MIT/LCS/TM-187

$\Omega(n \log n)$ LOWER BOUNDS ON LENGTH OF BOOLEAN FORMULAS

Michael J. Fischer
Albert R. Meyer
Michael S. Paterson

November 1980

November 10, 1980

$\Omega(n \log n)$ LOWER BOUNDS ON LENGTH OF BOOLEAN FORMULAS*

Michael J. Fischer
University of Washington
Seattle, Washington, USA

Albert R. Meyer
Massachusetts Institute of Technology
Cambridge, Massachusetts, USA

and

Michael S. Paterson
University of Warwick
Coventry, England

Abstract. *A property of Boolean functions of n variables is described and shown to imply lower bounds as large as $\Omega(n \log n)$ on the number of literals in any Boolean formula for any function with the property. Formulas over the full basis of binary operations ($\wedge$, $\oplus$, etc.) are considered. The lower bounds apply to all but a vanishing fraction of symmetric functions, in particular to all threshold functions with sufficiently large threshold and to the "congruent to zero modulo k" function for $k>2$. In the case $k = 4$ the bound is optimal.*

*This work was supported in part by The National Science Foundation, Grant Nos. MCS7702474, MCS 7719754, MCS 8010707, and by a grant to the M.I.T. Laboratory for Computer Science by the IBM Corporation. The results reported here appeared in weaker preliminary form in a paper with a similar title [FMP 75].

1.Introduction. We describe a property of Boolean functions of n variables which implies lower bounds on the size of all Boolean formulas for functions with the property. Let C_k^n be the Boolean function "congruent to zero modulo k" of n arguments, that is, $C_k^n(x_1,...,x_n)$ iff $\Sigma_{i=1}^n x_i \equiv 0 \pmod{k}$. We show that C_k^n has the property and conclude that there is a constant $\varepsilon > 0$ such that any Boolean formula for C_k^n over the full basis of binary and unary Boolean operations ($\wedge$, $\vee$, $\neg$, $\oplus$, *NAND*, etc.) is of length exceeding $\varepsilon n \log(n/k)$ for all $k \geq 3$ and all n. There are formulas for C_4^n of length asymptotic to $n \log_2 n$, so our bound is achieved to within a constant multiple in this case.

The logarithm of the minimum length of a formula for a Boolean function gives the minimum *time*, i.e., depth, of a combinational circuit computing the function. This remark provides some technological motivation for our results. The depth of formulas is also related to the space and parallel time of computations and so is of basic concern in the theory of computational complexity; see [Pat 76, McC 78a, 78b, Bor 77] for further discussion.

General counting arguments allow one to conclude that *most* Boolean functions of n variables require formulas of size asymptotic to $2^n/\log_2 n$ [RiS 42, Lup 60, Kri 61]. The largest lower bound provable for *explicit* examples however is proportional to $n^2/\log n$ by Neciporuk [Nec 66].[1] Although Neciporuk's method yields lower bounds for many explicit examples [cf. Pat 76, 77], no symmetric function possesses the property which implies Neciporuk's lower bounds. Hodes and Specker [HoS 68] provide another general property of functions which implies nonlinear lower bounds on the length of formulas, and Hodes [Hod 70] demonstrates that it is widely applicable.[2] For example, Hodes' and Specker's results imply that formulas for all but sixteen of the 2^{n+1} symmetric Boolean functions of n variables grow nonlinearly in n [Khr 76, Pat 76,77].

Our main theorem resembles that of Hodes and Specker. We essentially show that any function which can be defined by a "small" formula can be restricted to a "large" subset of its variables so that the resulting restricted formula is equivalent to the sum modulo two of a subset of its variables. Since C_k^n and indeed almost all symmetric functions do not have such large simple restrictions, they cannot have small formulas. Comparing our results to Hodes' and Specker's in the most interesting case of symmetric functions, we note that their theorem yields nonlinear lower bounds whenever ours does, but their bounds are much smaller.[3] Indeed, our bounds of $\Omega(n \log n)$ are the largest lower bounds on formula length known for *any* symmetric Boolean function. (We remind the reader that $\alpha(n) = \Omega(\beta(n))$ iff $\beta(n) = O(\alpha(n))$ iff lim inf $\alpha(n)/\beta(n) > 0$.)

In the next section we state the main theorem giving lower bounds and apply it to C_k^n and a related example. In Section 3 we derive a corollary which is easily applicable to arbitrary symmetric functions and then prove that all but a vanishing fraction of symmetric functions require formulas of length $\Omega(n \log n)$. Section 4 contains the proof of the main theorem. In the final Section 5, we compare known upper and lower bounds on formula length and mention some open problems.

2.The Lower Bound. Boolean formulas over the *full unary-binary basis* are constructed from variables and constants (0 and 1) possibly using any of the unary and binary Boolean connectives ($\wedge$, $\vee$, $\neg$, $\oplus$, *NAND*, etc.). Let L(f), the *length* of the formula f, be the number of occurrences of variables (not constants) in f. Let var(f) be the set of variables that appear in f. Formulas f and g are *equivalent*, denoted $f \equiv g$, iff f and g define the same function on var(f) $\cup$ var(g). Every Boolean formula g is easily shown to be equivalent to a Boolean formula f constructed from variables and constants using *only* the two connectives $\oplus$ ("exclusive or") and $\wedge$ ("and") such that f contains *exactly* the same number of occurrences of each variable as g. In particular L(g) = L(f), so without loss of generality we henceforth consider Boolean formulas constructed from variables and constants using only $\oplus$ and $\wedge$.

An *assignment*, A, over a set of variables, V, is a partial map from V into $\{0,1\}$; dom(A) $\subseteq$ V is the set of variables on which A is defined, i.e., the variables which A *fixes*. The *eccentricity*, ecc(A), of an assignment A is the excess of 1's over 0's in the assignment, that is, ecc(A) = $|A^{-1}(1)| - |A^{-1}(0)|$. A is *central* if ecc(A) is zero or one. Given a formula f and an assignment A, the *restriction*, $f|_A$, is the formula obtained by substituting A(x) for each occurrence of x in f, where x ranges over dom(A). If A is central and dom(A) $\subseteq$ var(f), then $f|_A$ is called a *central restriction* of f.

The *dimension*, dim(f), of f is the cardinality, |var(f)|, of var(f). The formula f is *affine* iff f is equivalent to some formula of the form $\oplus W \oplus c$ where $c \in \{0,1\}$ and W $\subseteq$ var(f). The theorem below shows that any Boolean formula of n variables, all of whose affine central restrictions have small dimension, has length $\Omega(n \log n)$. More precisely, let the *affine diameter*, diam(f), of f be the largest dimension of any affine central restriction of f.

Lower Bound Theorem. There is an $\varepsilon > 0$ such that for any Boolean formula f with n variables

$$L(f) \geq \varepsilon n \log(n/\mathrm{diam}(f)).$$

The theorem immediately applies to formulas for C_k^n. To see this, note that the only affine restrictions of C_k^n either are of dimension one or are equivalent to constant functions of dimension less than k, so $\mathrm{diam}(C_k^n) < k$. Therefore,

Example 1. $L(C_k^n) > \varepsilon n \log(n/k)$.

As another example, consider $n = km$ variables x_{ij} for $1 \leq i \leq k$, $1 \leq j \leq m$ and refer to the variables with second index j as the j^{th} block of variables. Let p_j denote the mod 2 sum of the j^{th} block, namely, $p_j = \oplus_{i=1}^{k} x_{ij}$, and let $f^{k,m}$ be the function $C_4^m(p_1,\ldots,p_m)$ of n variables. It is not hard to see that no restriction of a formula for $f^{k,m}$ which contains variables from three or more blocks is affine. Hence $\mathrm{diam}(f^{k,m}) \leq 2k$, so

Example 2. $L(f^{k,m}) \geq \varepsilon km \log(m/2)$ for ε as in the Lower Bound Theorem.

We remark that choosing $k = n^{1-\delta}$ still yields $\Omega(n \log n)$ lower bounds on $L(f^{k,m})$ even though $f^{k,m}$ has "large" affine diameter $n^{1-\delta}$. This is an example where Hodes' and Specker's results do not apply.

To establish an upper bound on $L(C_4^n)$, let x denote Boolean variables $x_1,\ldots,x_n$. Construct formulas $D_0^n(x)$ and $D_1^n(x)$ for the low order and second lowest order digits of the binary representation of $\Sigma_{i=1}^n x_i$ as follows. $D_0^1(x_1) = x_1$ and $D_1^1(x_1) = 0$. Let y denote $x_{n+1},\ldots,x_{2n}$. Then

$$D_0^{2n}(x,y) = \oplus_{i=1}^{2n} x_i \text{, and}$$

$$D_1^{2n}(x,y) = D_1^n(x) \oplus D_1^n(y) \oplus (D_0^n(x) \oplus D_0^n(y)).$$

Hence $L(D_0^n) = n$, and $L(D_1^{2n}) = 2(L(D_1^n) + L(D_0^n))$. This recurrence implies that $L(D_1^n) \leq n \log_2 n$ when n is a power of two. Now a formula for C_4^n is $\mathrm{NOR}(D_0^n, D_1^n)$, so $L(C_4^n) \leq n(1 + \log_2 n)$ when n is a power of two. For arbitrary n, one can obtain a formula for C_4^n of length $n\lceil \log_2 n \rceil + 2n - 2^{\lceil \log_2 n \rceil}$, so

Proposition 1. $L(C_4^n) < n\lceil 1 + \log_2 n \rceil$ for all n.

Since $L(f^{k,m}) \leq L(C_4^m) \cdot L(p_j)$ and $L(p_j) = k$, we also have

Proposition 2. $L(f^{k,m})$ is asymptotically at most $km \log_2 m$.

So the lower bounds on L in Example 1 for $k = 4$ and in Example 2 are achievable to within a multiplicative factor.

3.Lower Bounds For Symmetric Functions. For any Boolean formula f of dimension n which defines a symmetric function, there is by definition a *characteristic function*,

$$\chi_f:\{0,\ldots,n\} \to \{0,1\}, \text{ such that } f(x_1,\ldots,x_n) = \chi_f(\Sigma_{i=1}^n x_i).$$

Lemma. If $\chi_f(\lfloor n/2 \rfloor) \neq \chi_f(\lfloor n/2 \rfloor+2)$, then $L(f) \geq \varepsilon n \log(n/2)$.

Proof. The reader can easily verify that no *central* restriction of f which has three or more variables can be affine, viz., $\mathrm{diam}(f) \leq 2$. The bound on L(f) now follows immediately from the Lower Bound Theorem. □

Symmetric Function Lower Bound Theorem. There is an $\varepsilon > 0$ such that for every formula f of dimension n which defines a symmetric function, if $\chi_f(k) \neq \chi_f(k+2)$ for some k, $0 \leq k \leq n - 2$, then

$$L(f) \geq \varepsilon n \log \min(k, n - k).$$

Proof. Assume without loss of generality that $k \leq n/2$. Let A be any assignment such that $|\mathrm{dom}(A) \cap \mathrm{var}(f)| = n - 2k$ and $A(x) = 0$ for all $x \in \mathrm{dom}(A)$. Now $\chi_{f|_A}(j) = \chi_f(j)$ for $0 \leq j \leq 2k = \dim(f|_A)$, so applying the Lemma above to $f|_A$ yields

$$L(f|_A) \geq \varepsilon 2k \log(2k/2).$$

Therefore, at least one of the 2k variables of $f|_A$ occurs $\varepsilon \log k$ or more times in $f|_A$, and *a fortiori* also occurs that often in f.

By choosing dom(A) to be the $n - 2k$ most frequently occurring variables in f, we conclude that each variable in dom(A) occurs at least $\varepsilon \log k$ times in f, so

$$L(f) \geq (n - 2k)\varepsilon \log k + L(f|_A) \geq (n - 2k)\varepsilon \log k + 2k\varepsilon \log k = \varepsilon n \log k. \quad \square$$

Let T_k^n be the threshold k function of n variables, that is,

$$T_k^n(x_1,\ldots,x_n) = 1 \text{ iff } \Sigma_{i=1}^n x_i \geq k.$$

Since $\chi_{T_k^n}(k) = 0$ and $\chi_{T_k^n}(k + 2) = 1$, we have

Example 3. $L(T_k^n) \geq \varepsilon n \log \min(k, n - k)$.

More generally, there are exactly $4 \cdot 2^{2b}$ symmetric functions f of n variables such that $\chi_f(k) = \chi_f(k + 2)$ for all k, $b \leq k \leq n - b$. The preceding Theorem implies a bound of $\epsilon n \log b$ on length of formulas for the remaining $2^{n+1} - 4 \cdot 2^{2b}$ symmetric functions. Choosing any δ, $0 < \delta < 1$, and $b = \delta n$, we have:

Corollary. The minimum formula length for all but $o(2^{n+1})$ of the 2^{n+1} symmetric functions of n variables is $\Omega(n \log n)$.

Finally, we note that the Symmetric Function Lower Bound Theorem also applies to nonsymmetric functions f as long as $\chi_f(k)$ and $\chi_f(k+2)$ are well defined, i.e., as long as

$$\Sigma_{i=1}^{n} x_i = \Sigma_{i=1}^{n} y_i = m \text{ implies } f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)$$

for $m = k, k+2$. For example, the length of formulas for *any* function which agrees with $T^n_{\lfloor n/2 \rfloor}$ on arguments of weight $\lfloor n/2 \rfloor$ and $\lfloor n/2 \rfloor + 2$ is $\Omega(n \log n)$.

4.Proof of the Lower Bound. The Lower Bound Theorem follows directly from the Main Lemma below. The proof of the Main Lemma requires four elementary lemmas which are presented first.

Let f, g be formulas. We call g an *affine variant* of f iff $f \oplus g$ is affine. A formula f is an *r-formula* if no variable in f occurs more than r times; f is *r-minimal* with respect to some property of formulas if f is an r-formula and L(f) is minimal among the r-formulas with the property. (Note that $L(f) \leq r \cdot \dim(f)$ for any r-formula f, but this condition does not imply that f is necessarily an r-formula.)

Affine Variant Lemma: Let g be an affine variant of f. For all assignments A,

(i) $f|_A$ is affine if $g|_A$ is affine, and

(ii) if for some $r \geq 1$, g is an r-minimal affine variant of f and

$$\mathrm{dom}(A) \subseteq \mathrm{var}(g), \text{ then } \dim(f|_A) - \dim(g|_A) = \dim(f) - \dim(g).$$

Proof:(i) The formula $f \oplus g$ is affine by hypothesis, hence $f|_A \oplus g|_A$ is affine. If also $g|_A$ is affine, then adding the two together gives the affine function $f|_A$.

(ii) $\mathrm{var}(g) \subseteq \mathrm{var}(f)$, for if not, substituting constants for the variables in g which do not appear in f yields a shorter affine variant which is an r-formula, contradicting the r-minimality of g. The result follows easily. □.

An assignment B is an *extension* of A if B extends the partial function A. Let dom(B,A) denote dom(B) - dom(A), the set of new variables fixed by B.

Conjunction Lemma: Given a central assignment A and a formula f such that $f|_A \equiv g \wedge h$, where g and h are affine, there is a central extension B of A such that $\mathrm{dom}(B,A) \subseteq \mathrm{var}(f|_A)$, $f|_B$ is affine, and $\dim(f|_B) \geq \dim(f|_A)/3$.

Proof: We have

$$G \equiv \bigoplus P \oplus \bigoplus R \oplus c \quad \text{and} \quad H \equiv \bigoplus Q \oplus \bigoplus R \oplus d$$

where P, Q, R are disjoint subsets of $\mathrm{var}(f|_A)$ and $c,d \in \{0,1\}$. Let B_1, B_2, B_3 be central extensions of A fixing additionally the variables of $Q \cup R$, $P \cup R$, $P \cup Q$ respectively. Each of $f|_{B_i}$ for i=1,2,3 is affine and

$$\mathrm{var}(f|_{B_1}) \cup \mathrm{var}(f|_{B_2}) \cup \mathrm{var}(f|_{B_3}) = P \cup Q \cup R = \mathrm{var}(f|_A).$$

Hence, for some i, $\dim(f|_{B_i}) \geq \dim(f|_A)/3$. □

Partition Lemma: Given sets $S_1, S_2, \ldots, S_t$, let T be the elements which occur in two or more of the S_i. That is,

$$T = \bigcup_{i<j\leq t} (S_i \cap S_j).$$

Then there exists a partition $\{\lambda,\mu\}$ of $\{1,\ldots,t\}$ such that if $L = \bigcup_{i\in\lambda} S_i$ and $M = \bigcup_{i\in\mu} S_i$, then $|L \cap M| \geq |T|/2$.

Proof: The proof is by induction on t. The case t=1 is trivial. Given $S_1, \ldots, S_t, S_{t+1}$, we have by induction a partition $\{\lambda,\mu\}$ of $\{1,\ldots, t\}$ and sets L, M, and T satisfying the lemma. We now define a partition $\{\lambda',\mu'\}$ of $\{1, \ldots, t+1\}$ as follows.

Let $T_L = (S_{t+1} \cap L) - T$ and $T_M = (S_{t+1} \cap M) - T$. Assume without loss of generality that $|T_M| \geq |T_L|$ and define $\lambda' = \lambda \cup \{t+1\}$, $\mu' = \mu$. Now let

$$L' = \bigcup_{i\in\lambda'} S_i = L \cup S_{t+1}, \qquad M' = \bigcup_{i\in\mu'} S_i = M,$$

and let T′ be the elements which appear two or more times among $S_1, \ldots, S_{t+1}$. Note that T′ is the disjoint union of T, T_L, and T_M.

Since $|T_M| \geq |T_L|$, at least half the elements in T′ - T are in T_M. Also since L

$\cap M \subseteq T$, the hypothesis implies that at least half the elements in T are in $L \cap M$. But $T_M \cup (L \cap M) \subseteq L' \cap M'$ by definition. Hence at least half the elements in T′ are in $L' \cap M'$. □.

Beta Lemma: There exist constants $\alpha > 0$, $a > 1$ such that if we define $\beta(r) = (\alpha a^r C_r)^{-1}$ where $C_r = \binom{2r-2}{r-1}/r$ is the Catalan number, then

(i) $\beta(r) = \alpha/\Sigma_{s=1}^{r-1}(\beta(r)\beta(r-s))^{-1}$ for $r > 1$,

(ii) $\beta(r) \leq (1 - 15\alpha)/6 < 1$ for $r \geq 1$,

(iii) $\beta(r) \leq (1 - 5\alpha)/(1 - 5\alpha + 4r)$.

Proof: (i) The Catalan numbers satisfy the convolution property

$$C_r = \Sigma_{s=1}^{r-1} C_s C_{r-s}$$

[Knu 73, Section 2.3.4.4] from which the corresponding property (i) of β follows immediately.

(ii), (iii). Moreover, C_r is asymptotic to $dr^{-3/2}4^r$ for some fixed $d>0$ [Knu 73, Section 2.3.4.4]. This estimate makes it obvious that for any sufficiently small α one can choose a value for a which guarantees (ii) and (iii). Suitable values are $\alpha = 1/30$ and $a = 360$. □

Main Lemma: Let f be an r-formula with $r \geq 1$, and let A_0 be a central assignment. There exists a central extension A of A_0 such that $f|_A$ is affine, $\mathrm{dom}(A,A_0) \subseteq \mathrm{var}(f)$, and

$$\dim(f|_A) \geq \beta(r)\cdot\dim(f|_{A_0}).$$

Proof of Main Lemma: The proof is by course-of-values induction on r. Hence we assume $r \geq 1$ and that the lemma holds for all r′-formulas with $r' < r$. To show the lemma holds for all r-formulas, we proceed using a course-of-values subinduction on L(f). Hence we consider some r-formula f and some central assignment A_0, and further assume that the lemma holds for all r-formulas of length less than L(f).

Suppose that g is an r-minimal affine variant of $f|_{A_0}$ and $L(g) < L(f)$. Then by the subinduction hypothesis, there is a central extension A of A_0 satisfying the lemma for g. $f|_A$ is affine by the Affine Variant Lemma (i). Moreover,

$$\dim(f|_A) = \dim(g|_A) + (\dim(f|_{A_0}) - \dim(g)) \qquad \text{by Affine Variant Lemma (ii)}$$

$$\geq \beta(r)\cdot\dim(g) + (\dim(f|_{A_0}) - \dim(g)) \qquad \text{by induction}$$

$$\geq \beta(r)\cdot\dim(f|_{A_0}) \qquad \text{since } \beta(r) < 1 \text{ by Beta Lemma (ii).}$$

This shows the lemma holds for f using the same A.

Hence we can assume that f is an r-minimal affine variant of $f|_{A_0}$. In particular, we have $f = f|_{A_0}$ and $\mathrm{var}(f) \cap \mathrm{dom}(A_0) = \emptyset$.

Express f as $\oplus_{i=1}^{k} F_i$ where no F_i has $\oplus$ as its main connective. Clearly no F_i is affine since otherwise $(\oplus_{j\neq i} F_j)$ is an affine variant of f, contradicting the minimality of f. Hence, each F_i equals $G_i \wedge H_i$, and furthermore the minimality of f ensures that neither of the formulas G_i nor H_i are equivalent to constant functions.

We define a partition of each set $\mathrm{var}(F_i)$ into four sets as follows:

$\mathrm{global}(F_i) = \mathrm{var}(F_i) \cap (\cup_{j\neq i} \mathrm{var}(F_j))$;

$\mathrm{joint}(G_i,H_i) = (\mathrm{var}(G_i) \cap \mathrm{var}(H_i)) - \mathrm{global}(F_i)$;

$\mathrm{own}(G_i) = \mathrm{var}(G_i) - (\mathrm{joint}(G_i,H_i) \cup \mathrm{global}(F_i))$;

$\mathrm{own}(H_i) = \mathrm{var}(H_i) - (\mathrm{joint}(G_i,H_i) \cup \mathrm{global}(F_i))$.

Let **global** = $\cup_i$ $\mathrm{global}(F_i)$, **joint** = $\cup_i$ $\mathrm{joint}(G_i,H_i)$, and **own** = $\cup_i$ $(\mathrm{own}(G_i) \cup \mathrm{own}(H_i))$. So var(f) is the disjoint union of **global, joint,** and **own.**

The following four cases, defined solely in terms of the cardinalities of var(f), **global, joint,** and **own,** are obviously exhaustive. Let n = dim(f).

Case 1: $n \leq 1/\beta(r)$. In this case we can take any central extension A of A_0 such that $\mathrm{dom}(A, A_0) \subseteq \mathrm{var}(f)$ and $\dim(f|_A) = 1$. Any formula in a single variable is necessarily affine.

Case 2: $|\mathbf{global}| \geq 2\alpha n$. Noting that **global** equals the set of variables which occur in two or more of the sets $\mathrm{var}(F_i)$, we apply the Partition Lemma to the sets $\mathrm{var}(F_i)$, i=1, ..., k, and obtain a partition $\{\lambda,\mu\}$ of $\{1, ..., k\}$ such that

$$|\cup_{i\epsilon\lambda} \mathrm{var}(F_i) \cap \cup_{i\epsilon\mu} \mathrm{var}(F_i)| \geq |\mathbf{global}|/2 \geq \alpha n.$$

Now f is equivalent to $L \oplus M$ where $L = \oplus_{i\epsilon\lambda} F_i$, $M = \oplus_{i\epsilon\mu} F_i$. We use the fact that all the variables of $\mathrm{var}(L) \cap \mathrm{var}(M)$ must occur fewer than r times in each of L, M, to invoke the Main Lemma successively on the two parts. For $1 \leq s \leq r - 1$, let V_s be the set of those variables of $\mathrm{var}(L) \cap \mathrm{var}(M)$ which occur exactly s times in L (and hence at most r - s times in M). For some t,

$$|V_t| \geq \beta(r)n/(\beta(t)\beta(r-t))$$

since

$$\Sigma_{s=1}^{r-1} |V_s| = |\mathrm{var}(L) \cap \mathrm{var}(M)| \geq \alpha n = \Sigma_{s=1}^{r-1} [\beta(r)n/(\beta(s)\beta(r-s))]$$

by Beta Lemma (i).

Let B be any central extension of A_0 with $\mathrm{dom}(B,A_0) = \mathrm{var}(f) - V_t$, and let $L' = L|_B$, $M' = M|_B$. Thus $\mathrm{var}(L') = \mathrm{var}(M') = V_t$. The Main Lemma applied to the t-formula L′ yields an extension B′ of B such that $L'|_{B'}$ is affine and

$$\dim(M'|_{B'}) = \dim(L'|_{B'}) > \beta(t)\cdot\dim(L') \geq \beta(r)n/\beta(r-t).$$

The Lemma applied to the (r-t)-formula $M'|_{B'}$ yields an extension A of B′ such that $M'|_A$ is affine and $\dim(M'|_A) \geq \beta(r-t)\cdot\dim(M'|_{B'}) \geq \beta(r)n$. Since $(L \oplus M)|_A = ((L'|_{B'})|_A) \oplus (M'|_A)$ and is clearly affine, and $\dim((L \oplus M)|_A) = \dim(M'|_A) \geq \beta(r)n$, we have concluded the proof of Case 2.

Case 3: $|\mathbf{joint}| \geq 3\alpha n$.

Each variable in **joint** occurs in exactly one F_i, and at least once but strictly fewer than r times in G_i and in H_i. We will restrict to a subset of these variables and then apply the induction hypothesis for smaller values of r.

Let $u_i = |\mathrm{joint}(G_i,H_i)|$. As in Case 2, there is some t_i, $1 \leq t_i \leq r - 1$, such that if V_i is the set of variables in $\mathrm{joint}(G_i,H_i)$ that occur exactly t_i times in G_i (and hence at most $r-t_i$ times in H_i) then

$$|V_i| \geq u_i\beta(r)/(\alpha\beta(t_i)\beta(r-t_i)).$$

Let B_0 be any central extension of A_0 fixing all the variables in $\mathrm{var}(f) - \cup_i V_i$, and let $F_i' = F_i|_{B_0}$, $G_i' = G_i|_{B_0}$, $H_i' = H_i|_{B_0}$. G_i' is a t_i-formula and H_i' is an $(r-t_i)$-formula.

We now proceed in k stages. At the i^{th} stage, we find a central extension B_i of B_{i-1} such that $F_i'|_{B_i}$ is affine and $\dim(F_i'|_{B_i}) \geq u_i\beta(r)/(3\alpha)$.

Stage i: Since G_i' is a t_i-formula, $1 \leq t_i < r$, we apply the induction hypothesis to G_i' and B_{i-1} to obtain a central extension B_i' such that $G_i'|_{B_i'}$ is affine and $\dim(G_i'|_{B_i'}) \geq \beta(t_i)\cdot\dim(G_i')$. Since H_i' is an $(r-t_i)$-formula, $r-t_i < r$, we apply the induction hypothesis again to $H_i'|_{B_i'}$ to obtain a central extension B_i'' such that $H_i'|_{B_i''}$ is affine and $\dim(H_i'|_{B_i''}) \geq \beta(r-t_i)\cdot\dim(H_i'|_{B_i'})$. The restriction of an affine function is affine, so $G_i'|_{B_i''}$ affine. Hence, by the Conjunction Lemma there exists a central extension B_i of B_i'' such that $F_i'|_{B_i}$ is affine and has dimension at least $\dim(F_i'|_{B_i''})/3$. In calculating the dimension of $F_i'|_{B_i}$, we make use of the fact that $\mathrm{var}(F_i') = \mathrm{var}(G_i') = \mathrm{var}(H_i') = V_i$. We have

$$\begin{aligned}\dim(H_i'|_{B_i''}) &\geq \beta(r-t_i)\cdot\dim(H_i'|_{B_i'}) = \beta(r-t_i)\cdot\dim(G_i'|_{B_i'}) \\ &\geq \beta(r-t_i)\beta(t_i)|V_i| \geq u_i\beta(r)/\alpha.\end{aligned}$$

Then

$$\dim(F_i'|_{B_i}) \geq \dim(H_i'|_{B_i''})/3 \geq u_i\beta(r)/(3\alpha).$$

Now let $A = B_k$, the central assignment obtained after the final stage. Note that $f|_A = \oplus_{i=1}^{k} F_i'|_{B_i}$, and so $f|_A$ is affine. Moreover,

$$\dim(f|_A) = \Sigma_i \dim(F_i'|_{B_i}) \geq \Sigma_i u_i\beta(r)/(3\alpha) = |\mathrm{joint}|\beta(r)/3\alpha \geq \beta(r)n$$

by the defining condition for this case. This concludes the proof of Case 3.

Case 4: $|\mathrm{own}| \geq (1 - 5\alpha)n$ and $n > 1/\beta(r)$.

In this case, we will find a central extension B of A_0 such that $\mathrm{dom}(B) \subseteq \mathrm{var}(f)$ and $f|_B$ is functionally independent of some non-empty subset V of its variables. Let yield = $|V|$ and cost = yield + $|\mathrm{dom}(B,A_0)|$. If yield $\geq \beta(r)\cdot$cost, then we can find a central extension A of B satisfying the Lemma for f.

To see this, let g be the restriction of $f|_B$ obtained from some arbitrary assignment to V. Note that g is equivalent to $f|_B$ since $f|_B$ does not depend on V. Also, var(f) is the disjoint union of dom(B,A_0), V, and var(g); in particular, dim(f) = cost + dim(g). Now L(g) < L(f) since V is non-empty, so by the subinduction hypothesis there is a central extension A of B such that $g|_A$ is affine, dom(A,B) $\subseteq$ var(g), and dim($g|_A$) $\geq \beta$(r)·dim(g). But $f|_A$ is equivalent to $g|_A$, so $f|_A$ is also affine. Moreover, var($f|_A$) is the disjoint union of var($g|_A$) and V since dom(A) $\cap$ V = $\emptyset$. Therefore,

$$\dim(f|_A) = \dim(g|_A) + \text{yield} \geq \beta(r)\cdot\dim(g) + \beta(r)\cdot\text{cost} = \beta(r)\cdot\dim(f),$$

as required.

Thus, to complete the proof, we need only describe how to determine B and V.

Let g_i = |own(G_i)|, h_i = |own(H_i)|. Without loss of generality, we can assume $g_i \geq h_i$. We note that $\Sigma_i\, g_i \geq$ |own|/2.

For each i, we have two strategies which can remove the dependence of f on a subset of either own(G_i) or own(H_i). We will show below that at least one of these always has an adequate yield/cost ratio for some i.

Strategy A: This strategy is applicable only if there is a central extension of A_0 fixing only var(f) and making H_i equivalent to 0. Find a minimal central extension B of A_0 for which $H_i|_B \equiv 0$, var(H_i) $\subseteq$ dom(B) $\subseteq$ var(f), and dom(B) $\cap$ own(G_i) is as small as possible among such extensions. Since $F_i = G_i \wedge H_i$, we have $F_i|_B \equiv 0$, and so $f|_B$ is independent of any remaining variables of own(G_i). Thus V is own(G_i) - dom(B).

Strategy B: This strategy is applicable only if there is a central extension of A_0 fixing only var(H_i) $\cup$ dom(A_0) and making H_i equivalent to 1. Find a maximal set V $\subseteq$ own (H_i) for which there is a central extension B of A_0 satisfying $H_i|_B \equiv 1$ and dom(B,A_0) = var(H_i) - V. Since $f|_B$ is independent of V, the yield is |V| and the cost is dim(H_i).

We begin our analysis by noting that since f is r-minimal, no subformula of f is equivalent to a constant. Hence there is an extension B′ of A_0 such that $H_i|_{B'} \equiv 0$. Let d(H_i) be the least integer for which there is an extension B′ of A_0 such that dom(B′,A_0) = var(H_i), $H_i|_{B'} \equiv 0$, and

$$-d(H_i) \leq \text{ecc}(B') \leq d(H_i) + 1.$$

Clearly, d(H_i) $\leq$ dim(H_i).

Suppose Strategy A is applicable and B is the assignment required in the strategy. Let B′ be the restriction of the partial function B to $\mathrm{dom}(A_0) \cup \mathrm{var}(H_i)$. Since B is minimal central such that $H_i|_B \equiv 0$, it must be that $\mathrm{ecc}(B')$ equals either $-d(H_i)$ or $d(H_i) + 1$, and the variables in $\mathrm{dom}(B,B')$ are the minimal number which serve to extend B′ to a central assignment. Hence,

$$|\mathrm{dom}(B,A_0)| = \dim(H_i) + d(H_i).$$

Since B is defined to fix as few variables from $\mathrm{own}(G_i)$ as possible, either $\mathrm{dom}(B) \cap \mathrm{own}(G_i) = \varnothing$ or $\mathrm{own}(G_i) - \mathrm{dom}(B) = \mathrm{var}(f) - \mathrm{dom}(B)$. Therefore,

$$\mathrm{yield}_A = |\mathrm{own}(G_i) - \mathrm{dom}(B)| = \min(g_i, n - \dim(H_i) - d(H_i)), \text{ and}$$

$$\mathrm{cost}_A = \dim(H_i) + d(H_i) + \mathrm{yield}_A = \min(g_i + \dim(H_i) + d(H_i), n).$$

If Strategy A is not applicable, let $\mathrm{yield}_A = 0$ and $\mathrm{cost}_A = n$, so the preceding formulas for cost_A and yield_A always hold.

If $\mathrm{yield}_A/\mathrm{cost}_A \geq \beta(r)$ for some value of i, then Strategy A succeeds.

In any application of Strategy B, $|V| \geq \min(h_i, d(H_i) - 1)$. To see this, let V′ be any subset of $\mathrm{own}(H_i)$ such that $|V'| = \min(h_i, d(H_i) - 1)$, and let B′ be any central extension of A_0 with $\mathrm{dom}(B') = \mathrm{dom}(A_0) \cup (\mathrm{var}(H_i) - V')$. Let C be an arbitrary assignment with $\mathrm{dom}(C) = V'$. Then

$$\begin{aligned}
-d(H_i) &< -\min(h_i, d(H_i) - 1) && \text{trivially} \\
&= -|\mathrm{dom}(C)| \\
&\leq \mathrm{ecc}(B' \cup C) && \text{since } B' \text{ is central} \\
&\leq |\mathrm{dom}(C)| + 1 && \text{since } B' \text{ is central} \\
&= \min(h_i, d(H_i) - 1) + 1 \\
&< d(H_i) + 1.
\end{aligned}$$

By the minimality condition in the definition of d, $H_i|_{(B' \cup C)} \equiv 1$. This holds for any such C, so $H_i|_{B'} \equiv 1$, and $H_i|_{B'}$ does not depend on the variables in V′. Since Strategy B chooses V as large as possible, we have $|V| \geq |V'| \geq \min(h_i, d(H_i) - 1)$ as desired.

Eliminating V from the expression of cost for Strategy B, we get

$$\mathrm{yield}_B \geq \min(h_i, d(H_i) - 1)$$

and

$$\mathrm{cost}_B = \dim(H_i).$$

If Strategy B is inapplicable, let $\mathrm{yield}_B = 0$ and $\mathrm{cost}_B = \dim(H_i)$. Note that in this case $d(H_i) = 0$, so the preceding formulas for yield_B and cost_B always hold.

If $\mathrm{yield}_B/\mathrm{cost}_B \geq \beta(r)$ for some value of i, then Strategy B succeeds.

We prove by contradiction that there exists an i for which either Strategy A or Strategy B succeeds. Assume neither Strategy succeeds for any i. Since Strategy A fails, $\mathrm{yield}_A/\mathrm{cost}_A < \beta$. (We omit the argument r from β in the remainder of this analysis.) So for all i

(1) $(1 - \beta)\min(g_i + \dim(H_i) + d(H_i), n) < \dim(H_i) + d(H_i)$.

Since Strategy B fails, $\mathrm{yield}_B/\mathrm{cost}_B < \beta$, so for all i

(2) $\min(h_i, d(H_i) - 1) < \beta\cdot\dim(H_i)$.

Let $m = |\mathbf{global} \cup \mathbf{joint}| \leq 5\alpha n$. Counting up the sizes of the various sets and using the conditions for this case, we get

(3) $d(H_i) \leq \dim(H_i) \leq m + h_i \leq n - \Sigma_j g_j \leq n - |\mathrm{own}|/2 \leq (1 + 5\alpha)n/2$.

From (3) and (2), we get

(4) $d(H_i) - m - 1 \leq \min(h_i, d(H_i) - 1) < \beta\cdot\dim(H_i) \leq \beta n$.

Using (3), (4), the fact that $\beta n > 1$, and Beta Lemma (ii), we get

(5) $\dim(H_i) + d(H_i) \leq (1 + 5\alpha)n/2 + m + 1 + \beta n$

$$< (1 + 15\alpha)n/2 + 2\beta n \leq (1 - \beta)n.$$

Assuming the "min" in (1) equals its second argument contradicts (5). Hence, the first argument is always the smaller, and (1) gives

(6) $(1 - \beta)g_i < \beta \cdot (\dim(H_i) + d(H_i)) \leq 2\beta \cdot \dim(H_i)$ for all i.

Therefore,

(7) $(1 - \beta)(1 - 5\alpha)n/2 \leq (1 - \beta)|own|/2 \leq (1 - \beta)\Sigma_i\, g_i < 2\beta\Sigma_i \dim(H_i) < 2\beta rn$

since no variable occurs more than r times in all. Now (7) yields an immediate contradiction with Beta Lemma (iii).

We conclude that Strategy A or Strategy B succeeds for some i, completing this case and the proof of the Main Lemma. □

Proof of Lower Bound Theorem: Let f be a Boolean formula on n variables. Let $r = \lfloor 2L(f)/n \rfloor$, and let A_0 be a central assignment with

$$\mathrm{dom}(A_0) = \{x \mid x \text{ occurs more than } r \text{ times in } f\}.$$

Since $f|_{A_0}$ is an r-formula, by the Main Lemma there is a central extension A of A_0 such that $f|_A$ is affine, $\mathrm{dom}(A) \subseteq \mathrm{var}(f)$, and

(8) $\dim(f|_A) \geq \beta(r) \cdot \dim(f|_{A_0})$.

By the choice of A_0, $(r+1) \cdot |\mathrm{dom}(A_0)| \leq L(f)$, so

(9) $\dim(f|_{A_0}) = n - |\mathrm{dom}(A_0)| \geq n - L(f)/(r+1) \geq n/2$.

Also,

(10) $\beta(r) \geq 2/K^r$

for some $K > 1$ using the asymptotic estimate for C_r given in the proof of the Beta Lemma. Hence, from (8), (9), (10), we get

$$\dim(f|_A) \geq (2/K^r)(n/2) = n/K^r.$$

Solving for r, we obtain

(11) $r \geq \log(n/\dim(f|_A))/\log K$.

Therefore,

$$\begin{aligned} L(f) &\geq rn/2 && \text{by choice of } r \\ &\geq \varepsilon n \log(n/\dim(f|_A)) && \text{by (11) where } \varepsilon = 1/(2 \log K) \\ &\geq \varepsilon n \log(n/\mathrm{diam}(f)) && \text{by definition of diam(f).} \quad \square \end{aligned}$$

5.Conclusions and Open Problems. The conditions we have developed above for deducing lower bounds on length of formulas apply to many explicit examples but have their most interesting applications in the case of symmetric Boolean functions. Earlier results of Hodes and Specker [HoS 68] imply that except for sixteen functions, the length of formulas for symmetric functions of n variables grows nonlinearly in n.[4] The results in this paper show that all but a vanishing fraction of the symmetric functions require formulas of length $\Omega(n \log n)$. These are the strongest known lower bounds on length of formulas for any symmetric functions.

Polynomial *upper* bounds on the length of formulas for symmetric functions were first obtained by Khrapchenko [Khr 72] and Meyer and Vilfan [Vil 72]. The smallest currently known upper bound is $o(n^{3.37})$ by Peterson [Pet 78] following earlier work of Pippenger [Pip 74] and Paterson [Pat 77]. The constructions used to achieve the upper bounds are extensions of the construction given in Section 2 of formulas for C_4^n.

It remains an open problem to improve these bounds. We note three particularly challenging instances of this general problem.

The construction of formulas for C_4^n extends in an obvious way to yield formulas of length $O(n(\log n)^{p-1})$ for C_{2p}^n but even for C_3^n the best upper bound we can obtain is $\Omega(n^2)$.

Problem 1. Is $L(C_3^n) = o(n^2)$?

The Lower Bound Theorem above does not apply to threshold functions with bounded threshold, although Hodes' and Specker's theorem yields very slowly growing nonlinear bounds (cf. Note 3). For fixed k, Khasin [Kha 69] and Pippenger [Pip 76,KlP 77] have shown that $L(T_k^n) = O(n \log n)$.

Problem 2. Is $L(T_2^n) = o(n \log n)$?

The best currently known upper bound on length of formulas for the majority function $T_{\lfloor n/2 \rfloor}^n$ is the same as for arbitrary symmetric functions.

Problem 3. Is $n \log n = o(L(T_{\lfloor n/2 \rfloor}^n))$?

Notes.

1.A slightly larger lower bound of $\Omega(n^2)$ is due to Khrapchenko [Khr 71] for the special basis of operations $\wedge$, $\vee$, $\neg$, but our results are concerned with formulas in which *all* binary operations may appear.

2.Vilfan [Vil 72, 76] extends Hodes' and Specker's results to multivalued logic with arbitrary (not necessarily binary) operations and concludes for example that formulas for C_k^n grow nonlinearly in n using d-valued logic for $k > d!$.

3. Vilfan [Vi 72] notes that the nonlinear lower bounds of Hodes and Specker can be shown to be $O(n \log^* n)$ where $\log^* n$ is the least integer m such that

$$2^{2^{\cdot^{\cdot^{2}}}} \text{(height m)} \geq n.$$

4. The sixteen functions are all of the form

$$a \oplus b \bigoplus x_i \oplus c \Pi x_i \oplus d \Pi(1 \oplus x_i)$$

for $a,b,c,d \in \{0,1\}$. Each of these obviously has a formula of length at most 3n.

References.

[Bor 77] A. Borodin. On Relating Time and Space to Size and Depth, *SIAM J. Computing* 6,4 (1977), 733-744.

[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), 37-44.

[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*, H.A. Schmidt, K. Schutte, H.-J. Thiele, eds., North Holland, Amsterdam (1968), 175-188.

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

[Khr 71] V.M. Khrapchenko. On the complexity of the realization of the linear function in the class of π-circuits. *Mat. Zametki* 9,1 (1971), 35-40 (Russian). (A translation appears in [Vil 72].)

[Khr 72] V.M. Khrapchenko. The complexity of realization of symmetrical functions by formulae. *Math. Notes of the Academy of Sciences of the USSR* 11 (1972), 70-76; orig. in *Matematicheskie Zametki* 11,1 (1972), 109-120.

[Khr 76] V.M. Khrapchenko. Complexity of Realisation of Symmetric Algebraic Logic Functions on Finite Bases. (Russian) *Problemy Kibernet.* 31 (1976), 231-234.

[KlP 77] M. Kleiman and N. Pippenger. An explicit construction of short monotone formulas for the monotone symmetric functions. *Theoretical Computer Science* 7,3 (1977), 325-332.

[Knu 73] D.E. Knuth. *The Art of Computer Programming*, vol. 1, *Fundamental Algorithms*, Addison-Wesley, Reading, MA (1973), xxi+634pp.

[Kri 61] R.E. Krichevskii. Realizations of functions by superpositions. *Prob. Cybernetics* II, Pergamon Press (1961), 458-477 (translated from the Russian).

[Lup 60] O.B. Lupanov. Complexity of formula realisation of functions of logical algebra. *Problemy Kibernet.* 3 (1960), 61-80; *Problems of Cybernetics* 3 (1962), 782-811.

[McC 78a] W.F. McColl. Complexity Hierarchies for Boolean Functions. *Acta Informatica* 11 (1978), 71-77.

[McC 78b] W.F. McColl. The Circuit Depth of Symmetric Boolean Functions. *J. Computer and System Sci.* 17,1 (1978), 108-115.

[Nec 66] E.I. Neciporuk. A Boolean function. *Soviet Math. Dokl.* 2,4 (1966), 999-1000.

[Pat 76] M.S. Paterson. An introduction to Boolean function complexity. Stanford Computer Science Report STAN-CS-76-557 Stanford University (1976), 19pp.; also in *Asterisque* (journal of the French Mathematical Society) 38-39 (1976), 183-201.

[Pat 77] M.S. Paterson. New bounds on formula size. *Proc. 3rd GI Conf. f. Informatik*, Darmstadt, *Lecture Notes in Computer Science* 48, Springer Verlag (1977), 17-26.

[Pet 78] G.L. Peterson. An Upper Bound on the Size of Formulae for Symmetric Boolean Functions, extended abstract, Dept. of Computer Science Technical Report No. 78-03-01, Univ. of Washington, Seattle (1978), 9pp.

[Pip 74] N. Pippenger. Short formulae for symmetric functions, IBM Research Report RC-5143, Yorktown Hts., N.Y. (1974), 15pp.

[Pip 76] N. Pippenger. The realization of Monotone Boolean Functions. *Proc. 8th Ann. ACM Symp. Theory of Computing*, ACM, New York (1976), 204-209.

[RiS 42] J. Riordan and C.E. Shannon. The number of two-terminal series-parallel networks. *J. Math. and Phys.* 21 (1942), 83-93.

[Vil 72] B. Vilfan. The complexity of finite functions. Ph.D Thesis, Dept. of Electrical Engineering, Technical Report 97, Project MAC, Mass. Inst. Tech., Cambridge, MA (1972), 117 pp.

[Vil 76] B. Vilfan. Lower bounds for the size of expression for certain functons in *d*-ary logic. *Theoretical Computer Science* 2, 2 (1976), 249-269.