# A LOWER BOUND FOR THE SCHOLZ-BRAUER PROBLEM

KENNETH B. STOLARSKY

**1. Introduction.** In (**6**) Scholz asked if the inequality

$$l(2^q - 1) \leqq q + l(q) - 1 \tag{1.1}$$

held for all positive integers $q$, where $l(n)$ is the number of multiplications required to raise $x$ to the $n$th power (a precise definition of $l(n)$ in terms of addition chains is given in § 2). Soon afterwards, Brauer (**2**) showed, among other things, that $l(n) \sim (\log n)/(\log 2)$. This suggests the problem of calculating

$$\theta = \liminf (l(2^q - 1) - q) \cdot \frac{\log 2}{\log q}. \tag{1.2}$$

It can be deduced from (**2**) that $\theta \leqq 1$. If $\theta < 1$, (1.1) follows immediately for infinitely many $q$. My *main result*, Theorem 5 of § 4, merely shows that $\theta$ is slightly larger than $\frac{1}{3}$. Actually, I know of no case where (1.1) is not in fact an equality; a tedious calculation verifies this for $1 \leqq q \leqq 8$.

The usual approach to (1.1) is to look first for a formula giving $l(q)$ in terms of the binary representation of $q$. Write $q = 2^{n_1} + 2^{n_2} + \ldots + 2^{n_s}$, $n_1 > n_2 > \ldots > n_s \geqq 0$, and $B(q) = s$. Clearly, if $B(q) = 1$, $l(q) = n_1$, while if $B(q) = 2$, Utz (**8**) has shown that $l(q) = n_1 + 1$. If $B(q) = 3$, Gioia, Subbarao, and Sugunamma (**3**) have shown that $l(q) = n_1 + 2$, while if $B(q) = 4$ they have shown that $l(q) = n_1 + 2$ or $n_1 + 3$, and that both cases occur. In fact, they show that if $n_1 - n_2 = n_3 - n_4$, or $n_1 - n_2 = n_3 - n_4 + 1$, or $n_1 - n_2 = 3$ and $n_3 - n_4 = 1$, then the former case occurs; however, there is still another case here, namely $n_1 - n_2 = 5$, $n_2 - n_3 = 1$, and $n_3 - n_4 = 1$. I conjecture that aside from these cases, $B(q) = 4$ implies $l(q) = n_1 + 3$.

By means of such formulae, (1.1) was shown to hold for $B(q) = 1, 2$ in (**8**), and for $B(q) = 3$ in (**3**). A very short proof of (1.1) for $B(q) \leqq 3$, based on (**2**), was given by Whyburn (**9**). If my above conjecture were true, his method would also prove (1.1) for $B(q) = 4$. However, Hansen (**4**, *Satz* 1) shows that Whyburn's method fails to decide (1.1) for infinitely many $q$.

In § 2 the necessary definitions are developed, particularly the notion of a component of an addition chain. In § 3 the structure of such components is analyzed, and lower bounds for $\theta$ are given in § 4.

Received December 27, 1967. This research was partially supported by National Science Foundation Grant GP-5802.

## 2. Definitions.

*Definition* 1. A sequence $\{a_i\}_{i=0}^r$ is called an addition chain (AC) for $n$ of length $r$ if $1 = a_0 < a_1 < \ldots < a_r = n$ and $a_i = a_j + a_k$ for $1 \leqq i \leqq r$, with $0 \leqq j, k < i$. For fixed $n$, $l(n)$ is the smallest possible value of $r$. $\{a_i\}_{i=0}^\infty$ is said to be an (infinite) AC if $\{a_i\}_{i=0}^r$ is an AC for $a_r$ of length $r$, $r \geqq 1$.

*Definition* 2. A sequence of positive integers $\{b_i\}_{i=0}^r$ is said to be of type I if for $1 \leqq i \leqq j \leqq r - 1$,

$$2^{j-i} b_i < b_{j+1} \leqq 2b_j. \tag{2.1}$$

It is said to be of type II if for $j \geqq 0$, $b_{j+1} > b_j$ and for $j \geqq 1$ either $b_{j+1} = 2b_j$ or $b_{j+1} \leqq b_j + b_{j-1}$.

*Definition* 3. For $x > 0$ let $L(x) = [(\log x)/(\log 2)]$, where $[y]$ denotes the greatest integer less than or equal to $y$. For integers $q$, let $B(q)$ be the number of 1's in the binary representation of $q$. Let $\sigma(M, N) = \sigma(M, N; 1, 0)$ and $\sigma(M) = \sigma(M, 0)$, where

$$\sigma(M, N; c_1, c_2) = \sum_{j=N}^{M} 2^{c_1 j + c_2}.$$

Clearly, for positive integers $a$ and $b$,

$$B(a + b) \leqq B(a) + B(b) \quad \text{and} \quad B(ab) \leqq B(a)B(b), \tag{2.2}$$

$$B(a) \leqq L(a) + 1, \tag{2.3}$$

and

$$B(\sigma(M, N; c_1, c_2)) = M - N + 1. \tag{2.4}$$

*Definition* 4. Given a sequence of positive numbers $\{b_i\}$, let $e_i = i - L(b_i)$. Clearly, $e_i \geqq 0$ for sequences of types I and II. Let

$$\mathscr{C}_j = \mathscr{C}_j(\{b_i\}) = \{b_i | e_i = j\}. \tag{2.5}$$

The $\mathscr{C}_j$ are said to be the *components* of the sequence. Conversely, any sequence for which $L(b_{i+1}) - L(b_i) = 1$ is said to be a component.

One easily sees that every AC is of type II, and that the components of a sequence of type II are sequences of type I. Conversely, it can be shown that a sequence of type I is almost a component in the sense that for infinitely many relatively prime integers $m$, $L(b_{j+1}m) - L(b_j m) = 1$, $j = 1, \ldots, r - 1$. It is important to note that if $n \in \mathscr{C}_j(\mathscr{A})$, $\mathscr{A}$ an AC, then $l(n) \leqq L(n) + j$. Conversely, if $l(n) = L(n) + j$, then $n \in \mathscr{C}_j(\mathscr{A})$ for some AC $\mathscr{A}$.

*Definition* 5. The word $A = \prod_{j=1}^{r} S_j$ is said to correspond to the AC

$$\mathscr{A} = \{a_i\}_{i=0}^{r}$$

if the letter $S_j$ is given by:

(1) $S_j = H_{k,l}$ if $a_j = a_{j-k} + a_{j-l}$, $l > k \geqq 2$;
(2) $S_j = D_k$ if $a_j = 2a_{j-k}$, $k \geqq 2$;
(3) $S_j = F_k$ if $a_j = a_{j-1} + a_{j-1-k}$, $k \geqq 1$;
(4) $S_j = D$ if $a_j = 2a_{j-1}$.

Write $A \leftrightarrow \mathscr{A}$, $S_j \leftrightarrow a_j$, $S_jS_{j+1} \leftrightarrow a_j, a_{j+1}, \ldots$, etc. $A$ and $\mathscr{A}$ shall be used interchangeably, since either denotes the addition chain unambiguously. Furthermore, it will be convenient to let $B$ be a variable letter which never equals $D$.

For example, every AC $A$ begins with $D^2$ or $DF_1$. If $A = DF_1F_2(F_3F_2)^n$, then $\mathscr{C}_0 \leftrightarrow D$, $\mathscr{C}_1 \leftrightarrow F_1F_2$, and $\mathscr{C}_i \leftrightarrow F_3F_2$, $2 \leqq i \leqq n+1$. Words are always assumed to be in reduced form; e.g., $DD^2F_1F_1$ is always written $D^3F_1^2$. Also, since an AC is strictly monotonic, certain combinations of letters such as $DD_k$, $F_1H_{k,l}$, and $DH_{k,l}$, $k \geqq 2$, can never occur.

*Definition* 6. Given words $W$ and $W'$, $W'$ is said to be an internal segment of $W$ if there are words $W_1$ and $W_2$ (possibly empty) such that $W = W_1W'W_2$. If

$$W = \prod_{j=1}^{N} S_j \quad \text{and} \quad V = \prod_{j=1}^{i} S_jD^m, \qquad i \leqq N, m \geqq 0, \tag{2.6}$$

$V$ is said to be a truncation of $W$; if the number of letters $B$ in $W$ exceeds the number in $V$, the truncation is said to be proper.

**3. The structure of components.** The main result of this section, Theorem 1, classifies all possible combinations of letters which can occur in a component. Roughly, it states that long components consist mainly of $D$'s. A different result of this sort is used in (**4**): if $q$ is the last integer of an AC $A$, then there are at most $4B(q) - 4$ letters in $A$ other than $D$.

LEMMA 1. *If* $\{b_i\}_{i=0}^{4}$ *is of type* II, *and a component, then* $b_{j+1} = 2b_j$ *for some* $j$, $0 \leqq j \leqq 3$.

*Proof.* Otherwise, $b_1 \leqq 2b_0 - 1$, $b_2 \leqq 3b_0 - 1$, $b_3 \leqq 5b_0 - 2$, $b_4 \leqq 8b_0 - 3$, and $L(b_4) - L(b_0) \leqq 3$, a contradiction.

LEMMA 2. If $\{b_i\}_{i=0}^{\infty}$ *is of type* II, *and a component, and* $b_1 = 2b_0$, *then* $b_{j+1} \neq 2b_j$ *can occur at most twice for* $j \geqq 1$.

*Proof.* If $b_{j+1} \neq 2b_j$ has three solutions for $j \geqq 1$, then $b_jb_1^{-1}$ is bounded by one of the following four sequences, where $P \geqq 1$, $Q \geqq 1$, $R \geqq 2$:

$$1, 2, \ldots, 2^Q, 2^Q + 2^{Q-1}, 2^{Q+1} + 2^{Q-1}, 2^{Q+2}; \tag{3.1}$$

$$1, 2, \ldots, 2^P, 2^P + 2^{P-1}, 2^{P+1} + 2^{P-1}, \ldots, 2^{Q+1} + 2^{Q-1}, \\ 2^{Q+1} + 2^Q + 2^{Q-1} + 2^{Q-2} \leqq 2^{Q+2}; \tag{3.2}$$

$$(3.3)\quad 1, 2, \ldots, 2^P, 2^P + 2^{P-1}, \ldots, 2^Q + 2^{Q-1}, 2^{Q+1} + 2^{Q-2}, \\ 2^{Q+1} + 2^Q + 2^{Q-1} + 2^{Q-2} \leqq 2^{Q+2};$$

$$(3.4)\quad 1, 2, \ldots, 2^P, 2^P + 2^{P-1}, \ldots, 2^R + 2^{R-1}, 2^{R+1} + 2^{R-2}, \ldots, \\ 2^{Q+1} + 2^{Q-2}, 2^{Q+1} + 2^Q + 2^{Q-2} + 2^{Q-3} \leqq 2^{Q+2}.$$

In each case, $L(b_{Q+3}) - L(b_0) \leqq Q + 2$, a contradiction.

Henceforth, given an AC $A$, let $W = W_i(A) \leftrightarrow \mathscr{C}_i = \mathscr{C}_i(\mathscr{A})$. Clearly, $W = D^m$, $m \geqq 1$, for $i = 0$ while $W$ cannot begin with $D$ if $i > 0$.

LEMMA 3. *$\mathscr{C}_i$ contains at most three internal segments of the form $D^m$, $m \geqq 1$; if three occur, $\mathscr{C}_i$ is terminated by the last.*

*Proof.* Say that the word $W \leftrightarrow \mathscr{C}_i$ has an internal segment

$$(3.5)\qquad W' = D^{m_1}B_{11} \ldots B_{1r_1}D^{m_2}B_{21} \ldots B_{2r_2}D^{m_3}B_3,$$

where $m_1, m_2, m_3, r_1, r_2 \geqq 1$ and $B_{ij} \neq D$. Let $c_0$ be the number corresponding to the last letter of the AC before $W'$, and $c_1 = 2c_0, c_2, \ldots, c_f$ the numbers corresponding to the letters of $W'$. If $W'$ is replaced by

$$(3.6)\qquad W'' = D^{m_1}F_1D^{m_2+r_1-1}F_1D^{m_3+r_2-1}F_1,$$

let the corresponding numbers be $d_1 = c_1 = 2c_0, d_2, \ldots, d_f$. Here, $f = m_1 + m_2 + m_3 + r_1 + r_2 + 1$. Clearly, $d_f \geqq c_f$, and the $d_i$ form the sequence

$$(3.7)\quad 2c_0, \ldots, 2^{m_1}c_0, 2^{m_1-1} \cdot 3c_0, \ldots, 2^{m_1+m_2+r_1-2} \cdot 3c_0, 2^{m_1+m_2+r_1-3} \cdot 9c_0, \ldots, \\ 2^{f-5} \cdot 9c_0, 2^{f-6} \cdot 27c_0.$$

However, by (2.1), $2^{f-1}c_0 < c_f \leqq d_f = 2^{f-6} \cdot 27c_0$, a contradiction.

Next, denote the numbers of $\mathscr{C}_i$ by $b_1, b_2, b_3, \ldots$.

LEMMA 4. *A letter of $\mathscr{C}_i$ can be $D_k$ or $H_{k,l}$, $k \geqq 2$, only if it corresponds to $b_1$ or $b_2$.*

*Proof.* Otherwise, $\mathscr{C}_i$ would not be of type I.

It now follows from the above lemmas that $W \leftrightarrow \mathscr{C}_i$, $i > 0$, has one of the two forms ($g_i \geqq 0$)

$$(3.8)\qquad B^{g_1}, B^{g_1}D^{g_2}\prod_{j=1}^{g_3} F_{k_j}D^{g_4}\prod_{j=1}^{g_5} F_{h_j}D^{g_6},$$

where $1 \leqq g_1 \leqq 4$, $1 \leqq g_2$, and $g_3 + g_5 \leqq 2$.

LEMMA 5. *If $\{a_i\}_{i=0}^{\infty}$ is an AC, $L(a_{j+1}) - L(a_j) = 1$ for $j \geqq i$, $2^P \leqq a_i \leqq 2^P + 2^{P-2} + 2^{P-4}$, and $a_i + a_{i-1} < 2^{P+1}$, then $a_{j+1} = 2a_j$ for $j \geqq i$.*

*Proof.* Clearly, $2^{P+1} \leqq a_{i+1} = 2a_i \leqq 2^{P+1} + 2^{P-1} + 2^{P-3}$, and hence $a_i + a_{i+1} < 2^{P+2}$, thus, $a_{i+2} = 2a_{i+1}$, and so forth.

Theorem 1 can now be stated for $W \leftrightarrow \mathscr{C}_i$, $i > 0$, using the notation of Definitions 5 and 6.

THEOREM 1. *W is a truncation of an element of one of the following seven mutually exclusive classes of words, where $k \geqq 1$ and $m_i \geqq 0$:*
(1) $BBF_kF_1D^{m_1}$;
(2) $BBF_kD^{m_1}F_1D^{m_2}$, $m_1 \geqq 1$;
(3) $BBD^{m_1}F_kF_1D^{m_2}$, $m_1 \geqq 1$;
(4) $BBD^{m_1}F_1D^{m_2}F_1D^{m_3}$, $m_1, m_2 \geqq 1$;
(5) $BDF_kD^{m_1}F_1D^{m_2}$, $m_1 \geqq 1$, $k \geqq 2$;
(6) $BD^{m_1}F_kF_1D^{m_2}$, $m_1 \geqq 1$;
(7) $BD^{m_1}F_1D^{m_2}F_1D^{m_3}$, $m_1, m_2 \geqq 1$.

The proof requires four more lemmas. First, set $\alpha = L(b_1)$; then (recall Definition 3)

$$b_1 \leqq \sigma(\alpha) \quad \text{and} \quad b_2 < \sigma(\alpha + 1). \tag{3.9}$$

LEMMA 6. (a) *If $g_1 = 4$, then W belongs to class* (1). (b) *If $g_1 = 3$ and $g_3 \geqq 1$, then W belongs to class* (2).

*Proof.* In each case, $b_3 \leqq b_1 + b_2 \leqq 2^{\alpha+2} + \sigma(\alpha)$ by (3.9). In (a), $b_4 \leqq b_3 + b_2 \leqq 2^{\alpha+3} + \sigma(\alpha) < 2^{\alpha+3} + 2^{\alpha+1}$; therefore, $W$ has the form $BBF_kF_{k'}D^m$, $m \geqq 0$, by Lemmas 4 and 5. If $k' \geqq 2$, $b_4 \leqq b_3 + b_1 \leqq \sigma(\alpha + 2) < 2^{\alpha+3}$, a contradiction; hence, $W$ belongs to class (1). In (b), $b_{3+g_2} = 2^{g_2}b_3 \leqq 2^{g_2+\alpha+2} + \sigma(\alpha + g_2)$. Now $F_k$, $k \geqq 2$, cannot follow $D^{g_2}$ since then $b_{4+g_2} \leqq \sigma(g_2 + \alpha + 2)$, a contradiction. Hence, $F_1$ follows $D^{g_2}$, $b_{4+g_2} \leqq 2^{g_2+\alpha+3} + \sigma(g_2 + \alpha - 1)$, and by Lemma 5 only $D$'s can follow. Thus, $W$ belongs to class (2), and the proof is completed.

If $g_1 = 3$ and $g_3 = 0$, the reasoning of the proof of Lemma 6(b) shows that either $W$ belongs to (2), or else is a truncation of a word of (2). Thus, we need only consider the cases where $g_1 \leqq 2$.

LEMMA 7. *$W' = DF_kD^mF_{k'}$, $m \geqq 0$, $k' \geqq 2$, is not an internal segment of W.*

*Proof.* This is clear if $i = 0$. Otherwise, let $c_0$ be the number corresponding to the last letter of the AC before $W'$, and $c_1 = 2c_0, c_2, \ldots, c_{m+3}$ the numbers corresponding to the letters of $W'$. If $W'$ is replaced by $W'' = DF_1D^mF_2$ let the corresponding numbers be $d_1 = c_1 = 2c_0, d_2, \ldots, d_{m+3}$. Clearly, $d_{m+3} \geqq c_{m+3}$ and the $d_i$ form one of the sequences $2c_0, 3c_0, 4c_0$; $2c_0, 3c_0, 2 \cdot 3c_0, 8c_0$; $2c_0, 3c_0, 2 \cdot 3c_0, \ldots, 2^m \cdot 3c_0, 2^{m-2} \cdot 15c_0$ depending upon whether $m = 0$, $m = 1$, or $m \geqq 2$, respectively. However, for each of these, by (2.1), $2^{m+2}c_0 < c_{m+3} \leqq d_{m+3}$, a contradiction.

LEMMA 8. *If $g_1 = 2$, $g_3 = 1$, $g_5 = 1$, and $g_4 \geqq 1$, then $F_{k_1} = F_1$.*

*Proof.* Say $k_1 \geqq 2$. If $g_2 = 1$, (3.9) yields $b_3 \leqq \sigma(\alpha + 2)$, $b_4 \leqq b_3 + b_1 \leqq 2^{\alpha+3} + \sigma(\alpha)$, and $b_5 \leqq 2^{\alpha+4} + \sigma(\alpha + 1) < 2^{\alpha+4} + 2^{\alpha+2}$. Now $b_5 + b_4 < 2^{\alpha+5}$;

thus, by Lemma 5 only $D$'s can follow $b_5$, a contradiction since $g_5 = 1$. If $g_2 \geqq 2$, then $W' = D^2F_{k_1}D^{g_4}F_{h_1}$ is an internal segment of $W$; by Lemma 7, $W' = D^2F_{k_1}D^{g_4}F_1$. The argument used in Lemmas 3 and 7 (take $W'' = D^2F_2D^{g_4}F_1$) yields the contradiction $2^{g_4+3}c_0 < c_{g_4+4} \leqq d_{g_4+4} = 2^{g_4-1}\cdot 15c_0$.

From Lemmas 7 and 8, and the fact that $g_3 + g_5 \leqq 2$, it follows that if $g_1 = 2$, $W$ either belongs to (3) or (4), or is a truncation of a word of (3). Thus, it is now only necessary to consider the case $g_1 = 1$. If one of $g_3$, $g_4$ or $g_5$ is 0, $W$ belongs to (6) or is a truncation of a word of (6); this follows from Lemma 7.

LEMMA 9. *If* $g_1 = 1$, $g_3 = 1$, $g_4 \geqq 1$, $g_5 = 1$, *and* $k_1 \geqq 2$, *then* $g_2 = 1$.

*Proof.* If $g_2 = 2$, (3.9) yields $b_3 \leqq \sigma(\alpha + 2)$, $b_4 \leqq b_3 + b_1 \leqq 2^{\alpha+3} + \sigma(\alpha)$, $b_5 \leqq 2^{\alpha+4} + \sigma(\alpha + 1) < 2^{\alpha+4} + 2^{\alpha+2}$, and $b_4 + b_5 < 2^{\alpha+5}$. Thus, by Lemma 5, only $D$'s can follow $b_5$, a contradiction, since $g_5 = 1$. For $g_2 \geqq 3$ the proof is essentially the same.

Now by Lemma 7, if $W$ satisfies the hypothesis of Lemma 9, it belongs to (5). The only remaining case is $g_1 = 1$, $g_3 = 1$, $g_4 \geqq 1$, $g_5 = 1$, $k_1 = 1$; such a $W$ clearly belongs to (7).

*This completes the proof of Theorem* 1.

The structure of $\mathscr{C}_0$ and $\mathscr{C}_1$ is particularly simple; as mentioned before, $\mathscr{C}_0 \leftrightarrow D^m$, $m \geqq 1$, while $\mathscr{C}_1$ corresponds to a truncation of a word of class (1) or (6). In fact, the possibilities in the former case are $(m_1, m_2 \geqq 0, k \geqq 1) F_kD^{m_1}$, $F_kF_1D^{m_1}$, $F_kD_2D^{m_1}$, $F_1F_2D^{m_1}$, $F_1{}^3D^{m_1}$, while in the latter they are $F_1DF_2D^{m_1}$, $m_1 \geqq 0$, and $F_1D^{m_1}F_1D^{m_2}$, $m_1 \geqq 1$. (**3**, Lemma 3) follows from this and the discussion after Definition 4.

THEOREM 2. *There exist words $W$ belonging to each of the seven classes of Theorem* 1.

*Proof.* Let $m \geqq 0$. The $\mathscr{C}_2$ of the AC $D^2F_1F_3F_1{}^3D^m$ belongs to (1). The proof is completed by listing the remaining classes together with an AC whose $\mathscr{C}_3$ belongs to that class.

(2) $D^2F_1F_3DF_5F_1{}^2DF_1D^m$;
(3) $D^2F_1F_3DF_5F_1DF_2F_1D^m$;
(4) $D^2F_1F_3DF_5F_1D^2F_1DF_1D^m$;
(5) $D^2F_1F_3DF_5DF_2DF_1D^m$;
(6) $D^2F_1F_3DF_5DF_2F_1D^m$;
(7) $D^2F_1F_3DF_5DF_1DF_1D^m$.

**4. Lower bounds.** From the remarks after Definition 4, one easily deduces the following result.

LEMMA 10. *If* $B(c_i) \leqq C \cdot R^i$, $C > 0$, $R > 1$, *for all* $c_i \in \mathscr{C}_i \leqq A$, *where* $A$ *varies over all addition chains, then*

$$l(n) > L(n) + \frac{\log B(n)}{\log R} - \frac{\log CR}{\log R}. \tag{4.1}$$

https://doi.org/10.4153/CJM-1969-077-x Published online by Cambridge University Press

This suggests the following problem: if $c_i \in \mathscr{C}_i \leqq A$, where $A$ is an infinite addition chain, how rapidly can $B(c_i)$ grow with $i$? The example

$$A = D\prod_{n=0}^{\infty} F_{2^n}D^{2^{n+1}} \tag{4.2}$$

shows that $B(c_i) = 2^i$ is possible; I know of no case where $B(c_i)$ grows more rapidly. If the hypothesis of Lemma 10 held with $C = 1$, $R = 2$, it would follow that $\theta = 1$.

THEOREM 3. $\theta \geqq \frac{1}{4}$.

*Proof.* In any AC $\{a_j\}$, $B(a_j) = B(a_{j-1})$ if $a_j \leftrightarrow D$. By Theorem 1, $\mathscr{C}_i$ contains at most four non-$D$'s; thus, the hypothesis of Lemma 10 holds with $C = 1$, $R = 2^4$.

THEOREM 4. $\theta \geqq \frac{1}{3}$.

A preliminary result of independent interest will be obtained first. As in § 3, let $b_1, b_2, b_3, \ldots$ denote the elements of $\mathscr{C}_i$, $b_\omega$ being the last of these. Let $M = \max B(a_j)$, where $a_j$ varies over the elements of the AC which precede $b_1$. Let (1), . . . , (7) denote the word classes of Theorem 1, and let $\alpha$ be as in (3.9). If $B(b_\omega) \leqq RM$, we say that $R$ is attained if for every $\epsilon > 0$ there exist ACs such that $B(b_\omega)/M > R - \epsilon$.

LEMMA 11. *Abbreviate the statement "If $\mathscr{C}_i \leftrightarrow W \in (s)$, then $b_j \leqq u_1$, $b_{j+1} \leqq u_2$, $B(b_\omega) \leqq RM$, and $R$ is attained" by $(s); j; u_1, u_2; R$. Then*

$(1);\ 3;\ 2^{\alpha+2} + \sigma(\alpha),\ 2^{\alpha+3} + \sigma(\alpha);\ 5;$

$(2);\ m_1 + 3;\ 2^{\alpha+m_1+2} + \sigma(\alpha + m_1),\ 2^{\alpha+m_1+3} + \sigma(\alpha + m_1 - 1);\ 8;$

$(3);\ m_1 + 3;\ 2^{\alpha+m_1+2} + \sigma(\alpha + m_1),\ 2^{\alpha+m_1+3} + \sigma(\alpha + m_1);\ 6;$

$(4);\ m_1 + m_2 + 3;\ 2^{\alpha+m_1+m_2+2} + \sigma(\alpha + m_1 + m_2),\ 2^{\alpha+m_1+m_2+3} + \sigma(\alpha + m_1 + m_2 - 1);\ 6;$

$(5);\ m_1 + 3;\ 2^{\alpha+m_1+2} + \sigma(\alpha + m_1),\ 2^{\alpha+m_1+3} + \sigma(\alpha + m_1 - 1);\ 6;$

$(6);\ m_1 + 2;\ 2^{\alpha+m_1+1} + \sigma(\alpha + m_1 - 1),\ 2^{\alpha+m_1+2} + \sigma(\alpha + m_1 - 1);\ 4;$

$(7);\ m_1 + m_2 + 2;\ 2^{\alpha+m_1+m_2+1} + \sigma(\alpha + m_1 + m_2 - 1),\ 2^{\alpha+m_1+m_2+2} + \sigma(\alpha + m_1 + m_2 - 2);\ 4.$

LEMMA 12. *If $W \leftrightarrow \mathscr{C}_i$ is a proper truncation of a word belonging to one of the seven classes, then $B(b_\omega) \leqq 6M$, and for $W = BBD^{m_1}F_1D^{m_2}$, the bound 6 is attained.*

Only part of the first two statements of Lemma 11 will be proved; the remainder of Lemmas 11 and 12 is of the same nature, and in fact easier. The bounds on $b_j$, $b_{j+1}$ are almost immediate from (3.9).

Given numbers $a_1' < \ldots < a_s'$, $B(a_i') \leqq M$, $1 \leqq i \leqq s$, it is quite easy to see that there exists an AC $A = \{a_i\}$ containing the $a_i'$ such that $B(a_i) \leqq M$.

For the first statement of Lemma 11 let $s = 3$, and for $\alpha_3 > \alpha_2 \gg \alpha_1$ let $a_1' = \sigma(\alpha_1, 0; 6, 0)$, $a_2' = \sigma(\alpha_3, \alpha_2) + \sigma(\alpha_1, 0; 6, 2)$, $a_3' = \sigma(\alpha_3, \alpha_2) + \sigma(\alpha_1, 0; 6, 4)$. Define $i$ by

$$A = \bigcup_{j=0}^{i-1} \mathscr{C}_j$$

and form $\mathscr{C}_i$ by taking $b_1 = a_3' + a_1'$, $b_2 = b_1 + a_2'$, $b_3 = b_1 + b_2$, and $b_4 = b_3 + b_2 = 2^{\alpha_3+3} + \sigma(\alpha_3 - 1, \alpha_2 + 3) + 2^{\alpha_2+1} + 2^{\alpha_2} + \sigma(6\alpha_1 + 5, 0) - \sigma(\alpha_1, 0; 6, 2)$. By letting $\alpha_1, \alpha_2, \alpha_3 \to \infty$ under the condition $\alpha_2/6 > \alpha_1 \gg \alpha_3 - \alpha_2 > 6$ (say), it is easily seen by (2.4) that for any $\epsilon > 0$ there is an $A$ such that $B(a) \leqq M$ for $a \in \mathscr{C}_j$, $j < i$, and $B(b_4) > (5 - \epsilon)M$; hence, the bound 5 is attained. On the other hand, it is clear that $B(b_1) \leqq 2M$ and $B(b_2) \leqq 3M$. Write $b_3 = b_2 + x$. If $x \neq b_1$, then $B(x) \leqq M$; thus, by (2.2),

$$B(b_{4+m_1}) = B(b_4) = B(b_3 + b_2) = B(2b_2 + x) \leqq B(b_2) + B(x) \leqq 4M.$$

If $x = b_1$, there are two cases to consider: $B(b_2) \leqq 2M$ and $B(b_2) > 2M$. In the first of these, $B(b_{4+m_1}) \leqq B(b_2) + B(b_1) \leqq 4M$, while in the second, $b_2 = b_1 + y$, where $B(y) \leqq M$; therefore, again by (2.2),

$$\begin{aligned} B(b_{4+m_1}) = B(b_4) = B(b_3 + b_2) = B(2b_2 + b_1) &= B(3b_1 + 2y) \\ &\leqq B(3)B(b_1) + B(y) \leqq 5M. \end{aligned}$$

Hence $B(b_\omega) = B(b_{4+m_1}) \leqq 5M$.

For the second statement of Lemma 11 proceed as above with $s = 4$, $\alpha_3 > \alpha_2 \gg \alpha_1$, $a_1' = \sigma(\alpha_1, 0; 8, 0)$, $a_2' = \sigma(\alpha_3, \alpha_2) + \sigma(\alpha_1, 0; 8, 2)$, $a_3' = \sigma(\alpha_3, \alpha_2) + \sigma(\alpha_1, 0; 8, 4)$, $a_4' = \sigma(\alpha_3, \alpha_2) + \sigma(\alpha_1, 0; 8, 6)$, $b_1 = a_4' + a_1'$, $b_2 = b_1 + a_2'$, $b_3 = b_2 + a_3'$, $b_4 = 2b_3$, and $b_5 = b_4 + b_3 = 2^{\alpha_3+4} + \sigma(\alpha_3, \alpha_2 + 4) + 2^{\alpha_2+2} + 2^{\alpha_2+1} + 2^{\alpha_2} + \sigma(8\alpha_1 + 7, 0)$ to show that the bound 8 is attained. On the other hand, $B(b_1) \leqq 2M$ and $B(b_2) \leqq 3M$. There are two cases to consider: (1) $B(b_2) > 2M$ and (2) $B(b_2) \leqq 2M$. In (1), $b_2 = b_1 + x$, where $B(x) \leqq M$. If $b_3 = b_2 + y$, where $B(y) \leqq M$, then $B(b_3) \leqq B(b_1 + x + y) \leqq 4M$; otherwise, $b_3 = b_2 + b_1$ and $B(b_3) = B(2b_1 + x) \leqq 3M$. In (2), $B(b_3) \leqq 4M$ obviously holds. Now since only one non-$D$ (at $F_1$) remains, $B(b_\omega) \leqq 8$.

By Lemmas 11 and 12, the hypothesis of Lemma 10 holds with $C = 1$, $R = 8$.

*This completes the proof of Theorem* 4.

THEOREM 5. $\theta \geqq 2 \cdot (\log 2/\log 48) > \frac{1}{3}$.

*Proof.* It easily follows from the second statement of Lemma 11 that if $A = \bigcup \mathscr{C}_j$, $\mathscr{C}_i$ and $\mathscr{C}_{i+1}$ cannot both be words of (2); thus, $B(c_j)$, $c_j \in \mathscr{C}_j$, grows at most like $(6 \cdot 8)^{i/2}$.

More careful use of Lemmas 11 and 12 would probably yield a larger lower bound for $\theta$.

*Note added in proof.* A much more extensive bibliography will be found in D. E. Knuth's book (*The art of computer programming*, Vol. 2, Addison-Wesley, Reading, Massachusetts, to appear) along with numerical tables of $l(n)$, a proof of the conjecture at the end of the second paragraph of § 1, and related results.

## References


1. R. Bellman, *Advanced problem 5125*, Amer. Math. Monthly *70* (1963), 765.
2. A. T. Brauer, *On addition chains*, Bull. Amer. Math. Soc. *45* (1939), 736–739.
3. A. A. Gioia, M. V. Subbarao, and M. Sugunamma, *The Scholz-Brauer problem in addition chains*, Duke Math. J. *29* (1962), 481–487.
4. W. Hansen, *Zum Scholz-Brauerschen problem*, J. Reine Angew. Math. *202* (1959), 129–136.
5. A. M. Il'in, *On additive number chains*, Problemy Kibernet. *13* (1965), 245–248. (Russian)
6. A. Scholz, *Jahresbericht*, Deutsche Math.-Verein. *47* (1937), 41.
7. E. G. Straus, *Addition chains of vectors*, Amer. Math. Monthly *71* (1964), 806–808.
8. W. R. Utz, *A note on the Scholz-Brauer problem in addition chains*, Proc. Amer. Math. Soc. *4* (1953), 462–463.
9. C. T. Whyburn, *A note on addition chains*, Proc. Amer. Math. Soc. *16* (1965), 1134.


*The Institute for Advanced Study,*
*Princeton, New Jersey*