Abstract

We construct quasipolynomial-size proofs of the propositional pigeonhole principle in the deep inference system KS, addressing an open problem raised in previous works and matching the best known upper bound for the more general class of monotone proofs.

We make significant use of monotone formulae computing boolean threshold functions, an idea previously considered in works of Aterias et al. The main construction, monotone proofs witnessing the symmetry of such functions, involves an implementation of merge-sort in the design of proofs in order to tame the structural behaviour of atoms, and so the complexity of normalization. Proof transformations from previous work on atomic flows are then employed to yield appropriate KS proofs.

As further results we show that our constructions can be applied to provide quasipolynomial-size KS proofs of the parity principle and the generalized pigeonhole principle. These bounds are inherited by the class of monotone proofs, and we are further able to construct \( n^{O(\log \log n)} \)-size monotone proofs of the weak pigeonhole principle with \( (1 + \varepsilon)n \) pigeons and \( n \) holes for \( \varepsilon = 1/\log^k n \), thereby also improving the best known bounds for monotone proofs.

1. Introduction

The pigeonhole principle states that if \( m \) pigeons are sitting in \( n \) holes, and \( m > n \), then two pigeons must be in the same hole. It can be expressed in propositional logic as follows,

\[
\phi \equiv \bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} p_{ij} \rightarrow \bigvee_{j=1}^{m-1} \bigvee_{j'=i+1}^{m} p_{ij} \land p_{ij'}
\]

where \( p_{ij} \) should be interpreted as “pigeon \( i \) sits in hole \( j \)”. This encoding forms a class of propositional tautologies, for \( m > n \), that has become a benchmark in proof complexity [24]. For the case of \( m = n + 1 \) many propositional proof systems, such as the cut-free sequent calculus, Resolution and bounded-depth Frege, only have proofs of size exponential in \( n \) [21] [23], whereas small proofs (of size polynomial in \( n \)) have been constructed for Frege systems, and so also sequent calculi with cut [11].

This paper presents a novel proof structure for \( \text{PHP}_n^m \), inspired by previous works of Aterias et al. [2] [3], implemented in a presentation of monotone proofs [4] as branching derivations [18]. Consequently, we obtain quasipolynomial-size proofs of \( \text{PHP}_n^{n+1} \) in the minimal deep inference system for propositional logic, KS.

This answers questions previously raised in [9] [15] [25] [13] on the complexity of KS proofs of \( \text{PHP}_n^m \) by matching the best known bound for the more general class of monotone proofs [2].

By making certain generalizations we are able to apply our methods to obtain quasipolynomial-size KS proofs of the parity principle and the generalized pigeonhole principle, bounds that are inherited by the class of monotone proofs. Finally we show that our proof structure can be applied to yield \( n^{O(\log \log n)} \)-size monotone proofs of \( \text{PHP}_n^{n+1+\varepsilon} \) where \( \varepsilon = 1/\log^k n \) for \( k > 1 \), significantly improving the best known bound of \( n^{O(\log n)} \) inherited from proofs of \( \text{PHP}_n^{n+1} \) in [2] [7]. We point out that this is the first example where considerations in the complexity of deep inference have yielded improved results for more mainstream systems in proof complexity.

Deep inference systems for classical propositional logic were introduced by Guglielmi et al. [15] [8] and, despite significant progress in recent years on the complexity of deep inference, the classification of the system KS remains open.

In [9] it was shown that KS polynomially simulates (tree-like) cut-free sequent calculus but not vice-versa. This result was strengthened in [13] where it was shown that KS polynomially simulates certain fragments of Resolution and dag-like cut-free sequent calculus, and it was also shown that these systems, as well as bounded-depth Frege systems, cannot polynomially simulate KS. This work made significant use of proof transformations induced by certain graph rewriting techniques from [16]. In this way the complexity of normalizing a monotone proof to a KS proof was reduced to counting the number of paths in the associated atomic flow, the graph obtained by tracing the journey of each atom through the proof.

It was asked in [25] and [9] whether polynomial-size proofs of \( \text{PHP}_n^m \) exist in KS, and in [25] it was conjectured that no polynomial-size proofs exist. On the other hand, in [13] Jelánek gives proofs in an extended system of weaker variants of the pi-

1 Notice that the above formula allows the mapping from pigeons to holes to be many-many. Additional restrictions can be placed on the mapping, demanding that it is a function or that it is onto, resulting in a logically weaker formula, but here we consider only the version above.

2 A monotone proof is a proof in the sequent calculus free of negation-steps.

3 A quasipolynomial in \( n \) is a function of size \( n^{\log^{\Theta(1)} n} \).

4 This result also supports the more general conjecture in the community that the class of monotone proofs polynomially simulates Frege systems [3] [19] [20].
geonhole principle, where the mapping from pigeons to holes is required to be functional or onto, which normalize to KS proofs of polynomial size [13]. He uses an elegant black-box construction relying on the existence of the aforementioned Frege proofs, although he notes that this method does not seem to generalize to PHPm.

In this work we rely heavily on a propositional encoding of threshold functions, yielding formulae that count how many of their arguments are true, and our construction is inspired by the monotone proofs of PHPm given by Atserias et al. [2]. They use the same threshold formulae as us but our main construction, short proofs that permute the arguments of a threshold formula, is considerably more involved than the analogous construction in their paper due to technicalities of the weaker system KS. The tradeoff is that this more sophisticated proof structure enables us to later achieve the aforementioned improvement in upper bounds on the size of monotone proofs for the weak pigeonhole principle.

In [2] simple proofs are provided for each transposition, whence the result follows since each permutation can be expressed as a product of at most polynomially many transpositions, resulting in monotone proofs whose atomic flows have polynomial length. However due to this length bound such proofs normalize to exponential-size KS proofs under the aforementioned transformations. Instead we notice in Sect. 3 that the specific permutation required, corresponding to the transposition of a matrix, has a particularly simple decomposition into logarithmically many interleavings, which we implement as monotone proofs whose atomic flows have polylogarithmic length and hence normalize to KS proofs in quasipolynomial time.

In Sect. 4 we generalize this construction by noticing that any permutation can be decomposed into a product of logarithmically many riffle shuffles; this is equivalent to the action of applying merge-sort to the inverse of a permutation. In Sect. 5 we show that these techniques can be applied to yield the aforementioned proofs of the parity principle, generalized pigeonhole principle and the weak pigeonhole principle. In the final result the polylogarithmic suffix of the parity principle, generalized pigeonhole principle and the weak pigeonhole principle, where the mapping from pigeons to holes is required to be functional or onto, which normalize to KS proofs of polynomial size [13]. He uses an elegant black-box construction relying on the existence of the aforementioned Frege proofs, although he notes that this method does not seem to generalize to PHPm.

In Sect. 4 we generalize this construction by noticing that any permutation can be decomposed into a product of logarithmically many riffle shuffles; this is equivalent to the action of applying merge-sort to the inverse of a permutation. In Sect. 5 we show that these techniques can be applied to yield the aforementioned proofs of the parity principle, generalized pigeonhole principle and the weak pigeonhole principle. In the final result the polylogarithmic suffix of the parity principle, generalized pigeonhole principle and the weak pigeonhole principle, where the mapping from pigeons to holes is required to be functional or onto, which normalize to KS proofs of polynomial size [13]. He uses an elegant black-box construction relying on the existence of the aforementioned Frege proofs, although he notes that this method does not seem to generalize to PHPm.

For this reason we generally omit internal brackets of a formula, under associativity, as well as external brackets. For clarity we also use square brackets [.] for disjunctions and round ones (.) for conjunctions.

**Remark 1** (Equality). Equality of formulae \(=\), as defined above, is usually implemented as an inference rule in deep inference. It is decidable in polynomial time [9], and whether it is implemented as an inference rule or equivalence relation is purely a matter of convention. Nonetheless we sometimes use it as a ‘fake’ inference rule, to aid the reader.

It will sometimes be convenient to represent the arguments of a boolean function as a vector or matrix of atoms. However the order in which the atoms are to be read is sensitive, and so we introduce the following notation.

**Notation 2** (Vectors and Matrices of Variables). We use bold lowercase letters \(\mathbf{a}, \mathbf{b}, \ldots\) to denote (row-)vectors of atoms and bold uppercase letters \(\mathbf{A}, \mathbf{B}, \ldots\) to denote matrices of atoms. Vectors are read in their natural order, and we associate a matrix with the vector obtained by reading it rows-first. In this way the transpose of a matrix is equivalent to the vector obtained by reading it columns-first.

The notation \((\mathbf{a}, \mathbf{b})\) denotes the horizontal concatenation of vectors \(\mathbf{a}\) and \(\mathbf{b}\), and compound matrices are similarly written in the usual way. The notation \((\mathbf{a}_1, \ldots, \mathbf{a}_n)\) denotes the vector \((\mathbf{a}_1, \ldots, \mathbf{a}_n)\) of \(\mathbf{a}_i\)s.

**Definition 3** (Rules and Systems). An inference rule is a binary relation on formulae decidable in polynomial time, and a system is a set of rules. We define the deep inference system SKS as the set of all inference rules in Fig. 1 and also the subsystem KS = \(\{ai\}_i\\downarrow, aw_i\downarrow, ac\downarrow, s, m\). Note in particular the distinction between variables for atoms and formulae.

**Remark 4.** It is worth pointing out that the formulation of deep inference with units is very convenient for proof-theoretic manipulation of derivations, and we exploit this throughout. However we could equally formulate our systems without units with no significant change in complexity; this approach is taken in [25] and the equivalence of these two formulations is shown in [12].

**Definition 5** (Proofs and Derivations). We define derivations, and premiss and conclusion functions, \(pr, cn\) resp., inductively:

1. Each formula \(A\) is a derivation with premiss and conclusion \(A\).
2. If \(\Phi, \Psi\) are derivations and \(\star \in \{\land, \lor\}\) then \(\Phi \star \Psi\) is a derivation with premiss \(pr(\Phi) \star pr(\Psi)\) and conclusion \(cn(\Phi) \star cn(\Psi)\).
3. If \(\Phi, \Psi\) are derivations and \(\rho \vdash_{\Phi} \Psi\) is an instance of a rule \(\Phi \vdash_{\Psi}\) then \(\rho \vdash_{\Psi}\) is a derivation with premiss \(pr(\Phi)\) and conclusion \(cn(\Psi)\).

If \(pr(\Phi) = \top\) then we call \(\Phi\) a proof. If \(\Phi\) is a derivation where all inference steps are instances of rules in a system \(S\) with premiss \(A\), conclusion \(B\), we write \(\vdash_{S} A \rightarrow B\). Furthermore, if \(A = \top\), i.e. \(\Phi\) is a proof in a system \(S\), we write \(\vdash_{S} B\).

We extend our structural rules beyond atoms, to general formulae.

**Proposition 6** (Generic Rules). Each rule below has polynomial-size derivations in the system containing \(s, m\), and its respective
### Atomic structural rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{ai}^\downarrow \hspace{1em} \vdash \hspace{1em} A \lor \neg A$</td>
<td>$A \lor \neg A$</td>
</tr>
<tr>
<td>$\text{aw}^\downarrow \hspace{1em} \vdash \hspace{1em} a$</td>
<td>$a$</td>
</tr>
<tr>
<td>$\text{ac}^\downarrow \hspace{1em} \vdash \hspace{1em} a \lor a$</td>
<td>$a \lor a$</td>
</tr>
</tbody>
</table>

### Logical rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \land [B \lor C]$</td>
<td>$(A \land B) \lor C$</td>
</tr>
<tr>
<td>$A \lor [B \land C]$</td>
<td>$[A \lor B] \land C$</td>
</tr>
</tbody>
</table>

### Atomic flows and various rewriting systems on them were introduced formally in [16].

We emphasize that it is the existence of an ‘intermediate’ formula in normal derivations, e.g. $B$ in the proof above, that allows us to isolate all the $\uparrow$ steps and flip them into $\downarrow$ steps, resulting in a KS-proof. If we started with an arbitrary monotone derivation there may be no such formula, and so any choice of an intermediate formula would also flip some $\downarrow$ steps into $\uparrow$ steps.

### 2.3 Atomic Flows and Normalization

We are particularly interested in those monotone derivations that can be efficiently transformed to normal ones. A thorough analysis of the complexity of such transformations is carried out in [13] in the setting of graph rewriting. We state informally the main concepts and results here.

**Definition 10 (Atomic Flows and Dimensions).** The atomic flow, or simply flow, of a monotone derivation is the vertically directed graph obtained by tracing the paths of each atom through the derivation, designating the creation, destruction and duplication of atom occurrences by the following nodes:

- **Creation:** $\text{aw}^\downarrow \hspace{1em} \vdash \hspace{1em} a$ $\rightarrow \begin{array}{c} \downarrow \text{aw}^\downarrow \hspace{1em} \vdash \hspace{1em} a \lor a \\ \text{ac}^\downarrow \hspace{1em} \vdash \hspace{1em} a \land a \end{array}$
- **Duplication:** $\text{aw}^\uparrow \hspace{1em} \vdash \hspace{1em} a$ $\rightarrow \begin{array}{c} \uparrow \text{aw}^\uparrow \hspace{1em} \vdash \hspace{1em} a \lor a \\ \text{ac}^\uparrow \hspace{1em} \vdash \hspace{1em} a \land a \end{array}$

### Figure 1. Rules of the deep inference system SKS.

The significance of normal derivations is that they can be efficiently transformed into KS-proofs of the implication they derive, as demonstrated in the following proposition.

**Proposition 9.** A normal derivation $\Phi$ can be transformed into a KS-proof of $A \lor C$.

Proof Sketch. Define the derivation $\Phi \uparrow \{\text{aw}^\uparrow, \text{ac}^\uparrow, s, m\}$ by flipping the $\uparrow$ steps upside-down, replacing every atom with its dual, $\land$ for $\lor$ and vice-versa. $\text{aw}^\uparrow$-steps become $\text{aw}^\downarrow$-steps, $\text{ac}^\uparrow$-steps become $\text{ac}^\downarrow$-steps and $s$ and $m$ steps remain valid. Now construct the required $\Phi$ derivation:

- $\text{ai}^\downarrow \hspace{1em} \vdash \hspace{1em} A$
- $\text{aw}^\downarrow \hspace{1em} \vdash \hspace{1em} a$
- $\text{ac}^\downarrow \hspace{1em} \vdash \hspace{1em} a \lor a$

We often use these ‘generic’ rules in proof constructions, which should be understood as abbreviations for the derivations mentioned above.

**Definition 7 (Complexity).** The size of a derivation $\Phi$, denoted $|\Phi|$, is the number of atom occurrences in it. For a vector $\alpha$ or matrix $A$, let $|\alpha|$, $|A|$ denote its number of elements, respectively.

We will generally omit complexity arguments when they are routine, for convenience. However we outline the main techniques used to control complexity in the following sections.
We do not have nodes for s and m steps since they do not create, destroy or duplicate any atom occurrences, and we generally consider flows equivalent up to continuous deformation preserving the vertical order of edges.

The size of a flow is its number of edges. The length of a flow is the maximum number of times the node type changes in a (vertically directed) path. The width of a flow is the maximum number of input or output edges in a subgraph of a connected component.

For intuition, the width of a flow can be thought of as a measure of how much a configuration of ac↑ nodes increases the number of edges in a connected component before a configuration of ac↓ nodes decreases it.

**Example 11.** We give an example of a monotone derivation and its flow below:

\[
\begin{array}{c}
\text{ac}↑ \quad \text{a} \lor \text{a} \\
\text{ac↓} \quad \text{a} \land \text{a} \\
\hline
\text{m} \quad \text{a} \land \text{a} \lor \text{aw}↓ \\
\hline
\text{a} \lor \text{aw}↓ \\
\hline
\text{b} \\
\hline
\text{a} \\
\hline
\text{a} \lor \text{aw}↑ \\
\hline
\text{a} \land \text{a} \\
\hline
\text{a} \\
\hline
\end{array}
\]

The flow has length 3, measured from the top-right aw↓ node to the bottom-left ac↑ node, and width 4, measured either as the outputs of the two top ac↑ nodes or the inputs of the two bottom ac↓ nodes.

**Observation 12.** A normal derivation has flow length 1.

**Theorem 13 (Normalization).** A monotone derivation Φ whose flow has width w and length l can be transformed into a normal derivation of size |Φ| · w^{l+O(1)}, preserving premises and conclusion.

While the proof of the above theorem can be found in [13], we outline the main ideas to give the reader an intuition of the argument.

**Proof Sketch.** The graph rewriting rules in Fig. 2 induce transformations on monotone derivations by consideration of the corresponding rule permutations; note that, due to atomicity of the structural rules, permutations with logical steps are trivial. The system is terminating and the flows of normal derivations are all normal forms of this system. Each rewrite step preserves the number of maximal paths between pending edges, and a normal derivation has size polynomial in this measure.

Consequently the complexity of normalizing a monotone derivation is polynomial in its size and the number of maximal paths in its flow, and this is estimated by the given bound.

Notice, in particular, that any rewrite derivation on atomic flows acts independently on different connected components. Therefore the complexity of normalization is determined by the structural behaviour of individual atoms - there is no interaction between distinct atoms during normalization.

Finally, most of the proofs in this work are inductions, and for the base cases it will typically suffice to build any monotone proof of a single formula or simple class of formulae, since we are interested in how the size (or width, length) of the proofs grow and not their initial values. For this reason, the following result will be useful, and we implicitly assume it when omitting base cases of inductions.

**Proposition 14 (Monotone Implicational Completeness).** Let A, B be negation-free formulae such that A → B is valid. Then there is a monotone derivation \( \frac{A}{B} \).

**Proof Sketch.** Construct a disjunctive normal form \( A' \) of \( A \) and conjunctive normal form \( B' \) of \( B \) by distributivity. Note that all distributivity laws are derivable by Dfn. 19 and duality, so there are monotone derivations \( \parallel \) and \( \parallel \). Clearly each conjunction of \( A' \) logically implies each disjunction of \( B' \) and so there must be derivations in \( \{ \text{aw}↓, \text{aw}↑ \} \) witnessing this fact. Using these derivations and applying \( \parallel \) appropriately we can construct a monotone derivation \( \parallel \), whence the result follows by sequential composition of these derivations.

By appealing to Thm. 13 we then obtain the following result.

**Corollary 15.** Normal derivations are monotone implicationally complete.

### 3. Short Proofs of the Pigeonhole Principle

Throughout this section the variables \( m \) and \( n \) are powers of 2 and \( m \leq n \). All proofs in this section are monotone unless otherwise mentioned.

#### 3.1 Threshold Formulae and Permutations

**Threshold functions** are a class of boolean functions \( \text{TH}_k^n : \{0,1\}^n \rightarrow \{0,1\} \) by \( \text{TH}_k^n(\sigma_1 \cdots \sigma_n) = 1 \) just if \( \sum_{i=1}^n \sigma_i \geq k \).

In this section we define quasipolynomial-size monotone formulae computing such functions and construct derivations whose
flows have length $\log^{O(1)} n$ and width $O(n)$ that conduct certain permutations on the arguments of such formulae.

**Definition 16 (Threshold Formulae).** We define the formulae,

$$\text{th}_k^n(a) := \begin{cases} r & k = 0 \\ a & k = 1 \\ \bot & k > 1 \end{cases}$$

$$\text{th}_b^n(a, b) := \bigvee_{i+j=k} \text{th}_i^n(a) \land \text{th}_j^n(b)$$

for vectors $a, b$ of length $n$.

**Observation 17.** $\text{th}_k^n$ computes the threshold function $\text{TH}_k^n$, and has size $O(n \log n)$ and depth $O(\log n)$.

**Definition 18 (Interleaving).** For $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ let $a \parallel b$ denote the interleaving of $a$ with $b$: $(a_1, b_1, \ldots, a_n, b_n)$.

More generally, we denote by $a \parallel_m b$ the $m$-interleaving:

$(a_1, \ldots, a_m, b_1, \ldots, b_m, \ldots, a_{n-m+1}, \ldots, a_n, b_{n-m+1}, \ldots, b_n)$

**Definition 19 (Distributivity).** We define distributivity rules as abbreviations for the following derivations:

$$\text{dist}^\uparrow: \begin{pmatrix} A \to B \land A \lor C \\ (A \land B) \lor (A \land C) \end{pmatrix}$$

$$\text{dist}^\downarrow: \begin{pmatrix} c \land A \lor (A \land C) \\ (A \land B) \land (A \lor C) \end{pmatrix}$$

**Lemma 20.** There are monotone derivations,

$$\text{th}_b^n(a, b)$$

whose flows have length $O(\log n)$ and width $O(n)$.

**Proof.** We use the following identity:

$$(a, b) \parallel_m (c, d) = (a \parallel_m c, b \parallel_m d)$$

We give an inductive step from $n$ to $2n$ in Fig. 3 where derivations marked $IH$ are obtained by the inductive hypothesis.

The dist $\uparrow$ steps duplicate each atom at most $r$ times and so, analyzing the associated flow, each inductive step adds $O(r)$ configurations of $ac\uparrow$ and $ac\downarrow$ nodes of width $O(r)$ on top of $O(r)$ copies of the inductive hypothesis in parallel. The induction terminates in $\log_2 n$ steps, whence the bound on length is obtained.

**Observation 21.** For matrices $B$ and $C$ of equal dimensions we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^\top = \begin{pmatrix} A^\top & C^\top \\ B^\top & D^\top \end{pmatrix}$$

Recall that a matrix of atoms is equivalent to the vector obtained from a rows-first reading of it.

**Theorem 22 (Transposition).** There are monotone derivations,

$$\text{th}_b^n(X)$$

$$\text{th}_b^n(X^\top)$$

whose flows have length $O(\log^2 n)$ and width $O(n)$.

**Proof.** Let $A, B, C, D$ be the four quadrants of $X$. We give an inductive step from $n$ to $2n$,

$$\text{th}_b^{2n}(A, B) \lor \text{th}_b^{2n}(C, D)$$

$$\text{th}_b^n(A^\top, B^\top) \land \text{th}_b^n(C^\top, D^\top)$$

where the derivations marked $IH$ are obtained by the inductive hypothesis and Obs. 21 and the derivation marked ‘interleave’ is obtained by applying Lemma 20 to interleave the rows of the two matrices.

Analyzing the associated flow, each inductive step adds an interleaving below $O(k)$ copies of the inductive hypothesis in parallel, thereby adding $O(\log n)$ to the length and maintaining a width of $O(n)$, by Lemma 20. The induction terminates in $O(\log n)$ steps, whence the upper bound on length is obtained.

### 3.2 From Threshold Formulae to the Pigeonhole Principle

The previous section showed that there are ‘short’ derivations transposing a matrix of arguments of a threshold formula. We show here how such derivations are used to obtain quasipolynomial-size proofs of the pigeonhole principle.

In this section almost all derivations are normal, so we omit their flows and complexity analysis.

**Definition 23 (Pigeonhole Principle).** We define the following:

$$\text{LPHP}_n := \bigwedge_{i=1}^n \bigvee_{j=1}^{n-1} p_{ij}$$

$$\text{RPHP}_n := \bigvee_{j=1}^{n-1} \bigwedge_{i=1}^n \bigvee_{i' = i+1}^n (p_{i'j} \land p_{ij})$$

$$\text{PHP}_n := \text{LPHP}_n \to \text{RPHP}_n$$

**Definition 24.** Let $\perp_{mn}$ be the $(m \times n)$ matrix with the constant $\perp$ at every entry. Define $P_n = (\perp_{n1}) \perp_{1n}$, with $i, j$ ranging as in Dfn. 23 i.e. $P_n$ is obtained by extending $(p_{ij})$ with an extra column of $\perp$-entries, so that it is a square matrix.

Our aim in this section is to prove the following theorem, from which we can extract proofs of $\text{PHP}_n$ in KS by the results in earlier sections.

**Theorem 25.** There are normal derivations,

$$\text{LPHP}_n$$

$$\text{th}_b^n(P_n)$$

$$\text{RPHP}_n$$

of size $n^{O(\log n)}$.

Before we can give a proof, we need some intermediate results. It should be pointed out that similar results were provided in [2] for the monotone sequent calculus, which could be translated to deep inference by [7] [18], but we include them for completeness. Indeed, similar results appeared in [10]. These intermediate results are fairly routine, and there is nothing intricate from the point of view of complexity.
Proposition 26. For \( l \geq k \) there are normal derivations, \( th^n_i(a) \)
\[ th^n_i(a) \] of size \( n^{O(\log n)} \).

Proof. We give an inductive step from \( n \) to \( 2n \),
\[ \begin{align*}
    th^{2n}_{i+j}(a, b) &= \bigvee_{i+j=1} \left( th^n_i(a) \land th^n_j(b) \right) \\
    th^{2n}_{i+j}(a, b) &= \bigvee_{i+j=1} \left( th^n_i(a) \land th^n_j(b) \right)
\end{align*} \]
where \( i' \) and \( j' \) are chosen such that \( i' \leq i, j' \leq j \) and \( i' + j' = k \), and derivations marked \( IH \) are obtained by the inductive hypothesis.

Lemma 27 (Evaluation). There are normal derivations,
\[ th^n_m(a, b) \]
of size \( n^{O(\log n)} \).

Proof. Notice that if \( i + j = r + s \) then \( i > r \) or \( j > s \). We give a construction in Fig. 3 where \( \Phi \) and \( \Psi \) denote derivations obtained by Prop. 26.

Lemma 28. For vectors \( a^1, \ldots, a^m \) of atoms there are normal derivations,
\[ \bigvee_{r=1}^m th^n_r(a^r), \bigvee_{r=1}^m th^n_r(a^r) \]
of size \( n^{O(\log n)} \).

Figure 3. Interleaving the arguments of a threshold formula.

Proof. By induction on \( m \). Simply apply \( = \) and \( \land \) to fill out the formula.

We are now in a position to prove Thm. 25.

Proof Sketch of Thm. 25. Repeatedly apply Lemma 27 to \( th^n_i(P^i_r) \), always setting \( r = s \) or \( r = s + 1 \), until a disjunction of threshold formulae with \( n \) arguments each is obtained. By the ordering of the atoms in \( P^n_r \) these threshold formulae will have as arguments \( (p_j)_{j=1}^1 \) for some \( j \), or all \( \perp \); in the latter case any such formula is equivalent to \( \perp \), since the threshold will be at least 1.

In the former case, by the choice of \( r \) and \( s \) at each stage, we have that the threshold of each of these formulae is at least 2. From here Prop. 26 can be applied so that all thresholds are 2, whence \( \text{RPHP}_n \) can be easily derived.

For the other direction, construct each variable \( p_{ij} \) as a threshold formula \( th^n_i(P_{ij}) \) and apply Lemma 28 to obtain a derivation from \( \text{LPHP}_n \) to \( th^n_i(P) \).

In both cases normality is established by the normalization procedure of Thm. 13. We have chained together finitely many normal derivations so the length of the associated flows is bounded by a constant, whence the upper bound on size is obtained.

Theorem 29. There are normal derivations,
\[ \text{LPHP}_n \]
of size \( n^{O(\log^2 n)} \).

Proof. By Thms. 22 and 25 there are monotone derivations with same premiss and conclusion of length \( O(\log^2 n) \) and width \( O(n) \). The result then follows by Thm. 13.

Corollary 30. There are KS proofs of PHP \(_n \) of size \( n^{O(\log^2 n)} \).

Proof. By Prop. 9.
3.3 The Case when \( n \) is not a Power of 2

Though we have assumed that \( n \) is a power of 2 throughout this section, the proof is actually sufficient for all \( n \), as pointed out in [2].

**Definition 31.** For \( r \leq s \) given, define \( \text{LPHP}_s(r) \) by substituting \( \perp \) for every atom \( p_{ij} \) where \( i > r \) or \( j > r \). Define \( \text{RPHP}_s(r) \) analogously.

**Observation 32.** For all \( r < s \) we have that \( \text{LPHP}_s(r) = \text{LPHP}_s \) and \( \text{RPHP}_s(r) = \text{RPHP}_s \). Consequently a proof of \( \text{PHP}_s \) is just a proof of \( \text{PHP}_n \), where \( n \) is the power of 2 such that \( r \leq n < 2r \).

4. Arbitrary Permutations

Interleavings by themselves do not form a generating set for the symmetric group, and so cannot be used to generate derivations for arbitrary permutations of arguments of threshold formulae. However a generalization of them, corresponding to the set of riffle shuffles on a deck of cards, do form such a set. In this section we show how they may be used to generate arbitrary permutations on the arguments of threshold formulae.

The proofs in this section are similar to those in Sect. [3] and so we omit them for brevity, instead providing the general proof structure as intermediate results.

Recall that our original definition of threshold formulae used a symmetric divide-and-conquer strategy, generated from a complete binary tree in the natural way. In this section it will be useful to have a more general definition of threshold formulae, based on any tree decomposition of the divide-and-conquer strategy.

Throughout this section we assume all trees are binary.

**Definition 33.** For a tree \( T \), let \( d(T) \) denote its depth, \( l(T) \) its number of leaves and \( |T| \) denotes its number of nodes. For a binary tree \( T \), let \( T_0 \) denote its left subtree (from the root) and \( T_1 \) its right. Thus any string \( \sigma \in \{0, 1\}^n \) determines a unique subtree \( T_\sigma \) of \( T \), for \( k \leq d(T) \).

**Definition 34 (General Threshold Formulae).** For a binary tree \( T \) and vectors \( \mathbf{a}, \mathbf{b} \) with \( |\mathbf{a}| = l(T_0), |\mathbf{b}| = l(T_1) \), define

\[
\text{th}_k^T(\mathbf{a}, \mathbf{b}) = \bigvee_{i+j=k} \text{th}^T_{i}(\mathbf{a}) \land \text{th}^T_{j}(\mathbf{b})
\]

with the base case the same as in Dfn. [16].

The following proposition gives an estimate of the size of these threshold formulae.

**Proposition 35.** For a binary tree \( T \), \(|\text{th}_k^T(\mathbf{a})| = l(T)^{O(d(T))}\).

\*Recall that formulae are equivalent up to =.

**Proof.** In the worst case, every level of the binary tree is full, whence the bound is obtained by Obs. [17].

What we define as a shuffle below corresponds to the common riffle method of shuffling a deck of cards: cut the deck anywhere, partitioning it into a left and right part, and then interleave these in any way, maintaining the relative order of cards in either partition. Under this analogy each card of the deck will correspond to a leaf of the tree determining a threshold formula.

**Definition 36 (Cuts and Shuffles).** A cut of a vector \( (a_1, \ldots, a_n) \) is a pair \( \{(a_1, \ldots, a_m), (a_{m+1}, \ldots, a_n)\} \). A riffle shuffle, or simply shuffle, of length \( n \) is a string \( \sigma \in \{0, 1\}^n \).

For a vector \( \mathbf{a} \) and shuffle \( \sigma \) of length \( n = |\mathbf{a}| \) we write \( \sigma(\mathbf{a}) \) to denote the following action of \( \sigma \) on \( \mathbf{a} \): let \( \Sigma_i \) denote the number of 1s in \( \sigma_1 \cdots \sigma_i \), so that \( i - \Sigma_i \) is the number of 0s in \( \sigma_1 \cdots \sigma_i \), and \( k = \Sigma_n \) is the number of 1s in \( \sigma \); we give a componentwise definition of \( \sigma(\mathbf{a}) \):

\[
(\sigma(\mathbf{a}))_i = \begin{cases} a_{i-\Sigma_i} & \sigma_i = 0 \\ a_{n-k+i-\Sigma_i} & \sigma_i = 1 \end{cases}
\]

In the above definition, one should think of \( \sigma \) determining a cut \( \{(a_1, \ldots, a_{n-k}), (a_{n-k+1}, \ldots, a_n)\} \), and where each bit indicates which side of the cut the next element of \( \sigma(\mathbf{a}) \) comes from.

**Lemma 37 (Cutting).** For any tree \( T \) and cut \( \{(a, b)\} \) there are trees \( S_0, S_1 \) with \( d(S_0), d(S_1) \leq d(T) \) such that there are monotone derivations,

\[
\text{th}_k^T(\mathbf{a}, \mathbf{b}) = \bigvee_{i+j=k} \text{th}^{S_0}_i(\mathbf{a}) \land \text{th}^{S_1}_j(\mathbf{b})
\]

whose flows have length \( O(d(T)) \) and width \( O(l(T)) \).

**Proof of Lemma 37.** By induction on \( l(T) \). Without loss of generality, suppose \( b \) is contained entirely in \( T_1 \) (otherwise, \( a \) is contained entirely in \( T_0 \) and the argument is symmetric). We construct the
following derivation,

\[
\begin{align*}
\text{th}_{s'}^{n}(a, b) = & \bigvee_{i+j=m} \left( \text{th}_{s'}^{n}(a^1) \land \text{th}_{i}^{n}(b) \right) \\
\text{th}_{i+j=m}^{n}(a^2) \land \text{th}_{j}^{n}(b) \\
= & \bigvee_{i+j=m} \left( \text{th}_{i}^{n}(a^1) \land \text{th}_{j}^{n}(b) \right)
\end{align*}
\]

where the derivation marked \( IH \) is obtained by the inductive hypothesis.

\( \square \)

**Lemma 38 (Shuffling).** Let \( S \) be a tree and \( \sigma \) a shuffle of length \( l(S) \). There is a tree \( T \) with \( d(T) = O(d(S)) \) and monotone derivations,

\[
\text{th}_{s'}^{n}(\nu), \quad \text{th}_{\sigma(\nu)}^{n}
\]

whose flows have length \( O(d(S)^2) \) and width \( O(l(S)) \).

**Proof of Lemma 38** By induction on \( l(S) \), we give the inductive step in Fig. 3. The construction we set \( \nu = (\nu_1, \nu_2, \nu_3) \), defined by \( I(S_0) \) and \( I(S_1) \), and \( \sigma(\nu) = (\nu_2, \nu_3) \). The argument is analogous to the one in Lemma 3 with derivations marked `cut' obtained from Lemma 37 and derivations marked \( IH \) obtained from the inductive hypothesis.

In particular the cuts are chosen such that \( |b| = |c| \) and so that are shuffles \( \sigma_1, \sigma_2 \) with \( \sigma(\nu) = (\sigma_1(a, b, c), \sigma_2(b', c', d)) \)

\( \square \)

**Theorem 39 (Merge Sort).** For any tree \( S \) and permutation \( \pi \) on \( \{1, \ldots, l(S)\} \) there is a tree \( T \) with \( d(T) = O(d(S)) \) and monotone derivations,

\[
\text{th}_{s'}^{n}(a_\pi)_{i=1}^{n} = \text{th}_{\sigma(\pi)}^{n}
\]

whose flows have length \( O(d(S)^3) \) and width \( O(l(S)) \).

**Proof of Thm. 39** By induction on \( l(S) = l(T) \). We construct the following derivation,

\[
\begin{align*}
\bigvee_{i+j=m} \left( \text{th}_{s'}^{n}(a_\pi)_{i=1}^{m} \land \text{th}_{i}^{n}(b) \right) \land \text{th}_{j}^{n}(b) \\
\text{shuffles} \quad \text{th}_{i}^{n}(a^1) \land \text{th}_{j}^{n}(a^2) \\
\text{th}_{\sigma}^{n}(a_\pi)_{i=1}^{n}
\end{align*}
\]

where the derivations marked \( IH \) are obtained from the inductive hypothesis, sorting the inputs of the left and right subtrees of \( S \) to vectors \( a^1 \) and \( a^2 \) resp., and the derivation marked `shuffle', obtained from Lemma 38, carries out the unique shuffle on \( (a^1, a^2) \) resulting in a completely sorted vector.

\( \square \)

**Proposition 40 (Repartitionings).** For trees \( S, T \) with the same number of leaves there are monotone derivations,

\[
\text{th}_{\sigma}^{n}(a), \quad \text{th}_{\sigma}^{n}(a)
\]

whose flows have length \( O(d(S)^2) \) and width \( O(l(S)) \).

**Proof of Prop. 40** By induction on \( l(S) = l(T) \). Let \( \{b, c\} \) be the cut of \( \sigma \) such that \( |b| = l(T_0) \) and \( |c| = l(T_1) \). We construct the following derivation,

\[
\text{th}_{\sigma}^{n}(a), \quad \text{cut} \quad \text{th}_{\sigma}^{n}(a)
\]

where the derivation marked `cut' is obtained from Lemma 37 and the derivations marked \( IH \) are obtained from the inductive hypothesis.

\( \square \)

**Corollary 41.** For any tree \( T \) and permutation \( \pi \) on \( \{1, \ldots, l(T)\} \) there are normal derivations,

\[
\text{th}_{\pi}^{n}(a_\pi)_{i=1}^{n}, \quad \text{th}_{\pi}^{n}(a_\pi)_{i=1}^{n}
\]

of size \( l(T)^{O(d(T)^3)} \).

**Proof.** By Thm. 39 Prop. 40 and Thm. 13 

\( \square \)

5. Further Results and Applications

We give some examples of how the techniques developed in previous sections can be applied to yield further results, namely quasipolynomial-size normal proofs of the Generalized Pigeonhole principle and the Parity principle. Both bounds are also inherited for monotone proofs although, while these have not appeared in the literature, we point out that such monotone proofs could also have been constructed using the permutation arguments of Atserias et al. in [2].

More interestingly we provide \( n^{O((\log \log n)^2)} \)-size monotone proofs for the weak pigeonhole principle, with \( (1+\epsilon)n \) pigeons and \( n \) holes for every \( \epsilon = 1/\log l(T)^{1} \) improving the previous best known bound of \( n^{O((\log n)^2)} \) inherited from the proofs of PHP\( n \) given in [2].

5.1 Generalized Pigeonhole Principle

If there are 45 hats that are either red or green, then there must be 23 of the same colour. This exemplifies a generalization of the pigeonhole principle where sufficiently many pigeons may guarantee more than two in some hole [13]. If \( k+1 \) pigeons in some hole are required then \( n(k+1) \) pigeons are necessary, so this principle can be encoded as follows:

\[
\bigwedge_{i=0}^{n} \bigvee_{j=1}^{m} a_{ij} \Rightarrow \bigvee_{i_r, r=1}^{k+1} \bigwedge_{r=1}^{k+1} a_{i_r j}
\]
where

\[ k \]

harder

\[ j \]

The parity principle

5.2 Parity Principle

to this class of tautologies, by the same arguments as in Sect. 3.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.

Figure 5. Riffle shuffling the inputs of a threshold formula.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.

Figure 5. Riffle shuffling the inputs of a threshold formula.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.

Figure 5. Riffle shuffling the inputs of a threshold formula.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.

Figure 5. Riffle shuffling the inputs of a threshold formula.

This formula has size \( O(n^{k+1}) \), polynomial for fixed \( k \). If, however \( k \) is large relative to \( n \), e.g. \( n/2 \) or \( \sqrt{n} \), then one can always express the right hand side using threshold formulae to obtain an encoding of quasipolynomial-size.

It is simple to see that our proofs of PHP, can be generalized to this class of tautologies, by the same arguments as in Sect. 3.

Extended version of paper from CSL-LICS 2014.
bound how much worse the approximation develops as the interleaving and transposition arguments of Sect. 3.1 are applied.

5.3.1 Approximating Threshold Functions

It is not quite correct to call the formulae we define below as \( \varepsilon \)-approximators of threshold functions, since in fact they output incorrectly on a large proportion of inputs. Rather they output 1 just if the actual threshold is within some predetermined factor of the threshold being measured. The tradeoff is that we are able to define monotone formulae that are much smaller than the usual threshold formulae we have used until now.

Definition 42 (Threshold Approximators). Let \(|a| = |b| = n\). We define the \((p, q)\)-approximator \(T_k[p, q]\) of \(\text{TH}_n^k\) as follows,

\[
T_k[p, q](a, b) = \bigwedge_{i+j=p} T_{i,k}^{p,q}(a) \wedge T_{j,k}^{p,q}(b)
\]

where we assume that \(k\) is some power of \(q\) and \(n\) is a power of 2, for example by adding a string of \(T\)s and \(\bot\)s of appropriate format to the arguments.\(^8\)

It is not easy to understand the semantics of these approximators, and in the next section we provide solely proof-theoretic arguments rather than semantic intuition. We do, however, make the following observations, provable by straightforward inductions.

Observation 43. We have the following properties,

1. \(\text{TH}_n^k \Rightarrow T_k[p, q]\) for all \(p < q\).
2. \(T_k[p, q] \Rightarrow \text{TH}_k[p/q \cdot \log n, n] \)
3. \(|T_k[p, q](a)| = O(\log^k n)\)

where \(\Rightarrow\) denotes logical implication.

5.3.2 Manipulating Arguments in Threshold Approximators

In this section we return to the derivations proved in Sect. 3.1 on interleaving and transposing arguments of a formula. Since the approximators we now consider do not exactly compute threshold functions, they are no longer symmetric and so similar derivations cannot be constructed. Rather we show that witnessing certain permutations requires a bounded deterioration in the accuracy of the approximation. Ultimately we will choose an initial approximation that is accurate enough to ensure that this deterioration does not become too excessive.

We first state a basic fact allowing us to infer weaker approximations from stronger ones. The proof is straightforward and follows the same kind of induction argument as previous proofs.

Lemma 44. For \(p \geq p', k \geq k'\) there are normal derivations,

\[
T_{k'}[p', q]\bigl(\{a\}\bigr) \\
T_k[p, q]\bigl(\{a\}\bigr) \\
of size \(p^{O((\log n)^k)}\).
\]

The following is the main result that will control the deterioration in approximation throughout our overall argument.

Lemma 45. There are normal derivations,

\[
T_k[p, q]\bigl(\{a, b, c, d\}\bigr) \\
T_k[p-1, q]\bigl(\{a, b, c, d\}\bigr) \\
of size \(p^{O((\log n)^k)}\).
\]

We first need the following result, whose proof is straightforward.

Proposition 46. For \(x, y \geq 0\), if \((x + y) \in \mathbb{N}\) then \(x + y - \lfloor (\lfloor x \rfloor + \lfloor y \rfloor) \rfloor \leq 1\).

Proof of Lemma \(44\) We construct appropriate derivations in Fig. 6 where,

\[
s' = \lfloor \frac{i + k t}{p} \rfloor \\
t' = \lfloor \frac{i + k t}{p} \rfloor
\]

and,

\[
s' = \lfloor \frac{j p}{j t + j k + t} \rfloor \\
t' = \lfloor \frac{t j p}{j t + j k + t} \rfloor
\]

so we have \(s' + t', i' + j' \geq k' \geq t - 1\) by Prop. \(44\) and also \(i' + j' \leq i s, j' t' \leq j s, k' s' \leq k t, t' \leq k t\), so that the derivations marked ‘decrease’ are obtained by Lemma \(44\).

The following result has proof similar to that of Lemma \(20\) using the above lemma in the inductive steps to measure the deterioration of the approximator.

Proposition 47. There are monotone derivations,

\[
T_k[p, q]\bigl(\{a, b\}\bigr) \\
T_k[p - \log n, q]\bigl(\{a\} \cup \{b\}\bigr)
\]

of size \(p^{O((\log n)^k)}\) whose flows have length \(O((\log n)^k)\) and width \(O(p)\).

The following result has proof similar to that of Thm. \(22\).

Theorem 48. There are monotone derivations,

\[
T_k[p, q]\bigl(\{X\}\bigr) \\
T_k[p - \log n, q]\bigl(\{X'\}\bigr)
\]

of size \(p^{O((\log n)^k)}\) whose flows have length \(O((\log^2 n)^k)\) and width \(O(p)\).

5.3.3 From Approximators to the Weak Pigeonhole Principle

Recall the definition of \(\text{PHP}^m_n\), where \(m\) denotes an arbitrary number of pigeons greater than the number of holes \(n\), and define \(\text{LPHP}^m_n\) and \(\text{RPHP}^m_n\) analogously to Dfn. \(23\). In this section we essentially mimic the results of Sect. 3.2 to complete our proofs of the weak pigeonhole principle.

First we need the following well known result whose proof follows, for example, by consideration of the inclusion-exclusion principle in the binomial expansion.

Proposition 49. For \(\varepsilon \leq 1\) we have that \((1 - \varepsilon)^k \geq 1 - \varepsilon k\).

Proof. Let \(X_0, \ldots, X_{k-1}\) be independent identically distributed Bernoulli random variables with \(\Pr[X_i = 1] = \varepsilon\) and \(\Pr[X_i = 0] = (1 - \varepsilon)\) for each \(i\). Then:

\[
\begin{align*}
(1 - \varepsilon)^k & = \Pr\left[ \bigcap_{i < k} X_i = 0 \right] \text{ by independence.} \\
& = \Pr\left[ \bigcup_{i < k} X_i = 1 \right] \text{ by De Morgan laws.} \\
& = 1 - \Pr\left[ \bigcup_{i < k} X_i = 1 \right] \text{ by complements.} \\
& \geq 1 - \sum_{i < k} \Pr[X_i = 1] \text{ by the union bound.} \\
& \geq 1 - \varepsilon k \quad \square
\end{align*}
\]

The following result has proof similar to that of Thm. \(25\).
of size from Lemmata 50 and 48 we obtain monotone derivations from $q$ to $p$, $\forall x \in \mathbb{N}$.

Proof. We now need to check that $n > \frac{1}{2} \log^{3} n$ and $p = q - 1$. Since $\epsilon > \frac{1}{2}$, there is a trivial derivation from LPHP$_{(1-\epsilon)^{2}n}$ to LPHP$_{(1-\epsilon)^{2}n}$ in w$.\downarrow$, and by chaining this to the derivations from Lemmata [50] and [53] we obtain monotone derivations from LPHP$_{(1-\epsilon)^{2}n}$ to T$_{n}^{\min}[p - \log^{2} n, q](p_{i})$.

We now need to check that $n > \frac{1}{2} \log^{3} n$, $n^{\epsilon} = n^{\epsilon}$ before applying Lemma [50]. Now we have that,

\[
\left(\frac{p - \log^{2} n}{q}\right)^{\log n} = \left(\frac{3 \log^{3} n - \log^{2} n - \log n}{3 \log^{3} n + \log n}\right)^{\log n}
\]

\[
= \left(1 - \frac{\log^{2} n + 1}{3 \log^{3} n + \log n}\right)^{\log n}
\]

\[
\geq \left(1 - \frac{2}{3 \log^{3} n}\right)^{\log n}
\]

or

\[
\leq \left(\frac{2}{3 \log^{3} n}\right)^{\log n} 
\]

by Prop. [49]. Consequently we have that,

\[
\frac{1 - \epsilon}{(p - \log^{2} n)/q}^{\log n} \leq 1 - \frac{1}{3 \log^{3} n} < 1
\]

giving monotone derivations from LPHP$_{(1-\epsilon)^{2}n}$ to RPHP$_{(1-\epsilon)^{2}n}$ by Lemma [50]. From previous bounds, the size of these derivations is $p^{O(\log n)} = (\log n)^{O(\log n)} = n^{O(\log \log n)}$ as required.

Since the width of these derivations is $O(\log n)$ we also gain a minor improvement in the complexity of KS proofs of PHP$_{(1-\epsilon)^{2}n}$ over those appearing in Sect. 3.

Corollary 52. There are KS proofs of PHP$_{(1-\epsilon)^{2}n}$ for $\epsilon = 1/\log^{(1)} n$, of size $n^{O(\log \log n \log \log n)}$.

6. Final Comments

We constructed explicit quasipolynomial-size proofs of the pigeonhole principle in KS, and generalized our techniques to further yield quasipolynomial-size proofs of the parity principle and quite strong variants of the weak pigeonhole principle. In particular the existence of $n^{O(\log \log n)}$-size monotone proofs of the most common variant, with 2n pigeons and n holes, are implied by our construction. We repeat that this is the first time when considering the complexity of deep inference proofs have led to improvements for systems in mainstream proof complexity.

The various proof structures used throughout this work are similar in concept and fairly uniform, and so it might be pertinent to design high-level tools to more easily manipulate deep inference proofs, respecting certain complexity properties. One such approach might be to design an associated theory of bounded arithmetic, as done for other propositional proof systems, e.g. the theory I$\Delta_0$ for bounded-depth Frege systems [22]. Work in this direction is ongoing.

A natural question is whether the methods used here could be generalized to yield a simulation of Frege proofs, as done for KS+ in [10] [18]. That construction is also relies heavily on threshold formulae, however it is not clear how to restrict the length of flows in the same way as we did here.

Note that the proofs we have given, albeit $n^{O(\log^{2} n)}$ so quasipolynomial in size, are not in polynomial correspondence with those
constructed in [2] for the monotone sequent calculus, and so $KS^+$, which have smaller quasipolynomial size $n^{O(\log n)}$. In fact it is conjectured that there are polynomial-size proofs in $KS^+$, due to the more general conjecture that the monotone sequent calculus polynomially simulates the full sequent calculus over monotone sequents. Consequently we cannot rule out the possibility that proofs of $PHP_n$ witness a superpolynomial separation between $KS$ and $KS^+$.

References


