Pacific Journal of Mathematics

DECOMPOSITION OF SETS OF GROUP ELEMENTS

WALTER BALL LAFFER, I AND HENRY B. MANN

Vol. 14, No. 2 June 1964

DECOMPOSITION OF SETS OF GROUP ELEMENTS

W. B. LAFFER AND H. B. MANN

In this paper small letters will denote group elements or integers. Large letters will denote sets of these. The cardinal of a set S will be denoted by (S).

1. Sets in Abelian Groups. The problem of decomposition of sets of elements of a finite additive Abelian group, G, of order v, is the following. Given a set of group elements, C, when do there exist sets of group elements, A and B, with Min $(A), (B) \geqq 2$ and $C = A + B = \{a + b \mid a \in A, b \in B\}$? If there are such sets, A and B, then we say that A and B are components of C, and that C is decomposable. We are also concerned with the following question, given a set C and a set A, when is A a component of C? The problems of decomposition are stated analogously when C, A, and B are sets of nonnegative integers. The results for sets of group elements are analagous to the results for sets of nonnegative integers. We include the proofs for both cases because although the techniques used in handling additive problems in finite Abelian groups are analogous to the techniques used in handling additive problems for sets of nonnegative integers (see Mann [5], [6], [7]; Dyson [1]; and Kneser [4]), they are not identical.

In Theorems 1–5 all sets shall be sets of elements from a finite Abelian group, G, of order v.

THEOREM 1. *Let C be sets of elements from the finite Abelian group, G. Let $\bar{C} = \{\bar{c}_1, \bar{c}_1, \cdots, \bar{c}_r\}$ be the complement of C in G. Let $D = \{\bar{c}_r - \bar{C}\} = \{\bar{c}_r - \bar{c}_j \mid j = 1, \cdots, r\}$. Then A is a component of C, if and only if, for every $k \notin D$ we have $A + k \not\subset A + D$.*

Proof. Put $B = \bigcap_{i=1}^{r} \{\bar{c}_i - \bar{A}\}$. Then A is a component of C if and only if $A + B = C$.

Suppose for every $k \notin D$ we have $A + k \not\subset A + D$. Then, for every $k \notin D$ there is an $a \in A$ such that $a + k = \bar{a}_i + d_i$ for every $i = 1, \cdots, r$ where $d_i = \bar{c}_r - \bar{c}_i$ and $\bar{a}_i \in \bar{A}$. Hence for every $i = 1, \cdots, r$ we have $\bar{c}_r - k = a - \bar{a}_i + \bar{c}_i = a + \bar{c}_i - \bar{a}_i = a + b$ where $b \in B$. For every $c \in C$ put $k = \bar{c}_r - c$. Hence $c = a + b$ which implies that $A + B = C$. Thus A is a component of C.

Suppose $A + B = C$. If there is a $k \notin D$ such that $A + k \subset A + D$,

Received July 1, 1963. The first author was supported in part by an NSF cooperative fellowship.

then for every $a \in A$ there is an i such that $a + k = a_i + d_i$. Therefore, $\bar{c}_r - k = a + \bar{c}_i - a_i = a + \bar{b}$ where $\bar{b} \in \bar{B} = \bigcup_{i=1}^{r} \{\bar{c}_i - A\}$. Since $k \neq \bar{c}_r - \bar{c}_j$, we must have $k = \bar{c}_r - c$ for some $c \in C$. Hence for every $a \in A$ we have $c - a = \bar{b} \in \bar{B}$. Therefore, $c \notin A + B$. This is a contradiction and hence the theorem is true.

COROLLARY 1.1. *Let $\bar{C} = \{\bar{c}\}$. Then A is a component of C if and only if A is not a coset of some subgroup of G.*

COROLLARY 1.2. *If G is cyclic of prime order and $\bar{C} = \{\bar{c}\}$, then A is a component of C if and only if $1 < (A) < (C)$.*

DEFINITION. We say that A is an m component of C if and only if A is a component of C and $(A) = m$.

COROLLARY 1.3. *If $\bar{C} = \{\bar{c}_1, \cdots, \bar{c}_r\}$, then $\{0, a\}$ is a 2 component of C if and only if $2a = \bar{c}_i - \bar{c}_j$ implies $a = \bar{c}_i - \bar{c}_m$ for some m.*

Proof. Suppose $\{0, a\}$ is a 2 component of C. Let $2a = \bar{c}_i - \bar{c}_j$. By Theorem 1 if $k \notin D$ then $\{k, a + k\} \not\subset \{0, a\} + D$. Put $k = a + d_i$. Then $\{k, a + k\} = \{a + d_i, 2a + d_i\} = \{a + d_i, d_j\} \subset \{0, a\} + D$. If $k \notin D$, then $\{0, a\}$ is not a 2 component of C. Hence $k \in D$. Thus $k = a + d_i = d_m$ which implies $a = \bar{c}_i - \bar{c}_m$.

Suppose that $2a = \bar{c}_i - \bar{c}_j$ implies $a = \bar{c}_i - \bar{c}_m$ for some m. If $\{0, a\}$ is not a 2 component of C, then by Theorem 1 there is a $k \notin D$ such that $\{k, a + k\} \subset \{0, a\} + D$. This implies that $k = a + d_u$ for some $u = 1, \cdots, r$, and $a + k = 2a + d_u = d_s$. Thus $2a = \bar{c}_u - \bar{c}_s$ and by assumption this implies $a = \bar{c}_u - \bar{c}_t$. Therefore, $k = a + d_u = d_t \in D$. This is a contradiction, and hence $\{0, a\}$ is a 2 component of C.

In Corollaries 1.4–1.9 we shall assume that $\bar{C}$ is a difference set with parameters $v = (G)$, $r = (\bar{C})$, and $\lambda =$ the number of representations which each nonzero element of G has in the form $\bar{c}_i - \bar{c}_j$.

COROLLARY 1.4. *Let $(\bar{C}) = r < v$. If $2a = 0$ for $a \neq 0$, then $\{0, a\}$ is not a 2 component of C.*

Proof. If $\{0, a\}$ is a 2 component of C then $2a = \bar{c}_i - \bar{c}_i$ for every $i = 1, \cdots, r$, and by Corollary 1.3 we have $r = v$.

COROLLARY 1.5. *If $(\lambda, v) = 1$, then there does not exist an $a \neq 0$ such that $\{0, a\}$ is a 2 component of C.*

Proof. Suppose there is an $a \neq 0$ such that $\{0, a\}$ is a 2 component of C. Because of Corollary 1.4 we may assume $2a \neq 0$. Since

$\bar{C}$ is a difference set we have

(i) $2a = \bar{c}_{i_1} - \bar{c}_{j_1} = \bar{c}_{i_2} - \bar{c}_{j_2} = \cdots = \bar{c}_{i_\lambda} - \bar{c}_{j_\lambda}$.

By Corollary 1.3 we must have

(ii) $a = \bar{c}_{i_1} - \bar{c}_{m_1} = \bar{c}_{i_2} - \bar{c}_{m_2} = \cdots = \bar{c}_{i_\lambda} - \bar{c}_{m_\lambda}$.

Subtracting a from $2a$ we get

(iii) $a = \bar{c}_{m_1} - \bar{c}_{j_1} = \bar{c}_{m_2} - \bar{c}_{j_2} = \cdots = \bar{c}_{m_\lambda} - \bar{c}_{j_\lambda}$.

If there is an index m_s in (iii) that does not appear as a first index i_t in (ii), then a has at least $\lambda + 1$ distinct representations as an element of $\{\bar{C} - \bar{C}\}$. This contradicts the choice of $a \neq 0$. Hence we must have that every first index in (iii) appears as a first index in (ii).

Thus from (ii) we obtain $\lambda a = \sum_{k=1}^{\lambda} \bar{c}_{i_k} - \bar{c}_{m_k} = 0$. Since $(\lambda, v) = 1$, it follows that $a = 0$. This contradicts our choice of a, hence Corollary 1.5 is true.

COROLLARY 1.6. *If G is cyclic of order $n^2 + n + 1$, and if G has no simple difference set of order $n + 1$, then every set of n^2 elements has a 2 component.*

COROLLARY 1.7. *Let G be cyclic of order $n^2 + n + 1$, and let $n \leqq 1600$. If n is not a prime power, then every set of n^2 elements has a 2 component.*

Proof. This follows from Corollary 1.6 and the paper of Evans and Mann [2].

COROLLARY 1.8. *Let $\lambda > 2$. Suppose there is a cyclic subgroup H of G such that $(H) = \lambda$. Suppose $H + g \subset \bar{C}$ for some $g \in G$. Let $a \in H$ such that a has order λ. Then $\{0, a\}$ is a 2 component of C.*

Proof. If $\bar{C}$ is a difference set, then so is $\bar{C} - g$. Hence without loss of generality we may assume that $H \subset \bar{C}$.

If $a \in H$ and a has order λ, then $ja \in H$ for $0 \leqq j \leqq \lambda - 1$. Since $2a \neq 0$, we have that $2a = ja - (j - 2)a$ for $0 \leqq j \leqq \lambda - 1$ are the λ distinct representations of $2a$ as an element of $\{\bar{C} - \bar{C}\}$. Clearly, $a = ja - (j - 1)a$ for $0 \leqq j \leqq \lambda - 1$ are the λ distinct representations of a as an element of $\{\bar{C} - \bar{C}\}$. By Corollary 1.3 $\{0, a\}$ is a 2 component of C.

An example of a case where this situation actually occurs is the following. Let G be the residues modulo 15. Let $\bar{C} = \{0, 1, 2, 4, 5, 8, 10\}$. Here $\lambda = 3$, $a = 5$, and $g = 0$. This and other examples can be found in [3].

An immediate generalization of Corollary 1.8 is the following.

COROLLARY 1.9. *Let $(\lambda, v) = d > 2$. Suppose H is a cyclic sub-*

group of G of order d. Suppose there are exactly λ/d cosets of H contained in $\bar{C}$. If $a \in H$ such that a is of order d, then $\{0, a\}$ is a 2 component of C.

An example of a case where this situation occurs is again from [3]. It is the geometry modulo 63. We have $\bar{C} = \{0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 18, 19, 24, 26, 27, 28, 32, 33, 35, 36, 38, 41, 45, 48, 49, 52, 54, 56\}$. Here $\lambda = 15$, $d = 3$, and $a = 21$. We have $H = \{0, 21, 42\}$; and the 5 cosets are: $\{3, 24, 45\}$; $\{6, 27, 48\}$; $\{7, 28, 49\}$; $\{12, 33, 54\}$; and $\{14, 35, 56\}$.

DEFINITION. We say that C is indecomposable, if there do not exist sets, A and B, such that $\text{Min}\,(A), (B) \geqq 2$ and $A + B = C$.

THEOREM 2. *Let C be such that $(C) = 3$. If the elements of C are not in progression, then C is indecomposable.*

THEOREM 3. *Let $C = \{0, c_1, c_2, \cdots, c_s\}$. Let $s \geqq 3$ and let $C^* = \{0, c_1, c_2, \cdots, c_{s-1}\}$. If $c_s \notin \{C^* - C^*\} \cup \{C^* + C^*\}$, then C is indecomposable.*

Proof. Suppose there are sets, A and B, with $\text{Min}\,(A), (B) \geqq 2$ and such that $A + B = C$. Since $0 \in C$ we must have $0 = a_0 + b_0$ where $a_0 \in A$ and $b_0 \in B$. Let $A' = A - a_0$ and $B' = B - b_0$. Since $b_0 = -a_0$ we must have $A' + B' = A + B = C$. Thus we may assume without loss of generality that $0 \in A \cap B$. Hence $A \cup B \subset C$.

If $c_s \in A + B$, then $c_s = c_i + c_j$. If $i \neq s$ and $j \neq s$, then $c_s \in \{C^* + C^*\}$ contrary to hypothesis. Thus $c_s \in A \cup B$. Suppose $c_s \in A$. Since $(B) \geqq 2$, we have a $c \in B$ such that $c \neq 0$. We must have $c_s + c = c_i \in C$. Hence $c_s = c_i - c \in \{C^* - C^*\}$ which is contrary to hypothesis. Thus C is indecomposable.

The fact that $(C) \geqq 4$ is necessary is illustrated by the following example. Let $C = \{0, 2c, c\}$. Put $C^* = \{0, 2c\}$. We have $\{C^* - C^*\} \cup \{C^* + C^*\} = \{0, 2c, -2c, 4c\}$, and $c \notin \{C^* - C^*\} \cup \{C^* + C^*\}$ for any choice of c such that $3c \neq 0$. Yet $C = \{0, c\} + \{0, c\}$.

COROLLARY 3.1. *Let $s \geqq 3$. If $(G) = v > [3s(s-1)/2] + 1$, then there exists a set $C \subset G$ such that $(C) = s + 1$ and C is indecomposable.*

Proof. Let $C^* = \{0, c_1, c_2, \cdots, c_{s-1}\}$ be any set of $s - 1$ nonzero elements of G and zero.

We have $(\{C^* + C^*\}) \leqq [s(s-1)/2] + s$ and $(\{C^* - C^*) \leqq s(s-1) + 1$. Since $C^* \subset \{C^* + C^*\} \cap \{C^* - C^*\}$, we have $(\{C^* + C^*\} \cap \{C^* - C^*\}) \geqq s$.

Hence $(\{C^* + C^*\} \cup \{C^* - C^*\}) \leqq [3s(s-1)/2] + 1$.

Since $v > [3s(s-1)/2] + 1$, we must have an element $c_s \in G$ such that $c_s \notin \{C^* + C^*\} \cup \{C^* - C^*\}$. By Theorem 3 $C^* \cup \{c_s\}$ is indecomposable.

Theorem 2 and Corollary 3.1 give us the following.

THEOREM 4. *For any positive integer $s \geqq 2$ there always exists an Abelian group G and a subset C of G such that $(C) = s + 1$ and C is indecomposable.*

THEOREM 5. *Let $\{e_1, \cdots, e_u\} = \{\bar{C} - \bar{C}\}$. Let $s(x, y)$ be the number of solutions, of the group equation $xg = y$ where x is an integer. Suppose $m + 1 \leqq v - (\bar{C})$. If $v > \sum_{t=1}^{u} \sum_{x=2}^{m+1} s(x, e_t) = \delta$, then there exist sets A and B such that $0 \in A$, $(A) = m + 1$, A is in progression and $A + B = C$.*

Proof. There are at most δ solutions of the equations $xg = e_t$ where $2 \leqq x \leqq m + 1$ and $1 \leqq t \leqq u$. Hence if $v > \delta$, there exists an element $a \in G$ such that $xa \neq \bar{c}_i - \bar{c}_j$ for all $\bar{c}_i, \bar{c}_j \in \bar{C}$ and $x = 2, \cdots, m + 1$. We distinguish two cases:

I $m \equiv 0(2)$;

II $m \equiv 1(2)$;

Case I. $m \equiv 0(2)$. Put $A = \{0, a, -a, \cdots, ma/2, -ma/2\}$. For $k \notin D$ suppose that $A + k \subset A + D$. Then $k = ha + d_i$. Choose $|h|$ minimal.

If $h > 0$, then $k + [((m + 2)/2) - h]a = [(m + 2)/2]a + d_i = ja + d_t$. From our choice of a, in follows that $j = m/2$. Hence $a + d_i = d_t$, and so $k = (h - 1)a + d_t$, contradicting our choice of h.

If $h < 0$, then $k + [(-(m + 2)/2) - h]a = -[(m + 2)/2]a + d_i = ja + d_t$. From our choice of a it follows that $j = -m/2$. Hence $d_i = a + d_t$, and so $k = (h + 1)a + d_t$ contradicting our choice of h.

Thus by Theorem 1.1 A is a component of C.

Case II. $m \equiv 1(2)$. Put $A = \{0, a, -a, \cdots, [(m - 1)/2]a, -[(m - 1)/2]a, [(m + 1)/2]a\}$. The argument is the same as above replacing $m + 2$ with $m + 3$ and j will be either $(m + 1)/2$ or $-(m + 1)/2$.

COROLLARY 5.1. *Let $v > \delta$. Then there exist an A_i and a B_i for every i such that $2 \leqq i \leqq m + 1$ such that $0 \in A_i$, $(A_i) = i$, A_i is in progression, and $A_i + B_i = C$.*

COROLLARY 5.2. *If v is a prime, then $v > mu$ implies that for every i for which $2 \leqq i \leqq m+1$ there exist an A_i and a B_i such that $0 \in A_i$, $(A_i) = i$, A_i is in progression, and $A_i + B_i = C$.*

We note by an example that a set C may have an $i+1$ component and not have an i component. Let G be the integers modulo 13. Let $\bar{C} = \{1, 2, 4, 10\}$. By Corollary 1.5 C does not have a 2 component, since $\bar{C}$ is a simple difference set. But $\{0, 9, 12\} + \{0, 7, 9, 12\} = \{0, 3, 5, 6, 7, 8, 9, 11, 12\} = C$.

Sets of integers. From now on our sets shall be sets of nonnegative integers. In particular the complement of a set S, which shall be denoted by $\bar{S}$, shall mean the set of all nonnegative integers which are not in S.

DEFINITION. An n section is a set of nonnegative integers which contain all integers greater than n but does not contain n.

In Theorems 6 and 7 we shall assume that the sets A and C are $\bar{c}_r$ sections.

THEOREM 6. *Let $\bar{C} = \{\bar{c}_1 < \bar{c}_2 < \cdots < \bar{c}_r\}$. Let $D = \{d_i = \bar{c}_r - \bar{c}_i, i = 1, \cdots, r\}$. Then A is a component of C if and only if for every $k \notin D$, $k \leqq c_r$ we have $A + k \not\subset A + D$.*

Proof. Put $B = \bigcap_{i=1}^{r} \{\bar{c}_i - \bar{A}\}$. If $A + B_1 = C$, then $B_1 \subset B$ and also $A + B = C$. Hence, A is a component of C if and only if $A + B = C$.

Suppose for every $k \notin D$, $k \leqq \bar{c}_r$ we have $A + k \not\subset A + D$. Then, for every $k \notin D$, $k \leqq \bar{c}_r$ there is an $a \in A$ such that $a + k = \bar{a}_i + d_i$ for every $i = 1, \cdots, r$ where $d_i = \bar{c}_r - \bar{c}_i$ and $\bar{a}_i \in \bar{A}$. Hence, $\bar{c}_r - k = a - \bar{a}_i + \bar{c}_i$ for every $i = 1, \cdots, r$. Hence, $\bar{c}_r - k = a + b$ where $b \in B$. Put $k = \bar{c}_r - c$ where $c \in C$. Then $k \notin D$ and $k \leqq c_r$. Thus $c = a + b$. Hence $A + B = C$, and A is a component of C.

Now suppose A is a component of C. Hence $A + B = C$. If there is a $k \notin D$, $k \leqq \bar{c}_r$ such that $A + k \subset A + D$, then for every $a \in A$ there is an i such that $a + k = a_i + d_i$. Hence, $\bar{c}_r - k = a + \bar{c}_i - a_i = a + \bar{b}$, where $\bar{b} \in \bar{B}$. Since $k \neq \bar{c}_r - \bar{c}_j$ for any $j = 1, \cdots, r$, we must have $k = \bar{c}_r - c$ for some $c \in C$. Hence for every $a \in A$ we have $c - a = \bar{b} \in \bar{B}$. Therefore, $c \notin A + B$. This is a contradiction, and hence our theorem is true.

DEFINITION. For m a positive integer we say that A is an m set, if and only if, for all $a \in A$ we have $a + m \in A$.

COROLLARY 6.1. *Let A be an n section such that $0 \in A$. Then*

A is a component of $\{\overline{n}\}$, if and only if, A is not an m set for $m \leqq n$.

COROLLARY 6.2. *Let A be an m set for some m such that $m < n$. Let $\bar{A} = \{n_1 < n_2 < \cdots < n_r = n\}$. Then there is an $n_i < n_r$ such that*

$$\text{(i)} \qquad \frac{A(n_r)}{n_r + 1} \geqq \frac{A(n_i)}{n_i + 1}$$

where $A(x)$ denotes the usual counting function of all $a \in A$ such that $a \leqq x$.

Proof. At the end of Lemma 1 on page 911 of [7] it was shown that if the construction defined there fails at a gap $n_s < n_r = n$, then

$$\frac{C(n)}{n+1} \geqq \frac{A(n_s) + B(n_s) - 1}{n_s + 1} + \left(C(d_s - 1) - \frac{C(n)d_s}{n+1}\right)\frac{1}{n_s + 1}.$$

Now let $C = A$ and $B = \{0\}$. Then we have

$$\frac{A(n)}{n+1} \geqq \frac{A(n_s)}{n_s + 1} + \left(A(d_s - 1) - \frac{A(n)d_s}{n+1}\right)\frac{1}{n_s + 1}.$$

If we assume that $A(n_i)/(n_i + 1) > A(n)/(n + 1)$ for all $i = 1, \cdots, r - 1$ then it follows that for all $a \in A$ we have $A(a)/(a + 1) > A(n)(n + 1)$. Hence the remainder term, $[A(d_s - 1) - \{A(n)d_s/(n + 1)\}]1/(n_s + 1)$ is positive, and we have $A(n)/(n + 1) > A(n_s)/(n_s + 1)$. This contradicts the assumption that $A(n_i)/(n_i + 1) > A(n)/(n + 1)$ for all $i - 1, \cdots, r - 1$.

If the construction does not fail, then all gaps in C are filled except $n = n_r$. Since in our case $C = A$, we would have that A is a component of $\{\overline{n}\}$. But A is an m set for some $m < n$, and by Corollary 6.1 this is impossible.

An example of a case where we have equality in (i) is $A = \{0, 2, 4\}$. We have $A(1)/2 = A(3)/4 = A(5)/6 = 1/2$.

DEFINITION. The $\bar{c}_r$ section C has an m component if and only if there exist sets, A and B such that $A(\bar{c}_r) = m$ and $A + B = C$.

COROLLARY 6.3. *Let $\bar{C} = \{\bar{c}_1 < \bar{c}_2\}$ and let $0 \in C$. Then C has a 2 component, if and only if, $\bar{C}$ is not one of the following three sets*: {1, 2}; {2, 4}; {3, 5}.

COROLLARY 6.4. *If $\bar{c}_r$ is such that $\bar{c}_r - \bar{c}_1 > \bar{c}_{r-1}$, then C has a 2 component.*

Proof. One can easily verify that $\{0, \bar{c}_r - \bar{c}_1\}$ is a 2 component by Theorem 6.

THEOREM 7. *For a given r and m there exist at most a finite number of sets with r gaps which do not have an $m+1$ component.*

That is to say if $\bar{C} = \{\bar{c}_1 < \bar{c}_2 < \cdots < \bar{c}_r\}$, then there are sets A and B such that $A(\bar{c}_r) = m+1$, $0 \in A$, and $A + B = C$ except for at most a finite number of sets C. One can even impose the additional condition that A be in progression.

Proof. We first prove a lemma.

LEMMA. *If there exists an $a \in C$ such that*

$$(1) \quad xa \neq \bar{c}_i - \bar{c}_j \quad \text{for} \quad 1 \leqq j < i < r \quad \text{and} \quad x = 1, \cdots, m+1 ;$$

and

$$(2) \quad \text{either} \quad \bar{c}_j < a < (m+1)a < \bar{c}_{j+1} \quad \text{for some } j \text{ such that } 1 \leqq j \leqq r-1 \quad \text{or} \quad 0 < a < (m+1)a < \bar{c}_1 ;$$

then $A = \{0, a, 2a, \cdots, ma\}$ is an $m+1$ component of C.

Proof. By Theorem 6 A is a component of C, if and only if, for all $k \notin D$, $k \leqq \bar{c}_r$, we have $A + k \not\subset A + D$. If for some $k \notin D$, $k \leqq \bar{c}_r$ we have $A + k \subset A + D$, then $k = sa + di$ for some s and i such that $0 < s \leqq m$ and $1 \leqq i \leqq r$. Under the assumption that a satisfies (1) and (2), we shall show that $k + (m - s + 1)a \notin A + D$, and hence $A + k \not\subset A + D$ contrary to the assumption that $A + k \subset A + D$. Hence A will be an $m+1$ component of C.

We have $k + (m - s + 1)a = sa + d_i + (m - s + 1)a = (m+1)a + d_i$ for some i. If $k + (m - s + 1)a \in A + D$ then either

$$(3) \quad (m+1)a + d_i = ta + d_j \quad \text{for some} \quad t = 0, \cdots, m \quad \text{and} \quad j = 1, \cdots, r \quad \text{and} \quad j \neq i ;$$

or

$$(4) \quad (m+1)a + d_i > \bar{c}_r > sa + d_i .$$

Now (3) implies $(m + 1 - t)a = \bar{c}_i - \bar{c}_j$ contrary to (1), and (4) implies $(m+1)a > \bar{c}_i > sa \geqq a > 0$ contrary to (2). Hence A is an $m+1$ component of C. This completes the proof of the lemma.

Let $\delta = (\{\bar{c}_i - \bar{c}_j \mid 1 \leqq j < i \leqq r\})$. Then $1 \leqq \delta \leqq (r^2 - r)/2$. If there are at least $(m+1)\delta + 1$ choices for a between $\bar{c}_j + 1$ and $[\bar{c}_{j+1}/(m+1)] - 1$ inclusive or between 1 and $[\bar{c}_1/(m+1)] - 1$ inclusive,

then we can choose an a so that conditions (1) and (2) of the lemma are satisfied. Thus conditions (1) and (2) of the lemma are satisfied if either

$$(5) \qquad \bar{c}_{j+1} \geqq (m+1)(\delta(m+1) + \bar{c}_j + 2) \quad \text{for} \quad 1 \leqq j \leqq r-1$$

or

$$(6) \qquad \bar{c}_1 \geqq (m+1)(\delta(m+1) + 2) .$$

Let $\delta(m+1) + 2 = n$. If (5) and (6) both fail, then we must have $\bar{c} < (m+1)n$

$$\begin{aligned}
&\bar{c}_2 < (m+1)(n + \bar{c}_1) < n((m+1) + (m+1)^2) \\
&\vdots \\
&\bar{c}_i < (m+1)(n + \bar{c}_{i-1}) < n \sum_{q=1}^{i} (m+1)^q \\
&\vdots \\
&\bar{c}_r < (m+1)(n + \bar{c}_{r-1}) < n \sum_{q=1}^{r} (m+1)^q .
\end{aligned}$$

Hence if $c_r \geqq n \sum_{q=1}^{r} (m+1)^q$ then either condition (5) or condition (6) is satisfied and a can be chosen so that conditions (1) and (2) of the lemma are both satisfied.

Thus if $\bar{c}_r \geqq (\delta(m+1) + 2) \sum_{q=1}^{r} (m+1)^q$, then there is an $a \in C$ such that $\{0, a, 2a, \cdots, ma\}$ is an $m+1$ component of C. Since for a fixed r, δ is bounded, it follows that the number of sets C, with r gaps which do not have an $m+1$ component is finite.

In Theorems 8–11, we shall make no restriction on the number of gaps that a set C may have.

DEFINITION. A set C is said to be strictly decomposable if there are sets, A and B, such that $\operatorname{Min}(A), (B) \geqq 2$ and $A + B = C$.

DEFINITION. A set C is said to be asymptotically decomposable if there are sets, A and B, such that $\operatorname{Min}(A), (B) \geqq 2$ and $A + B = C^*$ where $(C^* \cap \bar{C}) < \infty$ and $(C \cap \bar{C}^*) < \infty$. We write $A + B \sim C$.

THEOREM 8. *Let C be given. Let $\{n_i\}$ be a monotonically increasing sequence of nonnegative integers. Let $C_k = C \cap [0, k]$. Then a necessary and sufficient condition that C be strictly decomposable is that for each n_i in the sequence there exist a pair of sets, A_{n_i} and B_{n_i}, such that $\{A_{n_i} + B_{n_i}\} \cap [0, n_i] = C_{n_i}$; and there exists a positive integer N such that whenever $n_i \geqq N$ we have $\operatorname{Min} A_{n_i}(N), B_{n_i}(N) \geqq 2$.*

Proof. If C is strictly decomposable, then we have a pair of sets,

A and B, such that Min $(A), (B) \geqq 2$ and $A + B = C$. Put $A_{n_i} = A \cap [0, n_i]$ and $B_{n_i} = B \cap [0, n_i]$. If for some n_i we have $\{A_{n_i} + B_{n_i}\} \cap [0, n_i] \neq C \cap [0, n_i]$, then $\{A + B\} \cap [0, n_i] \neq C \cap [0, n_i]$ which is a contradiction. Since Min $(A), (B) \geqq 2$ we must have a positive integer N such that Min $A(N), B(N) \geqq 2$. This clearly implies that for $n_i \geqq N$ we have Min $A_{n_i}(N), B_{n_i}(N) \geqq 2$. Hence our condition is necessary.

Now let $\{m_j\}_{j=0}^{\infty}$ be any monotonically increasing sequence of non-negative integers. Put $A_{m_0}, i = A_{n_i} \cap [0, m_0]$ and $B_{m_0}, i = B_{n_i} \cap [0, m_0]$. Since there are only a finite number, 2^{2m_0+2}, of choices for each pair of sets, A_{m_0}, i and B_{m_0}, i, there must be at least one pair, A_{m_0} and B_{m_0}, which is repeated for an infinite number of indices i.

Let $\{n_i^{(1)}\}$ be the subsequence of $\{n_i\}$ for which $A_{m_0} = A_{n_i}(1) \cap [0, m_0]$ and $B_{m_0} = B_{n_i}(1) \cap [0, m_0]$. Now $A_{m_0} + B_{m_0} \subset C$, since in the original construction of A_{m_0} and B_{m_0} the n_i may be chosen arbitrarily large. Also we have $\{A_{m_0} + B_{m_0}\} \cap [0, m_0] = C_{m_0}$.

We repeat this process using m_1 and the sequence $\{n_i^{(1)}\}$. Put $A_{m_1}, i = A_{n_i}(1) \cap [0, m_1]$ and $B_{m_1}, i = B_{n_i}(1) \cap [0, m_1]$. Again we must have at least one pair of sets, A_{m_1} and B_{m_1}, that repeats an infinite number of times. This pair, A_{m_1} and B_{m_1}, determines a subsequence $\{n_i^{(2)}\} \subset \{n_i^{(1)}\}$. We must have $A_{m_1} + B_{m_1} \subset C$ and $\{A_{m_1} + B_{m_1}\} \cap [0, m_1] = C_{m_1}$.

Continuing in this way, we have for each m_j a pair of sets, A_{m_j} and B_{m_j}, and a subsequence $\{n_i^{(j+1)}\} \subset \{n_i^{(j)}\}$ such that $A_{m_j} = A_{n_i}(j + 1) \cap [0, m_j]$ and $B_{m_j} = B_{n_i}(j + 1) \cap [0, m_j]$. For each m_j we also have $A_{m_j} + B_{m_j} \subset C$ and $\{A_{m_j} + B_{m_j}\} \cap [0, m_j] = C_{m_j}$.

Put $A = \bigcup_{j=0}^{\infty} A_{m_j}$ and $B = \bigcup_{j=0}^{\infty} B_{m_j}$. Since in each subsequence, $\{n_i^{(j)}\}$, there exists an $n_i^{(j)}$ such that $n_i^{(j)} \geqq N$, we have that Min $A_{m_j}(N)$, $B_{m_j}(N) \geqq 2$, and hence Min $(A), (B) \geqq 2$. If $A + B \neq C$, then there is a section of C, say C_k, for which the decomposition fails. Let $m_j > k$. Then for the subsequence, $\{n_i^{(j+1)}\}$, we have

$$\{A_{n_i}(j + 1) + B_{n_i}(j + 1)\} \cap C_{m_j} \neq C_{m_j} = C_{n_i}(j + 1) \cap [0, m_j] .$$

This contradicts the original hypothesis. Hence $A + B = C$ is a strict decomposition of C, and our condition is sufficient. This completes the proof of Theorem 8.

If C has a finite number of gaps, C is a section. If C has infinitely many gaps then Theorem 8 shows that the problem of strict decomposability reduces to the problem of decomposability of sections because we can choose for $\{n_i\}$ a sequence of gaps of C.

COROLLARY 8.1. *Let $\{n_i\}$ be an infinite sequence of elements of $\bar{C}$. Then C is strictly decomposable, if and only if, every section $\{C \cap [0, n_i)\} \cup [n_i + 1, \infty)$ is decomposable.*

THEOREM 9. *Let C be given. Let A be such that $\bar{A} \supsetneq \bar{C}$ and $(A) \geqq 2$. Let $f(\bar{a})$ be the number of representations of $\bar{a}$ in the form $a_i + \bar{c}_j - a_m$. If for every $\bar{a} \in \bar{A}$, such that $\bar{a} \geqq 0$, and such that $\bar{a} \in A + \bar{C} - A$ we have $f(\bar{a}) < A(\bar{a})$, then there exists a set B such that $A + B = C$ is a strict decomposition of* C.

Proof. Put $B = \bigcap_{i=1}^{\infty} \{\bar{c}_i - \bar{A}\}$. Now $B \neq \phi$ since $0 \in B$ and clearly $A + B \subset C$.

Let $\bar{a} \in \bar{A}$ such that $\bar{a} \in C$. If $\bar{a} \notin A + B$, then it must be true that for every $a \in A$ such that $a < \bar{a}$, we must have $\bar{a} - a \in \bar{B} = \bigcup_{i=1}^{\infty} \{\bar{c}_i - A\}$. Hence for every $a \in A$ such that $a < \bar{a}$ we must have that there exists a $\bar{c}_k \in \bar{C}$ and an $a' \in A$ such that $\bar{a} = a + \bar{c}_k - a' \in A + \bar{C} - A$. There exist at least $A(\bar{a})$ such representations of $\bar{a}$, since there are $A(\bar{a})a$'s in A such that $a < \bar{a}$. Hence $f(\bar{a}) \geqq A(\bar{a})$ contrary to hypothesis. Hence there is an $a \in A$ such that $\bar{a} - a \in B$. Hence $A + B = C$. Since $A \neq C$, $A \subset C$, we must have $(B) \geqq 2$, and thus this decomposition of C is strict.

THEOREM 10. *Let C be an infinite set. If C is asymptotically decomposable, then there is an integer k such that for all positive integers m there are infinitely many pairs of elements $c_1, c_2 \in C$ such that $m < c_1 < c_2 < c_1 + k$.*

Proof. Since C is asymptotically decomposable, there is a C^* such that $C^* \sim C$ and C^* is strictly decomposable. And if C^* satisfies the conclusions of Theorem 10, then so does C. Hence without loss of generality we may assume that C is strictly decomposable.

Since C is an infinite set, and since C is strictly decomposable, at least one of the two components is infinite. Suppose without loss of generality that $(B) = \infty$. Let $a_1, a_2 \in A$ where $0 \leqq a_1 < a_2 < k$. Let m be any positive integer. Then there are an infinite number of elements $b \in B$ such that $a_1 + b = c_1 > m$ and $a_2 + b = c_2$. Now $c_2 - c_1 = a_2 - a_1 < k$, and we have $m < c_1 < c_2 < c_1 + k$.

COROLLARY 10.1. *Let C be an infinite set. Let $f(n) = c_n - c_{n-1}$ for $n \geqq 2$ where c_{n-1} and c_n are consecutive elements of C. If there exists an integer m such that for $n \geqq m$, $f(n)$ is increasing, then C is asymptotically decomposable if and only if $f(n)$ is bounded.*

THEOREM 11. *Let $g(y) = \overline{\lim}_{x \to \infty} [C(x + y) - C(x)]$. If $g(y)$ is bounded for all y, then C is not asymptotically decomposable as the sum of two infinite sets.*

Proof. Suppose $C \sim A + B = C^*$ where $(A) = (B) = \infty$. Clearly

$\overline{\lim}_{x\to\infty}[C^*(x+y)-C^*(x)] = \overline{\lim}_{x\to\infty}[C(x+y)-C(x)] = g(y)$. Let $B = \{b_0 < b_1 < b_2 < \cdots\}$. Then $g(y) \geqq \overline{\lim}_{j\to\infty}[C^*(b_j+y)-C^*(b_j)] \geqq A(y)$. Since for all $a \leqq y$ and $a \in A$ we must have $b_j \leqq b_j + a \leqq b_j + y$. Hence for all $b_j \in B$ and y we must have $C^*(b_j+y)-C^*(b_j) \geqq A(y)$. But if $g(y)$ is bounded, then $A(y)$ is bounded and A is not an infinite set.

Let P be the set of all primes. It is easy to show that P is not strictly decomposable.

THEOREM 12. *If $A + B \sim P$, the set of all primes, then $(A) = (B) = \infty$.*

Proof. Suppose $A = \{a_1 < a_2 < \cdots < a_n\}$ and $A + B \sim P$. Then $A - a_1 + B + a_1 \sim P$. Thus we may without loss of generality assume $a_1 = 0$. Let $N = \max\{\overline{p} \in A + B, p \notin A + B\}$. Then whenever $b \in B$ and $b > N$, we must have $a_i + b \in P$ for $i = 1, \cdots, n$, and in particular $b \in P$.

Choose n primes $p_1, \cdots, p_n$ such that $(a_i, p_i) = 1 = (p_i, p_j)$ for $i \neq j$ and $i = 2, \cdots, n$ and $(p_1, a_i) = 1 = (p_1, p_i)$ for $i = 2, \cdots, n$. Consider the solutions to the simultaneous congruences. $x \equiv a_i(p_i)$ for $i = 2, \cdots, n$ and $x \equiv -a_2(p_1)$. The set of solutions forms an arithemetic progression $\{x + k\prod_{i=1}^{n} p_i\}_{k=0}^{\infty}$ with $(x, \prod_{i=1}^{n} p_i) = 1$. By the Dirichelet theorem there exist an infinite number of primes of the form $x + k\prod_{i=1}^{n} p_i$. Let q be such a prime, and let $q > N + a_n$. Then $q \in A + B$.

If $q = a_i + b$ for some $i = 2, \cdots, n$ and $b \in B$, then $b > N$ and $b \in P$. But $q = a_i + b$ implies that $b \equiv o(p_i)$ which is impossible for sufficiently large q. If $q = b \in B$, then $q + a_2 \in P$. But $q + a_2 \equiv 0(p_1)$ which is also impossible for sufficiently large q.

Hence $(A) = (B) = \infty$.

BIBLIOGRAPHY

1. F. J. Dyson, *A theorem on the densities of sets of integers*, J. London Math. Soc. Vol. XX, **77** (1945), 8-14.

2. T. A. Evans and H. B. Mann, *On simple difference Sets*, Sankhya: *The Indian Journal of Statistics*, Vol. 11, parts 3 and 4, (1951), 357-364.

3. Marshall, Jr. Hall, *A survey of difference sets*, Proc. Amer. Math. Soc., **7** (1956), 975-986.

4. Martin Kneser, *Abschaetzung der asymptotischen Dichte von Summen mengen*, Math. Zeitschrift Bd. **58** (1953), 459-484.

5. H. B. Mann, *A proof of the fundamental theorem on the density of sums of sets of positive integers*, Ann. of Math., **43**, No. 3, July, (1942), 523-527.

6. ———, *On products of sets of group elements*, Canadian J. Math., **4** (1952), 64-66.

7. ———, *A refinement of the fundamental theorem on the density of the sum of two sets of integers*, Pacific J. Math., **10** (1960), 909-915.

WESTERN WASHINGTON STATE COLLEGE
THE OHIO STATE UNIVERSITY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should by typewritten (double spaced), and on submission, must be accompanied by a separate author's résumé. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is $18.00; single issues, $5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $8.00 per volume; single issues $2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 14, No. 2 June, 1964