

$n^{O(\log \log n)}$ -size monotone proofs of the weak pigeonhole principle.

Anupam Das

INRIA & LIX, École Polytechnique

Abstract. We present $n^{O(\log \log n)}$ -size proofs in the (tree-like) monotone sequent calculus of the pigeonhole principle with $(1 + \varepsilon)n$ pigeons and n holes, for $\varepsilon = 1/\text{polylog } n$. This improves on the bound of $n^{O(\log n)}$ inherited from proofs of the usual pigeonhole principle, with $n + 1$ pigeons and n holes, by Atserias et al., and supports the more general conjecture that the monotone sequent calculus polynomially simulates Hilbert-Frege systems.

The pigeonhole principle states that if there are m pigeons in n holes, and $m > n$, then there must be some hole accommodating more than one pigeon. It is usually encoded in propositional logic as follows,

$$\text{PHP}_n^m: \bigwedge_{i=1}^m \bigvee_{j=1}^n p_{ij} \rightarrow \bigvee_{j=1}^n \bigvee_{i=1}^{m-1} \bigvee_{i'=i+1}^m p_{ij} \wedge p_{i'j}$$

where p_{ij} should be interpreted as “pigeon i sits in hole j ”.¹ This encoding forms a class of propositional tautologies, for $m > n$, that has become a benchmark in proof complexity [Raz02]. 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 [KPW95] [PBI93], whereas small proofs (of size polynomial in n) have been constructed for Frege systems by Buss [Bus87], and so also the sequent calculus with cut.

In [AGG00] Atserias et al. constructed quasipolynomial-size (tree-like) proofs of PHP_n^{n+1} in the monotone sequent calculus, i.e. the sequent calculus without negation rules. This was generalized in [AGP02] to yield a quasipolynomial simulation of all Hilbert-Frege proofs, thereby inheriting the previous bound from Buss’ proofs. Since then Jeřábek has proved that the (dag-like) monotone calculus polynomially simulates Hilbert-Frege systems, assuming the provable existence of certain expander graphs in some bounded arithmetic [Jeř11], which conditionally yields polynomial-size dag-like monotone proofs of PHP_n^{n+1} .

In this work we show that $n^{O(\log \log n)}$ -size tree-like monotone proofs of $\text{PHP}_n^{(1+\varepsilon)n}$ exist for $\varepsilon = 1/\text{polylog } n$. The basic idea behind all the above proofs is to encode some counting functions as propositional formulae and show that basic properties can be realized as small proofs. In particular, our proof begins with the same

¹ Notice that the above formula allows the mapping from pigeons to holes to be many-many, and we consider only this version in the current work.

reduction as in [AGG00] from PHP_n^m to the proofs witnessing the symmetry of counting functions. Our proofs fundamentally differ in the following ways:

1. We use monotone formulae that only approximate the number of true arguments. These have size $n^{O(\log \log n)}$ and this is ultimately the reason why we are able to achieve this bound on the size of proofs.
2. These functions are no longer symmetric, but we can nonetheless apply previous constructions if we allow deteriorations in the accuracy of the approximation. Unfortunately the method used in [AGG00], which decomposes permutations into a product of transpositions, deteriorates the accuracy of approximation too much to gain any sensible bounds, so we instead consider the merge-sort decomposition of a permutation and show that proofs can be thus constructed achieving the necessary bounds.

In fact, the proof structure described in (2) was initially designed to reason about the complexity of certain *deep inference* systems [Das14], to satisfy certain constraints on the structural rules. It is interesting, we believe, that considerations in the complexity of deep inference has transferred to bounds in more mainstream proof complexity. However we also acknowledge that this improvement is perhaps minor, in light of the more general program that aims to show a polynomial simulation of all Hilbert-Frege proofs in the monotone calculus.

This is partially based on work that will appear in the proceedings of CSL-LICS 2014 [Das14].

References

- [AGG00] Albert Atserias, Nicola Galesi, and Ricard Gavaldà. Monotone proofs of the pigeon hole principle. 2000.
- [AGP02] Albert Atserias, Nicola Galesi, and Pavel Pudlák. Monotone simulations of non-monotone proofs. *Journal of Computer and System Sciences*, 65(4):626–638, 2002.
- [Bus87] Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52(4):916–927, 1987.
- [Das14] Anupam Das. On the pigeonhole and related principles in deep inference and monotone systems. In *Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic (CSL) and the 29th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2014. To appear.
- [Jeř11] Emil Jeřábek. A sorting network in bounded arithmetic. *Annals of Pure and Applied Logic*, 162(4):341–355, 2011.
- [KPW95] Jan Krajíček, Pavel Pudlák, and Alan Woods. An exponential lower bound to the size of bounded depth frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995.
- [PBI93] Toniann Pitassi, Paul Beame, and Russell Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3:97–140, 1993. 10.1007/BF01200117.
- [Raz02] Alexander A. Razborov. Proof complexity of pigeonhole principles. In Werner Kuich, Grzegorz Rozenberg, and Arto Salomaa, editors, *Developments in Language Theory*, volume 2295 of *Lecture Notes in Computer Science*, pages 100–116. Springer Berlin Heidelberg, 2002.