PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 2, 1982

ZERO-INDUCING FUNCTIONS ON FINITE ABELIAN GROUPS

G. L. O'BRIEN

Let G be a finite abelian group and let $f: G \to G$ be any function. Let $r_x: G \to G$ be the function $r_x(y) = x + y$, $x \in G$. A study is made of conditions on f such that the semi-group of functions generated by f and all r_x under composition contains the zero function. If G is cyclic, it is necessary and sufficient that f not be one-to-one. In general some necessary conditions are given and a partial converse is given for these conditions, which involve the behaviour of f on subgroups and cosets of G.

1. Introduction. Let G be any finite set and let $\mathscr{F}$ be a collection of functions from G into G. Let $\mathscr{A}$ be the semigroup of functions $A: G \to G$ which is generated by $\mathscr{F}$; that is, $A \in \mathscr{A}$ iff A can be expressed as a composition $A = h_1 h_2 \cdots h_k$ where each $h_i \in \mathscr{F}$. The question we examine is the following: does $\mathscr{A}$ contain any constant functions? Let $V = V(\mathscr{F}) = \min\{|A(G)|: A \in \mathscr{A}\}$ where $|\cdot|$ denotes cardinality. Obviously, $\mathscr{A}$ contains a constant function if and only if $V = 1$. A more general problem is to evaluate V.

We mainly consider a very special case of the situation described above. Except in §2, we assume throughout that G is a finite abelian group (with additive notation and identity 0) and that $\mathscr{F}$ consists of all the functions $r_x: G \to G$ given by $r_x(y) = x + y$ (translation by x) and one other function $f: G \to G$. We do *not* assume f is a homomorphism. In this situation, we write $V(f)$ for $V(\mathscr{F})$. If $\mathscr{A}$ contains any constant function, it clearly contains them all. We say f is *zero-inducing* if $\mathscr{A}$ contains the zero function.

In §2, we give two simple lemmas for the general (non-group) case. In §3, we apply these to the group case. An obvious necessary condition for f to be zero-inducing is that f not be one-to-one. Corollary 1 states that this is sufficient if $|G|$ is prime. If $|G|$ is not prime, it is not sufficient, as is easily seen from some of the examples in §3. That section also contains a lower bound for V which involves the behaviour of f on subgroups of G and their cosets. In §4, the adequacy of this lower bound is discussed.

The problem of whether f is zero-inducing arose as a result of an attempt to solve the "road-coloring conjecture" of Adler, Goodwyn, and Weiss [1]. This graph-theoretic conjecture, which reduces in some case to the present problem (see [2]), arose in turn from their study of ergodic theory. Our zero-inducing question is also related

to some questions in computer science which deal with resetting the state of a computer to zero before beginning a new program. The problem has independent interest, whatever the original motivation. The road-colouring conjecture only involves the case when G is cyclic, but the results we present here apply equally well to other finite abelian groups. Some of the theorems are a little more complicated in the general case.

It is clear that $V(f) = V(r_x f)$ for any $x \in G$. Taking $x = -f(0)$, we observe in particular that $r_x f(0) = f(0) - f(0) = 0$. We may therefore assume without loss of generality that $f(0) = 0$. Similarly we note that the set

$$(1) \qquad \mathscr{A}_0 \equiv \{A \in \mathscr{A} : |A(G)| = V \quad \text{and} \quad A(0) = 0\}$$

is non-empty.

We use the following notation. If $X, Y \subseteq G$, then $X + Y = \{x + y : x \in X, y \in Y\}$ If $g \in G$, we write $g + Y$ for $\{g\} + Y$. We let $X \oplus Y$ denote $X + Y$ only if the sums $x + y$ for $x \in X$ and $y \in Y$ are distinct. If H and K are groups, we let $H \oplus K$ be the group $\{(h, k) : h \in H, k \in K\}$ with componentwise addition. Finally, Z_n denotes the cyclic group $\{0, 1, \cdots, n-1\}$ with addition performed modulo n.

2. The general case. In this section, we obtain two simple equivalent formulations of $V(\mathscr{F})$ under the general conditions described in the first paragraph of Section 1. For $k \geqq 1$, a *k-collection* is a non-empty set $\mathscr{C}$ of subsets of G such that each $Y \in \mathscr{C}$ has exactly k elements and such that for any $\{y_1, \cdots, y_k\} \in \mathscr{C}$ and any $h \in \mathscr{F}$, the set $\{h(y_1), \cdots, h(y_k)\} \in \mathscr{C}$. In particular, for $Y \in \mathscr{C}$, the restriction of h to Y is one-to-one. The set of singleton sets of elements of G is evidently a 1-collection.

LEMMA 1. *$V(\mathscr{F})$ is the largest value of k for which there exists a k-collection.*

Proof. Suppose $\mathscr{C}$ is a k-collection and $\{y_1, \cdots, y_k\} \in \mathscr{C}$. By induction on the number of composing factors making up A (the non-uniqueness of this number does not matter), the set $\{A(y_1), \cdots, A(y_k)\} \in \mathscr{C}$ for any $A \in \mathscr{A}$. Thus $|A(G)| \geqq |A(\{y_1, \cdots, y_k\})| = k$ so that

$$(2) \qquad V(\mathscr{F}) \geqq k .$$

Now suppose $A \in \mathscr{A}_0$ and let $A(G) = \{y_1, y_2, \cdots, y_V\}$. Define $Y_B = \{B(y_1), \cdots, B(y_V)\}$ for $B \in \mathscr{A}$ and let $\mathscr{C} = \{Y_B : B \in \mathscr{A}\}$. If $B(y_i) = B(y_j)$ for any B and any i, j, then $|BA(G)| = |B(\{y_1, \cdots, y_V\})| < V$ unless $i = j$. Thus each $Y_B \in \mathscr{C}$ has V elements. It follows that $\mathscr{C}$ is a V-collection. This and (2) together prove Lemma 1.

It is all too clear that Lemma 1 is not much direct help in finding V. The next lemma shows that the V-collection produced in the above proof has associated with it some further structure which is useful for finding V, especially, as we will see in § 3, in the case of groups.

A *k-partition* $(\mathscr{P}, \mathscr{C})$ of G is a partition $\mathscr{P} = \{P_1, \cdots, P_k\}$ of the set G together with a k-collection $\mathscr{C}$ such that for each $\{y_1, \cdots, y_k\} \in \mathscr{C}$, there is a permutation π on $\{1, 2, \cdots, k\}$ such that $y_{\pi(i)} \in P_i$, $i = 1, 2, \cdots, k$.

LEMMA 2. *$V(\mathscr{F})$ is the largest value of k for which there exists a k-partition.*

Proof. If G has a k-partition, $V(\mathscr{F}) \geqq k$ by Lemma 1. Let $A \in \mathscr{A}_0$ with $A(G) = \{y_1, \cdots, y_V\}$ and let $\mathscr{P} = \{A^{-1}(y_1), \cdots, A^{-1}(y_V)\}$. By Lemma 1,

$$\mathscr{C} \equiv \{\{B(y_1), \cdots, B(y_V)\}: B \in \mathscr{A}\}$$

is a V-collection. If for any $B \in \mathscr{A}$, $B(y_i)$ and $B(y_j)$ are both in the same set $A^{-1}(y_k)$, then $|ABA(G)| = |AB(\{y_1, \cdots, y_V\})| < V$ unless $i = j$. Thus $(\mathscr{P}, \mathscr{C})$ is a V-partition of G.

3. The case when G is a group. We assume henceforth that G is a finite abelian group and that $\mathscr{F}$ contains r_x for all $x \in G$ and exactly one other function f. It is equivalent, of course, for $\mathscr{F}$ to contain f and r_x for all x in a set which generates G. We begin by establishing a stock of examples. These examples kindled most of the results of this paper.

EXAMPLE 1. Let $G = Z_6$ and let $f(0) = 0$, $f(1) = 4$, $f(2) = 1$, $f(3) = 4$, $f(4) = 2$ and $f(5) = 3$. Then $V(f) = 1$ since $A = r_2 f r_5 f f f r_1 f f$ is the zero function.

EXAMPLE 2. Let $G = Z_2 \oplus Z_2$. Let $f(0, 0) = f(0, 1) = (0, 0)$, $f(1, 1) = (1, 1)$ and $f(1, 0) = (1, 0)$. Since f is not one-to-one, $V < 4$. It is easily seen (and it follows from Theorem 2) that $V = 2$.

EXAMPLE 3. Again take $Z_2 \oplus Z_2$ but now take $f(0, 0) = f(0, 1) = (0, 0)$ and $f(1, 0) = f(1, 1) = (1, 1)$. Once more, $V = 2$.

EXAMPLE 4. Let $G = Z_8$ and let $f(g) = f(g + 2) = g$ for $g = 0, 1, 4, 5$. Then $V = 4$.

EXAMPLE 5. Let $G = Z_{12}$ and let $f(0) = f(2) = f(4) = 0$, $f(6) =$

$f(8) = f(10) = 1$, $f(1) = f(5) = f(9) = 6$, and $f(3) = f(7) = f(11) = 7$. Then $V = 4$.

EXAMPLE 6. Let $G = Z_3 \oplus Z_3 \oplus Z_2$ and let $f(x, y, 0) = (y, y, 0)$ and $f(x, y, 1) = (x, 2x, 0)$ for all $x, y \in Z_3$. Then $V = 3$.

EXAMPLE 7. Let $G = Z_n$ for some n and let f be any homomorphism. It is easily seen that in this case, $V = \min\{|f^m(G)|: m = 1, 2, \cdots\}$. Also, $V = 1$ if and only if every prime factor of n divides $f(1)$.

An inspection of Example 1 and other examples leads to the following condition for $V = 1$.

THEOREM 1. *Let* $X_0 = \{0\}$ *and, for* $k > 0$, *let*

$$X_k = \{x \in G: x \in X_{k-1} \text{ or } f(x + y) - f(y) \in X_{k-1} \text{ for some } y \in G\} .$$

Then $V = 1$ *if and only if*

$$G = \bigcup_{k=1}^{\infty} X_k .$$

Proof. Since $\{X_k\}$ is a nondecreasing sequence of sets, it is equivalent to show $V = 1$ if and only if $G = X_k$ for some k. Suppose first that $G = X_k$. Let $A \in \mathscr{A}$ be such that $A(0) = 0$ and $A(x) \neq 0$ for some $x \in G$. Then $x \in X_j$ but $x \notin X_{j-1}$ for some $j > 0$. Thus, there exists $y \in G$ such that

$$z \equiv r_{-f(y)} f r_y(x) = f(x + y) - f(y) \in X_{j-1} .$$

Also,

$$r_{-f(y)} f r_y(0) = f(y) - f(y) = 0 .$$

Applying the same argument to z and continuing the process, we may construct $B \in \mathscr{A}$ such that $B(x) = B(0) = 0$. Thus $V \leqq |BA(G)| < |A(G)|$. By the arbitrary nature of A, it follows that $V = 1$.

Now suppose $V = 1$. Then $A(G) = \{0\}$ for some $A \in \mathscr{A}$. Clearly, A may be written in the form

$$A = r_{x_n} f r_{x_{n-1}} f \cdots f r_{x_1} f r_{x_0}$$

for some $n \geqq 1$ and $x_0, x_1, \cdots, x_n \in G$. Let $v_1 = x_0$ and for $i = 2, 3, \cdots, n$, let $v_i = x_{i-1} + f(v_{i-1})$. Let $g_i = r_{-f(v_i)} f r_{v_i}$, $i = 1, 2, \cdots, n$. Then $g_i(0) = 0$ for each i and

$$\begin{aligned} g_n g_{n-1} \cdots g_1 &= r_{-f(v_n)} f r_{v_n - f(v_{n-1})} f \cdots f r_{v_2 - f(v_1)} f r_{v_1} \\ &= r_{-f(v_n)} f r_{x_{n-1}} f \cdots f r_{x_0} \\ &= r_{-x_n - f(v_n)} A = A . \end{aligned}$$

The last step follows from the fact that both sides map 0 into 0. We will show by induction that

$$(3) \qquad (g_n g_{n-1} \cdots g_{n-i})^{-1}(0) \subseteq X_{i+1} .$$

This is true for $i = -1$ (where the compostion of no functions is taken to be the identity function). Assume (3) holds for $i-1$ and let $x \in (g_n g_{n-1} \cdots g_{n-i})^{-1}(0)$. Then $f(x + v_{n-i}) - f(v_{n-i}) = g_{n-i}(x) \in (g_n g_{n-1} \cdots g_{n-i+1})^{-1}(0) \subseteq X_i$. Therefore $x \in X_{i+1}$, so (3) holds for all i. Taking $i = n-1$, (3) gives $G = A^{-1}(0) \subseteq X_n$, which proves Theorem 1.

The sequence $\{X_k\}$ of sets in the above theorem is eventually constant. Moreover, if $X_k = X_{k-1}$, then all subsequent terms are identical, so it is clear when a maximal term has been reached. The main shortcoming of Theorem 1 is that it does not avoid an iterative procedure. In an attempt to avoid an iterative method, we apply the notions of §2 to the case of groups. We first demonstrate that the number of partitions which are eligible to be k-partitions is limited.

LEMMA 3. *Let $(\mathscr{P}, \mathscr{C})$ be a k-partition of G, let $\mathscr{P} = \{P_1, \cdots, P_k\}$ and let $Y \in \mathscr{C}$. Then*

$$G = P_i \oplus Y$$

for $i = 1, 2, \cdots, k$.

Proof. Let $u, v \in P_i$, $x, y \in Y$ and suppose $x + u = y + v$. Setting $w = x - v = y - u$, we obtain $r_{-w}(x) = x - (x - v) = v$ and $r_{-w}(y) = u$. By the definition of k-partition, it follows that $x = y$ and hence that $u = v$. The $|P_i|k$ sums $x + u$ where $x \in Y$ and $u \in P_i$ are distinct. Thus $|G| \geqq |P_i|k$. Also, $|G| = \sum_{i=1}^{k} |P_i|$ so that in fact $|P_i| = |G|k^{-1}$ for each i. Thus $G = P_i \oplus Y$ for each i.

Combining Lemmas 2 and 3 immediately gives

COROLLARY 1. *V divides $|G|$. In particular, if $G = Z_p$ for p prime, $V = 1$ if f is not one-to-one.*

To find V, one need only examine partitions $\mathscr{P} = \{P_1, \cdots, P_k\}$ such that each P_i has $|G|k^{-1}$ elements and such that there exists a set Y for which $G = Y \oplus P_i$ for each i. An obvious candidate for a k-partition is the collection of cosets of a subgroup of G. This leads us to the next theorem, which gives a lower bound for V, and thereby gives a necessary condition for $V = 1$. We need the following definitions.

A subgroup H of G is called *f-regular* if for each $a \in G$, $f(a + H) \subseteq$

$f(a) + H$, i.e., if f maps cosets into cosets. Since $f(0) = 0$ by assumption, this implies in particular that $f(H) \subseteq H$. A pair (L, K) of subgroups of G is *noncombinative* of order $\alpha = \alpha(L, K)$ if L and K are f-regular, and there exist subgroups $H_1, \cdots, H_m$ of index α in K and elements $x_1, \cdots, x_\alpha$ of K such that $x_j - x_k \notin \bigcup_{i=1}^m H_i$ for distinct j and k, $\bigcap_{i=1}^m H_i = L$, and if $x, y \in G$ are such that $x - y \in K$ but $x - y \notin \bigcup_{i=1}^m H_i$, then $f(x) - f(y) \notin \bigcup_{i=1}^m H_i$.

It is clear that the above condition are unaffected if x_j is replaced by $x_j - x_1$ for each j, so we may assume that $x_1 = 0$. Suppose (L, K) is noncombinative of order α and suppose the quantity m equals one. This is necessarily the case if K (or G) is cyclic, since the subgroups $H_1, H_2, \cdots, H_m$ are all of the same order. Then $H_1 = L$, $[K: L] = \alpha$ and one of $x_1, \cdots, x_\alpha$ is in each coset of L. Conversely, if L and K are f-regular subgroups with $L \subseteq K$ and if $x - y \in K$ but $x - y \notin L$ imply $f(x) - f(y) \notin L$, then (L, K) is non-combinative of order α (with $m = 1$).

THEOREM 2. *Suppose G has subgroups $L_1 \subset K_1 \subseteq L_2 \subset K_2 \subseteq \cdots \subseteq L_r \subset K_r$ where each pair (L_j, K_j) is noncombinative of order α_j. Then*

$$V(f) \geq \prod_{j=1}^{r} \alpha_j . \tag{4}$$

Proof. Let $\beta_k = \prod_{j=1}^{k} \alpha_j$ and $\gamma_k = \prod_{j=k}^{r} \alpha_j$ for $k = 1, \cdots, r$ and let $\beta_0 = \gamma_{r+1} = 1$. We show $V \geq \beta_r$ by constructing a β_r-collection and by applying Lemma 1. For $j = 1, 2, \cdots, r$, let H_{ji}, $i = 1, 2, \cdots, m_j$, and x_{ji}, $i = 1, 2, \cdots, \alpha_j$ be the subgroups and elements of K_j with the properties indicated in the definition of non-combinative. As noted above, we may assume $x_{j1} = 0$ for $j = 1, 2, \cdots, r$.

Let $\mathscr{C}$ be the collection of all subsets of G with β_r elements such that for $Y \in \mathscr{C}$

(i) for $j = 1, 2, \cdots, r$, exactly γ_{j+1} of the cosets of K_j each contain exactly β_j elements of Y.

(ii) for $j = 1, 2, \cdots, r$ and $i = 1, 2, \cdots, m_j$, exactly γ_j of the cosets of H_{ji} each contain exactly β_{j-1} elements of Y.

Note that $\mathscr{C}$ is nonempty since the set $\{x_{1i_1} + \cdots + x_{ri_r} : 1 \leq i_j \leq \alpha_j, 1 \leq j \leq r\}$ is in $\mathscr{C}$. If $Y \in \mathscr{C}$, it follows from (i) and (ii) that

(iii) the distinct cosets of K_j which intersect Y are contained in distinct cosets of $H_{j+1,i}$ for $j = 1, 2, \cdots, r-1$ and $i = 1, 2, \cdots, m_j$.

Let $Y \in \mathscr{C}$. It is obvious that for any $x \in G$ the set $r_x(Y) = \{x + y : y \in Y\}$ is also in $\mathscr{C}$. We will show that $f(Y)$ is also in $\mathscr{C}$. First, suppose there exist $y, z \in Y$ such that $y - z \in \bigcup_{i=1}^m H_{ji}$ but $f(y) + H_{ji} = f(z) + H_{ji}$ for some j and i. Since (L_j, K_j) is non-combinative, $y + K_j \neq z + K_j$. By (iii), $y - z \in \bigcup_{i=1}^m H_{j+1,1}$ while, on

the other hand, it is clear that $f(y) + H_{j+1,i} = f(z) + H_{j+1,i}$. Proceeding by induction, we conclude that $y + K_r \neq z + K_r$, which contradicts (i) for $j = r$. Thus

$$(5) \qquad y - z \notin \cup H_{ji} \Longrightarrow f(y) - f(z) \notin \cup H_{ji}$$

for all $y, z \in Y$ and all i, j. Now let $y, z \in Y$ be such that $y + K_j \neq z + K_j$ for some j. By (i), $j < r$. Then $y + H_{j+1,1} \neq z + H_{j+1,1}$ by (iii). By (5), $f(y) + H_{j+1,i} \neq f(z) + H_{j+1,i}$. Since $K_j \subseteq H_{j+1,1}$, we conclude that

$$(6) \qquad y + K_j \neq z + K_j \Longrightarrow f(y) + K_j \neq f(z) + K_j$$

for $y, z \in Y$ and any j. It follows from (5) with $j = 1$ that f is one-to-one on Y and then from (5) and (6) that $f(Y) \in \mathscr{C}$. We have proved $\mathscr{C}$ is a β_r-collection. By Lemma 1, $V \geqq \beta_r$, which proves Theorem 2.

REMARKS. It is easy to construct a β_r-partition $(\mathscr{P}, \mathscr{C})$ under the hypotheses of Theorem 2, by taking $\mathscr{C}$ to be as in the proof and $\mathscr{P}$ to be constructed from unions of cosets of the subgroups.

Let $\delta = \delta(f)$ denote the maximum value that can be attained by a product of the type given in (4). Since the pair (G, G) is always noncombinative of order 1, we set $\delta = 1$ if there are no noncombinative pairs (L, K) of subgroups with $L \subset K$. Finding $\delta(f)$ for a given f is generally not too difficult since attention may be restricted to f-regular subgroups.

4. How good is the bound $V \geqq \delta$? To answer this, we first look at the examples discussed earlier.

In Example 1, it is obvious that $\delta = V = 1$. In Example 2, the value $\delta = 2 = V$ is obtained by taking $r = 1$, $K_1 = G$, and $L_1 = \{(0, 0), (0, 1)\}$. In Example 3, the value $\delta = 2 = V$ can be obtained in two ways. Either take $r = 1$, $K_1 = G$ and $L_1 = \{(0, 0), (0, 1)\}$ or take $r = 1$, $K_1 = \{(0, 0), (1, 1)\}$ and $L_1 = \{(0, 0)\}$. In Example 4, the value $\delta = 4$ is achieved by taking $r = 2$, $L_1 = \{0\}$, $K_1 = \{0, 4\}$, $L_2 = \{0, 2, 4, 6\}$ and $K_2 = G$. The value $\delta = 4$ cannot be attained if only one noncombinative pair is used. In Example 5, $\delta = 1 \neq V$. In Example 6, $\delta = 3 = V$ is attained by taking $r = 1$, $K_1 = \{x, y, x) \in G: z = 0\}$ and $L_1 = \{(0, 0, 0)\}$. The pair (L_1, K_1) is noncombinative with $H_{11} = \{0, 0, 0), (1, 0, 0), (2, 0, 0)\}$, $H_{12} = \{(0, 0, 0), (0, 1, 0), (0, 2, 0)\}$, $x_1 = (0, 0, 0)$, $x_2 = (1, 1, 0)$, and $x_3 = (2, 2, 0)$. Finally, in Example 7, let $a = f(1)$ and let m be sufficiently large that $V = |f^m(G)|$. The value $\delta = V$ is attained by taking $r = 1$, $L_1 = \{0\}$, and $K_1 = \{0, a^m, 2a^m, \cdots, (V-1)a^m\}$.

Example 5 shows that it is not always true that $\delta = V$, and in

fact it is possible that $V > 1$ when $\delta = 1$. Consider the simple upper bound for V, namely

$$V(f) \leqq |f(G)| .$$

Note that in Examples 3, 4 and 5, V attains this upper bound. We were unable to construct *any* example for which

$$\delta < V < |f(G)| .$$

(Furthermore, in every example we have studied for which $V<|f(G)|$, the value of δ is attainable by using one noncombinative pair of order δ in Theorem 2.) On the other hand, we have not been able to prove that no such examples exist. The difficulty in proving such a result is underlined by the length of the proof of the following very special result.

THEOREM 3. *Suppose* $V \leqq 3$. *Then* G *has a non-combinative pair of subgroups of order* $\alpha = V$.

Proof. The case $V = 1$ is obvious. Assume $V = 2$ or 3. Define

$$Y = \{y \in G: \exists A \in .\mathscr{S}_0 \text{ such that } y \in A(G)\} \tag{7}$$

and let K be the subgroup generated by Y. Define

$$\mathscr{H}' = \{H: H = A^{-1}(0) \cap K \text{ for some } A \in .\mathscr{S}_0\}$$

and let $L = \bigcap_{H \in \mathscr{H}'} H$. We will show that (L, K) is noncombinative of order V. We break the proof into several lemmas.

LEMMA 4. *Let* $B \in .\mathscr{S}$ *and* $z \in G$. *Then* $B(z + K) \subseteqq B(z) + K$. *In particular (taking* $B = f$*),* K *is* f*-regular.*

Proof. Let $u = B(z)$ and observe that

$$r_{-u}Br_z(0) = r_{-u}B(z) = 0 .$$

For any $y \in Y$,

$$B(z + y) - u = r_{-u}Br_z(y) \in Y \subseteqq K .$$

Thus $B(z + y) \in u + K$. Now, every element of K is a sum of elements of Y. The lemma follows by induction on the number of terms in the sum.

The next step is to show each $H \in \mathscr{H}'$ is a subgroup of K. Fix $A \in .\mathscr{S}_0$ for now and let $H = A^{-1}(0) \cap K$. Denote the elements of $A(G)$ by $\{x_0 = 0, x_1, x_2, \cdots, x_{V-1}\}$, First, let f_K be the restriction of f to K

and let $\mathscr{A}_K$ be the semi-group of functions on K generated by f_K and r_x, $x \in K$. The collection $\mathfrak{P} = \{A^{-1}(x_i) \cap K: x_i \in A(G)\}$ is a partition of K. Let $\mathscr{C} = \{\{B(x_0), \cdots, B(x_{V-1})\}: B \in \mathscr{A}_K\}$. It is clear that $(\mathfrak{P}, \mathscr{C})$ is a V-partition of K.

By Lemma 3,

$$|H| = |A^{-1}(0) \cap K| = |K|V^{-1} . \tag{8}$$

LEMMA 5. *Let $a \in G$ and let $B \in \mathscr{A}_0$. Let $B(G) = \{u_0, u_1, \cdots, u_{V-1}\}$. For $i, j = 0, 1, \cdots, V-1$, exactly one of the expressions*

$$a + u_j - u_k, \; k = 0, 1, \cdots, V-1 \tag{9}$$

and one of the expressions

$$a + u_k - u_j, \; k = 0, 1, \cdots, V-1 \tag{10}$$

is in each set $A^{-1}(x_i) \cap (a + K)$.

Proof. Obviously, each element of (9) is in $a + K$. Suppose $a + u_j - u_k$ and $a + u_j - u_l$ are both in $A^{-1}(x_i)$. Then

$$Ar_{a+u_j-u_k-u_l}(u_l) = Ar_{a+u_j-u_k-u_l}(u_k) = x_i . \tag{11}$$

By the definition of V,

$$|Ar_{a+u_j-u_k-u_l}B(G)| = V$$

so (11) implies that $k = l$. This proves the first statement. The second is proved similarly.

We now assume $V = 3$. A similar proof will show the result in the case $V = 2$. Lemma 5 has particularly strong implications for these two values of V. Denote the elements of Y by $y_0 = 0, y_1, y_2, \cdots, y_l$ and let

$$I_i = \{j: y_j \in A^{-1}(x_i)\} , \quad i = 0, 1, 2 . \tag{12}$$

In particular, $I_0 = \{0\}$. No I_i is empty since for any $B \in \mathscr{A}_0$, $B(G)$ has 3 elements, one in each $A^{-1}(x_i)$.

LEMMA 6. *Let $b \in A^{-1}(x_{i_0})$, $B \in \mathscr{A}_0$, $B(G) = \{u_0, u_1, u_2\}$. Let j_1, j_2 and j_3 be distinct elements of $\{0, 1, 2\}$. Suppose $b + (u_{j_1} - u_{j_2}) \in A^{-1}(x_{i_1})$ and $b + 2(u_{j_1} - u_{j_2}) \in A^{-1}(x_{i_2})$. Then i_0, i_1 and i_2 are distinct and $b + r(u_{j_1} - u_{j_2}) \in A^{-1}(x_{i'})$ where $i' = i_0, i_1$ or i_2 according as $r \equiv 0, 1$ or $2 \pmod 3$.*

Proof. Let $a = b + (u_{j_1} - u_{j_2}) \in A^{-1}(x_{i_1})$. Since $a = a + (u_{j_1} - u_{j_1}) \in A^{-1}(x_{i_1})$, it follows from Lemma 5 that $a + (u_{j_1} - u_{j_2}) \notin A^{-1}(x_i)_1$ and

$b = a + (u_{j_2} - u_{j_1}) \notin A^{-1}(x_{i_1})$. Thus $i_0 \neq i_1$ and $i_1 \neq i_2$. Suppose $i_0 = i_2$. Then $a + (u_{j_2} - u_{j_1}) \in A^{-1}(x_{i_0})$ and $a + (u_{j_1} - u_{j_2}) \in A^{-1}(x_{i_0})$. By Lemma 5, we must have $a = a + (u_{j_3} - u_{j_3}) \in A^{-1}(x_{i_0})$, which is a contradiction. Therefore i_0, i_1 and i_2 are distinct. The rest of the lemma follows easily by induction.

LEMMA 7. *Let $z \in K$. Then $z \in A^{-1}(x_k)$ iff z can be expressed in the form*

$$z = \sum_{j=1}^{t} c_j y_j \tag{13}$$

where the c_j's are non-negative integers and

$$\sum_{j \in I_1} c_j + 2 \sum_{j \in I_2} c_j \equiv k \pmod 3 . \tag{14}$$

Also, H is a subgroup of K and $[K: H] = 3$.

Proof. Since any $z \in K$ can be written in the form (13) for *some* non-negative c_j's it is enough to prove the sufficiency. We do this by induction on $m = \sum_{j=1}^{t} c_j$. The statement is true for $m = 0$. If $m = 1$, then one $c_j = 1$ and all others are zero. Then $z = y_j$ for some j and the result is obvious for $j \in I_1$ or $j \in I_2$. Now assume the result holds whenever $m \leqq m_0$, where $m_0 \geqq 1$. Let $c_1, c_2, \cdots, c_t$ be such that $\sum c_j = m_0$ and let $a = \sum c_j y_j$. Let $j_0 \in I_1 \cup I_2$. It suffices to show the result holds for $a + y_{j_0}$. Let $D(k) = A^{-1}(x_k)$, $k = 0, 1, \cdots, V - 1$. By the inductive hypothesis

$$a \in D(k) \tag{15}$$

where k is given by (14). Suppose initially that $c_{j_0} > 0$. Then

$$a - y_{j_0} \in D(k - i_0) \tag{16}$$

where i_0 is such that $j_0 \in I_{i_0}$. [Here and throughout, the arguments for D are calculated *modulo* 3.] It follows from Lemma 6 that

$$a + y_{j_0} \in D(k + i_0) \tag{17}$$

as required. Now suppose $c_{j_0} = 0$. Since $m_0 \geqq 1$, there is some j_1 such that $c_{j_1} > 0$. Then

$$a - y_{j_1} \in D(k - i_1) \tag{18}$$

where i_1 is such that $j_1 \in I_{i_1}$. We then have

$$a - y_{j_1} + y_{j_0} \in D(k - i_1 + i_0) \tag{19}$$

and, by the previous case,

$$a + y_{j_1} \in D(k + i_1) \,. \tag{20}$$

By (15), $a + y_{j_0} \notin D(k)$ and by (19), $a + y_{j_0} \notin D(k - i_1 + i_0)$. If $i_1 \neq i_0$, these two facts imply (17). If $i_1 = i_0$, it could also happen that

$$a + y_{j_0} \in D(k - i_0) \,. \tag{21}$$

By Lemma 6, (19) and (21) together imply that

$$a + y_{j_1} + y_{j_0} \in D(k + i_1) \,,$$

which cannot happen, by Lemma 6 and (20). Thus, (21) does not hold, which means that (17) holds in this case also. This proves the first statement in the Lemma. The second is an obvious corollary of the first and of (8).

Since every $H \in \mathscr{H}$ is a subgroup of K, it is clear that L is also a subgroup. Let $x, y \in G$ be such that $x - y \in L$. By the definition of L, $A(x - y) = 0$ for all $A \in \mathscr{A}_0$. Define $B = r_{-f(y)} f r_y$ and note that $B(0) = 0$ and $B(x - y) = f(x) - f(y)$. For $A \in \mathscr{A}_0$, $A(f(x) - f(y)) = AB(x - y) = 0$ since $AB \in \mathscr{A}_0$. Therefore $f(x) - f(y) \in L$. We conclude that L is f-regular.

Let $B \in \mathscr{A}_0$ and let $B(G) = \{x_1, x_2, x_3\}$. Suppose $x_i - x_j \in H$ where $H \in \mathscr{H}$ and $i \neq j$. For some $A \in \mathscr{A}_0$, $Ar_{-x_j}(x_j) = 0$ and $Ar_{-x_j}(x_j) = A(x_j - x_j) = 0$, which is impossible. Therefore x_1, x_2, x_3 are such that $x_i - x_j \notin \bigcup_{H \in \mathscr{H}} H$. Similarly, if $x, y \in G$ are such that $x - y \in K$ but $x - y \notin \bigcup_{H \in \mathscr{H}} H$, then $f(x) - f(y) \notin \bigcup_{H \in \mathscr{H}} H$. This shows that (L, K) is noncombinative of order V and thereby completes the proof of Theorem 3.

REMARKS. It is an easy consequence of Theorem 3 that $V = \delta$ if $|G| = 4$, 6 or 9. We were unable to extend Theorem 3 to any cases with $V > 3$. Note that Lemmas 4 and 5 hold for any V, as does (8). It is not true in general that $H = A^{-1}(0) \cap K$ is a group for any $A \in \mathscr{A}_0$. In Example 5, $H = \{0, 2, 4\}$ if $A = f$. It may be that Theorem 3 is valid whenever V is prime. It this is the case, we could conclude that $V = \delta$ whenever $|G|$ is the product of two primes (not necessarily distinct).

REFERENCES

1. R. L. Adler, L. W. Goodwyn and B. Weiss, *Equivalence of topological Markov shifts*, Israel J. Math., **27** (1977), 49-63.

2. G. L. O'Brien. *The road-colouring problem*, Israel J. Math., **39** (1981), 145-154.

Received July 30, 1980. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada. I am indebted to Cornell University, whose kind hospitality I enjoyed while working on this problem.

YORK UNIVERSITY
DOWNSVIEW, ONTARIO M3J IP3, CANADA