THE UNIVERSITY OF WARWICK

The University of Warwick

THEORY OF COMPUTATION REPORT

NO. 7

THE DEPTH OF ALL BOOLEAN FUNCTIONS

W. F. McCOLL
M. S. PATERSON

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF WARWICK
COVENTRY CV4 7AL
ENGLAND

AUGUST 1975

THE DEPTH OF ALL BOOLEAN FUNCTIONS

by

W.F. McColl and M.S.Paterson

Department of Computer Science
University of Warwick, Coventry
ENGLAND

Abstract It is shown that every Boolean function of n arguments has a circuit of depth n+1 over the basis $\{f | f : \{0,1\}^2 \rightarrow \{0,1\}\}$.

1. Introduction

Spira showed in [1] that for any $k > 0$, there is a number $N(k)$ such that if $n > N(k)$ then any n argument Boolean function has a circuit of depth $n + \underbrace{\log_2 \log_2 \ldots \log_2}_{k \text{ times}} n$.

Upper bounds on depth for specific values of n, given by Preparata and Muller [2], are

$$\begin{array}{lll} n & \text{for} & n \leq 8 \\ n+1 & \text{for} & n \leq 2^8 + 8 = 264 \\ n+2 & \text{for} & n \leq 2^{264} + 264 \\ \text{etc.} & & \end{array}$$

Whereas Knuth has shown, by computer analysis, that there are 4 argument Boolean functions requiring depth 4.

In this paper, we describe a construction which yields an upper bound of n+1 for all values of n.

2. Schemes

Our present constructions, and all previous ones for minimizing depth that we know of, have the property of being "uniform" for all functions of n arguments. The same directed graph with the same assignment of arguments to inputs is used for all the functions, the necessary variation being only in the assignment of base functions to the nodes. Lupanov's construction for minimizing formula size [3] is notable for escaping this form.

We formalize this restriction in our definition of "circuit scheme" and show that for schemes our construction achieves the optimal depth to within an additive constant.

Let

$$B_n = \{f | f : \{0,1\}^n \to \{0,1\}\}$$

and $Xn = \langle x_0, x_1, \ldots, x_{n-1} \rangle$ be the set of formal arguments we shall use in formulae and circuits.

Definition. A <u>circuit scheme</u> is a connected acyclic directed graph in which nodes have either in-degree 2 (<u>gates</u>) in which case the pair of incoming arcs are ordered, or else in-degree 0 (<u>input nodes</u>) in which case an argument x_i is assigned to the node. A <u>formula scheme</u> is a circuit scheme in which all gates have out-degree at most one.

Let $C_n \subseteq B_n$ and $b \subseteq B_2$. A circuit scheme S <u>covers C_n over basis b</u> if for each $f \in C_n$ there is an assignment of functions from b to the gates of S such that the resulting circuit computes f. Figure 1 shows a formula scheme which covers B_3 over basis B_2. This follows from the expansion

$$f(x_0, x_1, x_2) = (x_0 \wedge f_1(x_1, x_2)) \oplus f_0(x_1, x_2)$$

where $\oplus$ denotes sum modulo 2, $f_0(x_1,x_2) = f(0,x_1,x_2)$ and $f_1(x_1,x_2) = f(1,x_1,x_2) \oplus f(0,x_1,x_2)$. We have verified that this is the unique formula scheme (to within obvious symmetries) with fewer than five gates that covers B_3. Its depth of 3 is therefore optimal.

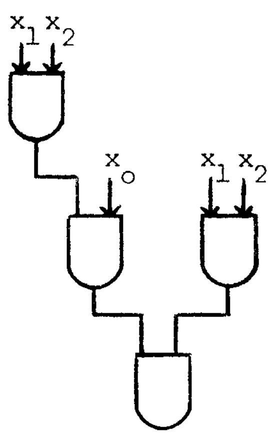

Fig.1.

We prove a lower bound on the depth of schemes by a simple counting argument.

Theorem 1. Any circuit scheme which covers B_n over any basis $b \subseteq B_2$ has depth at least n-1.

Proof. A scheme of depth D has at most 2^D-1 gates, and so by varying the assignment to gates from b can cover a set of at most $|b|^{2^D-1}$ different functions.

Since $|B_n| = 2^{2^n}$ we have

$$16^{2^D-1} \geqslant 2^{2^n}$$

which yields $D \geqslant n-1$ □

Note that this argument produces no better bound even when $|b| = 2$.

In the next two sections we describe the main result of the paper, a scheme of depth n+1 to cover B_n over basis B_2. The first stage is to produce an "approximation" to such a scheme in depth n.

3. The approximation of depth n.

If $C = \langle c_1,\ldots,c_k\rangle \in \{0,1\}^k$ and $Y = \langle y_1,\ldots,y_k\rangle$, we shall write $Y = C$ for $\bigwedge_{1\leqslant i\leqslant k} y_i = c_i$ and 0 for $\langle 0,\ldots,0\rangle$.

Another abbreviation will be to write $f(Y)$ for $f(y_1,\ldots,y_k)$, $g(Y,Z)$ for $g(y_1,\ldots,y_k,z_1,\ldots)$, etc.

Definition. Given $S = \{R_1,\ldots,R_k\}$ where $R_j \subseteq Xn$ for all j, and any $f(Xn)$, we define $g(Xn)$, the <u>approximation to f with respect to S</u> by

$$g(Xn) = 0 \text{ if } \exists R_j \in S \text{ such that } R_j = 0$$
$$= f(Xn) \text{ otherwise}$$

Any function $f(Y,Z) \in B_{k+m}$ may be expressed as a disjunctive expansion about Z by

$$f(Y,Z) = \bigvee_{C\in\{0,1\}^m} \delta_C(Z) \wedge f(Y,C)$$

where $\delta_C(Z) = 1$ if $Z = C$

$= 0$ otherwise

Dually, the conjunctive expansion about Z is

$$f(Y,Z) = \bigwedge_{C} \bar{\delta}_C(Z) \vee f(Y,C)$$

where $\bar{\delta}_C$ denotes the complement (negation) of δ_C .

It is evident that δ_C and $\bar{\delta}_C$ require formulae of depth only $\lceil \log_2 m \rceil$.

For each $n>3$, we may define sequences of positive integers $\langle r_o, r_1, \ldots, r_p \rangle$ which satisfy the following conditions, where $S_m = \sum_{i=o}^{m} r_i$ for all m :

(i) $r_o = r_1 = 2$

(ii) $S_p = n$

(iii) $r_m \leqslant 2^{S_{m-2}}$ for $m > o$ and m even

(iv) $r_m \leqslant 2^{S_{m-2}} - 2^{S_{m-3}}$ for $m > 1$ and m odd

For each such n, let p be maximal such that,

$$\frac{p(p+1)}{2} + 1 < n$$

We choose the sequence defined by

$$r_o = 2$$

$$r_i = i+1 \quad \text{for} \quad p>i>o$$

$$r_p = n-S_{p-1}$$

For example if n=12 we get <2,2,3,4,1>. This sequence satisfies (i)-(iv). The fastest-growing sequence satisfying (i)-(iv) begins, for large n, with $\langle 2,2,4,12,256,2^{20}-256, 2^{276},\ldots\rangle$

Given $\langle r_o,\ldots,r_p\rangle = \langle 2,2,3,4,\ldots\rangle$ let $R_o,R_1,\ldots,R_p$ be a corresponding partition of Xn with $|R_i| = r_i$ for all i.

We shall describe our construction in terms of formulae rather than in a more abstract way as schemes. It will be clear throughout however that the formulae are uniform.

Theorem 2. For all $f \in B_n$, (n>4), there is a formula of depth n for the approximation to f w.r.t. $S = \{R_1,\ldots,R_{p-1}\}$.

Proof. Since n > 4, then p > 1. We express f as an expansion about R_p which is disjunctive if p is odd and conjunctive if p is even. Each of the 2^{r_p} terms in this **expansion** is expressed in depth S_{p-1} by using the results and constructions of the following lemma □

For an inductive proof we must incorporate a more detailed specification of the formulae at each stage.

Lemma. Let $R_o,R_1,\ldots R_m$(m>o) be disjoint sets of arguments with their cardinalities $r_o,\ldots,r_m$ satisfying conditions (i), (iii) and (iv) above. Then for any function $f(R_o,\ldots,R_m)$, there is a formula for its approximation g w.r.t. $\{R_1,\ldots,R_m\}$ consisting of:-

Case(a): if m is odd, a disjunction of $2^{r_m}-1$ subformulae each of depth S_{m-1}

Case(b): if m is even, a conjunction of $2^{r_m}-1$ subformulae each of depth S_{m-1} and another subformula of depth S_{m-2}.

Proof. We proceed by induction on m using two alternative expansions.

In case (a),

$$g(R_o,\ldots,R_m) = \bigvee_{C\neq 0}(\delta_C(R_m) \wedge g_C(R_o,\ldots,R_{m-1}))$$

and in case (b),

$$g(R_o,\ldots,R_m) = \bar{\delta}_0(R_m) \wedge \bigwedge_{C\neq 0}(\bar{\delta}_C(R_m) \vee g_C(R_o,\ldots,R_{m-1}))$$

where in each case g_C is the approximation to $f(R_o,\ldots,R_{m-1},C)$ over $\{R_1,\ldots,R_{m-1}\}$.

The validity of these expansions is easily verified. If $m = 1$, then the first expansion is of the required form since both δ_C and g_C have depth 1 and so we have a conjunction of 3 formulae of depth 2. If $m > 1$ and m is odd then in the same expansion we may, by the inductive hypothesis, take g_C to be a conjunction of $2^{r_{m-1}}-1$ subformulae of depth S_{m-2} and a smaller subformula of depth S_{m-3}. Since δ_C is essentially a conjunction of r_m arguments and $r_m \leq 2^{S_{m-2}} - 2^{S_{m-3}}$, it may be conjoined with the smaller subformula to produce a formula of depth S_{m-2}. The resulting conjunction of $2^{r_{m-1}}$ formulae of depth S_{m-2} can be written in depth $r_{m-1} + S_{m-2} = S_{m-1}$. The requirements of case (a) are thereby met.

If m is even then the second expansion is used, the $\bar{\delta}_C$ are themselves of depth S_{m-2} and case (b) is easily satisfied □

The lemma may be illustrated with n=17, m=3 and the sequence <2,2,3,10>. The resulting approximation $g(R_o,R_1,R_2,R_3)$ is a disjunction of 1023 formulae each of the form:

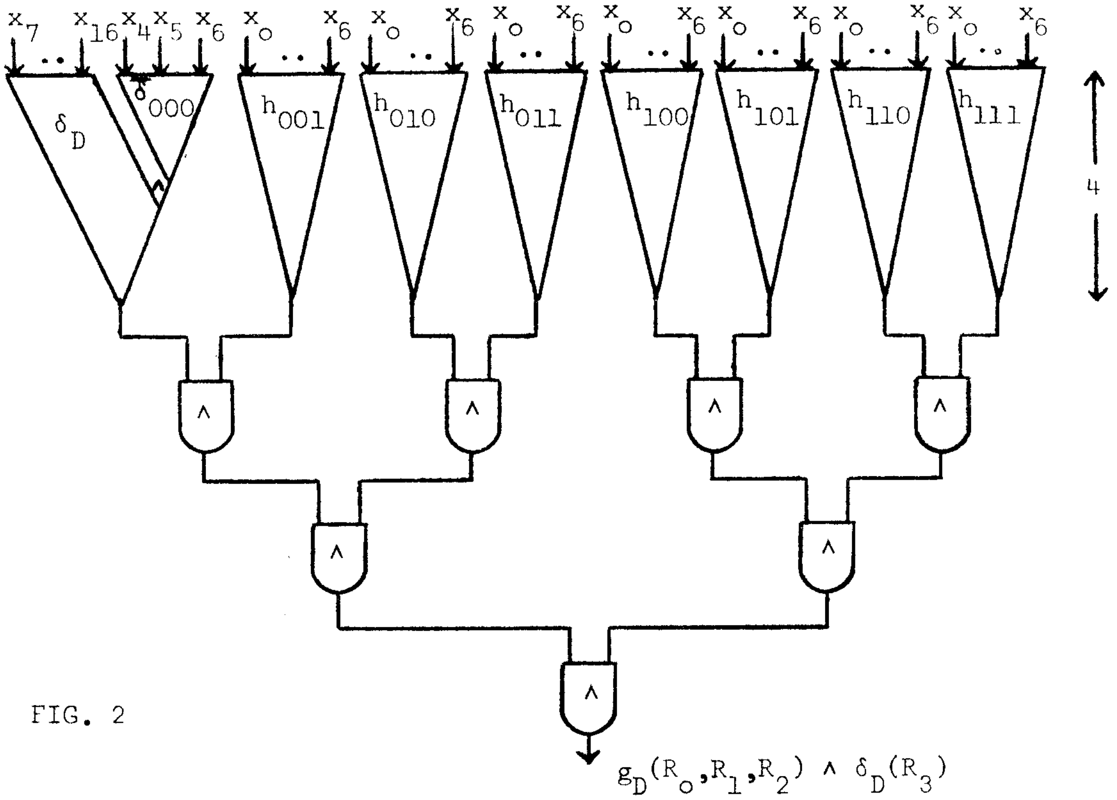

FIG. 2

The leftmost subformula may be given in more detail as:

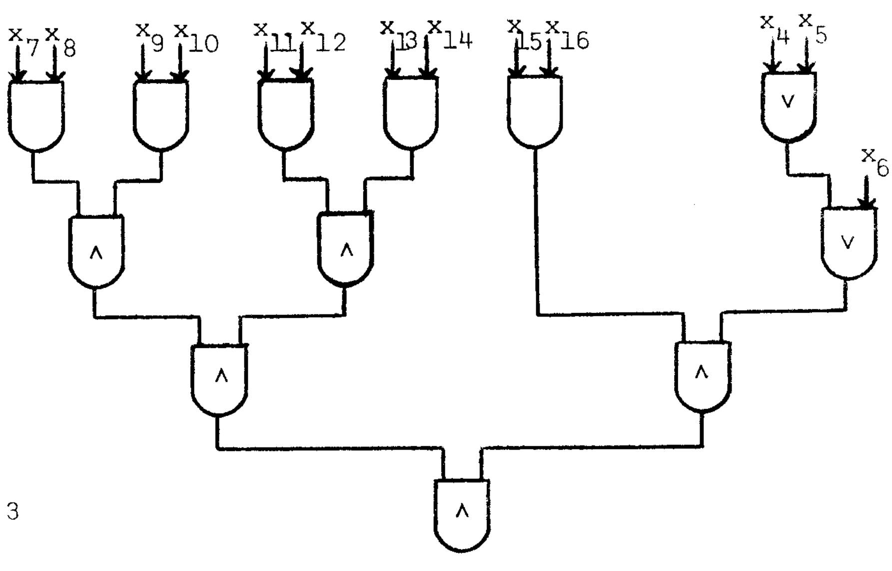

FIG. 3

where the base functions associated with certain gates are not defined if they depend on D.

Each of the $h_C(R_o,R_1,R_2)$ subformulae are of the form:

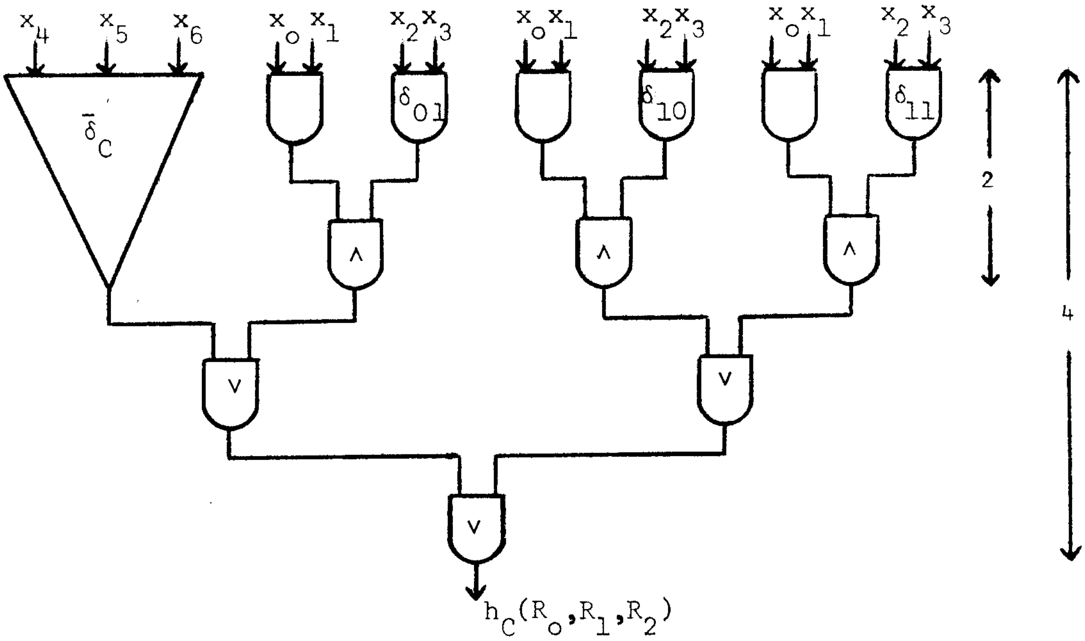

FIG. 4

where the leftmost subformula is:

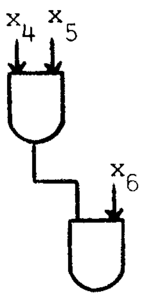

FIG. 5

and the associated base functions depend on C.

4. Main Result

It remains to be shown how the approximation g to f over $R_1,\ldots,R_{p-1}$ can be used to compute f.

Lemma. Suppose $R_1,\ldots,R_k$ are disjoint subsets of Xn. For all f(Xn), there exist $f_1(Xn-R_1),\ldots,f_k(Xn-R_k)$ such that $g_k(Xn) = f \oplus \bigoplus_{i=1}^{k} f_i$

is an approximation to some function w.r.t. $\{R_1,\ldots,R_k\}$

Proof. This is by induction on k. The lemma holds trivially for k=0. Let k>0, and suppose the result is true for k-1. Then, there exist $f_1(Xn-R_1),\ldots,f_{k-1}(Xn-R_{k-1})$ such that for all i, $1 \leq i < k$,

$$R_i = 0 \Rightarrow g_{k-1}(Xn) = f \oplus \bigoplus_{i=1}^{k-1} f_i = 0$$

We define
$$f_k(Xn-R_k) = 0 \text{ if } \exists i,\ 1 \leq i \leq k,\ R_i = 0$$
$$= g_{k-1}\Big|_{R_k=0} \quad \text{otherwise}$$

and can verify that g_k has the required property □

Main Theorem

For all n, $n \geq 1$, there is a formula scheme with depth n+1 which covers B_n over B_2.

Proof. Schemes for B_1, B_2 are obvious, while for B_3, B_4 expansions can be made about 1 and 2 arguments respectively to yield schemes of depth 3 and 4. By the previous lemma, any function f(Xn) may be computed as $g_{p-1}(Xn) \oplus \bigoplus_{i=1}^{p-1} f_i(Xn-R_i)$ where $g_{p-1}(Xn)$ is an approximation to some function w.r.t. $\{R_1,\ldots,R_{p-1}\}$.

By Theorem 2, any function $f(Xn)$ may be approximated w.r.t. $\{R_1,\ldots,R_{p-1}\}$ within depth n.

Thus for $n>4$, there is an approximation f_o with depth n and we need to "add in" appropriate functions $f_1,\ldots,f_{p-1}$ where f_i has $n_i = n - i - 1$ arguments. Whenever $n_i \leqslant 4$, a formula for f_i is constructed directly, otherwise the present construction is used recursively to yield a formula of depth $n_i + 1 = n - i$.

Thus f is expressed as

$$f_o(Xn) \oplus \bigoplus_{i=1}^{p-1} f_i(Xn-R_i)$$

or, after reassociation, as

$$f_o \oplus (f_1 \oplus (f_2 \oplus \ldots \oplus f_{p-1}))\ldots)$$

Since f_i has depth n-i for $i=o,\ldots,p-1$, this represents a formula of depth n+1.

Again it is clear that the construction is uniform and thus yields a scheme □

5. Restricted Bases

The formulae considered so far have used all of B_2 as the basis. Provided that the basis b permits a scheme to cover B_2 and contains at least one function from each of the following three types:

$\wedge$-type	$p^* \wedge q^*$
$\vee$-type	$p^* \vee q^*$
$\oplus$-type	$p^* \oplus q$

where a starred variable represents either the variable or its complement, the construction can be followed more or less as before, complementing subformulae as necessary to achieve depth n+2.

An interesting basis is the set which excludes the two $\oplus$-type functions. In using this <u>unate</u> basis we may replace $\oplus$ by

$$p \oplus q = p \wedge \bar{q} \ .\vee.\ \bar{p} \wedge q$$

In order to fit in the correcting functions efficiently we choose a new sequence

$$\langle r_0, r_1, r_2, \ldots \rangle = \langle 2,2,4,6,8,10,\ldots \rangle$$

so that each f_i contains <u>2</u> fewer arguments than the previous one. The result is a scheme of depth n+3.

For b consisting of one $\wedge$-type function and one $\vee$-type function we can obtain n+4 by taking the unate construction and complementing subformulae as necessary.

Conjecture. For any $b \subseteq B_2$, if there is a scheme over b which covers B_2 then there is a constant c such that for all n there is a scheme over b of depth n+c which covers B_n.

For $b = \{\bar{p} \vee \bar{q},\ p\}$ we have, at present, achieved no better than $n + O(\log_2 n)$.

We must distinguish the notions of complete bases for formulae and for schemes. For example, b = {NAND} is complete for formulae but obviously no singleton basis can be complete for schemes, hence the condition on b given in the conjecture.

6. Conclusion

We have described a uniform scheme for expressing all n-argument Boolean functions in depth n+1, and have matched this upper bound with a lower bound of n-1 under the restriction of uniformity. For a basis of unate functions only, our upper bound is n+3.

In our construction we used a sequence $\langle 2,2,3,4,5,\ldots \rangle$, but a sequence which grows much faster could be used instead. The effect of the choice of sequence on formula size has not been considered but easy counting arguments limit the possible size to within 2^{n-1} and 2^{n+1} for our method. Lupanov's construction [3] yields formulae of size about $2^n/\log_2 n$, though not of course using schemes. This raises the following:

Open problem : Does a lower bound of "n-constant" on depth still hold when the restriction to schemes is removed?

References

[1] Spira, P.M., "On the time necessary to compute switching functions", IEEE Trans. Computers Vol.C-20 (Jan.1971), 104-105.

[2] Preparata, F.P. and Muller, D.E., "On the delay required to realise Boolean functions", IEEE Trans. Computers Vol.C-20 (Apr.1971), 459-461.

[3] Lupanov, O.B., "Complexity of Formula Realisation of Functions of Logical Algebra", Prob. Cybernetics Vol.3 (1962), 782-811.