A Note on Polynomial-Size Monotone Proofs of the Pigeon Hole Principle

Albert Atserias*
Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
c/ Jordi Girona Salgado, 1-3, Edif. C6.
08034 Barcelona, Spain.
atserias@lsi.upc.es

August 8, 2000

Abstract

We see that the version of the pigeon-hole principle in which every hole is forced to receive a pigeon (called onto) and the version in which every pigeon is mapped into exactly one hole (called functional) have polynomial-size proofs in the tree-like monotone sequent calculus. The proofs are surprisingly simple reductions to the non-monotone case.

1 Introduction

The Pigeon Hole Principle (PHP) states that there is no one-to-one correspondence from a set of $n+1$ elements into a set of n elements. Cook and Reckhow [CR79] formalized this principle as a propositional tautology, and suggested studying the complexity of proving it in proof systems such as Resolution or Frege Systems. Since then, several upper and lower bounds were proved, the most remarkable being the exponential lower bounds for Resolution by Haken [Hak85], the exponential lower bounds for Bounded Depth Frege Systems by Beame, Impagliazzo, Krajícek, Pitassi, Pudlák and Woods [BIK$^+$92], and the polynomial upper bounds for Frege Systems by Buss [Bus97].

More recently, Pudlák suggested studying the complexity of proving the PHP in non-classical calculi whose power presumably falls in between the systems for which upper and lower bounds are known. In particular, he suggested the study of the Monotone Sequent

*Supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532, and partially supported by ALCOM-FT, IST-99-14186.

Calculus, that is, the standard Sequent Calculus of Gentzen restricted to monotone formulas. It is easily seen that the Monotone Sequent Calculus subsumes Resolution and is subsumed by the Frege Systems (see the paper by Pudlák [Pud98] for more motivation on this problem). A recent paper by Atserias, Galesi and Gavaldà [AGG00] addresses this problem and shows that the PHP has quasipolynomial-size proofs in the Monotone Sequent Calculus, ruling out exponential lower bounds thereby.

In this note we consider two well-known variants of the PHP. The Onto PHP states that there is no one-to-one correspondence from a set of $n+1$ elements *onto* a set of n elements. The Functional PHP states that there is no one-to-one *function* from a set of $n+1$ elements into a set of n elements (a correspondence differs from a function in that it each element may have more than one image in the former, but not in the latter). All three principles PHP, Onto PHP, and Functional PHP, have been used more or less interchangeably in the literature since little difference is known between them. As a matter of fact, Cook and Reckhow considered the Functional PHP in their original paper.

The main result of this note is proving that the Onto PHP and the Functional PHP have polynomial-size proofs in the tree-like Monotone Sequent Calculus. Surprisingly enough, the proof is a simple reduction to the (non-monotone) upper bound of Buss, and it does not seem to extend to the more general PHP.

2 Monotone Calculus

All our propositional formulas are over the basis $\{\vee, \wedge, \neg\}$ without constants. We say that a formula is in De Morgan normal form if all the negations occur in front of the variables. For every formula φ, let $p(\varphi)$ be a formula in De Morgan normal form that is equivalent to φ. Observe that $p(\varphi)$ is uniformly obtained from φ by pushing the negations to the atoms according to the De Morgan rules. Observe that $p(\neg\neg\varphi) = p(\varphi)$, and that the size of $p(\varphi)$ is linear in the size of φ.

We assume some familiarity with the standard propositional Gentzen Calculus (LK). A concrete definition of the system may be found in the book by Takeuti [Tak87]. The Monotone Gentzen Calculus (MLK) is the subsystem of LK in which all formulas are positive; that is, all formulas are over the monotone basis $\{\wedge, \vee\}$, and the negation rules are prohibited. We also let LK-De Morgan be the subsystem of LK in which all formulas are in De Morgan normal form; that is, all formulas have the negations pushed down to the atoms, and the negation rules are only allowed over variables. The size of a proof is the number of symbols in it. We say that a proof is tree-like if each sequent is used at most once as a premise of a rule.

Lemma 1 *For every formula φ, the sequents $\vdash p(\varphi), p(\neg\varphi)$ and $p(\varphi), p(\neg\varphi) \vdash$ have tree-like* LK-*De Morgan proofs of size linear in the size of φ.*

Proof: The proof is by induction on the structure of φ. If φ is atomic, say x, then the sequents $\vdash x, \neg x$ and $x, \neg x \vdash$ are derivable in one step from the axiom $x \vdash x$. Suppose next that φ is of the form $\psi \wedge \theta$. By induction hypothesis, the sequents $\vdash \psi, p(\neg\psi)$ and $\vdash \theta, p(\neg\theta)$ have tree-like LK-De Morgan proofs of size linear in the sizes of ψ and θ respectively. By means of weakening we derive $\vdash \psi, p(\neg\psi), p(\neg\theta)$ and $\vdash \theta, p(\neg\psi), p(\neg\theta)$. Right $\wedge$-introduction followed by right $\vee$-introduction gives $\vdash \psi \wedge \theta, p(\neg\psi) \vee p(\neg\theta)$. The size of the proof is clearly linear in the size of φ. The sequent $\psi \wedge \theta, p(\neg\psi) \vee p(\neg\theta) \vdash$ is derived similarly. When φ is of the form $\psi \vee \theta$ reason dually. Finally, suppose that φ is of the form $\neg\psi$. By induction hypothesis, the sequent $\vdash p(\psi), p(\neg\psi)$ has a tree-like LK-De Morgan proof of linear size in the size of ψ. Since $p(\neg\neg\psi) = p(\psi)$, we immediately have a tree-like LK-De Morgan proof of $\vdash p(\neg\psi), p(\neg\neg\psi)$ of the same size. Reason similarly for the sequent $p(\neg\psi), p(\neg\neg\psi) \vdash$. $\square$

Theorem 1 *Let Σ and Γ be sequences of formulas. If $\Sigma \vdash \Gamma$ has a tree-like* LK*-proof of size S, then $p(\Sigma) \vdash p(\Gamma)$ has a tree-like* LK*-De Morgan proof of size $O(S)$.*

Proof: Suppose that $\Sigma \vdash \Gamma$ has a tree-like LK-proof P of size S. Consider the following transformation of P. First, replace each formula φ in P by $p(\varphi)$. For each right $\neg$-introduction rule in P of the form

$$\frac{\Sigma', \varphi \vdash \Gamma'}{\Sigma' \vdash \neg\varphi, \Gamma',}$$

we simulate the inference

$$\frac{p(\Sigma'), p(\varphi) \vdash p(\Gamma')}{p(\Sigma') \vdash p(\neg\varphi), p(\Gamma')}$$

in the new proof by means of a cut with $\vdash p(\varphi), p(\neg\varphi)$, which can be derived in $O(S)$ steps according to Lemma 1. Similarly, each left $\neg$-introduction rule in P is replaced by an inference involving a cut with $p(\varphi), p(\neg\varphi) \vdash$. The size of the new proof is clearly $O(S)$. $\square$

Theorem 2 *Let Σ and Γ be sequences of monotone formulas with all variables within $x_1, \ldots, x_n$. Suppose that for every $i \in \{1, \ldots, n\}$ there exists a monotone formula φ_i such that the sequents $\Sigma \vdash x_i, \varphi_i, \Gamma$ and $\Sigma, \varphi_i, x_i \vdash \Gamma$ have tree-like* MLK*-proofs of size at most R. Then, if $\Sigma \vdash \Gamma$ has a tree-like* LK*-proof of size S, then it has a tree-like* MLK*-proof of size $O(S + RS)$.*

Proof: Suppose that $\Sigma \vdash \Gamma$ has a tree-like LK-proof of size S. Since Σ and Γ are sequences of monotone formulas, we have that $p(\Sigma) = \Sigma$ and $p(\Gamma) = \Gamma$. Therefore, by Theorem 1, the sequent $\Sigma \vdash \Gamma$ has a tree-like LK-De Morgan proof P of size $O(S)$. Consider the following transformation on P. First, add Σ to the left of each sequent and Γ to the right of each sequent by weakening on the axioms. Then, replace each occurrence of $\neg x_i$ in P by φ_i. It remains to see how to simulate the rules of $\neg$-introduction. Consider such an application in P

$$\frac{\Sigma', x_i \vdash \Gamma'}{\Sigma' \vdash \neg x_i, \Gamma'.}$$

We need to simulate the inference

$$\frac{\Sigma, \Sigma', x_i \vdash \Gamma', \Gamma}{\Sigma, \Sigma' \vdash \varphi_i, \Gamma', \Gamma.}$$

This is straightforward: derive $\Sigma \vdash x_i, \varphi_i, \Gamma$, cut on x_i, and apply some structural rules. The simulation of a left $\neg$-introduction rule is symmetrical by means of a cut with $\Sigma, \varphi_i, x_i \vdash \Gamma$. The size of the new proof is clearly $O(S + RS)$. $\square$

3 Pigeon-hole Principles

We consider the following propositional formulations of PHP, Onto PHP and Functional PHP: We let PHP_n^{n+1} be the sequent

$$\bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} p_{i,j} \vdash \bigvee_{k=1}^{n} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n+1} (p_{i,k} \wedge p_{j,k}).$$

We let OPHP_n^{n+1} be the sequent

$$\bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} p_{i,j} \wedge \bigwedge_{j=1}^{n} \bigvee_{i=1}^{n+1} p_{i,j} \vdash \bigvee_{k=1}^{n} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n+1} (p_{i,k} \wedge p_{j,k}).$$

Finally, we let FPHP_n^{n+1} be the sequent

$$\bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} p_{i,j} \vdash \bigvee_{k=1}^{n} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n+1} (p_{i,k} \wedge p_{j,k}) \vee \bigvee_{k=1}^{n+1} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n} (p_{k,i} \wedge p_{k,j}).$$

We are ready to state and prove our result:

Theorem 3 FPHP_n^{n+1} *and* OPHP_n^{n+1} *have tree-like* MLK-*proofs of size polynomial in* n.

Proof: Buss proved that PHP_n^{n+1} has a Frege proof of size polynomial in n, and therefore, so do FPHP_n^{n+1} and OPHP_n^{n+1} Since tree-like LK polynomially simulates any Frege system, they also have polynomial-size tree-like LK-proofs. We first consider FPHP_n^{n+1}. For every $i \in \{1, \ldots, n+1\}$ and $j \in \{1, \ldots, n\}$, let φ_{ij} be the formula $\bigvee_{j' \neq j} p_{i,j'}$ where j' ranges over $\{1, \ldots, n\}$. Let LFPHP_n^{n+1} be the left hand side of the sequent FPHP_n^{n+1}, and let RFPHP_n^{n+1} be the right hand side of the sequent FPHP_n^{n+1}. We claim that the sequents

$$\mathrm{LFPHP}_n^{n+1} \vdash p_{i,j}, \varphi_{ij}, \mathrm{RFPHP}_n^{n+1} \tag{1}$$

$$\mathrm{LFPHP}_n^{n+1}, \varphi_{ij}, p_{i,j} \vdash \mathrm{RFPHP}_n^{n+1} \tag{2}$$

have tree-like MLK-proofs of size polynomial in n. The result will follow for FPHP_n^{n+1} by Theorem 2. For sequent (1) reason as follows. For every $j' \in \{1, \ldots, n\}$, we have $p_{i,j'} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}_n^{n+1}$ by right weakening on the axiom $p_{i,j'} \vdash p_{i,j'}$ and structural rules. By left $\vee$-introduction we get $\bigvee_{j=1}^{n} p_{i,j} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}_n^{n+1}$. Left weakening and left $\wedge$-introduction gives $\mathrm{LFPHP}_n^{n+1} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}_n^{n+1}$. Finally, some structural rules and right $\vee$-introduction give sequent (1). For sequent (2) reason as follows. For every $j, j' \in \{1, \ldots, n+1\}$ such that $j \neq j'$, we have $p_{i,j}, p_{i,j'} \vdash p_{i,j} \wedge p_{i,j'}$ easily. Left weakening, right weakening and right $\vee$-introduction gives $\mathrm{LFPHP}_n^{n+1}, p_{i,j}, p_{i,j'} \vdash \mathrm{RFPHP}_n^{n+1}$. Finally, left $\vee$-introduction for every $j' \neq j$ gives sequent (2). As regards OPHP_n^{n+1}, one simply needs define φ_{ij} as $\bigvee_{i' \neq i} p_{i',j}$ where i' ranges over $\{1, \ldots, n+1\}$, and reason analogously. $\square$

Acknowledgments I am grateful to Nicola Galesi for suggesting rewriting an old proof via Liar Games into a direct proof in Sequent Calculus.

References

[AGG00] A. Atserias, N. Galesi, and R. Gavaldà. Monotone proofs of the pigeon-hole principle. In *27th International Colloquium on Automata, Languages and Programming*, 2000. To appear in Mathematical Logic Quarterly.

[BIK+92] P. Beame, R. Impagliazzo, J. Krajícek, T. Pitassi, P. Pudlák, and A. Woods. Exponential lower bounds for the pigeonhole principle. In *24th Annual ACM Symposium on the Theory of Computing*, pages 200–220, 1992.

[Bus97] S. R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52(4):916–927, 1997.

[CR79] S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[Hak85] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Pud98] P. Pudlák. On the complexity of the propositional calculus. To appear in Logic Colloquium'97, 1998.

[Tak87] G. Takeuti. *Proof Theory*, North-Holland, second edition, 1987.