n^c}$, if that can be done at all. As a contrast, the techniques of [2] for proving lower bounds for the pigeonhole principle in bounded-depth Frege systems can only prove lower bounds for PHP_n^{n+c}, and it is again open whether lower bounds can be proved when the number of pigeons in greater than $n+c$. Regarding upper bounds, it is known that PHP_n^{2n} has quasipolynomial-size proofs in bounded-depth Frege [15, 14].

We work with the proof system Res(2), proposed by Krajíček [13], that can be viewed either as an extension of Resolution, or as a restriction of bounded-depth Frege. In this system the clauses do not only contain literals, but can also have conjunctions of two literals. The resolution rule gets modified to be able to eliminate a conjunction of two literals from a clause. We prove that PHP_n^{cn} requires exponential-size proofs in Res(2). This is, to our knowledge, the first lower bound proof for the weak pigeonhole principle in a subsystem of bounded-depth Frege that extends Resolution. We note that the quasipolynomial upper bound for bounded-depth Frege mentioned above can be carried over in depth-0.5 LK [14], which is equivalent to Res(log) (the analogue of Res(2) when we allow conjunctions of up to polylog literals). As a consequence of our lower bound, there is an exponential separation between Res(2) and Res(log).

Combining our techniques with those of [3], we also obtain an exponential-size lower bound for Res(2)-refutations of random unsatisfiable k-CNF formulas with clause density near the threshold. Again, this is the strongest system beyond Resolution for which such a lower bound is known. This result may be considered as a first step towards proving them hard for bounded-depth Frege.

Another important question to ask is whether Res(2) is more powerful than Resolution. Here we prove that Resolution cannot polynomially simulate Res(2), and therefore Res(2) is superpolynomially more efficient than Resolution. As a corollary, we see that Res(2) does not have the feasible monotone interpolation property, solving this way a conjecture of Krajíček [13].

Another motivation for working with the system Res(2) is to see how useful it can be in automated theorem proving. Given that it is more efficient than Resolution (at least there is a superpolynomial separation), it might be a good idea to try to find good heuristics to find proofs in Res(2) to be able to use it as a theorem prover.

2 Definitions and Overview of the Lower Bound Proof

A *k-term* is a conjunction of up to k literals. A *k-disjunction* is an (unbounded fan-in) disjunction of k-terms. If F is a k-disjunction, a 1-term of F is also called a *free-literal.* The refutation system Res(k), defined by Krajíček [13], works with k-disjunctions. There are three inference rules in Res(k): Weakening, $\wedge$-Introduction, and Cut

$$\frac{A}{A \vee \bigwedge_{i\in I} l_i} \qquad \frac{A \vee \bigwedge_{i\in I} l_i \quad B \vee \bigwedge_{i\in J} l_i}{A \vee B \vee \bigwedge_{i\in I\cup J} l_i} \qquad \frac{A \vee \bigwedge_{i\in I} l_i \quad B \vee \bigvee_{i\in I} \bar{l}_i}{A \vee B}$$

where A and B are k-disjunctions, I, J are sets of indices such that $|I \cup J| \leq k$, and the l_i's are literals. As usual, if l is a literal, $\bar{l}$ denotes its negation. Observe that Res(1) coincides with Resolution with the Weakening rule. The size of a Res(k)-refutation is the number of symbols in it. Mainly, we will work with Res(2).

Let $G = (U \cup V, E)$ be a bipartite graph on the sets U and V of cardinality m and n respectively, where $m > n$. The G-PHP^m_n, defined by Ben-Sasson and Wigderson [5], states that there is no matching of U into V. For every edge $(u, v) \in E$, let $x_{u,v}$ be a propositional variable meaning that u is mapped to v. The principle is then formalized as the conjunction of the following set of clauses:

$$x_{u,v_1} \vee \cdots \vee x_{u,v_r} \qquad u \in U,\ N_G(u) = \{v_1, \ldots, v_r\} \tag{1}$$
$$\bar{x}_{u,v} \vee \bar{x}_{u',v} \qquad v \in V,\ u, u' \in N_G(v),\ u \neq u'. \tag{2}$$

Here, $N_G(w)$ denotes the set of neighbors of w in G. Observe that if G is the complete bipartite graph K^m_n, then G-PHP^m_n coincides with the usual pigeonhole principle PHP^m_n. It is easy to see that a lower bound for the size of Res(2)-refutations of G-PHP^m_n implies the same lower bound for the size of Res(2)-refutations of PHP^m_n.

Ben-Sasson and Wigderson proved that whenever G is expanding in a sense defined next, every Resolution refutation of G-PHP^m_n must contain a clause with many literals. We observe that this result is not unique to Resolution and holds in a more general setting. Before we state the precise result, let us recall the definition of expansion:

Definition 1. [5] *Let $G = (U \cup V, E)$ be a bipartite graph where $|U| = m$, and $|V| = n$. For $U' \subset U$, the* boundary *of U, denoted by $\partial U'$, is the set of vertices in V that have exactly one neighbor in U'; that is, $\partial U' = \{v \in V : |N(v) \cap U'| = 1\}$. We say that G is (m, n, r, f)-*expanding *if every subset $U' \subseteq U$ of size at most r is such that $|\partial U'| \geq f \cdot |U'|$.*

The proof of the following statement is the same as in [5] for Resolution.

Theorem 1. [5] *Let $\mathcal{S}$ be a sound refutation system with all rules having fan-in at most two. Then, if G is (m, n, r, f)-expanding, every $\mathcal{S}$-refutation of G-PHP^m_n must contain a formula that involves at least $rf/2$ distinct literals.*

With these definitions, we are ready to outline the argument of the lower bound proof. In section 3, we will prove the existence of a bipartite graph $G = (U \cup V, E)$ with $|U| = cn'$ and $|V| = n'$ such that if we remove a small random subset of nodes from V, and the corresponding edges, the resulting graph is (m, n, r, f)-expanding for certain m, n, r and f. Then we will argue that G-$\mathrm{PHP}^{cn'}_{n'}$ requires exponential-size Res(2)-refutations as follows. Assume, for contradiction, that Π is a small refutation of G-$\mathrm{PHP}^{cn'}_{n'}$. We say that a 2-disjunction in Π is large if it contains at least $d = rf/2$ distinct literals. We apply a random restriction ρ_1 to the refutation such that for every large C, either $C|_{\rho_1}$ contains many free literals, or the total number of literals in $C|_{\rho_1}$ is less than d. Then we extend ρ_1

to a new random restriction $\rho \supseteq \rho_1$ that knocks out all those large C such that $C|_{\rho_1}$ contains many free literals, ignoring those that are not free. After applying ρ, we obtain a refutation of $G(\rho)$-PHP_n^m where all 2-disjunctions have less than $rf/2$ literals and $G(\rho)$ is (m,n,r,f)-expanding. This contradicts Theorem 1.

3 Random Graphs and Restrictions

In this section we will prove the existence of a bipartite graph G as claimed in Section 2. The principle G-PHP_n^m will require exponential size Res(2)-proofs.

Let $\mathcal{G}(m,n,p)$ denote the distribution on bipartite graphs on sets U and V of sizes m and n respectively, with edge probability p independently for each edge.

Lemma 1. *If G is drawn from $\mathcal{G}(m,n,p)$, then* $\Pr[\forall v \in V : mp/2 < \deg_G(v) < 2mp] \geq 1 - 2ne^{-\frac{mp}{8}}$.

Proof: Fix a vertex $v \in V$. Then, $\deg_G(v) \sim \mathrm{Bin}(m,p)$, so that $\mathrm{E}[\deg_G(v)] = mp$. By Chernoff bounds, $\Pr[\deg_G(v) \geq 2mp] \leq e^{-mp/3}$ and $\Pr[\deg_G(v) \leq mp/2] \leq e^{-mp/8}$. By a union bound, $\Pr[\exists v \in V : \deg_G(v) \leq mp/2 \vee \deg_G(v) \geq 2mp] \leq ne^{-mp/3} + ne^{-mp/8} \leq 2ne^{-mp/8}$, and so $\Pr[\forall v \in V : mp/2 < \deg_G(v) < 2mp] \geq 1 - 2ne^{-mp/8}$. □ (lemma 1)

Lemma 2. *Let $m = kn$, $p = 48k\ln(m)/m$, $\alpha = 1/mp$ and $f = np/6$. Let G be drawn from $\mathcal{G}(m,n,p)$. Then, $\Pr[G$ is $(m,n,\alpha m,f)$-expanding$] \geq 1/2$.*

Proof: Fix $U' \subseteq U$ of size $s \leq \alpha m$, and $v \in V$. Then, $\Pr[v \in \partial U'] = sp(1-p)^{s-1}$. Let $q = \Pr[v \in \partial U']$. Let X_v be the indicator random variable for the event that $v \in \partial U'$. Then, $|\partial U'| = \sum_{v \in V} X_v$. Observe that X_v and $X_{v'}$ are independent whenever $v \neq v'$. Hence, $|\partial U'| \sim \mathrm{Bin}(n,q)$, so that $E[|\partial U'|] = nq$. By Chernoff bound, $\Pr[|\partial U'| \leq nq/2] \leq e^{-nq/8}$. On the other hand, $nq = nsp(1-p)^{s-1} \geq snp(1-p)^{\alpha m}$. Moreover, $(1-p)^{\alpha m} = (1-p)^{1/p}$ approaches $1/e$ for sufficiently large m. Therefore, $nq \geq snp/3$. It follows that $nq/2 \geq sf$ and $e^{-nq/8} \leq e^{-snp/24}$. We conclude that $\Pr[|\partial U'| < f \cdot |U'|] \leq \Pr[|\partial U'| \leq nq/2] \leq e^{-nq/8} \leq e^{-snp/24}$. Finally, we bound the probability that G is not $(m,n,\alpha m,f)$-expanding by

$$\sum_{s=1}^{\alpha m} \binom{m}{s} e^{-snp/24} \leq \sum_{s=1}^{\alpha m} m^s e^{-snp/24} \leq \sum_{s=1}^{\alpha m} (me^{-np/24})^s. \tag{3}$$

Recall that $p = 48k\ln(m)/m$ and $m = kn$. So $me^{-np/24} \leq me^{-2\ln(m)} = m^{-1} < 1/4$. Hence the sum in (3) is bounded by $\sum_{s=1}^{\infty} \frac{1}{4^s} \leq \frac{1}{2}$. □ (lemma 2)

Let G be a fixed bipartite graph on $\{1,\dots,m\}$ and $\{1,\dots,n\}$. A *restriction* (for G) is a sequence of pairs $\rho = ((u_1,v_1),\dots,(u_r,v_r))$ such that $(u_i,v_i) \in E(G)$, and all v_i's are distinct. We let $R_r(G)$ be the set of restrictions of length r. We define a distribution $\mathcal{R}_r(G)$ on $R_r(G)$ as follows: Let $V_0 = \{1,\dots,n\}$; for every $i \in \{1,\dots,r\}$ in increasing order, choose a hole v_i uniformly at random in

V_{i-1}, choose a pigeon u_i uniformly at random in $N_G(v_i)$, and let $V_i = V_{i-1} - \{v_i\}$. The final restriction is $((u_1, v_1), \ldots, (u_r, v_r))$.

We define a distribution $\mathcal{D}(m, n, p, r)$ on the set of pairs (G, ρ) with $\rho \in R_r(G)$: the graph G is drawn from $\mathcal{G}(m, n + r, p)$ first, and then ρ is drawn from $\mathcal{R}_r(G)$. In other words, if (H, π) is a fixed pair with $\pi \in R_r(H)$, then $\Pr[G = H \wedge \rho = \pi] = p^{e(H)}(1-p)^{m(n+r)-e(H)}|R_r(H)|^{-1}$.

If G is a bipartite graph on $\{1, \ldots, m\}$ and $\{1, \ldots, n+r\}$, and ρ a restriction $((u_1, v_1), \ldots, (u_r, v_r)) \in R_r(G)$, then $G(\rho)$ denotes the graph that results from deleting $v_1, \ldots, v_r$ from G, and renaming nodes in an order-preserving way. With this definitions we are ready to prove:

Lemma 3. *Let $m = kn$, $p = 48k\ln(m)/m$, $\alpha = 1/mp$ and $f = np/6$. Let (G, ρ) be drawn from $\mathcal{D}(m, n, p, r)$. Then, $\Pr[G(\rho)$ is $(m, n, \alpha m, f)$-expanding$] \geq 1/2$.*

Proof: Let A be the event that $G(\rho)$ is $(m, n, \alpha m, f)$-expanding. Let $S = \{R \subseteq \{1, \ldots, n + r\} : |R| = r\}$. Then, $\Pr[A] = \sum_{R \in S} \Pr[A \mid \mathrm{ran}(\rho) = R] \Pr[\mathrm{ran}(\rho) = R]$. The proof that $\Pr[A \mid \mathrm{ran}(\rho) = R] \geq 1/2$ is the same as the proof of Lemma 2 replacing V by $V - R$. The result follows. $\Box$ (lemma 3)

Lemma 4. *Let $m = kn$, $p = 48k\ln(m)/m$, $\alpha = 1/mp$ and $f = np/6$. For every $r \leq n$, there exists a bipartite graph H on $\{1, \ldots, m\}$ and $\{1, \ldots, n + r\}$ such that the following two properties hold:*

(i) $mp/2 \leq \deg_H(v) \leq 2mp$ *for every* $v \in \{1, \ldots, n + r\}$,
(ii) $\Pr[H(\rho)$ *is* $(m, n, \alpha m, f)$*-expanding*$] \geq 1/3$,

when ρ is drawn from $\mathcal{R}_r(H)$.

Proof: Let (G, ρ) be drawn from $\mathcal{D}(m, n, p, r)$. According to Lemmas 3, we have We have that $\Pr[G(\rho)$ is $(m, n, \alpha m, f)$-expanding$] \geq 1/2$. Moreover, $\Pr[\forall v \in V : mp/2 < \deg_G(v) < 2mp] \geq 1 - (n+r)e^{-mp/9} \geq 5/6$ by Lemma 1. Let $E(G, \rho)$ be the event that $G(\rho)$ is expanding *and* every right-node in G has degree between $mp/2$ and $2mp$. Combining both equations above we have that $\Pr[E(G, \rho)] \geq 1/3$. On the other hand, $\Pr[E(G, \rho)] = \sum_H \Pr[E(G, \rho) \mid G = H] \Pr[G = H]$ where H ranges over all bipartite graphs on m and $n + r$ nodes. Therefore, there exists some fixed H such that $\Pr[E(G, \rho) \mid G = H] \geq 1/3$. Moreover, $\Pr[E(G, \rho) \mid G = H]$ equals $\Pr[E(H, \pi)]$ when π is drawn from $\mathcal{R}_r(H)$. Finally, since this probability is strictly positive, it must be the case that H satisfies property (i) in the lemma since it is independent of π. $\Box$ (lemma 4)

4 The lower bound argument

Before we start the lower bound proof, we need a normal form for Res(2)-refutations of G-PHP^m_n. We claim that every Res(2)-refutation of G-PHP^m_n can be turned into a Res(2)-refutation of similar size in which no 2-term is of the form $x_{u,v} \wedge x_{u',v}$ with $u \neq u'$. To check this, observe that such a 2-term must have been introduced at some point by the rule of $\wedge$-introduction with clauses, say, $A \vee x_{u,v}$ and $B \vee x_{u',v}$. Cutting them with the axiom $\bar{x}_{u,v} \vee \bar{x}_{u',v}$ we get $A \vee B$ that can be used to continue the proof because it subsumes $A \vee B \vee (x_{u,v} \wedge x_{u',v})$.

Theorem 2. *Let $c > 1$ be a constant. For all sufficiently large n, every* Res(2)*-refutation of* PHP_n^{cn} *has size at least* $e^{n/(\log n)^{14}}$.

Proof: Let $k = c+1$, $r = n/c$, $n' = n+r$, and $m = kn = cn'$. Let $G = (U \cup V, E)$ with $|U| = m$ and $|V| = n+r$ be the bipartite graph of Lemma 4. We show that every Res(2)-refutation of G-PHP has size at least $e^{n/(\log n)^{14}}$. This will imply the Theorem since a Res(2)-refutation of $\mathrm{PHP}_{n'}^{cn'}$ gives a Res(2)-refutation of G-PHP of no bigger size.

Let us assume, for contradiction, that G-PHP has a Res(2)-refutation Π of size $S < e^{n/(\log n)^{14}}$. Let C be a 2-disjunction, and let $(u, v) \in E(G)$. We let $C|_{(u,v)}$ be the result of assigning $x_{u,v} = 1$ and $x_{u',v} = 0$ for every $u' \in N_G(v) - \{u\}$ to C, and simplifying as much as possible. This includes replacing subformulas of the form $l \vee (l \wedge l')$ by l, and subformulas of the form $\bar{l} \vee (l \wedge l')$ by $\bar{l} \vee l'$ in some specified order; here l and l' are literals. Given a restriction $\rho = ((u_1, v_1), \ldots, (u_r, v_r))$, we let $C|_\rho$ be the result of applying $(u_1, v_1), \ldots, (u_r, v_r)$ successively in this order. For every $i \in \{1, \ldots, r\}$, we let $\rho_i = ((u_1, v_1), \ldots, (u_i, v_i))$. We say that C is *large* if it contains at least $d = n/12$ distinct literals; otherwise, C is *small*. We say that C is *wide* if it contains at least $s = n/(\log n)^5$ free literals; otherwise, C is *narrow*. We say that a pair $(u, v) \in E(G)$ *hits* C if either $x_{u,v}$ occurs positively in C, or $x_{u',v}$ occurs negatively in C for some $u' \in N_G(v) - \{u\}$. Equivalently, (u, v) hits C if it sets some literal of C to 1. If the literal is free, it knocks out the 2-disjunction. If the literal is part of a conjunction, it will locally create a free literal. In general, we say that $(u, v) \in E(G)$ *knocks* C if $C|_{(u,v)} \equiv 1$. We say that $(u, v) \in E(G)$ is a *bad pair* for C if it does not knock it and there exists $u' \in N_G(v) - \{u\}$ such that (u', v) knocks C. A bad pair may or may not be a hit.

In all probabilities that follow, ρ is drawn from the distribution $\mathcal{R}_r(G)$. Our main goal is to prove that the probability that a fixed 2-disjunction C of Π remains large is exponentially small; that is, we aim for a proof that

$$\Pr[C|_\rho \text{ is large}] \leq e^{-n/(\log n)^{13}}. \tag{4}$$

This will suffice because then $\Pr[\exists C \in \Pi : C|_\rho \text{ is large}] \leq S e^{-n/(\log n)^{13}} < e^{n/(\log n)^{14}} e^{-n/(\log n)^{13}} < 1/3$, and also $\Pr[G(\rho) \text{ not } (m, n, \alpha m, f)\text{-expanding}] \leq 2/3$ by Lemma 4. This means that there exists a restriction $\rho \in R_r(G)$ such that $G(\rho)$ is $(m, n, \alpha m, f)$-expanding and every 2-disjunction in $\Pi|_\rho$ has less than $d = \alpha m f/2$ literals. This is a contradiction with Theorem 1.

For $i \in \{1, \ldots, r\}$, let A_i be the event that $C|_{\rho_i}$ is large, and let B_i be the event that $C|_{\rho_i}$ is narrow. Recall that $\rho_i = ((u_1, v_1), \ldots, (u_i, v_i))$. Then,

$$\begin{aligned}
\Pr[C|_\rho \text{ is large}] &\leq \Pr\left[A_r \wedge \bigvee_{j \geq r/2} B_j\right] + \Pr\left[A_r \wedge \bigwedge_{j \geq r/2} \overline{B_j}\right] \leq \\
&\leq \sum_{j=r/2}^{r} \Pr[A_j \wedge B_j] + \Pr\left[A_r \wedge \bigwedge_{j \geq r/2} \overline{B_j}\right].
\end{aligned}$$

We will show that every term in this expression is exponentially small. The bound on terms of the form $\Pr[A_j \wedge B_j]$ will be proven in Lemma 6. For the last term, we use an argument similar in spirit to the one by Beame and Pitassi [4]:

Lemma 5. $\Pr\left[A_r \wedge \bigwedge_{j\geq r/2} \overline{B_j}\right] \leq e^{-n/(\log n)^8}$.

Proof: Let S_i be the indicator random variable for the event that (u_i, v_i) knocks $C|_{\rho_{i-1}}$. Then,

$$\begin{aligned}
\Pr\left[A_r \wedge \bigwedge_{j\geq r/2} \overline{B_j}\right] &\leq \Pr\left[\bigwedge_{i>r/2} S_i = 0 \wedge \bigwedge_{j\geq r/2} \overline{B_j}\right] = \\
&= \prod_{i>r/2} \Pr\left[S_i = 0 \wedge \bigwedge_{j\geq r/2} \overline{B_j} \;\middle|\; \bigwedge_{r/2<j<i} S_j = 0\right] \leq \\
&\leq \prod_{i>r/2} \Pr\left[S_i = 0 \wedge \overline{B_{i-1}} \;\middle|\; \bigwedge_{r/2<j<i} S_j = 0\right] \leq \\
&\leq \prod_{i>r/2} \Pr\left[S_i = 0 \;\middle|\; \overline{B_{i-1}} \wedge \bigwedge_{r/2<j<i} S_j = 0\right].
\end{aligned}$$

Fix $i \in \{r/2+1, \ldots, r\}$ and let H be the set of holes that occur in a free literal of $C|_{\rho_{i-1}}$. Given that $\overline{B_{i-1}}$ holds, $C|_{\rho_{i-1}}$ is wide which means that there are at least s free literals. Therefore $|H| \geq s/2\Delta$, where $\Delta = 2mp$ is an upper bound on the right-degree of G. Moreover, every $v \in H$ gives a possible knock, and different holes give different knocks. The reason is the following: if $x_{u,v}$ is a free literal, then (u, v) is a knock; and if $\bar{x}_{u,v}$ is a free literal, then (u', v) is a knock for every $u' \in N_G(v) - \{u\}$, which is non-empty since the right-degree of G is at least two. Therefore,

$$\Pr\left[S_i = 1 \;\middle|\; \overline{B_{i-1}} \wedge \bigwedge_{r/2<j<i} S_j = 0\right] \geq \frac{|H|}{\Delta(n+r-i+1)} \geq \frac{s}{3\Delta^2 n}.$$

Therefore,

$$\Pr\left[A_r \wedge \bigwedge_{j\geq r/2} \overline{B_j}\right] \leq \left(1 - \frac{s}{3\Delta^2 n}\right)^{r/2} \leq e^{-\frac{sr}{6\Delta^2 n}} \leq e^{-n/(\log n)^8}. \quad \square \text{ (lemma 5)}$$

Lemma 6. *Let j be such that $r/2 \leq j \leq r$. Then,* $\Pr[A_j \wedge B_j] \leq e^{-n/(\log n)^{11}}$.

Proof: Recall that A_j is the event that $C|_{\rho_j}$ is large, and B_j is the event that $C|_{\rho_j}$ is narrow. We let S_i be the indicator random variable for the event that (u_i, v_i) hits $C|_{\rho_{i-1}}$, where $\rho_{i-1} = ((u_1, v_1), \ldots, (u_{i-1}, v_{i-1}))$. Let $S = \sum_{i=1}^{j} S_i$.

Then, for every h,

$$\Pr[A_j \wedge B_j] = \Pr[A_j \wedge B_j \wedge S < h] + \Pr[A_j \wedge B_j \wedge S \geq h] \leq$$
$$\leq \Pr[A_j \wedge S < h] + \Pr[A_j \wedge B_j \wedge S \geq h].$$

We show that each term in this expression is exponentially small. More precisely, we show that $\Pr[A_j \wedge S < h] \leq e^{-n/(\log n)^3}$ and $\Pr[A_j \wedge B_j \wedge S \geq h] \leq e^{-n/(\log n)^{10}}$ which is clearly enough to prove Lemma 6.

Claim 1 *Let $h = n/(\log n)^4$. Then,* $\Pr[A_j \wedge S < h] \leq e^{-n/(\log n)^3}$.

Proof: Let $Y = \{(a_1, \ldots, a_j) \in \{0,1\}^j : \sum_{i=1}^{j} a_i < h\}$. Observe that A_j implies A_i for every $i \leq j$ because if $C|_{\rho_j}$ is large, so is $C|_{\rho_i}$ for every $i \leq j$. Then,

$$\Pr[A_j \wedge S < h] = \Pr\left[\sum_{i=1}^{j} S_i < h \wedge A_j\right] = \sum_{\overline{a} \in Y} \Pr\left[\bigwedge_{i=1}^{j} S_i = a_i \wedge A_j\right] =$$
$$= \sum_{\overline{a} \in Y} \prod_{i=1}^{j} \Pr\left[S_i = a_i \wedge A_j \;\middle|\; \bigwedge_{k=1}^{i-1} S_k = a_k\right] \leq$$
$$\leq \sum_{\overline{a} \in Y} \prod_{i=1}^{j} \Pr\left[S_i = a_i \wedge A_{i-1} \;\middle|\; \bigwedge_{k=1}^{i-1} S_k = a_k\right] \leq$$
$$\leq \sum_{\overline{a} \in Y} \prod_{i=1}^{j} \Pr\left[S_i = a_i \;\middle|\; A_{i-1} \wedge \bigwedge_{k=1}^{i-1} S_k = a_k\right].$$

Fix $i \in \{1, \ldots, j\}$. Let H be the set of holes that occur in $C|_{\rho_{i-1}}$. We have $|H| \geq d/2\Delta$ given that A_{i-1} holds. Again, $\Delta = 2mp$ is an upper bound to the right-degree of G. Moreover, every $v \in H$ gives a possible hit, and different holes give different hits (the reason is the same as in Lemma 5 for knocks). Therefore,

$$\Pr\left[S_i = 1 \;\middle|\; A_{i-1} \wedge \bigwedge_{k=1}^{i-1} S_k = a_k\right] \geq \frac{|H|}{\Delta(n + r - i + 1)} \geq \frac{d}{3\Delta^2 n}.$$

Since there are at least $j - h$ zeros in $(a_1, \ldots, a_j)$, we obtain

$$\Pr[A_j \wedge S < h] \leq \sum_{\overline{a} \in Y} \left(1 - \frac{d}{3\Delta^2 n}\right)^{j-h} \leq \sum_{i<h} \binom{j}{i} e^{-\frac{d(j-h)}{3\Delta^2 n}} \leq h j^h e^{-\frac{d(j-h)}{3\Delta^2 n}} \leq$$
$$\leq \exp\left(-\frac{j-h}{36\Delta^2} + h\log(j) + \log(h)\right) \leq e^{-n/(\log n)^3}. \square \text{(claim 1)}$$

Claim 2 $\Pr[A_j \wedge B_j \wedge S \geq h] \leq e^{-n/(\log n)^{10}}$.

Proof: During this proof we will drop the subindex j in A_j and B_j since it will always be the same. For every $i \in \{1, \ldots, r\}$, let $T_i \in \{\mathrm{k}, \mathrm{b}, \mathrm{n}\}$ be a random variable indicating whether (u_i, v_i) is a knock, a bad pair, or none of the previous respectively for $C|_{\rho_{i-1}}$. For $t \in \{\mathrm{k}, \mathrm{b}, \mathrm{n}\}$, let S_i^t be the indicator random variable for the event that $T_i = t$, and let $S^t = \sum_{i=1}^{j} S_i^t$. Thus, S^{k} is the number of knocks and S^{b} is the number of bad pairs of ρ_j.

Fix $\rho = ((u_1, v_1), \ldots, (u_r, v_r))$ such that $A \wedge B \wedge S \geq h$ holds under ρ. Observe that (u_i, v_i) does not knock $C|_{\rho_{i-1}}$ for any $i \in \{1, \ldots, j\}$ since $C|_{\rho_j}$ must be large. Hence, $S^{\mathrm{k}} = 0$ under ρ. Let $b = (h - s)/(2\Delta + 1)$. We now claim that $S^{\mathrm{b}} \geq b$. Suppose for contradiction that the number of bad pairs is less than b. Every bad pair (u_i, v_i) removes at most 2Δ free literals since at most those many literals about hole v_i may appear. Moreover, since there are no knocks, every hit (u_i, v_i) that is not a bad pair increases the number of free literals by at least one. The reason is that such a hit turns a conjunction into a free literal whose hole component must be different from v_i for otherwise a knock would be available; recall that the right-degree of G is at least three, and that conjunctions of the form $x_{u,v} \wedge x_{u',v}$ with $u \neq u'$ do not occur in the refutation. It follows that the number of free literals in $C|_{\rho_j}$ is at least $(S - S^{\mathrm{b}}) - 2\Delta S^{\mathrm{b}} > h - (2\Delta + 1)b = s$, a contradiction with the fact that B holds under ρ. We have proved that $\Pr[A \wedge B \wedge S \geq h] \leq \Pr[S^{\mathrm{k}} = 0 \wedge S^{\mathrm{b}} \geq b]$. The intuition behind why this probability is small is that every bad pair could have been a knock. This makes unlikely that ρ produces many bad pairs and no knocks. In what follows, we will prove this intuition using martingales.

For $t \in \{\mathrm{k}, \mathrm{b}, \mathrm{n}\}$ and $i \in \{1, \ldots, j\}$, let P_i^t denote the random variable $\Pr[T_i = t \mid \rho_0, \ldots, \rho_{i-1}]$. We define a martingale $X_0, \ldots, X_j$ with respect to $\rho_0, \ldots, \rho_j$ as follows: Let $X_0 = 0$, and $X_{i+1} = X_i + S_{i+1}^{\mathrm{b}} - P_{i+1}^{\mathrm{b}}$. Recall that S_{i+1}^{b} is the indicator random variable for the event that $T_{i+1} = \mathrm{b}$. So

$$\begin{aligned} \mathrm{E}[X_{i+1} \mid \rho_0, \ldots, \rho_i] &= (X_i + 1 - P_{i+1}^{\mathrm{b}}) \cdot P_{i+1}^{\mathrm{b}} + (X_i - P_{i+1}^{\mathrm{b}}) \cdot (1 - P_{i+1}^{\mathrm{b}}) = \\ &= (X_i - P_{i+1}^{\mathrm{b}})(P_{i+1}^{\mathrm{b}} + 1 - P_{i+1}^{\mathrm{b}}) + P_{i+1}^{\mathrm{b}} = X_i. \end{aligned}$$

Hence, $\{X_i\}_i$ is a martingale with respect to $\{\rho_i\}_i$. Observe also that $X_j = S^{\mathrm{b}} - \sum_{i=1}^{j} P_i^{\mathrm{b}}$. Similarly, we define $Y_0, \ldots, Y_j$ as follows: Let $Y_0 = 0$, and $Y_{i+1} = Y_i + S_{i+1}^{\mathrm{k}} - P_{i+1}^{\mathrm{k}}$. It is also easy to see that $\{Y_i\}_i$ is a martingale with respect to $\{\rho_i\}_i$. Again, $Y_j = S^{\mathrm{k}} - \sum_{i=1}^{j} P_i^{\mathrm{k}}$.

Subclaim 1 *$P_i^{\mathrm{k}}(\rho) \geq P_i^{\mathrm{b}}(\rho)/\Delta$ for every $\rho \in R_r(G)$ and $i \in \{1, \ldots, j\}$.*

Proof: Fix $i \in \{1, \ldots, j\}$ and $\rho = ((u_1, v_1), \ldots, (u_r, v_r))$. We want to show that $P_i^{\mathrm{k}}(\rho) \geq P_i^{\mathrm{b}}(\rho)/\Delta$. Define three sets as follows: $Q = \{(u, v) \in E(G) : v \notin \{v_1, \ldots, v_{i-1}\}\}$, $Q^{\mathrm{k}} = \{(u, v) \in Q : (u, v)$ is a knock for $C|_{\rho_{i-1}}\}$, and $Q^{\mathrm{b}} = \{(u, v) \in Q : (u, v)$ is a bad pair for $C|_{\rho_{i-1}}\}$. Observe that $P_i^{\mathrm{b}}(\rho) = |Q^{\mathrm{b}}| \cdot |Q|^{-1}$ and $P_i^{\mathrm{k}}(\rho) = |Q^{\mathrm{k}}| \cdot |Q|^{-1}$. On the other hand, every bad pair $(u, v) \in Q^{\mathrm{b}}$ gives a possible knock $(u', v) \in Q^{\mathrm{k}}$ by definition. Moreover, bad pairs with different hole components give different possible knocks. Grouping Q^{b} by holes, we have that $|Q^{\mathrm{k}}| \geq |Q^{\mathrm{b}}|/\Delta$. Consequently, $P_i^{\mathrm{k}}(\rho) \geq P_i^{\mathrm{b}}(\rho)/\Delta$ as required. □ (subclaim 1)

To complete the proof of claim 2 we will need the following form of Azuma's Inequality: Let $X_0, \ldots, X_n$ be a martingale such that $|X_i - X_{i-1}| \leq 1$; then,

$\Pr[|X_n - X_0| \geq \lambda] \leq 2e^{-\lambda^2/n}$ for every $\lambda > 0$ [11]. Now,

$$\Pr[S^{\mathrm{k}} = 0 \wedge S^{\mathrm{b}} \geq b] = \Pr[S^{\mathrm{k}} = 0 \wedge S^{\mathrm{b}} \geq b \wedge X_j \geq b/2] + \\ + \Pr[S^{\mathrm{k}} = 0 \wedge S^{\mathrm{b}} \geq b \wedge X_j < b/2].$$

The first summand is bounded by $\Pr[X_j \geq b/2] \leq 2e^{-b^2/4j}$ by Azuma's Inequality. The second summand is bounded by

$$\Pr\left[S^{\mathrm{k}} = 0 \wedge \sum_{i=1}^{j} P_i^{\mathrm{b}} \geq b/2\right] \leq \Pr\left[S^{\mathrm{k}} = 0 \wedge \sum_{i=1}^{j} P_i^{\mathrm{k}} \geq b/2\Delta\right] \leq \\ \leq \Pr[Y_j \leq -b/2\Delta] \leq 2e^{-b^2/4\Delta^2 j}.$$

The first inequality follows from Subclaim 1, and the third follows from Azuma's Inequality again. The addition of the two summands is then bounded by $e^{-n/(\log n)^{10}}$ as required. $\square$ (claim 2 and lemma 6)

We are ready to complete the proof of our goal: equation (4). We have shown that

$$\Pr[C|_\rho \text{ large}] \leq \sum_{j=r/2}^{r} e^{-n/(\log n)^{11}} + e^{-n/(\log n)^{8}} \leq e^{-n/(\log n)^{13}}. \ \square \text{ (theorem 2)}$$

The most general form of the previous theorem gives a lower bound for PHP_n^m of $e^{\frac{n^9}{(m \log m)^8 \log^3 n}}$, using $r = n/8$, $h = n^3/((m \log m)^2 \log n)$ and $s = h/2$, therefore the best result is an exponential lower bound for $\mathrm{PHP}_n^{n^{9/8-\epsilon}}$.

Given that Res(log) and depth-0.5 LK are polynomially equivalent, and given that PHP_n^{2n} has quasipolynomial-size proofs in depth-0.5 LK [14], we obtain:

Corollary 1. *There is an exponential separation between* Res(2) *and* Res(log)*.*

The model of random k-CNF formulas that we use is the one considered in [10, 3]. The distribution is denoted $\mathcal{F}_m^{k,n}$ and consists in choosing m clauses of exactly k literals independently with replacement. The following result can be obtained by an argument similar to that of Theorem 2. The proof can be found in the complete version of the paper.

Theorem 3. *Let $F \sim \mathcal{F}_{5n}^{3,n}$. Almost surely,* Res(2)*-refutations of F require size* $2^{\Omega(n^{1/3}/(\log(n))^2)}$.

5 Separation between Res(2) and Resolution

In this section we prove that Resolution cannot polynomially simulate Res(2). More precisely, we prove that a certain Clique-Coclique principle, as defined by Bonet, Pitassi and Raz in [6], has polynomial-size Res(2)-refutations, but every Resolution refutation requires quasipolynomial size.

The Clique-Coclique principle that we use, $\mathrm{CLIQUE}^n_{k,k'}$, is:

$x_{i,1} \vee \cdots \vee x_{i,n}$	$1 \le l \le k$
$\bar{x}_{l,i} \vee \bar{x}_{l,j}$	$1 \le l \le k,\ 1 \le i,j \le n,\ i \ne j$
$\bar{x}_{l,i} \vee \bar{x}_{l',i}$	$1 \le l,l' \le k,\ 1 \le i \le n,\ l \ne l'$
$y_{1,i} \vee \cdots \vee y_{k',i}$	$1 \le i \le n$
$\bar{y}_{l,i} \vee \bar{y}_{l',i}$	$1 \le l,l' \le k',\ 1 \le i \le n,\ l \ne l'$
$\bar{x}_{l,i} \vee \bar{x}_{l',j} \vee \bar{y}_{t,i} \vee \bar{y}_{t,j}$	$1 \le l,l' \le k,\ 1 \le t \le k',\ 1 \le i,j \quad \le n,\ l \ne l',\ i \ne j$

Theorem 4. *Let $k' < k \le n$. If $\mathrm{PHP}^k_{k'}$ has Resolution refutations of size S, then $\mathrm{CLIQUE}^n_{k,k'}$ has $\mathrm{Res}(2)$-refutations of size Sn^c for some constant $c > 0$.*

The proof can be found in the complete version of the paper. We reduce the formula $\mathrm{CLIQUE}^n_{k,k'}$ to $\mathrm{PHP}^k_{k'}$ in $\mathrm{Res}(2)$. The meaning of variable $p_{i,j}$ is that pigeon i sits in hole j. We perform the following substitutions:

$$p_{i,j} \equiv \bigvee_{l=1}^{n} (x_{i,l} \wedge y_{i,l}) \qquad\qquad \bar{p}_{i,j} \equiv \bigvee_{l=1, j' \ne j}^{n} (x_{i,l} \wedge y_{j',l})$$

We will use the Monotone Interpolation Theorem for Resolution together with the following result of Alon and Boppana [1] establishing a lower bound to the size of monotone circuits that separate large cliques from small cocliques. In the following, $F(m,k,k')$ is the set of monotone functions that separate k-cliques from k'-cocliques on m nodes. Let $S^+(f)$ be the monotone circuit size of f.

Theorem 5. *If $f \in F(m,k,k')$, $3 \le k' \le k$ and $k\sqrt{k'} \le m/(8\log m)$, then*

$$S^+(f) \ge \frac{1}{8}\left(\frac{m}{4k\sqrt{k'}\log m}\right)^{(\sqrt{k'}+1)/2}.$$

Theorem 6. *Let $k = \sqrt{m}$ and $k' = (\log m)^2/8\log\log m$. Then, (i) $\mathrm{CLIQUE}^m_{k,k'}$ has $\mathrm{Res}(2)$-refutations of size polynomial in m, and (ii) every Resolution refutation of $\mathrm{CLIQUE}^m_{k,k'}$ has size at least $\exp(\Omega((\log m)^2/\sqrt{\log\log m}))$.*

Proof: Regarding (i), we have that $k'\log k' \le \frac{1}{4}(\log m)^2$, and so $2^{\sqrt{k'\log k'}} \le m^{1/2} = k$. On the other hand, Buss and Pitassi [7] proved that $\mathrm{PHP}^k_{k'}$ has Resolution refutations of size polynomial in k whenever $k \ge 2^{\sqrt{k'\log k'}}$. Therefore, by Theorem 4, $\mathrm{CLIQUE}^m_{k,k'}$ has $\mathrm{Res}(2)$-refutations of size polynomial in m. Regarding (ii), we apply the feasible monotone interpolation theorem for Resolution. We have $\log m/(3\sqrt{\log\log m}) \le \sqrt{k'} \le \log m$. Therefore, by Theorem 5, if $f \in F(m,k,k')$ is a monotone interpolant, then

$$S^+(f) \ge \frac{1}{8}\left(\frac{m}{4\sqrt{m}(\log m)^2}\right)^{\frac{\log m}{6\sqrt{\log\log m}}} \ge \frac{1}{8}\left(\frac{m}{m^{3/4}}\right)^{\frac{\log m}{6\sqrt{\log\log m}}},$$

which is $\exp(\Omega((\log m)^2/\sqrt{\log\log m}))$. $\square$ (theorem 6)

As a corollary, we solve an open problem posed by Krajíček [13].

Corollary 2. $\mathrm{Res}(2)$ *does not have the feasible monotone interpolation property.*

6 Discussion and Open Problems

We proved that there is a quasipolynomial separation between Resolution and Res(2). It is an open question whether the separation could be exponential, or a quasipolynomial simulation of Res(2) by Resolution exists. It is important to notice, that our lower bound for PHP would not follow from such a simulation. Indeed, the lower bound that would follow from that would be of the form $2^{n^{\epsilon}}$.

The previous separation was obtained using a lower bound for Resolution via the monotone interpolation theorem. It is open whether this separation (or a stronger one) could be obtained via the size-width trade-off [5]. It would also be interesting to see what would that mean in terms of possible size-width trade-offs for Res(2). We conjecture that Res(2) does not have a strong size-width trade-off. Notice that Res(log) does not have it. This is because (a) Res(log) is equivalent to depth-0.5 LK, (b) PHP_n^{2n} has quasipolynomial-size proofs in depth-0.5 LK [14], and (c) PHP_n^{2n} has $\Omega(n)$ width lower bounds for Res(log).

We extended the width lower bound technique beyond Resolution. A very interesting open question is whether the technique can be extended for Res(3), etc. This is related to the optimality of the Res(log) upper bound for PHP_n^{2n}.

References

1. N. Alon and R. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7(1):1–22, 1987.
2. P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for PHP. In *STOC92*, pages 200–220, 1992.
3. P. Beame, R. Karp, T. Pitassi, and M. Saks. The efficiency of resolution and Davis-Putnam procedures. Submitted. Previous version in STOC'98, 1999.
4. P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *FOCS96*, pages 274–282, 1996.
5. E. Ben-Sasson and A. Wigderson. Short proofs are narrow: Resolution made simple. In *STOC99*, pages 517–527, 1999. Revised version (2000).
6. M. Bonet, T. Pitassi, and R. Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):708–728, Sept. 1997.
7. S. Buss and T. Pitassi. Resolution and the weak pigeonhole principle. In *CSL: 11th Workshop on Computer Science Logic*. LNCS, Springer-Verlag, 1997.
8. S. R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *The Journal of Symbolic Logic*, 52(4):916–927, Dec. 1987.
9. S. R. Buss and G. Turán. Resolution proofs on generalized pigeonhole principles. *Theoretical Computer Science*, 62(3):311–317, Dec. 1988.
10. V. Chvátal and E. Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.
11. G. Grimmet and D. Stirzaker. *Probability and Random Processes*. Oxford, 1982.
12. A. Haken. The intractability of resolution. *TCS*, 39(2-3):297–308, Aug. 1985.
13. J. Krajíček. On the weak PHP. To appear in Fundamenta Mathematicæ, 2000.
14. A. Maciel, T. Pitassi, and A. Woods. A new proof of the weak pigeonhole principle. In *STOC00*, pages 368–377, 2000.
15. J. B. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *The Journal of Symbolic Logic*, 53(4):1235–1244, 1988.