ABELIAN SUBSEMIGROUPS, ENUMERATION, AND UNIVERSAL MATRICES

KIM KI-HANG BUTLER AND JAMES RICHARD KRABILL

1. Let B_n be the semigroup of all binary relations on a set with n elements represented as $n \times n$ matrices over the Boolean algebra of order 2. Let J_n be the universal matrix of order n, that is, the $n \times n$ matrix in B_n with all entries 1. Let C_n be the subsemigroup of all circulants, and let $C(J_n)$ be the set of $C \in C_n$ such that $C^p = J_n$ for some positive integer p. The set $C(J_n)$ is enumerated and is shown to be an abelian subsemigroup. Related results on C_n were obtained by the authors in [3]. Some new subsets, denoted K_n, K_n' and K_n'', are defined and are shown to be maximal abelian subsemigroups, which are of much larger cardinality than C_n, when $n > 2$. Further, if $K \in K_n$ but K is not in the center of B_n, then $K^2 = J_n$. Another subset, not a subsemigroup, is defined and enumerated. This set, denoted L_n, has the property that $L \in L_n$ implies $L^2 = J_n$. Relations between these sets are given.

B. M. Schein asked for the maximal abelian subgroup of B_n [8]. The authors [3] showed that C_n, the set of all circulants in B_n, is a maximal abelian subsemigroup of B_n with cardinality 2^n. The term "maximal" is used in the sense that the abelian subsemigroup is not properly contained in any abelian subsemigroup of B_n. In this paper new maximal abelian subsemigroups are defined which provide further partial solutions to Schein's question. The other main result of [3] is the following theorem.

THEOREM 0. *Let $C \in C_n$, $n > 1$. There exists a positive integer p such that $C^p = J_n$ if and only if $(\delta(C), n) = 1$ and for every divisor d of n, $d > 1$, there exist $i, j \in \Delta(C)$ such that $i \not\equiv j \pmod{d}$. Here, matrix rows and columns are labelled 0 through $(n-1)$ respectively, $\Delta(C) = \{i : c_{0,i} = 1, 0 \leq i \leq n-1, c_{jk} \in C \in C_n\}$, and $\delta(C)$ is the greatest common divisor of the elements of $\Delta(C)$. If p exists, then $p \leq n - 1$.*

2. This theorem provides a partial answer to a problem considered by N. S. Mendelsohn [7], I. J. Good [6], and N. G. de Bruijn [1]. The problem, in our terminology, is to find all A, $A \in B_n$, such that some power of A, A^p, is the universal matrix J_n. A related problem is to find all A in B_n whose square is the universal matrix. We remark that by the above theorem, $C^p = J_n$, p minimal, if and only if $\delta(C)$ is a basis of order p of the integers modulo n under addition modulo n. We now define $C(J_n)$ to be the set of all circulants C for which some power of C is the universal matrix J_n. The product of two matrices A and B will be indicated by juxtaposition. Let $N = \{1, 2, \cdots, n, \cdots\}$ and $n \in N$ throughout this paper.

Received February 23, 1973.