A New Proof of the Weak Pigeonhole Principle

Alexis Maciel*
Clarkson University

Toniann Pitassi†
University of Toronto and University of Arizona

Alan R. Woods‡
University of Western Australia

April 30, 2001

Abstract

The exact complexity of the weak pigeonhole principle is an old and fundamental problem in proof complexity. Using a diagonalization argument, Paris, Wilkie and Woods [16] showed how to prove the weak pigeonhole principle with bounded-depth, quasipolynomial-size proofs. Their argument was further refined by Krajíček [9]. In this paper, we present a new proof: we show that the weak pigeonhole principle has quasipolynomial-size LK proofs where every formula consists of a single AND/OR of polylog fan-in. Our proof is conceptually simpler than previous arguments, and is optimal with respect to depth.

1 Introduction

The pigeonhole principle is a fundamental axiom of mathematics, stating that there is no one-to-one mapping from m pigeons to n holes when $m > n$. It expresses

*Department of Mathematics and Computer Science, Clarkson University, Potsdam, NY 13699-5815, U.S.A. alexis@clarkson.edu. Research supported by NSF grant CCR-9877150.

†Department of Computer Science, University of Toronto, Toronto, Ontario, Canada. toni@cs.toronto.edu. Research supported by NSF Grant CCR-9457782, US-Israel BSF Grant 95-00238, Grant INT-9600919/ME-103 from NSF and MŠMT (Czech Republic), and an NSERC grant.

‡Department of Mathematics and Statistics, University of Western Australia, Nedlands, WA 6907, Australia. woods@maths.uwa.edu.au

a very basic fact about cardinalities of sets and is used ubiquitously in almost all areas of mathematics. As examples, the induction principle is simply a special case of the pigeonhole principle, and many combinatorial counting arguments reduce to the pigeonhole principle.

Perhaps not surprisingly, then, the inherent difficulty of proving the pigeonhole principle is tightly connected to important questions in proof theory and circuit complexity. It has served as the classic hard example for proof complexity, and versions of it have been used to obtain some of the strongest lower bounds and separations known to date. Examples include Resolution, bounded-depth Frege systems, Cutting Planes, and relativized bounded arithmetic.

There are several important open problems connected to the complexity of the weaker forms of the pigeonhole principle, and in particular with the *weak pigeonhole principle* which we define to be the case in which $n \leq m/2$. First, as initially noticed by Macintyre [14] in the context of the existence of quadratic nonresidues, the weak pigeonhole principle is intimately connected to how much number theory can be proven in $I\Delta_0$, a weak system of arithmetic. Paris, Wilkie and Woods [16] show that a considerable part of elementary number theory, including the existence of infinitely many primes, is provable in $I\Delta_0$ with the weak pigeonhole principle for Δ_0-definable functions added as an axiom scheme. It is a longstanding open question [24] whether or not one can dispense with the weak pigeonhole principle, by proving the existence of infinitely many primes within $I\Delta_0$.

Secondly, the complexity of the weak pigeonhole principle is related to the complexity of approximate counting. The problem of recognizing the approximate size of a set is in the polynomial-time hierarchy. However, all known proofs of this fact rely on the weak pigeonhole principle. These results translate downwards: there are bounded-depth, polynomial-size circuits that can approximately count the number of 1's in a 0/1 bit string. However, once again, all known proofs of correctness require much higher proof-theoretic complexity. This is a perplexing situation: is it possible to prove that small circuits exist for approximate counting, and also to prove that any correctness proof for these small circuits is inherently more complex than these circuits? A positive answer would follow if one could prove superpolynomial lower bounds on the size of bounded-depth Frege proofs of the weak pigeonhole principle for the case when $n = m/2$.

Lastly, the complexity of the weak pigeonhole principle is connected to the inherent complexity of *proving* circuit lower bounds. In the last decade, substantial effort has gone into understanding the metamathematics of the P versus NP question. In pioneering work, Razborov and Rudich [21] show that most circuit lower bounds are natural, and hence, under certain cryptographic assumptions, these methods cannot be extended to proving P $\neq$ NP. It would be a big breakthrough to extend this type of result to show that there can be no proof of P $\neq$ NP (formalized in a reasonable way) in bounded arithmetic. Razborov [20] has shown that this question is connected to the difficulty of proving the weak pigeonhole principle, since the circuit lower bound statement can encode the weak pigeonhole principle in a certain sense.

Resolving the above three questions amounts to understanding the exact complexity of proving the pigeonhole principle. This tautology is expressed propositionally by a formula of size polynomial in m, where the underlying variables are $P_{i,j}$, for $i \leq m$ and $j \leq n$. Three key complexity parameters are d, n and S: the first parameter, d, measures the depth of the Frege proof; the second parameter, n, is the number of holes; S is the size of the proof. Clearly, as d and S increase and n decreases, the pigeonhole principle becomes easier to prove. The ultimate goal is to obtain a precise and smooth characterization of the smallest value for S as we vary the other two parameters, d and n.

In [16], Paris, Wilkie and Woods use a delicate diagonalization argument to give constant-depth, quasipolynomial-size Frege proofs of the weak pigeonhole principle. This is surprising, especially since it has been shown that any constant-depth Frege proof of the pigeonhole principle requires exponential size whenever n is at least $m - c$, for c a constant [17, 13]. Their argument actually translates into depth-3.5, quasipolynomial-size proofs in the sequent calculus, and Krajíček [9] extends their argument to obtain depth-1.5, quasipolynomial-size proofs. (Depth $d + .5$, for any nonnegative integer d, means that each formula has depth at most $d + 1$, but the bottom level of gates are restricted to polylog fan-in.) Despite this breakthrough, there are still huge gaps in our overall understanding in terms of the three parameters mentioned above. In particular, are these results optimal in terms of depth? Is there a more constructive, constant-depth proof of the weak pigeonhole principle? Can the size be improved from quasipolynomial to polynomial?

The main result of this paper is a new proof of the weak pigeonhole principle. Our new proof is a step toward resolving the above-mentioned questions, and the exact complexity of the weak pigeonhole principle. We show that the weak pigeonhole principle has quasipolynomial-size proofs where every formula consists of a single AND/OR of polylog fan-in. In the above terminology, we obtain a depth-.5 proof. Translated to bounded arithmetic, it follows from our proof that the weak pigeonhole principle with respect to a function whose graph is given by a relation R can be proven in $T_2^2(R)$.

Our proof is optimal with respect to depth as exponential lower bounds are known for depth-0 sequent calculus proofs, i.e., Resolution proofs, of the weak pigeonhole principle [7]. Our upper bound is also tight in another sense: [11, 23] show that the proof cannot be made tree-like, unless the size becomes exponential. Moreover, our proof is conceptually simpler than the previous upper bound due to Paris, Wilkie and Woods: it is a simple divide and conquer, along the lines of the upper bounds for Resolution proofs of the weak pigeonhole principle [6], combined with an amplification phase which allows us to speed up the induction.

The outline for the remainder of the paper is as follows. In Section 2, we give precise definitions of the pigeonhole principle tautology and of the proof system that we will be working with. In Section 3, we give an overview and generalization of the Resolution upper bound of [6]. In Section 4, we present our main result. We then also show how to extend our techinques to the not quite so weak pigeonhole principle with $m - n = n/(\log n)^{O(1)}$. In Section 5, we optimize the argument given in Section 4. In Section 6, we state uniform versions of our results for bounded arithmetic. Finally, in Section 7, we put our new upper bound in perspective with the many previous results that are known in this area, and conclude with open problems.

2 Definitions

The propositional proof system that we will study in this paper is the sequent calculus, LK, modified to allow unbounded fan-in connectives. Formulas are built up using the connectives $\wedge$, $\vee$, and $\neg$. All connectives are assumed to have unbounded fan-in. The formula $\wedge(A_1, \ldots, A_n)$ denotes the logical AND of the multi-set consisting of $A_1, \ldots A_n$, and similarly for $\vee$. Thus commutativity and associativity of the connectives is implicit. Our proof system operates on sequents which are sets of formulas of the form $A_1, \ldots, A_i \to B_1, \ldots, B_j$. The intended meaning is that the conjunction of the A_i's implies the disjunction of the B_j's. A proof of a sequent S in LK is a sequence of sequents, $S_1, ..., S_q$, such that each sequent S_i is either an initial sequent, or follows from previous sequents by one of the rules of inference, and the final sequent, S_q, is S. The size of the proof is $\sum_{1 \le i \le q} \text{size}(S_i)$ and its depth is $\max_{1 \le i \le q}(\text{depth}(S_i))$.

The *initial sequents* are of the form: (1) $x \to x$ where x is a literal; (2) $\to \wedge()$; $\vee() \to$. The rules of inference are as follows. First we have simple structural rules such as weakening (formulas can always be added to the left or to the right), contraction (two copies of the same formula can be replaced by one), and permutation (formulas in a sequent can be reordered). The remaining rules are the cut rule, and logical rules which allow us to introduce each connective on both the left side and the right side. The cut rule allows the derivation of $\Gamma, \Gamma' \to \Delta, \Delta'$ from $\Gamma, A \to \Delta$, and $\Gamma' \to A, \Delta'$. The logical rules are as follows.

1. (Negation-left) From $\Gamma \to A, \Delta$, we can derive $\neg A, \Gamma \to \Delta$.

2. (Negation-right) From $A, \Gamma \to \Delta$, derive $\Gamma \to \neg A, \Delta$.

3. (And-left) From $A_1, \wedge(A_2, \ldots, A_n), \Gamma \to \Delta$ derive $\wedge(A_1, \ldots, A_n), \Gamma \to \Delta$.

4. (And-right) From $\Gamma \to A_1, \Delta$ and $\Gamma \to \wedge(A_2, \ldots, A_n), \Delta$ derive $\Gamma \to \wedge(A_1, \ldots, A_n), \Delta$

5. (Or-left) From $A_1, \Gamma \to \Delta$ and $\vee(A_2, \ldots, A_n), \Gamma \to \Delta$ derive $\vee(A_1, \ldots, A_n), \Gamma \to \Delta$

6. (Or-right) From $\Gamma \to A_1, \vee(A_2, \ldots, A_n), \Delta$ derive $\Gamma \to \vee(A_1, \ldots, A_n), \Delta$.

Definition 1 *Let d be a nonnegative integer. A formula is of depth $d + .5$ if it is of depth d or of depth $d + 1$ but with the arity of the level 1 connectives restricted to polylogarithmic in the size of the formula. Depth $d + .5$ is also referred to as Σ-depth d in the literature.*

A sequent calculus proof is of depth $d + .5$ if all the formulas that appear in it are either of depth d or of depth $d+1$ but with the arity of the level 1 connectives restricted to polylogarithmic in the size of the final sequent. LK proofs of depth .5 are also referred to as the system $R(\log)$.

There is a well-known translation between predicate calculus proofs of first order sentences in systems of bounded arithmetic with an extra symbol R denoting an "arbitrary" relation, and propositional proofs of the corresponding constant-depth tautologies expressing the same principle. In particular, it is well-known that $S_2(R)$, or $T_2(R)$, proofs of statements (such as the pigeonhole principle for a function given by R) can be translated into quasipolynomial-size, bounded-depth proofs. Similarly, $I\Delta_0(R)$ proofs can be translated into polynomial-size, bounded-depth proofs. So these proof systems for bounded arithmetic can be viewed as uniform versions of propositional proof systems. The upper bounds that we will be presenting for propositional systems are all sufficiently uniform that the reverse translation is possible. In particular, our proofs can be straightforwardly translated to show that the weak pigeonhole principle with respect to R has a proof in $S^3_2(R)$. As $S^3_2(R)$ is known to be conservative over its subsystem $T^2_2(R)$ for statements of that general form, the proof can also be carried out in $T^2_2(R)$.

The pigeonhole principle on m pigeons and n holes says that there is no one-to-one function from a set of size m to a set of size n. Formally, this can be stated as follows:

$$\mathrm{PHP}^m_n : \ldots, \bigvee_{y \in [n]} P_{xy}, \ldots \to \ldots, P_{x_1 y} P_{x_2 y}, \ldots$$

where, on the left, x ranges over $[m]$ and, on the right, $x_1 \neq x_2$ range over $[m]$ and y ranges over $[n]$. Note that PHP^m_n is actually more general than the informal statement above since it asserts the nonexistence of any injective, many-valued function from $[m]$ to $[n]$.

Clearly as n decreases, the principle becomes weaker and weaker. When $n = m-1$, it is usually referred to as just the pigeonhole principle, and when $n \leq m/2$ it is referred to as the *weak* pigeonhole principle. The *onto* pigeonhole principle is a weaker version stating that there is no one-to-one, onto, many-valued function from m pigeons to n holes.

3 The Resolution upper bound

As mentioned in the introduction, the new proof of the weak pigeonhole principle presented in this paper uses some of the same ideas as the Resolution upper bound of Buss and Pitassi [6]. More precisely, they show that PHP_n^m has polynomial-size Resolution proofs whenever $n \leq (\log m)^2/\log\log m$. In this section, we provide an overview and generalization of this result.

First note that when $n = O(\log m)$ there are trivially polynomial-size Resolution proofs, by ignoring all but $n+1$ pigeons, and performing a brute-force refutation on these pigeons and holes.

Now assume for sake of contradiction that there is a mapping from m to n (for appropriately chosen n). Divide the m pigeons up into blocks, each of size $\log m + 1$. (Here, as at many places below, we will write as if m, or n, has some particular number theoretic shape – in the present case that $m/(\log m + 1)$ is an integer. This is done in the interests of clarity, it being left to the reader to verify that the proofs can easily be made quite general.)

The first case is that some block of pigeons maps in a one-to-one way into the first $\log m$ holes, and in this case we get a direct contradiction by brute force. The other case is where no block of pigeons all map to the first $\log m$ holes. But in this case, each block of pigeons can be viewed as a metapigeon, and now we have a one-to-one map from $m/(\log m + 1)$ metapigeons to the last $n - \log m$ holes, and we can proceed inductively. This argument can be translated into a Resolution proof because each inductive instance of the pigeonhole principle is still a conjunction of a set of clauses.

We can use this idea more generally to prove PHP_n^m with a size-S Resolution refutation, where $n \leq \log m \log S/\log\log S$. Let the block size be b, where $b = \log S$. Dividing up the m pigeons into m/b blocks, each of size b, either some block maps one-to-one into the first b holes, or not. In the first case, we can use brute-force to get a size $O(S)$ refutation, and in the second case, we have $m/(\log S)$ metapigeons, and $n - \log S$ holes. Continuing for $k = n/(\log S)$ iterations, as long as $n \leq \log m \log S/(\log\log S)$, we reach the desired contradiction.

Thus, we obtain polynomial-size Resolution refutations of PHP_n^m for $n = O((\log m)^2/\log\log m)$, quasipolynomial-size Resolution refutations for $n = O(\log m)^c$, etc.

Our new upper bound gives small proofs of PHP_n^m for much larger n, but the depth increases slightly, from 0 to .5.

4 Our new upper bound

Our goal is to show that PHP_n^{2n} has a quasipolynomial-size, tree-like proof of depth 1.5. We start by presenting the argument that we will then formalize as a sequent calculus proof.

The proof is in two parts: first we prove $\mathrm{PHP}_n^{n^2}$ and then we prove PHP_n^{2n}. Let us start with $\mathrm{PHP}_n^{n^2}$. By contradiction, suppose that there is an injective, many-valued function from $A = [n^2]$ to $B = [n]$. (For the remainder of this section, we will simply speak of functions even though we really mean many-valued functions.) Let $A_1, \ldots, A_n$ be the partition of A into sets of size n. Let B_1, B_2 be the partition of B into sets of size $n/2$. Then either

1. all the pigeons of some block A_i are sent to holes in the first block B_1, or
2. in every block there is at least one pigeon that is sent to a hole in the second block B_2.

If the first case occurs, then we have an injective function from a set of n pigeons to a set of $n/2$ holes. The function is injective because the original function is.

We now claim that the second case also gives an injective function from a set of n pigeons to a set of $n/2$ holes. View each block as a new superpigeon. Send each superpigeon to all the holes where its member pigeons are sent. We are guaranteed that each superpigeon is sent to at least one hole in the second block. The induced function from these n superpigeons to the $n/2$ holes in B_2 is injective again because of the injectivity of the original function.

This is the first step of the proof. In this step, the number of pigeons was reduced to n and the number of holes was reduced by half. In the second step, we will *amplify* the number of pigeons back up to n^2. Let f be the original function from $[n^2]$ to $[n]$ and let g be the new function from $[n]$ to $[n/2]$. Define a function h from $[n^2]$ to $[n/2]$ by setting $h(i) = k$ iff there is $j \in [n]$ such that $f(i) = j$ and $g(j) = k$. This new function h is injective because of the injectivity of both f and g.

We now repeat these two steps to obtain a sequence of injective functions from $[n]$ to $[n/4]$, from $[n^2]$ to $[n/4]$, from $[n]$ to $[n/8]$, from $[n^2]$ to $[n/8]$, $\ldots$, until an injective function from $[n]$ to $[1]$ is obtained. This is the desired contradiction, which proves $\mathrm{PHP}_n^{n^2}$.

Now we prove PHP_n^{2n}. Again by contradiction, suppose that there is an injective function f from $[2n]$ to $[n]$. We define a function g from $[4n]$ to $[2n]$ as follows.

Partition $[4n]$ into two blocks A_1, A_2 of size $2n$ and partition $[2n]$ into two blocks B_1, B_2 of size n. The function g is defined by using f to map A_1 to B_1 and a *translated* version of f to map A_2 to B_2. Now compose g and f as was done above to obtain a function h from $[4n]$ to $[n]$. Both g and h are injective because of the injectivity of f. This process can be generalized and repeated to obtain a sequence of injective functions with increasingly larger domain. Eventually, we get an injective function from $[n^2]$ to $[n]$, which contradicts $\mathrm{PHP}_n^{n^2}$ and completes the proof of PHP_n^{2n}.

We now turn to the formalization of this argument as a quasipolynomial-size, tree-like sequent calculus proof of depth 1.5. The proof will consist of a sequence of alternations between the two steps mentioned above. Since pigeons will eventually be not just simple pigeons but superpigeons, as a result of the reduction step, and since the function from pigeons to holes will eventually be the composition of earlier functions, as a result of the amplification step, we generalize the statement of the pigeonhole principle as follows. Let A and B be any two sets.

$$\mathrm{PHP}_B^A(Q): \ldots, \bigvee_{y\in B} Q_{xy}, \ldots \rightarrow \ldots, Q_{x_1y}Q_{x_2y}, \ldots$$

where, on the left, x ranges over A and, on the right, $x_1 \neq x_2$ range over A and y ranges over B. Here, the Q_{xy} can be arbitrary formulas and not just propositional variables.

In fact, in our proof, each Q_{xy} will be a OR of small AND's, say $\bigvee_k Q_{xy}^{(k)}$. Since our goal is to obtain a proof of depth 1.5, we have to be able to state $\mathrm{PHP}_B^A(Q)$ in depth 1.5. To achieve this, we say that $\bigvee_{y\in B} Q_{xy}$ actually stands for $\bigvee_{y\in B}\bigvee_k Q_{xy}^{(k)}$, and that $Q_{x_1y}Q_{x_2y}$ stands for $\bigvee_{k_1,k_2} Q_{x_1y}^{(k_1)}Q_{x_2y}^{(k_2)}$.

The following two lemmas establish that the reduction and amplification steps in the above argument can be carried out by a quasipolynomial-size, tree-like sequent calculus proof of depth 1.5.

Lemma 2 *Let A be any set of size n^2 and let B be any set of size $m \leq n$. Let $A_1, \ldots, A_n$ be the partition of A into sets of size n and let B_1, B_2 be the partition of B into sets of size $m/2$. For every set of size-s, depth-1.5 formulas $(Q_{xy})_{x\in A, y\in B}$ of the form OR of small AND's, there is a set of size-(ns), depth-1.5 formulas $(R_{iy})_{i\in[n], y\in B_2}$ of the form OR of small AND's such that $\mathrm{PHP}_B^A(Q)$ has a size-$(ns)^{O(1)}$, tree-like, depth-1.5 sequent calculus proof from $\mathrm{PHP}_{B_1}^{A_1}(Q)$, ..., $\mathrm{PHP}_{B_1}^{A_n}(Q)$ and $\mathrm{PHP}_{B_2}^{n}(R)$.*

Proof For the moment, ignore the fact that the Q_{xy}'s are formulas and pretend that they are simple propositional variables. $\mathrm{PHP}_B^A(Q)$ can be written as follows:

$$\mathrm{PHP}_B^A(Q): \ldots, \bigvee_{y\in B} Q_{xy}, \ldots \rightarrow \ldots, Q_{x_1y}Q_{x_2y}, \ldots$$

where, on the left, x ranges over A and, on the right, $x_1 \neq x_2$ range over A and y ranges over B. For any $i \in \{1, \ldots, n\}$, $\mathrm{PHP}^{A_i}_{B_1}(Q)$ can be written as

$$\mathrm{PHP}^{A_i}_{B_1}(Q) : \ldots, \bigvee_{y \in B_1} Q_{xy}, \ldots \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots$$

where, on the left, x ranges over A_i and, on the right, $x_1 \neq x_2$ range over A_i and y ranges over B_1.

The idea behind the set of R formulas is the following: R_{iy} will say that some pigeon from the ith block A_i is sent hole y. This is formalized as

$$R_{iy} = \bigvee_{x \in A_i} Q_{xy}.$$

$\mathrm{PHP}^n_{B_2}(R)$ can then be written as

$$\mathrm{PHP}^n_{B_2}(R) : \ldots, \bigvee_{y \in B_2} R_{iy}, \ldots \to \ldots, R_{iy} R_{jy}, \ldots$$

where, on the left, i ranges over $[n]$ and, on the right, $i \neq j$ range over $[n]$ and y ranges over B_2. Of course, it is understood that $R_{iy} R_{jy}$ actually stands for

$$\bigvee_{x_1 \in A_i} \bigvee_{x_2 \in A_j} Q_{x_1 y} Q_{x_2 y}.$$

The proof of $\mathrm{PHP}^A_B(Q)$ from $\mathrm{PHP}^{A_1}_{B_1}(Q)$, $\ldots$, $\mathrm{PHP}^{A_n}_{B_1}(Q)$ and $\mathrm{PHP}^n_{B_2}(R)$ starts with the following sequents:

$$\bigvee_{y \in B} Q_{xy} \to \bigvee_{y \in B_1} Q_{xy}, \bigvee_{y \in B_2} Q_{xy} \quad (x \in A). \tag{1}$$

For every i, cut $\mathrm{PHP}^{A_i}_{B_1}(Q)$ with the corresponding sequents in (1). This gives

$$\ldots, \bigvee_{y \in B} Q_{xy}, \ldots \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots, \ldots, \bigvee_{y \in B_2} Q_{xy}, \ldots \quad (i \in [n]) \tag{2}$$

where, on the left, x ranges over A_i and, on the right, $x_1 \neq x_2$ range over A_i, y ranges over B_1 and x ranges over A_i.

Now consider the following sequents:

$$Q_{xy} \to R_{iy} \quad (i \in [n], x \in A_i, y \in B_2). \tag{3}$$

By using the OR-left rule and then the OR-right rule, combine the sequents in (3) that correspond to the various values of y:

$$\bigvee_{y \in B_2} Q_{xy} \to \bigvee_{y \in B_2} R_{iy} \quad (i \in [n], x \in A_i). \tag{4}$$

Cut each of the sequents in (2) with the corresponding sequents in (4) to obtain

$$\ldots, \bigvee_{y \in B} Q_{xy}, \ldots \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots, \bigvee_{y \in B_2} R_{iy} \quad (i \in [n]) \tag{5}$$

where, on the left, x ranges over A_i and, on the right, $x_1 \neq x_2$ range over A_i and y ranges over B_1. Cut each of these sequents with $\mathrm{PHP}^n_{B_2}(R)$ to obtain

$$\ldots, \bigvee_{y \in B} Q_{xy}, \ldots \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots, \ldots, R_{iy} R_{jy}, \ldots \tag{6}$$

On the left of this sequent, x ranges over A. On the right, we have one $Q_{x_1 y} Q_{x_2 y}$ for every $x_1 \neq x_2 \in A_i$, every $i \in [n]$ and every $y \in B_1$. On the right, we also have one $R_{iy} R_{jy}$ for every $i \neq j \in [n]$ and every $y \in B_2$.

Finally, recall that $R_{iy} R_{jy}$ actually stands for

$$\bigvee_{x_1 \in A_i} \bigvee_{x_2 \in A_j} Q_{x_1 y} Q_{x_2 y}.$$

Consider the following sequents:

$$R_{iy} R_{jy} \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots \quad (i \neq j \in [n], y \in B_2) \tag{7}$$

where, on the right, x_1 ranges over A_i and x_2 ranges over A_j. Cut each of these sequents with (6) to obtain

$$\ldots, \bigvee_{y \in B} Q_{xy}, \ldots \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots, \tag{8}$$

where, on the left, x still ranges over A, but, on the right, we now have one $Q_{x_1 y} Q_{x_2 y}$ for every $i \in [n]$, every $x_1 \neq x_2 \in A_i$ and every $y \in B_1$, and another $Q_{x_1 y} Q_{x_2 y}$ for every $i \neq j \in [n]$, every $x_1 \in A_i$, every $x_2 \in A_j$ and every $y \in B_2$. $\mathrm{PHP}^A_B(Q)$ can now be easily obtained by weakening, which completes the proof.

This was all done under the assumption that the Q_{xy}'s are simple propositional variables. Generalizing to OR's of small AND's is fairly easy since it requires only minor modifications of the proof. To illustrate, suppose that $Q_{xy} = \bigvee_k Q^{(k)}_{xy}$. Then the sequents in (7) become

$$\bigvee_{x_1 \in A_i} \bigvee_{k_1} \bigvee_{k_2} \bigvee_{x_2 \in A_j} Q^{(k_1)}_{x_1 y} Q^{(k_2)}_{x_2 y} \to \ldots, \bigvee_{k_1, k_2} Q^{(k_1)}_{x_1 y} Q^{(k_2)}_{x_2 y}, \ldots \quad (i \neq j \in [n], y \in B_2) \tag{9}$$

where, on the right, x_1 ranges over A_i and x_2 ranges over A_j. These sequents are proved in essentially the same way as the sequents in (7). We leave the remaining details to the reader as well as the straightforward task of verifying that the proof is tree-like and of size $(ns)^{O(1)}$. $\square$

Lemma 3 *For every set C of size n, for every set D, for every set of size-s, depth-1.5 formulas $(Q_{xy})_{x \in C, y \in D}$ of the form OR of small AND's, and for every set of size-t, depth-1.5 formulas $(P_{wx})_{w \in [n^2], x \in [n]}$ of the form OR of small AND's, there is a set of size-$O(nst)$, depth-1.5 formulas $(R_{wy})_{w \in [n^2], y \in D}$ of the form OR of small AND's such that $\mathrm{PHP}^C_D(Q)$ weakened by the cedents of $\mathrm{PHP}^{n^2}_n(P)$ has a size-$(nst)^{O(1)}$, tree-like, depth-1.5 sequent calculus proof from $\mathrm{PHP}^{n^2}_D(R)$.*

Proof Suppose that $Q_{xy} = \bigvee_k Q^{(k)}_{xy}$ and that $P_{wx} = \bigvee_j P^{(j)}_{wx}$. $\mathrm{PHP}^C_D(Q)$ weakened by the cedents of $\mathrm{PHP}^{n^2}_n(P)$ can be written as follows:

$$\ldots, \bigvee_{x \in [n]} P_{wx}, \ldots, \ldots, \bigvee_{y \in D} Q_{xy}, \ldots \to \ldots, P_{w_1 x} P_{w_2 x}, \ldots, \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots \qquad (10)$$

where, on the left, w ranges over $[n^2]$ and x ranges over C, and, on the right, x ranges over $[n]$, $x_1 \neq x_2$ range over C and y ranges over D. As mentioned earlier, it is understood that $\bigvee_{y \in D} Q_{xy}$ stands for

$$\bigvee_{y \in D} \bigvee_k Q^{(k)}_{xy},$$

that $Q_{x_1 y} Q_{x_2 y}$ stands for

$$\bigvee_{k_1, k_2} Q^{(k_1)}_{x_1 y} Q^{(k_2)}_{x_2 y},$$

and similarly for P.

We now want to define a set of R formulas that will allow us to prove the above sequent from $\mathrm{PHP}^{n^2}_D(R)$. The P formulas describe a function between a set of size n^2 and a set of size n, while the Q formulas describe a function between a set C of size n and a D set of size m. The idea is that the R formulas will describe the composition of those two functions. First, in what follows, we will identify C with $[n]$. More precisely, let f be any one-to-one, onto function from $[n]$ to C. Whenever x is in $[n]$ and we write Q_{xy}, we will actually mean $Q_{f(x)y}$. Now R_{wy} will be defined as follows:

$$R_{wy} = \bigvee_{x \in [n]} P_{wx} Q_{xy}.$$

Once again, this last formula actually stands for

$$\bigvee_{x \in [n]} \bigvee_j \bigvee_k P^{(j)}_{wx} Q^{(k)}_{xy}.$$

The sequent $\mathrm{PHP}^{n^2}_D(R)$ can be written as follows:

$$\mathrm{PHP}^{n^2}_D(R) : \ldots, \bigvee_{y \in D} R_{wy}, \ldots \to \ldots, R_{w_1 y} R_{w_2 y}, \ldots \qquad (11)$$

where, on the left, w ranges over $[n^2]$ and, on the right, $w_1 \neq w_2$ range over $[n^2]$ and y ranges over D. In other words, this sequent says that if every w is sent to some y, then at least two w's will be sent to the same y.

The proof of (10) from this sequent consists of two main steps. First, we show that if two w's go to the same y, then either two w's go to the same x or two x's go to the same y. This can be written as

$$R_{w_1 y} R_{w_2 y} \to \ldots, P_{w_1 x} P_{w_2 x}, \ldots, \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots \quad (w_1 \neq w_2 \in [n^2], y \in D) \tag{12}$$

where, on the right, x and $x_1 \neq x_2$ range over $[n]$.

Second, we show that if w goes to some x and every x goes to some y, then w goes to some y. That is,

$$\bigvee_{x \in [n]} P_{wx}, \ldots, \bigvee_{y \in [D]} Q_{xy}, \ldots \to \bigvee_{y \in D} R_{wy} \quad (w \in [n^2]) \tag{13}$$

where, on the left, x ranges over $[n]$. Applying the cut rule to (11) and all the sequents in (12) and (13) produces the desired result, i.e., sequent (10).

We now examine in more detail the proofs of the sequents in (12) and (13). For the sequents in (12), consider arbitrary values of $w_1 \neq w_2 \in [n^2]$ and $y \in D$. First note that $R_{w_1 y} R_{w_2 y}$ stands for

$$\bigvee_{x_1 \in [n]} \bigvee_{j_1} \bigvee_{k_1} \bigvee_{x_2 \in [n]} \bigvee_{j_2} \bigvee_{k_2} P^{(j_1)}_{w_1 x_1} Q^{(k_1)}_{x_1 y} P^{(j_2)}_{w_2 x_2} Q^{(k_2)}_{x_2 y}.$$

Now start with the following sequents:

$$P^{(j_1)}_{w_1 x_1} Q^{(k_1)}_{x_1 y} P^{(j_2)}_{w_2 x_2} Q^{(k_2)}_{x_2 y} \to P^{(j_1)}_{w_1 x_1} P^{(j_2)}_{w_2 x_2} \quad (x_1, x_2 \in [n], j_1, j_2, k_1, k_2) \tag{14}$$

and

$$P^{(j_1)}_{w_1 x_1} Q^{(k_1)}_{x_1 y} P^{(j_2)}_{w_2 x_2} Q^{(k_2)}_{x_2 y} \to Q^{(k_1)}_{x_1 y} Q^{(k_2)}_{x_2 y} \quad (x_1, x_2 \in [n], j_1, j_2, k_1, k_2) \tag{15}$$

By using the OR-left rule, combine all the sequents in (14) with $x_1 = x_2$ and all the sequents in (15) with $x_1 \neq x_2$. This gives

$$R_{w_1 y} R_{w_2 y} \to \ldots, P^{(j_1)}_{w_1 x} P^{(j_2)}_{w_2 x}, \ldots, \ldots, Q^{(k_1)}_{x_1 y} Q^{(k_2)}_{x_2 y}, \ldots$$

where, on the right, x and $x_1 \neq x_2$ range over $[n]$ and j_1, j_2, k_1 and k_2 range over all possible values. Several applications of the OR-right rule now yield the desired sequent in (12).

Let us now turn to the proof of the sequents in (13). Let $w \in [n^2]$ be arbitrary. Again, first note that $\bigvee_{y \in D} R_{wy}$ stands for

$$\bigvee_{y \in D} \bigvee_{x \in [n]} \bigvee_{j} \bigvee_{k} P^{(j)}_{wx} Q^{(k)}_{xy}.$$

Start with the following sequents:

$$P_{wx}^{(j)}, Q_{xy}^{(k)} \to P_{wx}^{(j)} Q_{xy}^{(k)} \quad (x \in [n], y \in D, j, k) \tag{16}$$

By using the OR-left rule and then the OR-right rule, combine the sequents in (16) that correspond to the various values of k:

$$P_{wx}^{(j)}, Q_{xy} \to \bigvee_k P_{wx}^{(j)} Q_{xy}^{(k)} \quad (x \in [n], y \in D, j) \tag{17}$$

Again by using the OR-left rule and then the OR-right rule, combine the sequents in (17) that correspond to the various values of j:

$$P_{wx}, Q_{xy} \to \bigvee_j \bigvee_k P_{wx}^{(j)} Q_{xy}^{(k)} \quad (x \in [n], y \in D) \tag{18}$$

Once more, by using the OR-left rule and then the OR-right rule, combine the sequents in (18) that correspond to the various values of y:

$$P_{wx}, \bigvee_{y \in D} Q_{xy} \to \bigvee_{y \in D} \bigvee_j \bigvee_k P_{wx}^{(j)} Q_{xy}^{(k)} \quad (x \in [n]) \tag{19}$$

Finally, in a similar way, combine all the sequents in (19) to obtain the desired sequent in (13).

There only remains to say that it is easy to verify that the proof is tree-like and of size $(nst)^{O(1)}$. □

Theorem 4 *For every set of size-t, depth-1.5 formulas $(P_{xy})_{x \in [n^2], y \in [n]}$ of the form OR of small AND's,* $\mathrm{PHP}_n^{n^2}(P)$ *has a size-$(nt)^{O(\log n)}$, tree-like, depth-1.5 sequent calculus proof. In particular, if the P_{xy}'s are simple propositional variables, then the size of the proof is $n^{O(\log n)}$.*

Proof As mentioned earlier, the proof consists in a sequence of alternations between the reduction and amplification steps formalized in the preceding lemmas. Before describing the proof, first note that these two lemmas also hold when all the sequents involved are weakened by the cedents of $\mathrm{PHP}_n^{n^2}(P)$. This is simply because in every application of any of the inference rules, both the hypotheses and the conclusion can be weakened in this way. In what follows, we assume that all sequents are weakened by the cedents of $\mathrm{PHP}_n^{n^2}(P)$.

We describe the proof in a top-down fashion. Let c be the maximum of all the hidden constants in the statements of Lemmas 2 and 3. First, by Lemma 2, we prove $\mathrm{PHP}_n^{n^2}(P)$ from $\mathrm{PHP}_{B_1}^{A_1}(P), \ldots, \mathrm{PHP}_{B_1}^{A_n}(P)$ and $\mathrm{PHP}_{B_2}^{n}(R)$, where $A_1, \ldots, A_n$ is the partition of $[n^2]$ into sets of size n, B_1, B_2 is the partition of $[n]$ into sets of size $n/2$, and R is a set of size-(nt), depth-1.5 formulas. In other words, we prove $\mathrm{PHP}_n^{n^2}(P)$ from $n+1$ sequents of the form $\mathrm{PHP}_D^C(Q)$ where $|C| = n$, $|D| = n/2$ and the Q's are sets of size-(nt), depth-1.5 formulas.

Second, by Lemma 3, we prove each of these sequents from a sequent of the form $\mathrm{PHP}_D^{n^2}(R)$ where the R's are sets of size-$c(nt)^2$, depth-1.5 formulas.

We continue using the two lemmas in alternation. Each time Lemma 2 is used, the size of the formulas is multiplied by n. Each time Lemma 3 is used, the size of the formulas is multiplied by cnt. This is because it is always the original set of formulas P that is used in each application of Lemma 3. It is then easy to verify that after k reductions and amplifications, we will be left with proving $(n+1)^k$ sequents of the form $\mathrm{PHP}_{n/2^k}^{n^2}(R)$ where the R's are sets of size-$(cnt)^{2k}$, depth-1.5 formulas.

After $\log n$ steps, we are left with only sequents of the form $\mathrm{PHP}_1^{n^2}(R)$, and these are very easy to prove.

It is easy to see that the entire proof is tree-like. To calculate its size, note that the largest subproofs occur in the last amplification step. There, we have $(n+1)^{\log n}$ proofs of size at most $(cnt)^{2c\log n}$. The total size of the proof is therefore $(nt)^{O(\log n)}$.

□

The next lemma formalizes the proof of PHP_n^{2n} from $\mathrm{PHP}_n^{n^2}$ that was outlined at the beginning of this section.

Lemma 5 *For every set of size-s, depth-1.5 formulas $(Q_{xy})_{x\in[2n],y\in[n]}$ of the form OR of small AND's, there is a set of size-$(ns)^{O(\log n)}$, depth-1.5 formulas $(R_{wy})_{w\in[n^2],y\in[n]}$ of the form OR of small AND's such that $\mathrm{PHP}_n^{2n}(Q)$ has a size-$(ns)^{O(\log n)}$, tree-like, depth-1.5 sequent calculus proof from $\mathrm{PHP}_n^{n^2}(R)$.*

Proof The overall structure of the proof is similar to the amplification step that was formalized in Lemma 3. For the sake of clarity, we will assume that the Q_{xy}'s are simple propositional variables and leave to the reader the generalization to the case where the Q_{xy}'s are formulas.

The sequent $\mathrm{PHP}_n^{2n}(Q)$ can be written as follows:

$$\mathrm{PHP}_n^{2n}(Q) : \ldots, \bigvee_{y\in[n]} Q_{xy}, \ldots \to \ldots, Q_{wy}Q_{xy}, \ldots \tag{20}$$

where, on the left, x ranges over $[2n]$, and, on the right, $w \neq x$ range over $[2n]$ and y ranges over $[n]$.

We now define a set of R formulas that will allow us to prove the above sequent from $\mathrm{PHP}_n^{n^2}(R)$. The Q variables describe a function from $[2n]$ to $[n]$. We will use this function to define, for $c = 1, \ldots, \log n$, a function from $[2^c n]$ to $[2^{c-1}n]$. The R formulas will then describe the composition of all these functions.

Consider $[n^2]$ and $[n^2/2]$. Partition $[n^2]$ into blocks $A_1, \ldots, A_{n/2}$ of size $2n$ and partition $[n^2/2]$ into blocks $B_1, \ldots, B_{n/2}$ of size n. The idea is to use the function defined by the Q variables to define a function from each A_i to the corresponding B_i. The function from $[n^2]$ to $[n^2/2]$ will then be defined by putting all these functions side by side. More precisely, if x is in A_i, let $\rho(x)$ denote B_i. Then, for every $x \in [n^2]$ and $y \in [n^2/2]$, if $y \in \rho(x)$, let Q_{xy} denote Q_{uv} where u and v are the ranks of x and y in their respective blocks.

Note that for arbitrary $c \in \{1, \ldots, \log n\}$, $(Q_{xy})_{x \in [2^c n], y \in [2^{c-1} n]}$ defines a function from $[2^c n]$ to $[2^{c-1} n]$. Now let $t = \log n$ and define the R_{wy} as follows:

$$R_{wy} = \bigvee_{u_1 \in \rho(w)} \bigvee_{u_2 \in \rho(u_1)} \cdots \bigvee_{u_{t-1} \in \rho(u_{t-2})} Q_{wu_1} Q_{u_1 u_2} \cdots Q_{u_{t-1} y}.$$

In other words, R_{wy} says that w is sent to y by saying that there is a sequence of intermediate points $u_1, u_2, \ldots, u_{t-1}$, all belonging to the appropriate blocks, such that w is sent to u_1, each u_i is sent to u_{i+1}, and u_{t-1} is sent to y.

The sequent $\mathrm{PHP}_n^{n^2}(R)$ can be written as follows:

$$\mathrm{PHP}_n^{n^2}(R) : \ldots, \bigvee_{y \in [n]} R_{wy}, \ldots \to \ldots, R_{w_1 y} R_{w_2 y}, \ldots \tag{21}$$

where, on the left, w ranges over $[n^2]$ and, on the right, $w_1 \neq w_2$ range over $[n^2]$ and y ranges over $[n]$. In other words, this sequent says that if every w is sent to some y, then at least two w's will be sent to the same y.

The proof of (20) from this sequent consists of two main steps. First, we show that if R sends two w's to the same y, then Q sends two x's to the same y. This can be written as

$$R_{w_1 y} R_{w_2 y} \to \ldots, Q_{x_1 y} Q_{x_2 y}, \ldots \quad (w_1 \neq w_2 \in [n^2], y \in [n]) \tag{22}$$

where, on the right, $x_1 \neq x_2$ range over $[2n]$.

Second, we show that if Q sends every x to some y, then R sends w to some y. That is,

$$\ldots, \bigvee_{y \in [n]} Q_{xy}, \ldots \to \bigvee_{y \in [n]} R_{wy} \quad (w \in [n^2]) \tag{23}$$

where, on the left, x ranges over $[2n]$. Applying the cut rule to (21) and all the sequents in (22) and (23) produces the desired result, i.e., sequent (20).

We now examine in more detail the proofs of the sequents in (22) and (23). For the sequents in (22), consider arbitrary values of $w_1 \neq w_2 \in [n^2]$ and $y \in [n]$. First note that $R_{w_1 y} R_{w_2 y}$ stands for

$$\bigvee_{u_1 \in \rho(w_1)} \bigvee_{u_2 \in \rho(u_1)} \cdots \bigvee_{u_{t-1} \in \rho(u_{t-2})} \bigvee_{v_1 \in \rho(w_2)} \bigvee_{v_2 \in \rho(v_1)} \cdots \bigvee_{v_{t-1} \in \rho(v_{t-2})} Q_{w_1 u_1} Q_{u_1 u_2} \cdots Q_{u_{t-1} y} Q_{w_2 v_1} Q_{v_1 v_2} \cdots Q_{v_{t-1} y}.$$

Set $u_0 = w_1$, $v_0 = w_2$ and $u_t = v_t = y$. For every term T in the disjunction defining $R_{w_1y}R_{w_2y}$, there is a smallest number $j(T)$ such that $u_{j(T)} = v_{j(T)}$ but $u_{j(T)-1} \neq v_{j(T)-1}$. Now start with the following sequents, one for every term T in $R_{w_1y}R_{w_2y}$:

$$T \to Q_{u_{j(T)-1}u_{j(T)}}Q_{v_{j(T)-1}v_{j(T)}} \quad (T \text{ is a term in } R_{w_1y}R_{w_2y}) \tag{24}$$

By using the OR-left rule, combine all the sequents in (24). This gives

$$R_{w_1y}R_{w_2y} \to \ldots, Q_{u_{j(T)-1}u_{j(T)}}Q_{v_{j(T)-1}v_{j(T)}}, \ldots$$

where, on the right, T ranges over all the terms in $R_{w_1y}R_{w_2y}$. To obtain the corresponding sequent in (22) from this sequent, we only need to argue that each $Q_{u_{j(T)-1}u_{j(T)}}Q_{v_{j(T)-1}v_{j(T)}}$ is actually of the form $Q_{x_1z}Q_{x_2z}$ with $x_1 \neq x_2$. But this is clear since, first of all, $u_{j(T)} = v_{j(T)}$. Second, this implies that $u_{j(T)-1}$ and $v_{j(T)-1}$ are in the same block. That combined with the fact that $u_{j(T)-1} \neq v_{j(T)-1}$ implies that $u_{j(T)-1}$ and $v_{j(T)-1}$ have different ranks within that block. The desired sequent in (22) can therefore be obtained by weakening.

Let us now turn to the proof of the sequents in (23). Let $w \in [n^2]$ be arbitrary. Again, first note that $\bigvee_{y\in[n]} R_{wy}$ stands for

$$\bigvee_{y\in[n]} \bigvee_{u_1\in\rho(w)} \bigvee_{u_2\in\rho(u_1)} \cdots \bigvee_{u_{t-1}\in\rho(u_{t-2})} Q_{wu_1}Q_{u_1u_2}\cdots Q_{u_{t-1}y}.$$

Start with the following sequents:

$$Q_{wu_1}, Q_{u_1u_2}, \ldots, Q_{u_{t-1}y} \to Q_{wu_1}Q_{u_1u_2}\cdots Q_{u_{t-1}y}$$
$$(u_1 \in \rho(w), u_2 \in \rho(u_1), \ldots, u_{t-1} \in \rho(u_{t-2}), y \in [n]) \tag{25}$$

By using the OR-left rule and then the OR-right rule, combine the sequents in (25) that correspond to the various values of y:

$$Q_{wu_1}, Q_{u_1u_2}, \ldots, Q_{u_{t-2}u_{t-1}}, \bigvee_{y\in[n]} Q_{u_{t-1}y} \to \bigvee_{y\in[n]} Q_{wu_1}Q_{u_1u_2}\cdots Q_{u_{t-1}y}$$
$$(u_1 \in \rho(w), u_2 \in \rho(u_1), \ldots, u_{t-1} \in \rho(u_{t-2})) \tag{26}$$

Again by using the OR-left rule and then the OR-right rule, combine the sequents in (26) that correspond to the various values of u_{t-1}:

$$Q_{wu_1}, Q_{u_1u_2}, \ldots, Q_{u_{t-3}u_{t-2}}, \bigvee_{u_{t-1}\in\rho(u_{t-2})} Q_{u_{t-2}u_{t-1}}, \ldots, \bigvee_{y\in[n]} Q_{u_{t-1}y}, \ldots$$
$$\to \bigvee_{u_{t-1}\in\rho(u_{t-2})} \bigvee_{y\in[n]} Q_{wu_1}Q_{u_1u_2}\cdots Q_{u_{t-1}y}$$
$$(u_1 \in \rho(w), u_2 \in \rho(u_1), \ldots, u_{t-2} \in \rho(u_{t-3}))$$

where, on the left, there is one formula $\bigvee_{y \in [n]} Q_{u_{t-1}y}$ for every $u_{t-1} \in \rho(u_{t-2})$. Now recall that each $Q_{u_{t-1}y}$ is actually of the form Q_{xy} where $x \in [2n]$ is the rank of u_{t-1} within its block. Similarly, each $Q_{u_{t-2}u_{t-1}}$ is of the form Q_{xy} where $x \in [2n]$ is the rank of u_{t-2} within its block and $y \in [n]$ is the rank of u_{t-1} within its block. Therefore, by weakening and contraction, we obtain

$$
\begin{aligned}
&Q_{wu_1}, Q_{u_1u_2}, \ldots, Q_{u_{t-3}u_{t-2}}, \ldots, \bigvee_{y \in [n]} Q_{xy}, \ldots \\
&\quad \to \bigvee_{u_{t-1} \in \rho(u_{t-2})} \bigvee_{y \in [n]} Q_{wu_1} Q_{u_1u_2} \cdots Q_{u_{t-1}y} \\
&\qquad\qquad\qquad (u_1 \in \rho(w), u_2 \in \rho(u_1), \ldots, u_{t-2} \in \rho(u_{t-3}))
\end{aligned}
$$

where, on the left, x ranges over $[2n]$. This can be repeated $t-2$ times, by using the OR-left, OR-right and contraction rules, to produce the desired sequent in (23).

Once again, it is a simple matter to verify that the proof is tree-like and of size $(ns)^{O(\log n)}$. □

The main result of this section now follows directly from Lemma 5 and Theorem 4.

Theorem 6 *For every set of size-t, depth-1.5 formulas $(P_{xy})_{x \in [2n], y \in [n]}$ of the form OR of small AND's, $\mathrm{PHP}_n^{2n}(P)$ has a size-$(nt)^{O(\log n)^2}$, tree-like, depth-1.5 sequent calculus proof. In particular, if the P_{xy}'s are simple propositional variables, then the size of the proof is $n^{O(\log n)^2}$.*

Actually it is possible to decrease the difference between the number of pigeons and n, the number of holes, to $o(n)$ at the expense of increasing the size of proof, while still keeping it tree-like and of depth 1.5 with quasipolynomial size. One way of doing this, given PHP_n^{2n}, is based on the following idea. Start with a function f from $[n+h]$ to $[n]$ where h is at least $n/(\log n)^{O(1)}$. It is convenient to extend the domain of f by putting $f(z) = z - h$ whenever $z > n + h$. Since all these new values are greater than n, this extension would still be injective if the original f mapping to $[n]$ was. Let $f^{(j)}$ denote the function obtained from j iterations of f. By induction on j, $f^{(j)}$ takes $[n+jh]$ to $[n]$. A suitable choice of $q = (\log n)^{O(1)}$ makes $n + qh \geq 2n$. Therefore the function $f^{(q)}$ takes $[2n]$ to $[n]$. By PHP_n^{2n}, $f^{(q)}$ cannot be injective, and inductively if $f^{(j+1)}$ is not injective, then at least one of $f^{(j)}$, f is not injective. So at $j = 1$ we conclude that f is not injective.

As an aid to formalizing this argument, observe that if r is the least positive integer such that $z \leq n + rh$ then $f^{(j)}(z) = z - jh > n$ for $j < r$, while for $j \geq r$, $f^{(j)}(z) = y_j \in [n]$ where $y_r = f(z - (r-1)h)$, $y_{j+1} = f(y_j)$ and f is the original function (without extension).

Lemma 7 *For every set of size-t, depth-1.5 formulas $(P_{xy})_{x\in[n+h],y\in[n]}$ of the form OR of small AND's with $h = n^{O(1)}$, there is for any positive integer $q = (\log n)^{O(1)}$, a set of size-$(nt)^{O(q)}$, depth-1.5 formulas $(R_{zy})_{z\in[n+qh],y\in[n]}$ of the form OR of small AND's such that $\mathrm{PHP}_n^{n+h}(P)$ has a size-$(nt)^{O(q)}$, tree-like, depth-1.5 sequent calculus proof from $\mathrm{PHP}_n^{n+qh}(R)$.*

In particular, taking $h = n/(\log n)^k$, $q = (\log n)^k$ for any constant $k > 0$, $\mathrm{PHP}_n^{n+h}(P)$ has a size-$(nt)^{O(\log n)^k}$, tree-like, depth-1.5 sequent calculus proof from $\mathrm{PHP}_n^{2n}(R)$.

Proof For each value of $j = 1, \ldots, q$ we will define a set of depth-1.5 formulas $(R_{zy}^{(j)})_{z\in[n+jh],y\in[n]}$ corresponding to the function $f^{(j)}(z) = y$ of the informal description, restricted to domain $[n + jh]$. The required formulas R_{zy} will be obtained as $R_{zy}^{(q)}$. The claimed proof will be constructed from segments of size-$(nt)^{O(q)}$ deriving $\mathrm{PHP}_n^{n+jh}(R^{(j)})$, weakened by the cedents of $\mathrm{PHP}_n^{n+h}(P)$, from $\mathrm{PHP}_n^{n+(j+1)h}(R^{(j+1)})$ similarly weakened. As $R_{zy}^{(1)}$ will be P_{zy} by the definition given below, this will clearly suffice.

For notational consistency, y, with or without a subscript/superscript, will range over elements of $[n]$ throughout the argument.

Given $z \in [n+jh]$, let r be the least positive integer such that $z \leq n+rh$. Clearly $1 \leq r \leq j$. Choose $R_{zy}^{(j)}$ to be

$$\bigvee_{y_r\in[n]} \bigvee_{y_{r+1}\in[n]} \cdots \bigvee_{y_{j-1}\in[n]} P_{z-(r-1)h\, y_r}\, P_{y_r y_{r+1}} \ldots P_{y_{j-1} y}.$$

This is interpreted to mean $P_{z-(j-1)h\, y}$ if $r = j$, and $\bigvee_{y_{j-1}\in[n]} P_{z-(r-1)h\, y_{j-1}}\, P_{y_{j-1} y}$ if $r = j-1$. As before we really mean the depth-1.5 formula obtained by using the distributive law to make $R_{zy}^{(j)}$ an OR of small AND's. If the formulas P_{xy} have size t, then each of these "multiplied out" formulas $R_{zy}^{(j)}$ has size $(nt)^{O(j)}$ which is at most $(nt)^{O(q)}$.

Starting with the sequent

$$\ldots, \bigvee_{y\in[n]} R_{zy}^{(j+1)}, \ldots, \bigvee_{y\in[n]} P_{xy}, \ldots \to \ldots, R_{zy}^{(j+1)} R_{z'y}^{(j+1)}, \ldots, P_{xy} P_{x'y}, \ldots$$

where on the left, x ranges over $[n+h]$ and z ranges over $[n+(j+1)h]$, while on the right, $x \neq x'$ range over $[n+h]$, $z \neq z'$ range over $[n+(j+1)h]$ and y ranges over $[n]$, we wish to derive

$$\ldots, \bigvee_{y\in[n]} R_{zy}^{(j)}, \ldots, \bigvee_{y\in[n]} P_{xy}, \ldots \to \ldots, R_{zy}^{(j)} R_{z'y}^{(j)}, \ldots, P_{xy} P_{x'y}, \ldots .$$

Here the ranges are the same except that z, z' are now restricted to $[n+jh]$. It will be left to the reader to check that the derivation we describe, and hence the whole proof, is of size $(nt)^{O(q)}$.

The derivation can be broken down into components of two sorts. Firstly a proof, for each fixed $z \in [n+(j+1)h]$, of

$$\bigvee_{y_j \in [n]} R^{(j)}_{zy_j}, \ldots, \bigvee_{y \in [n]} P_{xy}, \ldots \rightarrow \bigvee_{y \in [n]} R^{(j+1)}_{zy} \tag{27}$$

where x ranges over $[n+h]$ on the left and $\bigvee_{y_j \in [n]} R^{(j)}_{zy_j}$ is left out if $z > n+jh$. Secondly, for each fixed choice of $z \neq z'$ from $[n+(j+1)h]$ and $y \in [n]$, a proof of the sequent

$$R^{(j+1)}_{zy} R^{(j+1)}_{z'y} \rightarrow \ldots, R^{(j)}_{zy_j} R^{(j)}_{z'y_j}, \ldots, P_{xy} P_{x'y}, \ldots \tag{28}$$

having $x \neq x'$ ranging over $[n+h]$ and y_j ranging over $[n]$ on the right. Here the formulas $R^{(j)}_{zy_j} R^{(j)}_{z'y_j}$ are omitted if either of z, z' is greater than $n+jh$. The rest of the derivation consists of obvious applications of structural rules and cut.

The form of the proof of (27) depends on the magnitude of z. If $z > n+jh$ then the formula $\bigvee_{y \in [n]} R^{(j+1)}_{zy}$ on the right of (27) is $\bigvee_{y \in [n]} P_{z-jh\, y}$ which is also one of the formulas on the left, so the proof is easy. If $z \leq n+jh$ then $R^{(j)}_{zy}$ makes sense and the proof proceeds via the sequents

$$R^{(j)}_{zy_j}, P_{y_j\, y} \rightarrow R^{(j)}_{zy_j} P_{y_j\, y} \quad \text{for each fixed } y, y_j \in [n],$$

whose proof requires (only) a little thought remembering that the right hand side really denotes an OR of small AND's. Weakening and repeated use of the OR rules leads to

$$R^{(j)}_{zy_j}, \bigvee_{y \in [n]} P_{y_j\, y} \rightarrow \bigvee_{y \in [n]} R^{(j)}_{zy_j} P_{y_j\, y} \quad \text{for each fixed } y_j \in [n],$$

and then

$$\bigvee_{y \in [n]} R^{(j)}_{zy}, \ldots, \bigvee_{y \in [n]} P_{y_j\, y}, \ldots \rightarrow \bigvee_{y_j \in [n]} \bigvee_{y \in [n]} R^{(j)}_{zy_j} P_{y_j\, y},$$

where on the left y_j ranges over $[n]$. Observe that the right hand side is $\bigvee_{y \in [n]} \bigvee_{y_j \in [n]} R^{(j)}_{zy_j} P_{y_j\, y}$ which is just another notation denoting $\bigvee_{y \in [n]} R^{(j+1)}_{zy}$, so this sequent is (27) except that further weakening is needed on the left.

In proving (28) there are three cases to consider. The most involved is when both z, z' are in $[n+jh]$. For each fixed choice of $y \in [n]$ and distinct elements $z, z' \in [n+jh]$, the sequent (28) which we want to prove can be rewritten as

$$\bigvee_{y_j \in [n]} \bigvee_{y'_j \in [n]} R^{(j)}_{zy_j} P_{y_j y} R^{(j)}_{z'y'_j} P_{y'_j y} \rightarrow \ldots, R^{(j)}_{zy_j} R^{(j)}_{z'y_j}, \ldots, P_{xy} P_{x'y}, \ldots \tag{29}$$

where on the right, $x \neq x'$ ranges over $[n+h]$ and y_j ranges over $[n]$. Now it is easy to prove

$$\bigvee_{y_j \in [n]} \bigvee_{y'_j \in [n]} R^{(j)}_{zy_j} P_{y_j y} R^{(j)}_{z'y'_j} P_{y'_j y} \to \ldots, R^{(j)}_{zy_j} P_{y_j y} R^{(j)}_{z'y'_j} P_{y'_j y}, \ldots \tag{30}$$

Here each clause $R^{(j)}_{zy_j} R^{(j)}_{z'y'_j} P_{y_j y} P_{y'_j y}$ occurring on the right of (30) corresponds to a particular choice of y_j, y'_j from $[n]$. If $y_j = y'_j$ there is a simple proof of

$$R^{(j)}_{zy_j} R^{(j)}_{z'y'_j} P_{y_j y} P_{y'_j y} \to R^{(j)}_{zy_j} R^{(j)}_{z'y_j} ,$$

while if $y_j \neq y'_j$,

$$R^{(j)}_{zy_j} R^{(j)}_{z'y'_j} P_{y_j y} P_{y'_j y} \to P_{y_j y} P_{y'_j y} ,$$

is easily derived and has a right hand side of the form $P_{xy} P_{x'y}$ with $x \neq x'$. In either situation we can cut $R^{(j)}_{zy_j} R^{(j)}_{z'y'_j} P_{y_j y} P_{y'_j y}$ from the right of (30), replacing it with one of the formulas on the right of (29). Doing this for each such clause clearly leads to a proof of (29).

The remaining two cases are similar. Briefly, if exactly one of z, z' (z' for definiteness) satisfies $z' > n + jh$, so $n < z' - jh \leq n + h$, then the sequent (28) which we want to prove can be rewritten as

$$\bigvee_{y_j \in [n]} R^{(j)}_{zy_j} P_{y_j y} P_{z' - jh\, y} \to \ldots, P_{xy} P_{x'y}, \ldots$$

and we use the fact that $P_{y_j y} P_{z' - jh\, y}$ is of the form $P_{xy} P_{x'y}$ with $x \neq x'$ for $x = y_j \leq n < z' - jh = x'$. If $z > n + jh$ and $z' > n + jh$, then (28) is

$$P_{z - jh\, y} P_{z' - jh\, y} \to \ldots, P_{xy} P_{x'y}, \ldots$$

where $x \neq x'$ range over $[n+h]$. As $z \neq z'$ are in $[n + (j+1)h]$, the left hand side is one of the formulas on the right. $\square$

Combining Lemma 7 and Theorem 6 gives:

Theorem 8 *Let $k > 0$ be a fixed constant, and put $h = n/(\log n)^k$. Then for every set of size-t, depth-1.5 formulas $(P_{xy})_{x \in [n+h], y \in [n]}$ of the form OR of small AND's, $\mathrm{PHP}^{n+h}_n(P)$ has a size-$(nt)^{O(\log n)^{k+2}}$, tree-like, depth-1.5 sequent calculus proof. In particular, if the P_{xy}'s are simple propositional variables, then the size of the proof is $n^{O(\log n)^{k+2}}$.*

Let us mention an alternative approach to PHP_n^{n+h} with $h = n/(\log n)^k$, $k > 0$ constant, which also yields a tree-like proof of depth 1.5 and quasipolynomial size. Given an function f from $[n+h]$ to $[n]$, we will construct a new function f^* from $[(n+h)^q]$ to $[n^q]$ where $q = (\log n)^k$. Identify $[(n+h)^q]$ with the Cartesian product $[n+h]^q$ of q copies of $[n+h]$, and similarly $[n]^q$ with $[n^q]$. Define f^* as mapping the sequence $x_1x_2...x_q \in [n+h]^q$ of elements $x_j \in [n+h]$, to the sequence $y_1y_2...y_q \in [n]^q$ where $y_j = f(x_j)$. As $n = qh$ we see that $(n+h)^q/n^q = (q+1)^q/q^q \geq 2$. (This last inequality can be proved even in quite weak axiom systems for bounded arithmetic by showing $(q+1)^j \geq q^j + jq^{j-1}$ via induction on $j \geq 1$.) Letting $N = n^q$ it follows that $(n+h)^q \geq 2N$ so if f is supposed injective, then f^* takes $[2N]$ injectively into $[N]$ and therefore violates PHP_N^{2N}.

5 Optimal depth

In this section we will show how to prove PHP_n^{2n} in depth .5. Note that the statement of PHP_n^{2n} itself has depth 1, so in order for the theorem to make sense, we will need to convert the proof into refutation form. Let Clauses(PHP_n^{2n}) denote the set of depth-0 sequents that underly the pigeonhole principle. That is, Clauses(PHP_n^{2n}) consists of the sequents $\to P_{i1}, \ldots, P_{in}$ for each $i \in [2n]$, and the sequents $P_{ik}, P_{jk} \to$ for each $i \neq j \in [2n]$, $k \in [n]$. The following lemma shows that it is easy to convert a proof of PHP_n^{2n} into a refutation of Clauses(PHP_n^{2n}) with no significant change in size or depth.

Lemma 9 *Let* PHP_n^{2n} *have a size-*s*, tree-like, depth-*1.5 *sequent calculus proof. Then there is a size-*$O(s^2)$*, tree-like, depth-*1.5 *refutation of* Clauses(PHP_n^{2n}).

Proof Recall that PHP_n^{2n} is the following sequent:

$$\mathrm{PHP}_n^{2n} : \ldots, \bigvee_{k\in[n]} P_{ik}, \ldots \to \ldots, P_{ik}P_{jk}, \ldots$$

where, on the left, i ranges over $[2n]$ and, on the right, $i \neq j$ range over $[2n]$ and k ranges over $[n]$. Start with the sequents

$$\to P_{i1}, \ldots, P_{in} \quad (i \in [2n]).$$

By several applications of the OR-right rule, we get

$$\to \bigvee_{k\in[n]} P_{ik} \quad (i \in [2n]).$$

Now cut each of these sequents as well as each of the sequents $P_{ik}P_{jk} \to$ with PHP_n^{2n} to obtain the desired contradiction. The bound on the size of the refutation is easy to verify. □

We will now show how to convert a tree-like refutation of Clauses(PHP^{2n}_n) of depth-1.5 into a (dag-like) refutation of Clauses(PHP^{2n}_n) of depth-.5. The following result is due to Krajíček.

Theorem 10 ([9]) *Let Σ be a set of sequents of depth 0. That is, each sequent in Σ is of the form $\Gamma \to \Delta$ where Γ and Δ are sets of literals. Let d be a nonnegative integer. Suppose that there is a tree-like, depth-$(d+1.5)$ LK refutation of Σ of size S. Then Σ has a depth-$(d+.5)$ LK refutation of size polynomial in S.*

For completeness, we include the proof for the case of reducing the depth from 1.5 to .5.

Proof Consider an arbitrary sequent in the depth-1.5 LK refutation, of the form:

$$\begin{aligned}\Gamma, \bigvee_i A_i^1, \ldots, \bigvee_i A_i^m, \bigwedge_i C_i^1, \ldots, \bigwedge_i C_i^m \\ \to \bigvee_i B_i^1, \ldots \bigvee_i B_i^m, \bigwedge_i D_i^1, \ldots \bigwedge_i D_i^m, \Delta\end{aligned}$$

where Γ and Δ are sets of formulas of depth at most .5, and A_i^j, B_i^j, C_i^j and D_i^j are formulas of depth .5.

Let P be the tree-like, depth-1.5 LK refutation, and let P_k denote the first k lines of P. Assume that s_k is the sequent at line k, and assume without loss of generality that it has the above form. We will prove by induction on k that P_k can be efficiently converted into a dag-like, depth-.5 proof of

$$\begin{aligned}\Gamma, C_1^1, \ldots C_q^1, \ldots C_1^m, \ldots C_q^m \\ \to B_1^1, \ldots, B_q^1, \ldots B_1^m, \ldots, B_q^m, \Delta\end{aligned}$$

from Σ together with the additional axioms:

$$\begin{array}{ll}(1a) & \to A_1^1, \ldots, A_q^1 \\ (2a) & \to A_1^2, \ldots, A_q^2 \\ & \ldots \\ (ma) & \to A_1^m, \ldots, A_q^m \\ & \text{and} \\ (1b) & D_1^1, \ldots, D_q^1 \to \\ (2b) & D_1^2, \ldots, D_q^2 \to \\ & \ldots \\ (mb) & D_1^m, \ldots, D_q^m \to .\end{array}$$

This suffices to prove the theorem since the final line is $\rightarrow$.

When $k = 1$, s_k is an axiom of the form $x \rightarrow x$, or is in Σ, so the inductive statement holds. Now suppose that the k^{th} line follows from two previous lines by a rule. The two situations requiring work are the cut rule, and the OR-left (symmetrically the AND-right) rule. Considering the cut rule, suppose, for example, that the two previous lines have the form:

$$\Gamma, \bigvee_i A_i^1, \ldots, \bigvee_i A_i^m, \bigwedge_i C_i^1, \ldots, \bigwedge_i C_i^m, \bigvee_i E_i$$
$$\rightarrow \Delta, \bigvee_i B_i^1, \ldots, \bigvee_i B_i^m, \bigwedge_i D_i^1, \ldots, \bigwedge_i D_i^m$$

and

$$\Gamma, \bigvee_i A_i^1, \ldots, \bigvee_i A_i^m, \bigwedge_i C_i^1, \ldots, \bigwedge_i C_i^m$$
$$\rightarrow \Delta, \bigvee_i B_i^1, \ldots, \bigvee_i B_i^m, \bigwedge_i D_i^1, \ldots, \bigwedge_i D_i^m, \bigvee_i E_i$$

In the above notation, the formulas in Γ, Δ, and A_i^j, B_i^j, C_i^j, D_i^j and E_i have depth .5. And the k^{th} line, obtained by cutting on $\bigvee_i E_i$, has the form:

$$\Gamma, \bigvee_i A_i^1, \ldots, \bigvee_i A_i^m, \bigwedge_i C_i^1, \ldots, \bigwedge_i C_i^m$$
$$\rightarrow \Delta, \bigvee_i B_i^1, \ldots, \bigvee_i B_i^m, \bigwedge_i D_i^1, \ldots, \bigwedge_i D_i^m$$

By induction, there is a dag-like, depth-.5 proof, Q_1, of

$$\Gamma, C_1^1, \ldots, C_q^1, \ldots, C_1^m, \ldots, C_q^m$$
$$\rightarrow \Delta, B_1^1, \ldots, B_q^1, \ldots, B_1^m, \ldots, B_q^m$$

from axioms (1a) through (ma) and (1b) through (mb), and $\rightarrow E_1, \ldots E_q$ (together with Σ), and a dag-like, depth-.5 proof, Q_2, of

$$\Gamma, C_1^1, \ldots C_q^1, \ldots, C_1^m, \ldots, C_q^m$$
$$\rightarrow \Delta, B_1^1, \ldots, B_q^1, \ldots, B_1^m, \ldots, B_q^m, E_1, \ldots, E_q$$

from axioms (1a) through (ma) and (1b) through (mb). Because the original proof is tree-like, Q_1 and Q_2 can be assumed to be disjoint. We want to combine them to obtain a dag-like, depth-.5 proof, Q, of

$$\Gamma, C_1^1, \ldots C_q^1, \ldots C_1^m, \ldots, C_q^m$$
$$\rightarrow \Delta, B_1^1, \ldots, B_q^1, \ldots, B_1^m, \ldots, B_q^m$$

from axioms (1a) through (ma) and (1b) through (mb). Replace each axiom of the form $\rightarrow E_1, \ldots E_q$ in Q_1 by

$$\Gamma, C_1^1, \ldots C_q^1, \ldots, C_1^m, \ldots, C_q^m \\ \rightarrow \Delta, B_1^1, \ldots, B_q^1, \ldots, B_1^m, \ldots, B_q^m, E_1, \ldots, E_q$$

and carry the extra formulas throughout Q_1. Prefixing the result with the proof Q_2 of this sequent gives the desired proof Q. Because the original proof is tree-like, the sequents proved in the course of Q_1 are not used later than s_k, so this change in them causes no problems. (However this is where the new proof may cease to be tree-like. The sequent $\rightarrow E_1, \ldots E_q$ may be used at many places in Q_1, but we prevent an exponential explosion in size by appending only one copy of Q_2 and settling for Q being merely dag-like. We know by Theorem 13 below that this cannot be avoided in the case of PHP_n^{2n}, or even $\mathrm{PHP}_n^{n^2}$. Alternatively, writing out the conversion of the proof of $\mathrm{PHP}_n^{n^2}$ described in Theorem 4, for a small value of n, should convince the reader that multiple uses of $\rightarrow E_1, \ldots E_q$ really can have to be dealt with in order to transform a single use of the cut rule.)

The other cases, where the cut rule is applied to $\bigwedge_i E_i$, and the OR-left, AND-right rules, are all proven similarly; the other rules require little or no modifications.

In showing that the new proof is size-$S^{O(1)}$, we may ignore new sequents corresponding to uses of structural rules, as counting the size of these will only change the exponent by a constant factor. (The astute reader may already have noticed implicit uses of contraction and weakening above.) Under this proviso, besides the sequents originally present, each occurrence of a formula in the original proof can give rise to at most one additional sequent in the new proof. Consequently the number of sequents in the new proof is $O(S)$. At step k, in dealing with the kth sequent s_k of the original proof, the increase in the size of each sequent of the new proof is at worst proportional to the size of s_k, because the new formulas added are disjoint subformulas of s_k. Therefore the total size of each sequent of the new proof at the end of the conversion is $O(S)$. So by this reckoning, the new proof is size-$O(S^2)$. □

This result, combined with Theorem 6 and Lemma 9, gives the main theorem of this section.

Theorem 11 *The propositional weak pigeonhole principle,* PHP_n^{2n}*, has size-*$n^{O(\log n)^2}$*, depth-.5 LK proofs.*

Similarly, using Theorems 4 and 8 in place of Theorem 6 yields:

Theorem 12 $\mathrm{PHP}_n^{n^2}$ *has size-*$n^{O(\log n)}$*, depth-.5 LK proofs. For each constant* $k > 0$*,* $\mathrm{PHP}_n^{n+n/(\log n)^k}$ *has size-*$n^{O(\log n)^{k+2}}$*, depth-.5 LK proofs.*

Our upper bound in Theorem 11 is optimal with respect to depth since it is known that depth-0 proofs, i.e., Resolution proofs, of PHP_n^{2n} require exponential size [7]. In addition, our upper bound is tight in another sense: the proof cannot be made tree-like, unless the size becomes exponential, as the following theorem shows.

Theorem 13 ([11, 23]) *For sufficiently large n, if P is a tree-like LK refutation of* $\mathrm{Clauses}(\mathrm{PHP}_n^m)$*, where each formula in P involves at most k variables, then P has size at least $2^{\lfloor n/2k \rfloor}$.*

The results of [11, 23] are very elegant and apply to a large class of formulas. However, the exact form of the lower bound for the weak pigeonhole principle is not made explicit and their proof is more complicated than needed for the particular case that concerns us. Therefore, we will give here a simpler proof of the theorem, one that extends the lower bound for tree-like Resolution given in [6].

Proof The proof will consist of two stages.

1. Show that if there is a small tree-like, depth-.5 LK refutation of $\mathrm{Clauses}(\mathrm{PHP}_n^m)$, then there is a decision tree of the same structure, with nodes queried by decisions of the form $f(X) = 0/1$, where f is a function, and X is a set of at most k variables upon which f depends, with the property that each leaf is labeled by some clause of PHP_n^m that is falsified.

2. Show that any such decision tree for PHP_n^m has to be large.

We will prove the first step by induction on the size of the proof. The only rules that really matter are the ones that take two sequents to one sequent: these are AND-right, OR-left and cut.

First, suppose we derive $C = \Gamma \to \Delta$ from $A = \Gamma, g \to \Delta$ and $B = \Gamma \to g, \Delta$ by an application of the cut rule. Consider an assignment α that makes C false. Then if $g(\alpha)$ is false, then B is false. Otherwise, if $g(\alpha)$ is true, then A is false. So we label this node with g. Since the proof has depth .5, g is a function involving at most k variables, and so satisfies the conditions required of the decision tree.

Now suppose we derive $C = \Gamma \to \wedge(A_1 \ldots A_n), \Delta$ from $A = \Gamma \to A_1, \Delta$ and $B = \Gamma \to \wedge(A_2, \ldots A_k), \Delta$ by an application of the AND-right rule. Consider an assignment α that makes C false. This implies that $\wedge(A_1, \ldots, A_n)(\alpha)$ is false. Now if $A_1(\alpha)$ is false, then A is false. On the other hand, if $A_1(\alpha)$ is true, then $\wedge(A_2, \ldots A_n)$ is false and thus B is false. So we can label this node with A_1. The OR-left rule is handled in a similar way.

We will now prove step two. We want to show that any decision tree for solving the search problem associated with PHP_n^m, where the queries made are of the form $f(X)$, where each f depends on at most k variables, must have size at least $2^{\lfloor n/2k \rfloor}$.

Consider the critical truth assignments (cta's) where n pigeons are mapped to n holes, and the remaining $m-n$ pigeons are unassigned. Consider the restricted tree T, where we only care about paths that are followed by at least one critical truth assignment. Now we want to claim that T must be large.

We want to prove that along any path in T, the number of branching nodes must be at least $\lfloor n/2k \rfloor$, and hence the total size of T is at least $2^{\lfloor n/2k \rfloor}$. We will prove it by induction on n. When $n=0$, any of the m pigeons is a valid answer, and the size is therefore 1.

Now suppose $n>0$, and assume that Q is a decision tree for PHP^m_n. Let $f(X)$ be the first query in Q, and suppose that the the left subtree of Q is labeled by $f(X)=0$ and the right subtree of Q is labeled by $f(X)=1$. If all cta's are such that $f(X)=0$, then proceed on the left subtree. Similarly if all cta's are such that $f(X)=1$, then proceed on the right subtree.

Otherwise, $f(X)$ splits up the problem in two pieces in a nontrivial way. First consider the left subtree, the one labeled by $f(X)=0$. In this case, we want to find a restriction ρ_0 so that: (1) $f(X)$ is forced to 0 by ρ_0, and (2) ρ_0 is a partial one-to-one map from at most $2k$ pigeons to holes. To obtain ρ_0, since $f(X)$ is forced to 0 by some cta, select an assignment to the variables of X consistent with one of these cta's. Then minimally extend the assignment so that we are left with a partial assignment ρ_0 that leaves m' unassigned pigeons and n' unassigned holes, and the remaining pigeons are mapped in a one-to-one way onto the remaining holes. Since $|X| \leq k$, at most k pigeons and at most k holes are mentioned by ρ_0, and therefore the extended assignment leaves $m' \geq m-2k$ and $n' \geq n-2k$. Now applying ρ_0, it follows that the left subtree, Q_0, solves the decision problem for $\mathrm{PHP}^{m'}_{n'}$, where $m'=m-2k$, $n'=n-2k$. By the inductive hypothesis it follows that any path of Q_0 must have at least $\lfloor (n-2k)/2k \rfloor$ branching nodes.

Similarly, for the right subtree (labeled $f(X)=1$), we can find a restriction so that $f(X)$ is forced to 1 by ρ_1 and ρ_1 is a partial map from at most $2k$ pigeons to holes. Applying ρ_1 it follows that the right subtree Q_1 solves the decision problem for $\mathrm{PHP}^{m'}_{n'}$, and again by the inductive hypothesis, any path in Q_1 must have at least $\lfloor (n-2k)/2k \rfloor$ branching nodes.

Thus, in total, it follows that any path in Q has at least $\lfloor n/2k \rfloor$ branching nodes, and thus the size of Q is at least $2^{\lfloor n/2k \rfloor}$. $\square$

6 New results for bounded arithmetic

As mentioned earlier, our proofs of the weak pigeonhole principle are sufficiently uniform to be carried out in the corresponding systems of bounded arithmetic. We will follow the usual notations for systems of bounded arithmetic [3, 10, 8]. The theory T_2^i is the system of bounded arithmetic, with ordinary induction (IND) for all Σ_i^b formulas. The theory S_2^i is the system of bounded arithmetic, with polynomial induction (PIND) for all Σ_i^b formulas. Equivalently, polynomial induction (PIND) can be replaced by length induction (LIND). The theories $T_2^i(R)$ and $S_2^i(R)$ are relativized versions of T_2^i and S_2^i, where R is a new predicate symbol that can be used freely in $\Sigma_i^b(R)$ induction hypotheses.

Let $\mathrm{PHP}_n^m(R)$ denote the following first-order version of the pigeonhole principle.

$$n < m \ \wedge\ \forall x < m\, \exists y < n\, R(x,y) \ \rightarrow\ \exists x < m\, \exists x' < x\, \exists y < n\ (\, R(x,y) \wedge R(x',y)\,)$$

Notice that this is a $\Sigma_2^b(R)$ formula with free variables n, m, and it remains $\Sigma_2^b(R)$ even if R is replaced in it by an arbitrary $\Sigma_1^b(R)$ formula R'.

It was previously known [16, 9] that $\mathrm{PHP}_n^{2n}(R)$ is provable in $T_2^3(R)$. Also a theorem concerning $\mathrm{PHP}_n^{n^2}(R)$ and $\mathrm{PHP}_n^{2n}(R)$ with identical notation to the following, but actually referring to the weak *onto* pigeonhole principle, appears as Theorem 11.2.4 in Krajíček's book [10]. As he points out in [12] the following result, obtained by making the arguments given above uniform, is new even for $\mathrm{PHP}_n^{n^2}(R)$. It answers a question he posed in [11].

Theorem 14 *$\mathrm{PHP}_n^{n^2}(R)$, $\mathrm{PHP}_n^{2n}(R)$, and for k any fixed positive integer, $\mathrm{PHP}_n^{n+n/(\log n)^k}(R)$, are all provable in $T_2^2(R)$.*

Proof Of course $\mathrm{PHP}_n^{n+n/(\log n)^k}(R)$ contains the others, but they are proved in order, and in fact can be derived with R replaced by any $\Sigma_1^b(R)$ formula R'. By a relativization of Buss's witnessing theorem [5, 8, 10], the system $S_2^3(R)$ is conservative over $T_2^2(R)$ for $\Sigma_3^b(R)$ formulas, so it clearly suffices to show these principles are provable in $S_2^3(R)$.

Here we will sketch only the proof of $\mathrm{PHP}_n^{n^2}(R)$, which generalizes in an obvious way to a proof of $\mathrm{PHP}_n^{n^2}(R')$ when R' is $\Sigma_1^b(R)$. Limiting our attention to this case is justified because $\mathrm{PHP}_n^{2n}(R)$ can be reduced, working in $S_2^3(R)$, to $\mathrm{PHP}_n^{n^2}(R')$ with a suitable choice of $\Sigma_1^b(R)$ formula R'. This reduction using bounded arithmetic (a uniform version of our Lemma 5) is essentially just an argument which can already be found in detail in [16]. It trivially generalizes to handle $\mathrm{PHP}_n^{2n}(R'')$ when R'' is a $\Sigma_1^b(R)$ formula. Finally, no new ideas are involved in using the method of Lemma 7 of give an $S_2^3(R)$ reduction of $\mathrm{PHP}_n^{n+n/(\log n)^k}(R)$ to $\mathrm{PHP}_n^{2n}(R'')$ for some such R''.

Now to prove $\mathrm{PHP}_n^{n^2}(R)$ in $S_2^3(R)$, recall that the main idea used above was to start with the given relation $R(x,y)$ from $[n^2]$ to $[n]$, and then progressively construct new relations from $[n^2]$ to $[n/2]$, $[n^2]$ to $[n/4]$, etc.. At each step there were $n+1$ possible new relations to choose from, and we argued inductively that at least one of these choices must define a (possibly many-valued) function if the previous relation did. (For convenience we now take $[n] = \{0, 1, \ldots, n-1\}$, and for clarity make the inessential assumption that n is a power of 2.) If we replace $[n/2^i]$ by some appropriately chosen interval of length $n/2^i$ from the unique partition of $[n]$ into 2^i such intervals $I_j^{(i)}, j \in [2^i]$, then these new relations occur naturally as restrictions of certain relations from $[n^2]$ to $[n]$. It is easier to work with these bigger relations which, again by an easy induction, are injective provided R is.

The relations will be defined by a single formula $Q(l, W, x, y)$, where l is the number of steps (numbered $0, 1, \ldots, l-1$) and W is a parameter in $[(n+1)^l]$ that describes which of the $n+1$ possibilities was chosen at each step. The possibilities are "labelled" $0, 1, \ldots, n$, and that chosen at stage i is given by the ith digit W_i of the base $n+1$ expansion of W. (n also appears as a free variable in $Q(l, W, x, y)$ but we will not show occurrences of n explicitly.)

Similarly, in defining $Q(l, W, x, y)$ we will quantify over $X < n^{2(l+1)}$, thinking of X as denoting a length $l+1$ sequence of elements $X_i \in [n^2]$. Numbers l, W, x, y will satisfy $Q(l, W, x, y)$ just if there exists such a sequence X satisfying

$$X_l = x \ \wedge \ R(X_0, y)$$

and having the property that for every $i < l$, if $W_i < n$ then

$$\exists u < n \, (\, R(X_{i+1}, u) \ \wedge \ X_i = W_i \, n + u \,) \, ,$$

and if $W_i = n$, then

$$\exists u < n \, \exists v < n \, (\, R(X_{i+1}, u) \ \wedge \ X_i = un + v \,) \, .$$

Provided l is bounded by $\log n$, $Q(l, W, x, y)$ will clearly be a $\Sigma_1^b(R)$ formula. An easy induction on l shows that if W' is obtained from $W \in [(n+1)^l]$ by adjoining an $l+1$st digit $W_l \in [n+1]$ then Q satisfies the recursive "definition"

$$\begin{aligned} Q(0, W, x, y) \ &\equiv \ R(x, y) \, , \\ Q(l+1, W', x, y) \ &\equiv \ \begin{cases} \exists u < n \, (\, R(x, u) \wedge Q(l, W, W_l \, n + u, y) \,) & \text{if } \ W_l < n, \\ \exists u < n \, \exists v < n \, (\, R(x, u) \wedge Q(l, W, un + v, y) \,) & \text{if } \ W_l = n. \end{cases} \end{aligned}$$

Also it is not hard to show (by partitioning $I_j^{(l)}$ into two subintervals of length $n/2^{l+1}$) that given W satisfying $\forall x < n^2 \, \exists y \in I_j^{(l)} \, Q(l, W, x, y)$, at least one such W' satisfies

$$\exists j' < 2^l \, \forall x < n^2 \, \exists y \in I_{j'}^{(l+1)} \, Q(l+1, W', x, y) \, .$$

Armed with these and the requirement that $l \leq \log n$, $\Sigma_3^b(R)$-LIND establishes

$$\begin{aligned} &\forall x < n^2 \, \forall x' < x \, \forall y < n \, \neg \, (\, R(x, y) \wedge R(x', y) \,) \\ &\quad \to \ \forall \, W < (n+1)^l \, \forall x < n^2 \, \forall x' < x \, \forall y < n \, \neg \, (\, Q(l, W, x, y) \wedge Q(l, W, x', y) \,) \end{aligned} \tag{31}$$

(using only the recursive "definition" of Q) and

$$\forall x < n^2 \, \exists y < n \, R(x,y) \ \rightarrow \ \exists \, W < (n+1)^l \, \exists j < 2^l \, \forall x < n^2 \, \exists y \in I_j^{(l)} \, Q(l,W,x,y) \, .$$

Taking $l = \log n$, the interval $I_j^{(l)}$ of length $n/2^l$ has only one element, y say. So this becomes

$$\forall x < n^2 \, \exists y < n \, R(x,y) \ \rightarrow \ \exists \, W < (n+1)^l \, \exists y < n \, \forall x < n^2 \, Q(l,W,x,y) \, . \tag{32}$$

The conjunction of the left hand sides of (31) and (32) asserts $\neg \mathrm{PHP}_n^{n^2}(R)$ (provided $n < n^2$), while the conjunction of the right hands sides is easy to disprove for $n > 1$. □

Jan Krajíček has pointed out the following alternative presentation of our main theorem (Theorem 11), via bounded arithmetic. There is a known simulation [11] showing that $T_2^2(R)$ proofs can be simulated by quasipolynomial-size, depth-.5 LK proofs ($R(\log)$ proofs). Thus once we have shown that $\mathrm{PHP}_n^{2n}(R)$ (say) can be proven in $T_2^2(R)$, our main theorem follows, although perhaps with a poorer, but still quasipolynomial, size bound. He informs us that the explicit proof manipulations given in Section 4 correspond to similar manipulations obtained automatically via this simulation of $T_2^2(R)$ proofs by quasipolynomial-size $R(\log)$ proofs.

7 Discussion and related results

We summarize what is currently known in Table 1. The symbol * in the References column indicates the current paper. All of the lower bounds are exponential in n. (Some of these are actually proven generally, as a function of n and m.)

For depth-0 (Resolution proofs), the best known upper bound are polynomial-size proofs of PHP_n^m, where $n \leq (\log m)^2 / \log\log m$ [6]. As mentioned in the introduction, prior to the result of this paper, the only nontrivial constant-depth LK proof of the weak pigeonhole principle was that of [16], and the optimization with respect to depth of [9]. Krajíček also shows that the proof of [16] can also be modified to give depth-.5 LK proofs of the *onto* pigeonhole principle.

When $m - n = O(1)$, it is known that any bounded-depth LK proof of PHP_n^m requires exponential size. Moreover, it is known that even if one adds the onto pigeonhole principle as an axiom scheme, there is still no subexponential, bounded-depth LK proof of PHP_n^m.

In this paper, we have shown how to prove PHP_n^{2n}, and even $\mathrm{PHP}_n^{n+n/(\log n)^{O(1)}}$, with depth-.5, quasipolynomial-size LK proofs. It is not known whether or not there are constant-depth, *polynomial*-size LK proofs of the weak pigeonhole principle. If

	Upper Bounds			Lower Bounds	
	Ref.	$n \leq$	Size	Ref.	$n \geq$
Resolution	[6]	$\frac{(\log m)^2}{\log\log m}$	poly(m)	[6, 22]	$\frac{(\log m)^2}{\log\log m}$ (tree-like)
(depth-0 LK)	*	$\frac{\log m \log S}{\log\log S}$	poly(S)	[7]	$m^{1/2+\epsilon}$
				[18]	any n (regular)
				[19]	any n
Depth-.5 LK	*	$\sqrt{m}$	$m^{O(\log m)}$	[11, 23]	$\sqrt{m}$ (tree-like)
	*	$m/2$	$m^{O(\log m)^2}$		
	*	$m - \frac{m}{(\log m)^{O(1)}}$	$m^{(\log m)^{O(1)}}$		
Depth-1.5 LK	[16, 9]	$m/2$	$m^{O(\log m)}$	[17, 13, 1]	$m - m^{1/480}$
Depth-c LK	[15]	polylog m	poly(m)	[17, 13, 1]	$m - m^{o(1)}$
	[16]	$\sqrt{m}$	$m^{\log^{O(c)} m}$		

Table 1: Summary of related results.

we restrict attention to polynomial-size proofs, then all that is known is that one can prove PHP_n^m in constant depth, where $n = \text{polylog } m$. Moreover, the depth of the proof is dependent on the the exponent in the polylog m.

Lastly, by formalizing circuits that count, one can prove PHP_n^m for any $n < m$ with polynomial-size Frege proofs [4].

There are many interesting open problems that are raised by this work. Most importantly, are there polynomial-size, constant-depth proofs of either the weak pigeonhole principle, or the onto weak pigeonhole principle? A sufficiently uniform positive answer to either would answer longstanding open questions about the provability in $I\Delta_0$ of number theoretic statements. In the case of the weak pigeonhole principle, these include the existence of infinitely many primes [24, 16], and Lagrange's theorem about sums of four squares [14, 2].

The original proof of [16] actually shows that $\mathrm{PHP}_n^{n^2}$ has depth-d, size-$n^{\log^{O(d)} n}$

proofs. That is, as d increases, the size is reduced. We do not know how to extend the proof to this more general situation while maintaining our lower depth.

In the introduction, we mentioned a close connection between the weak pigeonhole principle and approximate counting. Here we elaborate further on this connection and a related open problem. Buss's Frege proof [4] of PHP_n^{n+1} views the pigeonhole variables as a bipartite graph with pigeons on the left and holes on the right. If every pigeon maps to at least one hole, then the number of edges out of the left side of the graph is at least m. To say this, we construct a polynomial-size circuit that counts the number of 1's in a binary string with one index for each of the edges of the graph, and prove inductively (using the pigeon axioms) that this circuit outputs a number of size at least m. Similarly, if each hole has at most one pigeon mapped to it, then the number of edges into the right side of the graph is at most n, and again we say this by proving inductively (using the hole axioms) that the counting circuit outputs a number of size at most n. Finally, if $m > n$, this gives us the desired contradiction.

Using a pairwise independent collection of hash functions, approximating the number of 1's in a binary string is computable with bounded-depth, polynomial-size circuits. It is tempting to try to use such circuits to prove the weak pigeonhole principle, in a similar manner to the above argument of Buss. However, the proofs of correctness of all known constructions involve probablistic counting and hence rely on the weak pigeonhole principle to prove correctness. It is not clear whether this can be avoided. We conjecture that it is not possible to prove the weak pigeonhole principle with polynomial-size, small-depth (say depth 2 or 3) Frege proofs. Such a result would be very striking, as it would be the first instance where there are known explicit constructions of circuits computing a function (in this case approximate counting), but where *any* proof of correctness of the function cannot be carried out in an equally feasible way.

8 Acknowledgements

We would like to thank Jan Krajíček for stimulating discussions that led to the writing of this paper. We also thank Jan, Paul Beame and Sam Buss for useful comments, including some from Sam long ago, and we thank Jan and Sam for clarifying the exact implications for bounded arithmetic.

References

[1] P. Beame and S. Riis. More on the relative strength of counting principles. In P. W. Beame and S. R. Buss, editors, *Proof Complexity and Feasible Arithmetics*,

volume 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 13–35. American Mathematical Society, 1998.

[2] A. Berarducci and B. Intrigila. Combinatorial principles in elementary number theory. *Ann. Pure Appl. Logic*, 55:35–50, 1991.

[3] S. R. Buss. *Bounded Arithmetic*, volume 3 of *Studies in Proof Theory*. Bibliopolis, Napoli, 1986.

[4] S. R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *J. Symbolic Logic*, 52:916–927, 1987.

[5] S. R. Buss. Axiomatizations and conservation results for fragments of bounded arithmetic. In W. Sieg, editor, *Logic and Computation: Proceedings of a Workshop held at Carnegie Mellon University, June 30 – July 2, 1987*, volume 106 of *Contemporary Mathematics*, pages 57–84. American Mathematical Society, 1990.

[6] S. R. Buss and T. Pitassi. Resolution and the weak pigeonhole principle. In *Computer Science Logic*, pages 149–156, 1997.

[7] S. R. Buss and G. Turán. Resolution proofs of generalized pigeonhole principles. *Theoret. Comput. Sci.*, 62:311–317, 1988.

[8] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Perspectives in Mathematical Logic Series. Springer-Verlag, Berlin, 1993.

[9] J. Krajíček. Lower bounds to the size of constant-depth propositional proofs. *J. Symbolic Logic*, 59:73–86, 1994.

[10] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1995.

[11] J. Krajíček. On the weak pigeonhole principle. Manuscript, August 1999.

[12] J. Krajíček. Seminar notes (15.11.99). Typeset page, November 1999.

[13] J. Krajíček, P. Pudlák, and A. Woods. Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms*, 7:15–39, 1995.

[14] A. J. Macintyre. The strength of weak systems. In *Logic, Philosophy of Science and Epistemology: Proceedings 11th International Wittgenstein Symposium, Kirchberg/Wechsel, Austria, 1986*, pages 43–59. Hölder-Pichler-Tempsky, Vienna, 1987.

[15] J. B. Paris and A. J. Wilkie. Counting problems in bounded arithmetic. In *Methods in Mathematical Logic: Proceedings of the 6th Latin American Symposium on Mathematical Logic 1983*, volume 1130 of *Lectures Notes in Mathematics*, pages 317–340, 1985.

[16] J. B. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *J. Symbolic Logic*, 53:1235–1244, 1988.

[17] T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Comput. Complexity*, pages 97–140, 1993.

[18] T. Pitassi, R. Raz. Lower bounds for regular resolutions proofs of the weak pigeonhole principle. Proceedings from STOC 2001.

[19] R. Raz. Lower bounds for resolution proofs of the weak pigeonhole principle. Manuscript, February 2001.

[20] A. A. Razborov. Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic. *Izvestiya of the R.A.N.*, 59(1):201–224, 1995.

[21] A. A. Razborov and S. Rudich. Natural proofs. *J. Comput. System Sci.*, 55:24–35, 1997.

[22] A. A. Razborov, A. Wigderson, and A. C. 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.

[23] S. Riis. A complexity gap for tree-resolution. Manuscript, September 1999.

[24] A. J. Wilkie. Some results and problems on weak systems of arithmetic. In A. Macintyre, L. Pacholski, and J. Paris, editors, *Logic Colloquium '77*, pages 237–248. North-Holland, 1978.