

## ON HIGHLY NON-ASSOCIATIVE GROUPOIDS

BY

J. H. FOLKMAN (SANTA MONICA, CALIFORNIA) AND R. L. GRAHAM  
(MURRAY HILL, NEW JERSEY)

**1.  $[n]$ -Systems.** Let  $(S, F)$  be a groupoid, i.e.,  $S$  is a set and  $F$  is a mapping of  $S \times S$  into  $S$ . For  $x_1, \dots, x_n \in S$ , it is well known that there are exactly

$$\frac{1}{2n-1} \binom{2n-1}{n}$$

distinct well-formed formal products  $E(x_1, \dots, x_n)$  in which each  $x_i$  occurs once and in the natural order (cf. [6]). For example, for  $n = 4$ , the five well-formed formal products are:

$$\begin{aligned} & F(F(F(x_1, x_2), x_3), x_4), \quad F(F(x_1, F(x_2, x_3)), x_4), \\ & F(F(x_1, x_2), F(x_3, x_4)), \quad F(x_1, F(F(x_2, x_3), x_4)), \\ & F(x_1, F(x_2, F(x_3, x_4))). \end{aligned}$$

If  $F$  satisfies

$$(1) \quad F(x_1, F(x_2, x_3)) = F(F(x_1, x_2), x_3), \quad x_1, x_2, x_3 \in S,$$

$F$  is said to be *associative* and  $(S, F)$  is known as a semigroup. Equation (1) is a rather strong condition as can be seen, for example, in [2], [3], and [7]. For any  $n \geq 1$ , a particular consequence of (1) is the following:

$(C_n)$  For any  $x_1, \dots, x_n \in S$ , if  $E(x_1, \dots, x_n)$  and  $E'(x_1, \dots, x_n)$  are two well-formed products of  $x_1, \dots, x_n$ , then  $E(x_1, \dots, x_n) = E'(x_1, \dots, x_n)$ .

In this note we initiate a study of systems  $(S, F)$  which for a fixed  $n$  not only fail to satisfy  $(C_n)$  but in fact fail in the strongest possible way.

**Definition.** We say that  $(S, F)$  is an  $[n]$ -system if the following condition is satisfied:

$(C'_n)$  For any  $x_1, \dots, x_n \in S$ , if  $E(x_1, \dots, x_n)$  and  $E'(x_1, \dots, x_n)$  are any two distinct well-formed products of  $x_1, \dots, x_n$ , then  $E(x_1, \dots, x_n) \neq E'(x_1, \dots, x_n)$ .

We give several examples of  $[n]$ -systems.

Example 1.  $n = 3$ .

$$S = \{a, b\}, \quad F: \begin{array}{cc} & a & b \\ a & \begin{array}{|c|c|} \hline b & b \\ \hline \end{array} \\ b & \begin{array}{|c|c|} \hline a & a \\ \hline \end{array} \end{array}$$

Table 1

Example 2.  $n = 4$ .

$$S = \{a, b, c, d, e, f\}, \quad F: \begin{array}{ccccc} & a & b & c & d & e & f \\ a & \begin{array}{|c|c|c|c|c|c|} \hline e & f & d & e & f & d \\ \hline \end{array} \\ b & \begin{array}{|c|c|c|c|c|c|} \hline e & f & d & e & f & d \\ \hline \end{array} \\ c & \begin{array}{|c|c|c|c|c|c|} \hline e & f & d & e & f & d \\ \hline \end{array} \\ d & \begin{array}{|c|c|c|c|c|c|} \hline b & c & a & b & c & a \\ \hline \end{array} \\ e & \begin{array}{|c|c|c|c|c|c|} \hline b & c & a & b & c & a \\ \hline \end{array} \\ f & \begin{array}{|c|c|c|c|c|c|} \hline b & c & a & b & c & a \\ \hline \end{array} \end{array}$$

Table 2

Note that a direct verification that  $(S, F)$  is a  $[4]$ -system requires checking  $\binom{5}{2} \cdot 6^4 = 12960$  inequalities.

Of course, if  $(S, F)$  is an  $[n]$ -system, then  $(S, F)$  is also an  $[m]$ -system for any  $m \leq n$ . On the other hand, if

$$|S| < \frac{1}{2m-1} \binom{2m-1}{m},$$

then  $(S, F)$  clearly can never be an  $[m]$ -system. It is not difficult to construct *infinite* systems which are  $[n]$ -systems for every integer  $n$ . In fact, every free groupoid with infinitely many generators is an  $[n]$ -system for every  $n$  (also, see [6]). We exhibit a more interesting construction in the following

Example 3.

$$S = \{1, 2, 3, \dots\}, \quad F(x, y) \equiv x \cdot 2^{2+\lceil \log_2 y \rceil} + 2y, \quad x, y \in S,$$

where  $[z]$  denotes the greatest integer  $\leq z$ .  $(S, F)$  is an  $[n]$ -system for all finite  $n$ . A partial table for  $F$  is given in Table 3.

		<i>y</i>					
		1	2	3	4	5	...
<i>x</i>	1	6	12	14	24	26	...
	2	10	20	22	40	42	...
	3	14	28	30	56	58	...
	4	18	36	38	72	74	...
	5	22	44	46	88	90	...
	⋮	...	...	...	...	...	...

Table 3

The proof that  $(S, F)$  is an  $[n]$ -system for every integer  $n$  is left as an exercise for the ambitious reader.

**2. Finite  $[n]$ -systems.** For a given  $n$ , it is not at all clear a priori that a finite  $[n]$ -system exists. However, their existence is guaranteed by the Theorem below and, therefore, the following definition is meaningful:

**Definition.** For each  $n \geq 2$ , let  $S(n)$  be defined to be the least integer  $m$  such that there exists an  $[n]$ -system  $(S, F)$  with  $|S| = m$ .

We have already noted that

$$S(n) \geq \frac{1}{2n-1} \binom{2n-1}{n}.$$

The main result of this paper is the

**THEOREM.**

$$(2) \quad S(2) = 1, \quad S(3) = 2, \quad S(4) = 6,$$

$$1 + \frac{1}{2n-1} \binom{2n-1}{n} \leq S(n) \leq n^{2n-2}, \quad n \geq 5.$$

The proof of the theorem will consist of several lemmas. We first make several remarks. It will be convenient to modify our notation slightly and make use of the parenthesis free notation of Łukasiewicz and Tarski [8], [10]. This means essentially removing all the parentheses and commas in the ordinary well-formed products. For example, the five products of  $x_1, x_2, x_3, x_4$  given in Section 1 are now written:

$$\begin{aligned} &FFFx_1x_2x_3x_4, \quad FFx_1Fx_2x_3x_4, \quad FFx_1x_2Fx_3x_4, \\ &Fx_1FFx_2x_3x_4, \quad Fx_1Fx_2Fx_3x_4. \end{aligned}$$

We remark that in this notation a string  $E$  of  $F$ 's and  $x$ 's is well-formed iff when each  $F$  is replaced by  $-1$  and each  $x$  is replaced by  $+1$ ,

all initial partial sums (i. e., partial sums starting from the left-hand side of  $E$ ) are  $\leq 0$ , except the last partial sum which is  $+1$  (cf. [9]). In fact, since for each string of  $(2n-1)$   $\pm 1$ 's with sum  $+1$ , there is exactly *one* cyclic permutation of the string which has all its proper initial partial sums  $\leq 0$  (cf. [5], [11]) and since all  $2n-1$  cyclic permutations are distinct, this shows that of the  $\binom{2n-1}{n}$  possible strings, exactly  $\frac{1}{2n-1} \binom{2n-1}{n}$  correspond to well-formed products. We shall also abbreviate a concatenation of  $n$   $F$ 's, i.e.,  $\overbrace{FF\dots F}^n$ , by  $F^n$ . We first show

LEMMA 1.

$$(3) \quad S(n) \leq n^{2n-2}.$$

Proof. Let  $E = E(x_1, \dots, x_n)$  be a well-formed product of  $x_1, \dots, x_n$ . There corresponds to  $E$  a unique "generation tree"  $T(E)$  formed in the obvious way (cf. [4]). For example, the five trees corresponding to the five possible products of  $x_1, x_2, x_3, x_4$  are shown in Fig. 1.

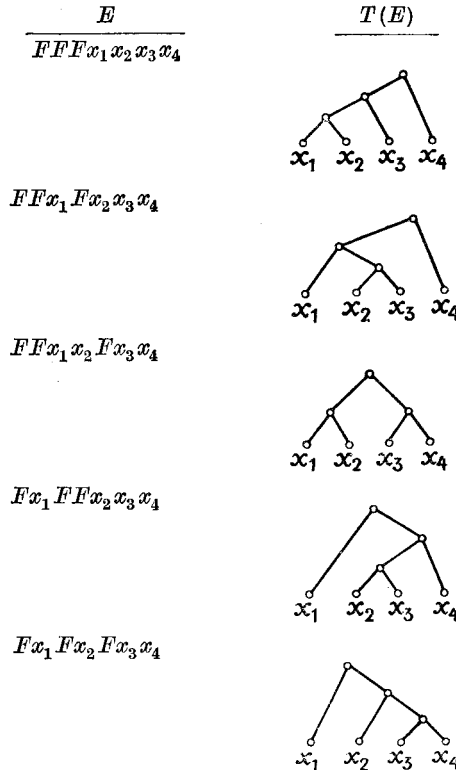
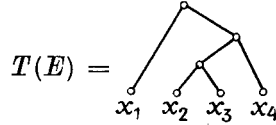


Fig. 1

The interpretation of the vertices of the trees as partial products of the  $x_i$  is immediate. Now, to each terminal vertex  $x_i$  of  $T(E)$  can be

assigned a binary sequence  $S(x_i)$  in the following manner: Start at the top vertex  $V$  of  $T(E)$  and traverse the unique path  $P$  down to  $x_i$ . Let  $v = v_1, v_2, \dots, v_{t_i} = x_i$  denote the sequence of vertices of  $P$ . Then  $S(x_i) \equiv (S_1^{(i)}, \dots, S_{t_i-1}^{(i)})$ , where  $S_j = 0$  if the left-hand branch below  $v_j$  was taken by  $P$ , and  $S_j = 1$  if the right-hand branch below  $v_j$  was taken. For example, if  $E = FF_1FF_2x_3x_4$ , then



$$S(x_1) = (0), \quad S(x_2) = (1, 0, 0), \quad S(x_3) = (1, 0, 1), \quad S(x_4) = (1, 1).$$

We remark that  $S(x_i)$  depends only on the structure of the part of  $E$  which precedes  $x_i$ . Also, we note that the binary sequences  $S(x_i)$ ,  $1 \leq i \leq n$ , form an optimal instantaneous binary (Huffman) code (cf. [1]). Finally, we assign to each sequence  $S(x_i) = (S_1^{(i)}, \dots, S_{t_i}^{(i)})$  a value  $\mu(S(x_i))$  by

$$(4) \quad \mu(S(x)) \equiv \sum_{j=1}^{t_i} S_j^{(i)} 2^{j-1}.$$

Let  $X = \{0, 1, \dots, n-1\}$ ,  $N = 2^{n-2}$ , and  $T = \{(x_0, \dots, x_{N-1}) : x_i \in X\}$ . Define the binary operation  $F$  on  $T \times T$  by

$$F(x_0, \dots, x_{N-1})(y_0, \dots, y_{N-1}) = (z_0, \dots, z_{N-1}),$$

where

$$z_i = \begin{cases} x_0 + 1 \pmod{n} & \text{if } i = 0, \\ x_{\lfloor i/2 \rfloor} & \text{if } i > 0 \text{ is even,} \\ y_{\lfloor i/2 \rfloor} & \text{if } i \text{ is odd.} \end{cases}$$

We claim that  $(T, F)$  is an  $[n]$ -system. To see this, let  $E(X_1, \dots, X_n)$  be a well-formed formal product of  $X_1, \dots, X_n$  where  $X_k = (x_{k,0}, \dots, x_{k,N-1})$ ,  $x_{k,j} \in X$ ,  $0 \leq j \leq N-1$ ,  $1 \leq k \leq n$ . Each  $X_i$  has the binary sequence  $S(X_i) = (S_1^{(i)}, \dots, S_{t_i}^{(i)})$  associated with it (as defined previously) with corresponding value  $\mu(S(X_i))$  given by (4). In general, the product  $E(X_1, \dots, X_n)$  is an  $N$ -tuple  $(z_0, \dots, z_{N-1})$ . The significance of  $S(X_i)$  rests with the following

Fact. Each  $k$ ,  $0 \leq k \leq N-1$ , has a unique representation as

$$k = j \cdot 2^{t_i} + \mu(S(X_i)), \quad 0 \leq j < 2^{n-t_i-2}, \quad 1 \leq i \leq n.$$

Further,

$$(5) \quad z_k = \begin{cases} x_{i,j} + w_i & \text{if } j = 0, \\ x_{i,j} & \text{if } j > 0, \end{cases}$$

where  $w_i$  is the length of the string of terminal 0's of  $S(x_i)$ .

The first statement in the Fact is a well-known property of Huffman codes (cf. [1], [4]); the second follows by an easy induction argument.

As an example, take  $n = 4$  and consider the previously used expression  $E = FX_1FFX_2X_3X_4$ . For this  $E$  we have:

$i$	$S(X_i)$	$\mu(S(X_i))$	$t_i$	$w_i$
1	(0)	0	1	1
2	(1, 0, 0)	1	3	2
3	(1, 0, 1)	5	3	0
4	(1, 1)	3	2	0

Table 4

Also,  $N = 2^{4-2} = 4$ . We calculate:

$$\begin{aligned} FX_2X_3 &= F(x_{20}, x_{21}, x_{22}, x_{23})(x_{30}, x_{31}, x_{32}, x_{33}) = (x_{20}+1, x_{30}, x_{21}, x_{31}), \\ FFX_2X_3X_4 &= F(x_{20}+1, x_{30}, x_{21}, x_{31})(x_{40}, x_{41}, x_{42}, x_{43}) = (x_{20}+2, x_{40}, x_{30}, x_{41}), \\ FX_1FFX_2X_3X_4 &= F(x_{10}, x_{11}, x_{12}, x_{13})(x_{20}+2, x_{40}, x_{30}, x_{41}) \\ &= (x_{10}+1, x_{20}+2, x_{11}, x_{40}). \end{aligned}$$

Of course, this result is asserted by the Fact.

Suppose now that  $E$  and  $E'$  are two *distinct* well-formed formal products of  $X_1, \dots, X_n$ , say

$$\begin{aligned} E &= F^{m_1}X_1F^{m_2}X_2 \dots F^{m_{n-1}}X_{n-1}X_n = (z_0, \dots, z_{N-1}), \\ E' &= F^{m'_1}X_1F^{m'_2}X_2 \dots F^{m'_{n-1}}X_{n-1}X_n = (z'_0, \dots, z'_{N-1}), \end{aligned}$$

where  $m_i, m'_i \geq 0$ . By assumption there is a least  $i$ ,  $1 \leq i \leq n$ , such that  $m_i \neq m'_i$ . We can assume without loss of generality that  $0 \leq m_i < m'_i < n$ . The definition of  $\mu$  shows for some  $k^*$

$$(6) \quad \mu(S(X_i)) = \mu(S'(X_i)) \equiv k^*,$$

where  $S'(X_i)$  denotes the binary sequence associated with  $E'$ . On the other hand, the definition of  $w_i$  gives

$$(7) \quad w_i = m_i, \quad w'_i = m'_i.$$

Hence by (6), (7) and the Fact for  $j = 0$  we have

$$(8) \quad z_{k^*} = x_{i,0} + m_i, \quad z'_{k^*} = x_{i,0} + m'_i,$$

where addition is modulo  $n$ . Since  $0 \leq m_i < m'_i < n$ , we get  $z_{k^*} \neq z'_{k^*} \pmod{n}$ . Consequently, the values of the products  $E$  and  $E'$  are different. This shows that  $(T, F)$  is an  $[n]$ -system. Since  $|T| = n^N = n^{2^{n-2}}$ , formula (3) is established. This proves Lemma 1.

The reader may note that it was not necessary to reduce *each* component of  $(x_0, \dots, x_{N-1})$  by  $n$  but in fact the argument will hold when we reduce the  $k^{\text{th}}$  component  $x_k$  by only  $n - [\log_2 k] - 1$  for  $k > 0$ . This implies the stronger (but less neat)

$$(9) \quad S(n) \leq n \prod_{k=0}^{n-3} (n-k-1)^{2^k}.$$

Let us call an  $[n]$ -system  $(S, F)$  *exact* if

$$|S| = \frac{1}{2n-1} \binom{2n-1}{n}.$$

We next show that if  $(S, F)$  is an exact  $[n]$ -system, then  $n \leq 3$ . This is best possible since Example 1 exhibits an exact  $[3]$ -system. We first require several definitions.

Let  $(S, F)$  denote a groupoid. The *dual groupoid*  $(S, \bar{F})$  is defined to have the same underlying set  $S$  and a binary operation  $\bar{F}$  on  $S$  given by  $\bar{F}xy = Fyx$ ,  $x, y \in S$ .

For  $x_1, \dots, x_r \in S$ , we denote by  $[x_1, \dots, x_r]$  the set of all values of well-formed products of  $x_1, \dots, x_r$ . Thus, if  $(S, F)$  is an exact  $[n]$ -system, then  $[x_1, \dots, x_r] = S$  for any  $x_1, \dots, x_r \in S$ . For  $e, x \in S$  we say that  $e$  is a *left (right) identity* for  $x$  if  $Fex = x$  ( $Fxe = x$ ). Finally, we say  $x$  has an *identity* if  $x$  has a left or right identity.

**LEMMA 2.** *Let  $(S, F)$  be an exact  $[n]$ -system with  $n \geq 4$ . Then no element of  $S$  has an identity.*

*Proof.* Suppose some  $x \in S$  has an identity. Then  $x$  has a left identity in either  $(S, F)$  or  $(S, \bar{F})$  so we may assume without loss of generality  $Fex = x$  for some  $e \in S$ . Consider the sequence of statements  $(T_r)$ ,  $r \geq 3$ , given by:

$(T_r)$  If  $z \in [x_1, \dots, x_r]$  and  $z \neq F^{r-1}x_1 \dots x_r$  then  $z \in [x_1, y_2, \dots, y_t]$  for some  $y_2, \dots, y_t \in S$  with  $2 \leq t < r$ .

$(T_3)$  is certainly valid since  $z \in [x_1, x_2, x_3]$  and  $z \neq FFx_1x_2x_3$  imply  $z = Fx_1Fx_2x_3 \in [x_1, Fx_2x_3]$ . Let  $r > 3$  and assume  $(T_{r-1})$  is true. If  $z \in [x_1, \dots, x_r]$ , then  $z = FXY$  where  $X \in [x_1, \dots, x_i]$  and  $Y \in [x_{i+1}, \dots, x_r]$  for some  $i$ ,  $1 \leq i < r$ . If  $i < r-1$ , then  $z \in [x_1, \dots, x_i, Y]$  and we are done. Suppose  $i = r-1$ . Then  $z = FXx_r$ . But  $z \neq F^{r-1}x_1 \dots x_r$  by hypothesis, so that  $X \neq F^{r-2}x_1 \dots x_{r-1}$ . By the induction hypothesis,  $X \in [x_1, y_2, \dots, y_t]$  for some  $y_2, \dots, y_t \in S$ , where  $2 \leq t < r-1$ . Hence  $z \in [x_1, y_2, \dots, y_t, x_r]$  and  $(T_r)$  is established.

Now let  $z$  be any element of  $S$  and define a sequence  $x_1, \dots, x_n$  by  $x_1 = \dots = x_{n-1} = x$ ,  $x_n = z$ . Since  $(S, F)$  is an exact  $[n]$ -system,  $x \in S = [x_1, \dots, x_n]$ . Suppose  $x \neq F^{n-1}x_1 \dots x_n$ . By  $(T_n)$  we have

$$(10) \quad x \in [x_1, y_2, \dots, y_t] = [x, y_2, \dots, y_t]$$

for some  $y_2, \dots, y_t \in S$  where  $2 \leq t < n$ . The sequence  $e, x, y_2, \dots, y_t$  has at most  $n$  terms and consequently all well-formed products of  $e, x, y_2, \dots, y_t$  must be different (since an  $[n]$ -system is also an  $[m]$ -system for any  $m \leq n$ ). By (10) we can write  $x = F^{m_1}x_1 F^{m_2}y_2 \dots F^{m_t}y_t$  some  $m_1, \dots, m_t \geq 0$ . Since  $x_1 = x$ , we have

$$(11) \quad FeF^{m_1}x_1 F^{m_2}y_2 \dots F^{m_t}y_t = Fex = x = F^{m_1}FexF^{m_2}y_2 \dots F^{m_t}y_t.$$

But now we have two distinct well-formed products of  $e, x, y_2, \dots, y_t$  which have the same value; this is a contradiction.

Thus we must have  $x = F^{n-1}x_1 \dots x_n$ . Let  $w = F^{n-2}x_1 \dots x_{n-1} = F^{n-2}x \dots x$ . We have just shown that  $Fwz = x$  for all  $z \in S$ . Since  $n \geq 4$ ,  $(S, F)$  is certainly a  $[4]$ -system. But

$$(12) \quad FwFxFxx = FwFFxxx = x$$

which *contradicts* the assertion that  $(S, F)$  is a  $[4]$ -system. This proves the lemma.

LEMMA 3. *If  $(S, F)$  is an exact  $[n]$ -system, then  $n \leq 3$ .*

Proof. Assume  $(S, F)$  is an exact  $[n]$ -system with  $n \geq 4$ . Let  $x \in S$  be an arbitrary fixed element and let  $x_1 = x_2 = \dots = x_n = x$ . Then

$$(13) \quad x = FAB,$$

where  $A \in [x_1, \dots, x_a]$ ,  $B = F^{s_1}x_1 \dots F^{s_b}x_b \in [x_1, \dots, x_b]$ , and  $a + b = n$ . By Lemma 1,  $A \neq x$ ,  $B \neq x$  so that  $a, b \geq 2$ . Write

$$(14) \quad A = F^i C x_1 \dots x_i, \quad i \geq 0,$$

where  $C \neq FDx$  for any  $D \in S$ . We claim that  $C = x$ .

For suppose  $C \neq x$ . Then  $C = FDE$  for some  $D = F^{t_1}x_1 \dots F^{t_d}x_d \in [x_1, \dots, x_d]$ ,  $E \in [x_1, \dots, x_e]$ ,  $e \geq 2$ . Of course,  $d + e + i + b = a + b = n$ . Consider the sequence

$$(15) \quad A, x_1, \dots, x_{b+d-1}, E, x_1, \dots, x_i, B.$$

Recall that all  $x_i = x$ . The sequence has length  $b + d + i + 2 \leq b + d + i + e = n$  so that all of its distinct well-formed products must be different. But

$$(16) \quad \begin{aligned} x &= FAB \\ &= FF^i C x_1 \dots x_i B \\ &= F^{i+1} FDE x_1 \dots x_i B \\ &= F^{i+2} F^{t_1} x_1 F^{t_2} x_2 \dots F^{t_d} x_d E x_1 \dots x_i B \\ &= F^{i+2} F^{t_1} F A B F^{t_2} x_2 \dots F^{t_d} x_d E x_1 \dots x_i B \\ &= F^{i+2} F^{t_1} F A F^{s_1} x_1 \dots F^{s_b} x_b F^{t_2} x_2 \dots F^{t_d} x_d E x_1 \dots x_i B. \end{aligned}$$



On the other hand,

$$\begin{aligned}
 (17) \quad x &= FAB \\
 &= FAF^{s_1}x_1 \dots F^{s_b}x_b \\
 &= FAF^{s_1}x_1 \dots F^{s_b}FAB \\
 &= FAF^{s_1}x_1 \dots F^{s_b}FF^iCx_1 \dots x_iB \\
 &= FAF^{s_1}x_1 \dots F^{s_b}FF^iFDEx_1 \dots x_iB \\
 &= FAF^{s_1}x_1 \dots F^{s_b}F^{i+2}F^{t_1}x_1 \dots F^{t_d}x_dEx_1 \dots x_iB.
 \end{aligned}$$

However, both of the terminal expressions of (16) and (17) are well-formed products from the sequence in (15). Moreover, a comparison of the initial powers of  $F$  shows that they are distinct. Since they have the same value  $x$ , we have reached a contradiction to assumption that  $C \neq x$ .

Hence, we have shown  $C = x$  and, consequently,  $A = F^{a-1}x_1 \dots x_a$ . In the dual groupoid  $(S, \bar{F})$ ,  $x = \bar{F}\bar{B}\bar{A}$ , where  $\bar{B}$  and  $\bar{A}$  are formed from  $B$  and  $A$  by replacing all  $F$ 's by  $\bar{F}$ 's. The preceding argument may be applied here to give  $B = \bar{F}x_1\bar{F}x_2 \dots \bar{F}x_{b-1}\bar{F}x_b$ . Let  $H = \bar{F}x_2 \dots \bar{F}x_{b-1}\bar{F}x_b$ ; thus  $B = \bar{F}xH$ . Consider the sequence

$$(18) \quad A, x_1, \dots, x_{b-2}, Fxx, x_1, \dots, x_{a-1}, H.$$

It contains  $a+b = n$  terms, so that all well-formed products must be distinct. But

$$\begin{aligned}
 (19) \quad FAH &= FF^{a-1}x_1 \dots x_aH \\
 &= FF^{a-1}FABx_2 \dots x_aH \\
 &= F^{a+1}AFx_1Fx_2 \dots Fx_{b-1}x_bx_2 \dots x_aH \\
 &= F^{a+1}AFx_1Fx_2 \dots Fx_{b-2}Fxx_2 \dots x_aH
 \end{aligned}$$

and

$$\begin{aligned}
 (20) \quad FAH &= FAFx_2 \dots Fx_{b-1}x_b \\
 &= FAFx_2 \dots Fx_{b-1}FAB \\
 &= FAFx_2 \dots Fx_{b-1}F^{a-1}x_1 \dots x_aB \\
 &= FAFx_2 \dots Fx_{b-1}F^{a-2}Fx_1x_2 \dots x_aFxH \\
 &= FAFx_2 \dots Fx_{b-1}F^{a-2}Fxx \dots x_aFxH.
 \end{aligned}$$

As before, an examination of the two terminal expressions of (19) and (20) shows that we have constructed two distinct well-formed products of the sequence in (18) with the same value. This is a contradiction and the lemma is proved.

For the case  $n = 4$ , Lemma 3 implies  $S(4) \geq 6$ , a fact which was first proved by M. C. Gray (unpublished). Example 2 shows  $S(4) \leq 6$ . The values  $S(2) = 1$  and  $S(3) = 2$  (Example 1) are immediate. These

observations, together with Lemmas 1 and 3 establish (2) and the Theorem.

**3. Concluding remarks.** The reader will no doubt notice that the bounds on  $S(n)$  given in (2) and (9) leave considerable room for improvement. It is not clear which bound is closer to the true order of growth of  $S(n)$ . The best upper bound currently known for  $S(5)$  is 96 (P 780). Another question which arises is for which values of  $m > S(n)$  can an  $[n]$ -system exist with  $|S| = m$ . For example, if  $(S, F)$  is an  $[n]$ -system for some  $n \geq 4$ , can  $|S|$  be a prime number? (P 781) Presumably, these and other questions could be answered if more were known in the way of structure theorems for  $[n]$ -systems. In view of the strength of condition  $(C'_n)$  which defines an  $[n]$ -system, it seems quite possible that such theorems exist.

#### REFERENCES

- [1] N. Abramson, *Information theory and coding*, New York 1963.
- [2] M. A. Arbib (editor), *Algebraic theory of machines, languages and semigroups*, New York 1968.
- [3] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, American Mathematical Society, Providence, 1961.
- [4] R. M. Fano, *Transmission of information*, Cambridge 1961.
- [5] R. L. Graham, *A combinatorial theorem for partial sums*, Annals of Mathematical Statistics 34 (1963), p. 1600-1602.
- [6] N. Jacobson, *Lectures in abstract algebra*, Vol. 1, New York 1951.
- [7] E. S. Ljapin, *Semigroups*, Translation of Math. Monographs, American Mathematical Society, Vol. 3, Providence 1963.
- [8] J. Łukasiewicz and A. Tarski, *Untersuchungen über den Aussagenkalkül*, Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III, 23 (1930), p. 1-21.
- [9] G. N. Raney, *Functional composition patterns and power series reversion*, Transactions of the American Mathematical Society 94 (1960), p. 441-451.
- [10] J. B. Rosser and A. R. Turquette, *Many-valued logics*, Amsterdam 1952.
- [11] L. Takács, *Ballot problems*, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete I (1962), p. 154-158.

THE RAND CORPORATION  
BELL TELEPHONE LABORATORIES

Reçu par la Rédaction le 16. 5. 1970