The University of Warwick

THEORY OF COMPUTATION

REPORT NO. 16

NEW BOUNDS FOR FORMULA SIZE

M.S. PATERSON

Department of Computer Science
University of Warwick
COVENTRY CV4 7AL
ENGLAND.

December 1976.

New bounds on formula size*

M. S. Paterson

University of Warwick

Abstract. A variety of theorems bounding the formula size of rather simple Boolean functions are described here for the first time. The principal results are improved lower and upper bounds for symmetric functions.

1. Introduction.

In preparing my presentation to this 1977 GI-Conference I have borne in mind the high level of knowledge and expertise in the audience at such a meeting. I resolved that it would be most appropriate to talk about some of the most recent research upon which I have been engaged. The results to be described have been obtained by myself usually in collaboration with others, notably Mike Fischer, Albert Meyer and Bill McColl, during the past year or so. One was completed only a few days ago and none has yet appeared in published form.

Boolean function complexity is a key area of theoretical computer science. Questions of actual and potential efficiency in computation appear here in their ultimately refined form. It is the sticking-place for many problems arising from circuit design, algorithmic analysis and automata theory. The principal measures of complexity for Boolean functions are circuit size, formula size and depth. While the first must be regarded as the most fundamental measure, it is an unhappy historical fact that no lower bound non-linear in the number of arguments has yet been proved for the circuit size of an explicitly described function. This can be juxtaposed with the classical result that all but a vanishing fraction

* Invited lecture at 2nd GI Conference, Darmstadt 1977.

of Boolean functions have exponential circuit size. In contradistinction several lower bound theorems have liberated formula size from this "linear strait-jacket", disclosing a richer structure of function complexities. It is to be hoped that the present exploration into formula size will be overtaken within the next decade by similar developments with respect to circuit size.

The technical nature of the results presented here makes it reasonable to assume that the interested reader has some previous knowledge of the definitions and basic results, so for example I shall not define "formula" explicitly. For a brief survey of the field may I suggest [Pat 76]; for a very full account, [Sav 76] is to be recommended.

2. Definitions.

Let $B_n = \{h : \{0,1\}^n \to \{0,1\}\}$ be the set of n-argument Boolean functions. We consider formulae for such functions composed of argument variables $x_1,\ldots,x_n$ and arbitrary binary connectives from the full set B_2. We find it convenient to account the size of a formula as the number of occurrences of variables in it. (The alternative count of the number of connectives would result in a size of exactly one less.) The formula size $F(h)$ of a function $h \in B_n$ is defined to be the size of the shortest formula representing h.

Our choice of the whole of B_2 as the set of connectives is important in that two kinds of complete basis for B_n can be distinguished. Strong ones contain either '$\oplus$' (not-equivalence, sum modulo 2) or '$\equiv$' (equivalence), and weak ones contain neither. Examples of minimal strong and weak bases are $\{\oplus,\to\}$ and {NAND} respectively. Pratt [Pra 75] has demonstrated that, to within a constant factor in formula size, there are just two equivalence classes of complete bases, the strong and the weak, and has quantified the

maximum disparity between them. For the results presented here, we could as well choose any strong complete basis.

The set S_n of symmetric functions contains just those functions in B_n which depend only on the number of 1's among their arguments. Equivalently, $h \in B_n$ is symmetric if and only if there is a function $\chi_h : \{0,\ldots,n\} \to \{0,1\}$, the characteristic function of h, such that for all x, $h(x) = \chi_h\,(\Sigma_i x_i)$. Hence we have $|S_n| = 2^{n+1}$, as compared with $|B_n| = 2^{2^n}$.

To express lower and upper complexity bounds more succinctly the following notation is convenient. Let f(n), g(n) be non-negative-valued functions from the natural numbers. We write

$f(n) = O(g(n))$ if $\exists a>0$ such that $f(n) \leq a.g(n)$ for all sufficiently large n

$f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$

$f(n) = \Theta(g(n))$ if $f(n) = O(f(n))$ and $f(n) = \Omega(g(n))$.

3. Neciporuk's theorem and corollaries.

A simple yet powerful theorem yielding lower bounds of up to $\Theta(n^2/\log n)$ on formula size is implicit in [Nec 66]. Suppose the arguments of some $h \in B_n$ to be partitioned into blocks $R_1,\ldots,R_p$. When for some i, the arguments in all the blocks R_j, $j \neq i$, are fixed to 0 or 1 in some way, the result is a restriction of h to R_i, a function h' depending only on R_i. Let m_i be the number of different such h' for all possible fixations of the other variables. In this notation the theorem is concisely expressed.

Theorem (Neciporuk) $\quad F(h) = \Omega\left(\sum_{i=1}^{p} \log m_i\right)$.

This result establishes lower bounds for a variety of functions of interest. Most applications have been to functions with a rather combinatorial nature

such as 'determinant' [Klo 66], 'marriage problem' [HaS 72] or indirect addressing schemes [Nec 66], [Pau 75]. Two corollaries of a somewhat different character have emerged recently.

If we identify the $n = t^r$ cells of a $t \times \overbrace{\ldots}^{r} \times t$ array in r dimensions with the arguments $x_1,\ldots,x_n$, then any predicate on patterns of black and white colourings of the cells corresponds with a function in B_n. Of particular appeal are those predicates of a geometric or topological natue. The predicate $CONN_r^{(n)} \in B_n$ which is true if and only if the black cells of the r-dimensional array are connected has been considered by Hodes [Hod 70].

Theorem (Paterson & Fischer) $F(CONN_r^{(n)}) = \Omega(n \log n)$ for $r \geq 2$.

The proof uses Neciporuk's theorem applied with blocks of size $2s = \theta(n^{1/2r})$. By embedding arbitrary permutation connections between s of these cells and the other s, we can show that at least s! restrictions are possible for each block. In the case $r = 1$, it is an easy observation that $F(CONN_r^{(n)}) = \theta(F(T_2^{(n)}))$, where T_2 is the threshold function defined in the next section.

With a similar correspondence we can identify a set of binary strings of length n with a function of B_n. For any $L \subseteq \Sigma^*$, where $\Sigma = \{0,1\}$, we define $g_L^{(n)} \in B_n$ to be the function corresponding to the set $L \cap \Sigma^n$. The lower bounds on context-free language recognition proved by Hotz [Hot 75] and Mehlhorn [Meh 76] can be improved slightly as follows.

Theorem There is a context-free language L such that

$$F(g_L^{(n)}) = \Omega(n^2/\log n).$$

The language used in the proof is defined by

$$L = \{0^* \; 1 \; w \; 00 \; \Sigma^* \; w^R \; \Sigma^* \mid w \in \Sigma^*\}.$$

The stated bound results from Neciporuk's theorem when we choose the arguments for each block and set the other arguments to impose a form

$$0^* \; 1 \; b_1 \; 1 \; b_2 \; \ldots \; 1 \; b_m \; 1 \; 00 \; \Sigma^*$$

where $b_1,\ldots,b_m$ are the block variables, and $m \sim 2 \log_2 n$. Each block in turn is thus forced into the rôle of 'w' in the definition of L.

An upper bound of $O(n^2 \log n)$ for $F(g_L^{(n)})$, encouragingly close to the lower bound proved, is demonstrable with a formula which is a disjunction of $O(n)$ formulae, each corresponding to 'folding' the string about some position. Each string of L is detected by a formula where the fold is at the centre of symmetry of w, w^R.

4. Bounds for symmetric functions.

Since $|S_m| = 2^{m+1}$, Neciporuk's theorem produces only trivial bounds when applied to symmetric functions. The first non-linear lower bounds for any function in S_n were proved by Hodes and Specker [HoS 68]. They are corollaries of the following general result. We write $\bigvee Y$ for $\bigvee_{x_i \in Y} x_i$ and similarly for $\bigoplus$.

Theorem (Hodes & Specker) There is a (very rapidly growing) function G such that for all c,m, if $n \geqslant G(m,c)$ and ϕ is any formula of size less than cn with argument set $X = \{x_1,\ldots,x_n\}$, then there is a subset $Y \subseteq X$ with $|Y| = m$ and constants b_o, b_1, b_2 such that the restricted formula ϕ_Y of m arguments got by setting the variables of $X \backslash Y$ to 0 is equivalent to

$$b_o \;.\oplus.\; b_1 \wedge \neg \bigvee Y \;.\oplus.\; b_2 \wedge \bigoplus Y$$

This theorem has been applied [Hod 70] to prove non-linear lower bounds for some geometric and topological predicates as considered earlier and also for some symmetric functions. The statement of the theorem is somewhat

complicated, but for application to S_n only, a considerable simplification is possible. The following corollary appears not to have been stated previously.

Theorem (Meyer & Paterson) For all $c > o$, for n sufficiently large,

only 16 functions of S_n have formula size less than cn.

The sixteen functions are characterized by the property of the characteristic function that

$$\chi(r) = \chi(r+2) \text{ for } 1 \leqslant r \leqslant n-3.$$

The threshold functions $T_k^{(n)}$ are defined by

$$\chi_{T_k}(r) = 1 \leftrightarrow r \geqslant k$$

so $F(T_k^{(n)})$ is certainly nonlinear in n for any fixed $k \geqslant 2$.

It is shown by Khasin [Kha 69] and Pippenger [Pip 75] that $F(T_k^{(n)}) = O(n \log n)$ for all fixed k, but only existence proofs are given. Elementary recursion using dichotomy generates explicit formulae with sizes which are $\Theta(n(\log n)^{k-1})$ for fixed k. McColl and Paterson have deferred this growth rate initially by using increasingly tortuous identities[McC 76].

Theorem For $2 \leqslant k \leqslant 6$, $F(T_k^{(n)}) = O(n.\log n\ (\text{loglog } n)^{k-2})$.

Our method is to partition the n arguments into $n^{\frac{1}{2}}$ blocks of size $n^{\frac{1}{2}}$. The predicate that at least r blocks satisfy $T_s^{(n^{\frac{1}{2}})}$ is abbreviated as $T_r(T_s)$. Then for example, our recursive construction for T_3 uses the identity.

$$T_3^{(n)} = T_3(T_1) \vee T_1(T_3) \vee (T_2(T_1) \wedge T_1(T_2)).$$

With the aim of raising the very slowly increasing lower bounds of Hodes' and Specker's theorem, Fischer, Meyer and Paterson weakened somewhat

the conclusion of the theorem and proved lower bounds of $\Omega(n.\log n/\log\log n)$ [FMP 75]. Recent improvements in both the scope of functions covered and the bound attained provide a theorem analogous to Hodes' and Specker's, with the following corollary for symmetric functions.

Theorem. For any $h \in S_n$, if $\chi_h(k) \neq \chi_h(k+2)$ for some $k = k(n)$, then

$$F(h) = \Omega(n.\log k).$$

For example, lower bounds of $\Omega(n.\log n)$ are established for threshold functions $T^{(n)}_{\theta n}$ where θ is constant, $0 < \theta < 1$, and for the congruence functions $C^{(n)}_k$, k fixed, $k > 2$, where C_k is defined by

$$\chi_{C_k}(r) = 1 \text{ if and only if } r \text{ is a multiple of } k.$$

Our especial favourite is C_4 since we now have

$$F(C^{(n)}_4) = \theta(n.\log n).$$

The upper bound is shown using the identity

$$C^{(n)}_4 = \neg D^{(n)}_1 \wedge \neg D^{(n)}_o$$

where $D_o, D_1, D_2, \ldots$ represent successive digits (lowest first) of the binary representation of the sum of the arguments. The D's are expressed recursively by constructing the D's for each of two equal halves of the argument set and performing a binary addition on the results. Thus

$$D^{(1)}_r(x) = x \text{ if } r = 0$$
$$= 0 \text{ if } r > 0$$

$$D^{(2n)}_o(\underset{\sim}{x}, \underset{\sim}{y}) = D^{(n)}_o(\underset{\sim}{x}) \oplus D^{(n)}_o(\underset{\sim}{y})$$

$$D^{(2n)}_1(\underset{\sim}{x}, \underset{\sim}{y}) = D^{(n)}_1(\underset{\sim}{x}) \oplus D^{(n)}_1(\underset{\sim}{y}) \oplus \left(D^{(n)}_o(\underset{\sim}{x}) \wedge D^{(n)}_o(\underset{\sim}{y})\right)$$

Since $F(D^{(n)}_o) = n$, we have $F(D^{(n)}_1) = O(n.\log n)$.

An arbitrary function of S_n is representable as some function of $D_o, D_1, \ldots, D_m$ where $m = \lceil \log(n+1) \rceil - 1$, and may be expressed in a formula using just one occurrence of D_m, two of D_{m-1}, four of D_{m-2}, et cetera.

Small formulae for the D's yield therefore small formulae for all S_n. Using approximately this method Pippenger [Pip 74] has determined that

$$F(S_n) \underset{\text{def}}{=} \max \{F(h) \mid h \in S_n\} = O(n^{\alpha})$$

where $\alpha = \log_2(6 + 4\sqrt{2}) \doteq 3{\cdot}54$.

In his binary adder Pippenger uses "full adders" to compute each new digit d of the sum and new carry digit c from two digits d', d'', of the summands and the previous carry c'. He employs the formula pair

$$d = d' \oplus d'' \oplus c'$$

$$c = (c' \wedge (d' \vee d'')) \vee (d' \wedge d'').$$

A small refinement in the construction is to replace the latter formula by

$$c = d' \oplus ((c' \oplus d') \wedge (d'' \oplus d'))$$

and split the argument set into two unequal parts at each stage. Optimization of the ratio of this split (with the help of Colin Whitby-Strevens and the Warwick University Burroughs 6700 computer) decreases the exponent.

Theorem. $F(S_n) = O(n^{\beta})$ where $\beta < 3{\cdot}41866705572$.

5. Conclusion.

A number of new bounds for symmetric, or otherwise fairly simple, functions are sketched here in a preliminary form. I hope that by the time of the GI meeting at least some may be available in a more polished and complete version.

I should like to acknowledge the cooperation and encouragement derived from many other people than those named explicitly, and the valuable stimulation provided by such international meetings as this.

References

[FMP 75] M.J. Fischer, A.R. Meyer and M.S. Paterson. "Lower bounds on the size of Boolean formulas: preliminary report", Proc. 7th Ann. ACM Symp. on Th. of Computing (1975), ~~45-49~~. 37-44

[HaS 72] L.H. Harper and J.E. Savage. "On the complexity of the marriage problem", Advances in Mathematics 9, 3 (1972), 299-312.

[Hod 70] L. Hodes. "The logical complexity of geometric properties in the plane", J. ACM 17, 2 (1970), 339-347.

[HoS 68] L. Hodes and E. Specker. "Lengths of formulas and elimination of quantifiers I", in Contributions to Mathematical Logic, K. Schutte, ed., North Holland Publ. Co., (1968), 175-188.

[Hot 75] G. Hotz. "Untere Schranken für das Analyseproblem kontext-freier Sprachen", Techn. Bericht, Univ. des Saarlandes, 1976.

[Kha 69] L.S. Khasin. "Complexity bounds for the realization of monotone symmetrical functions by means of formulas in the basis $\vee$, &, $\neg$.", Eng. trans. in Soviet Physics Dokl., 14 12 (1970),1149-1151; orig. Dokl. Akad. Nauk SSSR, 189, 4 (1969), 752-755.

[Klo 66] B.M. Kloss. "Estimates of the complexity of solutions of systems of linear equations", Eng. trans. in Soviet Math Dokl. 7, 6 (1966), 1537-1540; orig. Dokl. Akad. Nauk SSSR, 171, 4 (1966), 781-783.

[McC 76] W.F. McColl. "Some results on circuit depth", Ph.D. dissertation, Computer Science Dept., Warwick University, 1976.

[Meh 76] K. Mehlhorn. "An improved bound on the formula complexity of context-free recognition". Unpublished report, 1976.

[Nec 66] E.I. Neciporuk. "A Boolean function", Soviet Math. Dokl. 7, 4 (1966), 999-1000, orig. Dokl. Akad. Nauk SSSR 169, 4 (1966), 765-766.

[Pat 76] M.S. Paterson. "An introduction to Boolean function complexity". Stanford Computer Science Report STAN-CS-76-557 Stanford University, 1976; to appear in Astérisque.

[Pau 75] W. Paul. "A 2.5 N lower bound for the combinational complexity of Boolean functions", Proc. 7th Ann. ACM Symp. on Th. of Comp. Albuquerque (1975), 27-36.

[Pip 74] N. Pippenger. "Short formulae for symmetric functions", IBM Research Report RC-5143, Yorktown Hts., 1974.

[Pip 75] N. Pippenger. "Short monotone formulae for threshold functions". IBM Research Report RC 5405, Yorktown Hts., 1975.

[Pra 75] V.R. Pratt. "The effect of basis on size of Boolean expressions". Proc. 16th Annual IEEE Symposium on Foundations of Computer Science, 119-121.

[Sav 76] J.E. Savage. The Complexity of Computing, Wiley-Interscience, New York, 1976.

[Sha 49] C.E. Shannon. "The synthesis of two-terminal switching circuits", Bell System Technical Journal 28 (1949), 59-98.

{This is the full text of an invited lecture at the 3rd GI Conference on Theoretical Computer Science, March 1977, Darmstadt, Germany.}

December 1976

Department of Computer Science
University of Warwick
COVENTRY CV4 7AL
ENGLAND.