Resolution Proofs of Generalized Pigeonhole Principles

Samuel R. Buss*
Department of Mathematics
University of California, Berkeley

György Turán
Department of Mathematics, Statistics, and Computer Science
University of Illinois, Chicago
and
Automata Theory Research Group
Hungarian Academy of Sciences
Szeged, Hungary

February 1988

Abstract

We extend results of A. Haken to give an exponential lower bound on the size of resolution proofs for propositional formulas encoding a generalized pigeonhole principle. These propositional formulas express the fact that there is no one-one mapping from $c \cdot n$ objects to n objects when $c > 1$. As a corollary, resolution proof systems do not p-simulate constant formula depth Frege proof systems.

1. Introduction

S. Cook and R. Reckhow [2] introduced propositional formulas encoding the pigeonhole principle. These propositional formulas have polynomial size proofs in extended resolution proof systems (S. Cook, Reckhow [2]), in Frege proof systems (Buss [1]) and in cutting plane proof systems (W. Cook, Coullard, Turán [3]); however, A. Haken [4] showed they require exponential size proofs

*Supported in part by NSF postdoctoral fellowship DMS-8511465.

in a resolution proof system. The purpose of this paper is to extend Haken's exponential lower bound; in particular, we address the question of lower bounds on the size of resolution proofs of generalized pigeonhole principles which state that for $m > n$, if m pigeons sit in n holes then some hole contains more than one pigeon. For $m > n + 1$ the generalized pigeonhole principle is "more true" than the usual pigeonhole principle (where $m = n + 1$), and hence might have shorter resolution proofs.

We show below that any resolution proof of the generalized pigeonhole principle with $m = cn$ must be exponential size in n (for constant $c > 1$). This implies (using results of Paris and Wilkie [5] and Paris, Wilkie and Woods [6]) that resolution does not p-simulate constant formula depth Frege proof systems.

2. Resolution and the Pigeonhole Principle

We begin by recalling the basic facts about resolution (see Haken [4] for a more detailed exposition). A propositional variable ranges over the truth values *True* and *False*. A *literal* is either a variable x or the negation $\overline{x}$ of a variable x. A *clause* is a finite set of literals; the meaning of a clause is the disjunction of the variables in the clause. Hence a truth assignment satisfies a clause if it assigns the value *True* to some variable in the clause or the value *False* to a variable whose negation appears in the clause. The meaning of a set of clauses is the conjunction of the clauses, so any conjunctive normal form formula can be viewed as a set of clauses. The resolution rule is a form of modus ponens: if C_1 is a clause containing x and C_2 contains $\overline{x}$ then the clause $(C_1 \setminus \{x\}) \cup (C_2 \setminus \{\overline{x}\})$ is inferred by resolving on the variable x.

Resolution is a *refutation* proof system. Given a formula ϕ in disjunctive normal form, its negation can be expressed in conjunctive normal form and then as a set of clauses. A resolution proof of ϕ is by definition a resolution proof of the empty clause (a contradiction) from the set of clauses expressing the negation of ϕ. The completeness theorem for resolution guarantees that every tautology in disjunction normal form has a resolution proof; i.e., from any set of clauses such that no truth assignment can simultaneously satisfy all of them there is a derivation of the empty clause using only the resolution rule.

A resolution proof can be viewed as a sequence of clauses; each clause in the sequence is either an initial clause (an assumption) or is obtained by resolution from two earlier clauses. Alternatively a resolution proof can be viewed as a directed acyclic graph with an edge from one clause to another if the second is obtained by resolution from the first together with some other clause.

We shall use the following fact: given a resolution proof and a truth assignment α, there is a unique path $C_1, C_2, \ldots, C_t$ through the proof (viewed as a directed acyclic graph) such that C_1 is an initial clause and C_t is the empty clause and each C_{i+1} is inferred by resolution from C_i and one other clause. This is proved by working backwards starting at the root of the tree and by noting that if α does not satisfy a clause then α also does not satisfy exactly one of the two clauses from which it derived by resolution.

Since we are working in a resolution proof system the generalized pigeonhole principle PHP_n^m needs to be expressed as an unsatisfiable propositional formula in conjunctive normal form. The variables of PHP_n^m are $x_{i,j}$ with $1 \le i \le m$, $1 \le j \le n$; the variable $x_{i,j}$ is intended to denote the condition that pigeon i is sitting in hole j. The formula PHP_n^m is defined to be

$$\left(\bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} x_{i,j} \right) \wedge \left(\bigwedge_{j=1}^{n} \bigwedge_{1 \le i_1 < i_2 \le m} (\overline{x}_{i_1,j} \vee \overline{x}_{i_2,j}) \right)$$

where $\overline{x}_{i,j}$ denotes the negation of $x_{i,j}$. The first part of PHP_n^m expresses the condition that every pigeon sits in one or more holes; the second part that no hole is occupied by more than one pigeon. It is easy to see that the generalized pigeonhole principle for m pigeons and n holes is equivalent to PHP_n^m being unsatisfiable. Note that the size of PHP_n^m is $O(nm^2)$.

3. A Lower Bound for Resolution

In this section we prove the main result:

Theorem 1 *Every resolution proof of the unsatisfiability of* PHP_n^m *has length at least*

$$\frac{1}{2} \cdot \left(\frac{3}{2} \right)^{\frac{1}{50} \cdot \frac{n^2}{m}}$$

Thus, in particular, PHP_n^{cn} requires exponential length resolution proofs for any constant $c > 1$. The lower bound is superpolynomial for $m = o(n^2/\log n)$. We do not know whether $\mathrm{PHP}_n^{n^2}$ has polynomial length proofs. (By the length of resolution proof we mean the number of lines in the proof; however, this is polynomially related to the number of symbols in the proof since each clause in the proof will contain at most one instance of each variable.)

The proof follows A. Haken's argument. Although in his proof (and in the subsequent work of Urquhart [7]) the existence of critical truth assignments, which satisfy all but one clause, seems to play a central role, it turns out that by suitably modifying Haken's definitions his ideas carry over to our case as well — although here there are no critical truth assignments.

We shall picture the variables $x_{i,j}$ arranged in an $n \times m$ matrix with i (the pigeon) specifying the column and j (the hole) the row. Each clause in the resolution proof is described by an $n \times m$ matrix partially filled with $+$'s and $-$'s, where a $+$ (respectively, $-$) in a position (i,j) means that $x_{i,j}$ (respectively, $\overline{x}_{i,j}$) occurs in the clause. A truth assignment is pictured as an $n \times m$ matrix of 0's and 1's which indicate assigning *False* or *True* (respectively) to the corresponding variable.

Definition A truth assignment α is *maximal* if it contains exactly n 1's, all in different rows and columns. The $m-n$ columns which contain no 1's (and hence only 0's) are called the 0-*columns* of α.

Note that a maximal truth assignment assigns n of the pigeons to distinct holes and leaves the other $m-n$ pigeons unassigned.

Now suppose we are given an arbitrary resolution proof of the unsatisfiability of PHP^m_n. Recall that such a proof may be viewed either as a sequence of clauses ending with $\emptyset$ or as a directed acyclic graph with $\emptyset$ at the root. (The empty clause $\emptyset$ is not satisfiable.) Each clause in the proof must either be a clause from PHP^m_n or be deduced from prior clauses by resolution. The initial clauses from PHP^m_n consist either of one column filled with n $+$'s or of two $-$'s in one row.

Lemma 2 *For every maximal truth assignment α there is a clause C in the resolution proof such that*

(1) *α makes C false,*

(2) *C contains at most $\left\lfloor \frac{n}{2} \right\rfloor$ $+$'s in every 0-column of α,*

(3) *C contains $\left\lfloor \frac{n}{2} \right\rfloor$ $+$'s in exactly one 0-column of α.*

Proof In the resolution proof there is a unique path of clauses $C_1, \ldots, C_t$ such that α makes each C_i false, C_1 is an initial clause and $C_t = \emptyset$. Because α is maximal C_1 must consist of one column filled with $+$'s; this will be a 0-column of α. Let C be the *last* among these clauses which contains at least $\left\lfloor \frac{n}{2} \right\rfloor$ $+$'s in some 0-column of α. Then C satisfies (1) by definition, and it also satisfies (2) and (3) as $+$'s can disappear from a clause only one at a time. □

If α is a maximal truth assignment, let C_α denote the *first* clause in the resolution proof satisfying the conditions of Lemma 2. Define FS1 to be the set $\{S : S$ is a set of $\left\lfloor \frac{n}{4} \right\rfloor$ variables, all in different rows and columns$\}$. For $S \in \mathrm{FS1}$, C^S is the *first* clause in the proof sequence which is of the form C_α for some maximal truth assignment α which assigns 1's to each variable in S. Any such C^S is called a *complex clause.*

Lemma 3 *Every complex clause has at least $\left\lfloor \frac{n}{4} \right\rfloor + 1$ columns which contain either a $-$ or at least $\left\lfloor \frac{n}{2} \right\rfloor$ $+$'s.*

Proof Let C^S be a complex clause for $S \in \mathrm{FS1}$ and α be a maximal truth assignment assigning 1's to the variables in S such that $C_\alpha = C^S$. Let

$$\begin{aligned}\mathrm{COL}^{-} &= \{\ell : \text{column } \ell \text{ of } C^S \text{ contains a } -\},\\ \mathrm{COL}^{+} &= \{\ell : \text{column } \ell \text{ of } C^S \text{ contains at least } \lfloor \tfrac{n}{2} \rfloor \text{ +'s and no } -\text{'s}\\ &\qquad \text{and is not a 0-column of } \alpha\},\\ \ell_0 &= \text{the 0-column of } \alpha \text{ which contains exactly } \lfloor \tfrac{n}{2} \rfloor \text{ +'s in } C^S,\\ A &= \{x_{i,j} \notin S : \alpha_{i,j} = 1\}.\end{aligned}$$

Since α makes C^S false, COL^- cannot contain any 0-column of α; thus COL^-, COL^+ and $\{\ell_0\}$ are pairwise disjoint. By definition every 0-column of α other than ℓ_0 contains fewer than $\lfloor \frac{n}{2} \rfloor$ +'s in C^S. As ℓ_0 satisfies the conditions of the lemma, we have to show that $|\mathrm{COL}^-| + |\mathrm{COL}^+| \geq \lfloor \frac{n}{4} \rfloor$.

Claim 1: If $|\mathrm{COL}^-| + |\mathrm{COL}^+| < \lfloor \frac{n}{4} \rfloor$, then there exists an $x_{i,j} \in A$ such that (1) neither $x_{\ell_0,j}$ nor $\overline{x}_{\ell_0,j}$ occurs in C^S and (2) $i \notin \mathrm{COL}^- \cup \mathrm{COL}^+$.

Indeed, as (1) excludes $\lfloor \frac{n}{2} \rfloor$ elements of A (in fact column ℓ_0 contains only +'s) and (2) excludes $< \lfloor \frac{n}{4} \rfloor$ elements, the condition $|A| = \lceil \frac{3n}{4} \rceil$ implies the existence of such a variable.

To prove Lemma 3, suppose for the sake of a contradiction that the conditions of Claim 1 hold and let α^* be the maximal truth assignment constructed from α by changing the value of $\alpha_{i,j}$ to 0 and $\alpha_{\ell_0,j}$ to 1.

Claim 2: **(1)** α^* assigns 1's to all members of S and makes C^S false.

(2) All 0-columns of α^* contain less than $\lfloor \frac{n}{2} \rfloor$ +'s in C^S.

(1) follows by construction. The 0-columns of α^* are the 0-columns of α, except ℓ_0 being replaced by i, but as $i \notin \mathrm{COL}^+$, it contains less than $\lfloor \frac{n}{2} \rfloor$ +'s in C^S, proving (2).

By the method of proof of Lemma 2, it is clear that C_{α^*} is a clause preceding C^S in the proof sequence which contradicts the the definition of C^S. □

Proof of Theorem 1. Put $g(n) = \max_C \{ |\{S \in \mathrm{FS1} : C^S = C\}| \}$ and $h(n) = |\mathrm{FS1}|$. Then as in [4], $h(n)/g(n)$ is a lower bound to the length of a resolution proof, since it is clearly a lower bound on the number of distinct complex clauses in the resolution proof. Let $k = \lfloor \frac{n}{4} \rfloor$. To compute $h(n)$ and $g(n)$ suppose we have a particular complex clause C. By Lemma 3 we can choose $k+1$ columns which contain a $-$ or at least $\lfloor \frac{n}{2} \rfloor$ +'s. To count the total number of $S \in \mathrm{FS1}$ we let the variable i denote the number of variables in S in the chosen $k+1$ columns. Then we have:

$$h(n) = \sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i} \frac{n!}{(n-k)!}$$

Similarly, to get the upper bound $g(n)$ on the number of $S \in \mathrm{FS1}$ such that $C^S = C$ we let i be the number of variables of S in one of the $k+1$ columns. In each of these $k+1$ columns there are at most $\lceil \frac{n}{2} \rceil$ variables which can be in such an S; this is because a $+$ in C excludes the corresponding variable from S and a $-$ in C implies that if S has a variable from that column it must be the variable corresponding to the $-$. Thus,

$$g(n) \leq \sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i} \left\lceil \frac{n}{2} \right\rceil^i \frac{(n-i)!}{(n-k)!}$$

So,

$$\begin{aligned}
\frac{h(n)}{g(n)} &\geq \frac{\displaystyle\sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i}}{\displaystyle\sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i} \left\lceil \frac{n}{2} \right\rceil^i \frac{(n-i)!}{n!}} \\
&\geq \frac{\displaystyle\sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i}}{\displaystyle\sum_{i=0}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i} \left(\frac{2}{3}\right)^i}
\end{aligned}$$

since for $i \leq \lfloor \frac{n}{4} \rfloor$,

$$\left\lceil \frac{n}{2} \right\rceil^i \frac{(n-i)!}{n!} \leq \left(\frac{2}{3}\right)^i$$

The ratio of the $(i-1)$-st term over the i-th term in the summation in the denominator is

$$\frac{i(m-2k+i-1)}{\frac{2}{3}(k-i+1)(k-i+2)}$$

It is easily verified that this is less than 1 for $i \leq \frac{1}{25} \cdot \frac{n^2}{m}$, and hence the terms in the denominator are increasing while $i \leq \frac{1}{25} \cdot \frac{n^2}{m}$. Thus we can give a weaker lower bound (with smaller numerator and larger denominator):

$$\begin{aligned}
\frac{h(n)}{g(n)} &\geq \frac{\displaystyle\sum_{i=\frac{1}{50}\frac{n^2}{m}}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i}}{2 \cdot \displaystyle\sum_{i=\frac{1}{50}\frac{n^2}{m}}^{k} \binom{k+1}{i} \binom{m-k-1}{k-i} \left(\frac{2}{3}\right)^i} \\
&\geq \frac{1}{2} \left(\frac{3}{2}\right)^{\frac{1}{50}\frac{n^2}{m}}
\end{aligned}$$

which completes the proof of Theorem 1. □

4. Resolution versus Constant Formula Depth Frege Systems

The notion of the depth of a formula is defined in terms of the alternation of $\wedge$'s and $\vee$'s in the formula. A formula is of *depth* k iff it is in one of the classes Σ_k or Π_k:

Definition Σ_k and Π_k are the smallest sets of propositional formulas which satisfy the following inductive definition:

1. A propositional variable is in Σ_0 and in Π_0,
2. If A and B are in Σ_k (respectively, in Π_k) then $\neg A$ is in Π_k (resp., Σ_k), A is in $\Sigma_{k+1} \cap \Pi_{k+1}$, $A \vee B$ is in Σ_k (resp., Σ_{k+1}), $A \wedge B$ is in Π_{k+1} (resp., Π_k).

For instance, PHP_n^m is in Π_2.

A *formula-depth* k Frege proof system is a usual Frege proof system (see S. Cook, Reckhow [2]) with the additional restriction that every formula appearing in a proof be of depth k. Paris and Wilkie [5] established the following connection between provability in Bounded Arithmetic and provability in constant formula depth Frege proof systems. Let $\mathrm{WPHP}(f)$ be the sentence

$$\forall x[x \neq 0 \wedge (\forall y < x)(f(y) < \lfloor \tfrac{x}{2} \rfloor) \rightarrow (\exists y)(\exists z)(y \neq z \wedge f(y) = f(z))].$$

Let $I\Delta_0(f)+\Omega_1$ be the theory of arithmetic with induction on bounded formulas with f an additional function symbol allowed in induction formulas and with an axiom asserting that $x^{\log x}$ is a total function; then a slight strengthening of Theorem 26 of Paris-Wilkie [5] gives:

Proposition 4 *If $I\Delta_0(f) + \Omega_1 \vdash$ WPHP(f) then there are constants k_1 and k_2 such that for all n, PHP_n^{2n} has Frege proofs of size $O(n^{(\log n)^{k_1}})$ in which every formula is of depth k_2.*

Recently, Paris, Wilkie and Woods [6] established that $I\Delta_0(f) + \Omega_1$ does indeed prove $\mathrm{WPHP}(f)$. Combining our Theorem 1 with these results gives:

Theorem 5 *There is a constant k such that resolution does not polynomially simulate formula depth k Frege proof systems.*

To the best of the authors' knowledge, Theorem 5 is the only known separation result applying to constant formula depth Frege proof systems.

References

[1] S. R. Buss, *Polynomial size proofs of the propositional pigeonhole principle*, Journal of Symbolic Logic, 52 (1987), pp. 916–927.

[2] S. A. Cook and R. A. Reckhow, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic, 44 (1979), pp. 36–50.

[3] W. Cook, C. R. Coullard, and G. Turán, *On the complexity of cutting plane proofs*, Discrete Applied Mathematics, 18 (1987), pp. 25–38.

[4] A. Haken, *The intractability of resolution*, Theoretical Computer Science, 39 (1985), pp. 297–308.

[5] J. B. Paris and A. J. Wilkie, *Counting problems in bounded arithmetic*, in Methods in Mathematical Logic, Lecture Notes in Mathematics #1130, Springer-Verlag, 1985, pp. 317–340.

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

[7] A. Urquhart, *Hard examples for resolution*, J. Assoc. Comput. Mach., 34 (1987), pp. 209–219.