MINIMAL COMPLEMENTARY SETS

BY

GERALD WEINSTEIN

ABSTRACT. Let $G$ be a group on which a measure $m$ is defined. If $A, B \subset G$ we define $A \oplus B = C = \{c \mid c = a + b, a \in A, b \in B\}$. By $A_k \subset G$ we denote a subset of $G$ consisting of $k$ elements. Given $A_k$ we define $s(A_k) = \inf m \{B \subset G, A_k \oplus B = G\}$ and $c_k = \sup_{A_k \subset G} s(A_k)$. Theorems 1, 2, and 3 deal with the problem of determining $c_k$.

In the dual problem we are given $B$, $m(B) > 0$, and required to find minimal $A$ such that $A \oplus B = G$ or, sometimes, $m(A \oplus B) = m(G)$. Theorems 5 and 6 deal with this problem.

Let $A$ and $B$ be sets of nonnegative integers, with $0 \in A$. The set $B$ is called a complement of $A$ if each nonnegative integer is expressible in the form $a + b$ $(a \in A, b \in B)$. One of the basic problems in additive number theory is the determination, for a prescribed $A$, of a complement $B$ that is in some sense minimal. Erdös [1] and Lorentz [2] have discussed some problems and concepts for the case where $A$ is an infinite set; D. J. Newman [3] has dealt with finite sets $A$. We have also obtained some results for the case where $A$ is finite, and they will appear elsewhere [5]. Here we generalize this concept in several respects.

Let $G$ be a group on which a measure $m$ is defined. If $A, B \subset G$ we define $A \oplus B = \{c \mid c = a + b, a \in A, b \in B\}$. By $A_k \subset G$ we denote a subset of $G$ consisting of $k$ elements. Given nonempty $A$ we can find $B$ such that $A \oplus B = G$. We then say that $A$ and $B$ are complementary and render the situation asymmetrical by thinking of $A$ as a set of translates and $B$ as a set which is to be translated so that the union of its translates covers $G$.

Given $A_k$ one may ask for the set $B$ such that $A_k \oplus B = G$ and $m(B)$ is a minimum. More precisely, we define $s(A_k) = \inf m \{B \subset G, A_k \oplus B = G\}$. It is then natural to seek $s(A_k)$ for the "worst" $A_k$, i.e. $s(A_k)$ corresponding to the set of shifts which necessitates the "biggest" complementary set. We so define $c_k = \sup_{A_k \subset G} s(A_k)$. Theorems 1, 2, and 3 deal with the problem of determining $c_k$.

In the dual problem we are given $B$, $m(B) > 0$, and asked to find minimal $A$ such that $A \oplus B = G$ or, sometimes, $m(A \oplus B) = m(G)$. As before, we seek

Received by the editors May 23, 1974.

the "worst" $B$, i.e., the $B$ of given measure which necessitates the "largest" $A$.

The results obtained in connection with this problem are somewhat surprising.

If the question asked by Erdös could be answered in the affirmative they would be even more surprising. Theorems 5 and 6 deal with the dual problem.

**Definition.** $C_k = \sup_G \max_{A_k} \min_B d(B)$, where $G$ is a finite group containing at least $k$ elements, $A_k$ is a $k$ element subset of $G$, and $B$ is a complement of $A_k$ in $G$, i.e., $A_k \oplus B = G$.

**Theorem 1.** $C_k < (\log k + 2)/k$.

**Proof.** The proof that D. J. Newman [3] gives to show $c_k \leq (1 + \log k)/k$ is applicable here with slight change.

Let $G$ be a group of $N$ elements, $N > k$, and $A_k \subset G$, where $A_k = \{0 = a_1, \ldots, a_k\}$. For each element $a_n \in G$ we denote by $U_n$ the set of elements $-a_1 + a_n, -a_2 + a_n, \ldots, -a_k + a_n$. $U$ represents an unspecified class $U_n$ and $T$ denotes an unspecified set of $k$ elements. Clearly, there are $\binom{N}{k}$ sets $T$, and for each $n$, exactly $\binom{N-k}{k}$ of these sets do not meet the set $U_n$. Since there are at most $N$ different sets $U_n$, it follows that there are at most $N\binom{N-k}{k}$ disjoint pairs $T, U$. Consequently, at least one of the sets $T$ misses at most

\[
N \binom{N-k}{k} / \binom{N}{k}
\]

of the sets $U_n$. Let $S$ consist of such a set $T$, together with all elements $a_n$ for which $T \cap U_n = \emptyset$.

To see that $S$ is a complement of $A$, let $a_m \in G$. If $T \cap U_m = \emptyset$, we have the representation $a_m = 0 + a_m (0 \in A, a_m \in S)$.

If $T \cap U_m$ contains some element $-a_i + a_m$, we have the representation $a_m = a_i + (-a_i + a_m), (a_i \in A, -a_i + a_m \in S)$.

We now choose $K$ such that $N(\log k/k) < K < N(\log k/k) + 1$ and proceed to obtain an upper bound for the density of $S$:

\[
d(S) \leq d(T) + N \binom{N-k}{k} / \binom{N}{k} \cdot \frac{1}{N} = K \frac{1}{N} + \binom{N-k}{k} / \binom{N}{k}
\]

\[
\leq \frac{K}{N} + \left(1 - \frac{k}{N}\right)^K \leq \frac{K}{N} + e^{-kK/N}
\]

\[
\leq \frac{N(\log k/k) + 1}{N} + e^{-(k/N)(N\log k/k)} = \frac{\log k}{k} + \frac{1}{N} + \frac{1}{k}
\]

\[
\leq \frac{\log k + 2}{k}.
\]
This proves the assertion.

**Theorem 2.** Let $T^2$ be the 2-dimensional torus whose points are 2-tuples $(x_1, x_2)$ and where addition of points is modulo 1. Let $A_k = \{a_1, a_2, \ldots, a_k\}$ be an arbitrary set of $k$ distinct points in $T^2$. Then we can find a set $B \subset T^2$ such that $A_k \oplus B = T^2$ and $m(B) \leq K_2((\log k + 2)/k)$, where $K_2$ is a constant.

**Proof.** Let $L_n$ consist of all points $r_i = (p_i/n, q_i/n)$, where $p_1, q_i$ are integers, $0 \leq p_i < n$, $0 \leq q_i < n$. Clearly $L_n$ is a finite subgroup of $T^2$. Moreover, we may think of $L_n$ as partitioning $T^2$ into little squares, $S_i$, $i = 1, \ldots, n^2$, of side $1/n$. We assign to each square the index $i$ assumed by the point of its lower left-hand corner $r_i$.

Now for each point $a_j \in A_k$ there is at least one closest point in $L_n$. Let $r_i$ be such a point. This process must result in the assignment of $k$ different points of $L_n$ if $n$ is sufficiently large. If we define $A'_k = \{r_i, r_2, \ldots, r_k\}$, the set of grid points closest to $A_k$, then by Theorem 1 we can find $B'$, another subset of $L_n$, where $A'_k \oplus B' = L_n$ and $|B'| \leq ((\log k + 2)/k)n^2$. If we now define $B$ as the set of squares whose lower left-hand points are the elements of $B'$, then clearly $A'_k \oplus B = T^2$ and $m(B) \leq (\log k + 2)/k$.

If $a_j \in A_k$, $r_i$ is its closest point in $L_n$, and $S_m$ is an arbitrary square in $B$, then $r_i \oplus S_m$ exactly covers some other square $S_{m'}$, but $a_j \oplus S_{m'}$, while intersecting $S_{m'}$, will not completely cover it. Hence, $S_{m'}$ must be enlarged if we wish $S_{m'} \subset a_j \oplus S_{m}$, and it is certainly sufficient to double the length of each side of $S_{m'}$ while preserving its center. If we perform this operation for every square in $B$ and call the set of enlarged squares $B$, then $A_k \oplus B = T^2$ and $m(B) \leq 4((\log k + 2)/k)$. This proves the assertion.

**Corollary.** If $T^n$ is the $n$-dimensional torus and $A_k$ is an arbitrary set of $k$ points in $T^n$, then we can find a set $B \subset T^n$ such that $A_k \oplus B = T^n$ and $m(B) \leq K_n((\log k)/k)$, where $K_n \leq 2^n$.

**Proof.** Essentially the same as above.

**Note.** If the points in $A_k$ are all rational then they are all elements of $L_n$ for some $n$. Hence, no enlargement is necessary and we may take $K_n = 1$.

**Theorem 3.** Let $G$ be a compact, completely separable topological group and $\varepsilon > 0$. Then there exists $B \subset G$ with $m(B) < \varepsilon$ such that for all $A \subset G$ with $(\overline{A})^0 \neq \emptyset$ we have $A \cdot B = B \cdot A = G$.

**Proof.** Let $Z = \{z_1, z_2, \ldots\}$ be a dense denumerable subset of $G$ and $Z^{-1} = \{z_1^{-1}, z_2^{-1}, \ldots\}$ the set of its inverses. Let $T_i$ be an open set such that $z_{i}^{-1} \in T_i$ and $m(T_i) < \varepsilon/2^{i+1}$ and let $S_i$ be an open set such that $z_i \in S_i$, $S_i^{-1} \subset T_i$, and $m(S_i) < \varepsilon/2^{i+1}$, for $i = 1, 2, \ldots$. Define
Clearly \( m(S) < e/2, m(T) < e/2, \) and \( S^{-1} \subset T. \)

We first show \( xA \cap S \neq \emptyset \) for all \( x \in G. \) Clearly \( x(A)^0 \cap Z \neq \emptyset. \) So, for some \( i, z_i \in x(A)^0 \cap Z. \) Since \( z_i \) is a limit point of \( xA, \) \( S_i \) must contain a point of \( xA; \) hence \( xA \cap S \neq \emptyset. \) The same argument shows that \( Ax \cap S \neq \emptyset \) for all \( x \in G. \)

Now let \( B = S \cup T. \) We have \( xA \cap S \neq \emptyset, \) \( x \in G \Rightarrow A \cap xS \neq \emptyset, \) \( x \in G, \Rightarrow xS = a \Rightarrow x = s^{-1}a \) has a solution for every \( x, \) with \( a \in A, s^{-1} \in T \subset B. \) Hence \( A \cdot B = G. \)

Similarly, \( Ax \cap S \neq \emptyset, \) \( x \in G \Rightarrow A \cap Sx \neq \emptyset, \) \( x \in G, \Rightarrow sx = a \Rightarrow x = s^{-1}a \) has a solution for every \( x, \) with \( s^{-1} \in T \subset B, \) \( a \in A. \) Hence \( B \cdot A = G. \)

Since \( m(B) < e \) this proves the theorem.

**Definition.** \( \Delta^B_x = B \cup B_x - B \cap B_x \) where \( B_x = x \oplus B \) (mod 1).

**Theorem 4.** Let \( B \subset [0, 1) \) and \( m(B) = e > 0. \) Then, if \( m(\Delta^B_x) = 0 \) for all \( x \in [0, 1), e = 1. \)

**Proof.** We first note that \( m(B \cup B_x) \geq e \) and \( m(B \cap B_x) \leq e \) so that \( m(\Delta^B_x) = 0 \) implies \( m(B \cup B_x) = e. \)

Suppose there exists an interval \( (\alpha, \beta) \) such that \( m(B \cap (\alpha, \beta)) = 0. \) Then we can find \( x \) such that \( m(B_x \cap (\alpha, \beta)) > 0. \) This implies \( m(B \cup B_x) > e \) which implies \( m(\Delta^B_x) > 0. \) The contradiction shows that for every interval \( (\alpha, \beta) \) we have \( m(B \cap (\alpha, \beta)) > 0. \)

Suppose \( E \subset [0, 1) \) is such that \( m(B \cap E) = \delta. \) If there exists \( x \) such that \( m(B_x \cap E) \neq \delta \) then again this implies \( m(B \cup B_x) > e. \) Hence if \( m(B \cap E) = \delta \) then \( m(B_x \cap E) = \delta \) for all \( x \in [0, 1). \)

So if \( \beta - \alpha = 1/n, m(B \cap (\alpha, \beta)) = e \cdot 1/n \) because we can partition \( [0, 1) \) into \( n \) nonoverlapping intervals of length \( 1/n. \) Similarly, if \( \beta - \alpha = 1/(n + \theta), 0 \leq \theta < 1, \) then \( m(B \cap (\alpha, \beta)) > 1/n + \theta. \) Hence, by a result of Titchmarsh \( m(B) = 1. \)

**Note.** In all that follows addition is mod 1.

**Theorem 5(A).** For every \( e > 0 \) there exists \( B \subset [0, 1) \) such that \( m(B) \geq 1 - e \) and \( m(A \oplus B) = 1 \) implies \( A \) is infinite.

**Theorem 5(B).** For every \( B \subset [0, 1) \) and \( m(B) > 0, \) we can find \( A \) such that \( m(A \oplus B) = 1 \) and \( A \) is denumerable.

**Proof of (A).** Suppose \( B \subset [0, 1) \) is nowhere dense and \( m(B) = 1. \) Then \( m(B) = 1 \) implies \( (B)' \) is open and \( m(B)' = 0. \) Only \( \emptyset \) is open and has measure zero so \( B = [0, 1) \) and the contradiction shows there does not exist a nowhere dense set, in \( [0, 1), \) of measure 1.
It is well known that the class of all nowhere dense subsets of a metric space is a finitely additive class.

By changing the lengths of the extracted intervals in the construction of the Cantor ternary set, we can construct a perfect nowhere dense set $B$ in $[0, 1)$, which has measure greater than $1 - \epsilon$ for any $\epsilon > 0$.

Hence, if $A$ is any finite point set in $[0, 1)$ then $C = A \oplus B$ is nowhere dense and therefore $m(C) < 1$.

**Proof of (B).** Denote by $\bigcup B_{x_i}$ the set $\bigcup_{i=1}^{\infty} x_i + B$, where $\{x_i\}$ is an infinite sequence in $[0, 1)$.

Let $\alpha = \sup m(\bigcup B_{x_i})$ where the sup is over all such sequences. Then, for every $n$ we can find a sequence $\{x_i^{(n)}\}$ such that $m(\bigcup B_{x_i^{(n)}}) \geq \alpha - 1/n$. Clearly, $m(\bigcup_{i} B_{x_i^{(n)}}) = \alpha$ so that the sup is actually attained for some denumerable sequence $\{x_i^{(0)}\}$. Now we write $\beta = \bigcup B_{x_i^{(0)}}$ and note that we have just proved $m(\Delta^0_x) = 0$ for all $x \in [0, 1)$ and so, by Theorem 4, we have $\alpha = m(\beta) = 1$. If we let $A = \bigcup x_i^{(0)}$ then $m(A \oplus B) = 1$ and $A$ is denumerable.

**Note.** All sets are subsets of $I = [0, 1)$.

**Theorem 6.** (A) There exists $B \in \text{Cat. II}, m(B) = 1$ such that $A \oplus B = I$ implies $A$ is infinite.

(B) On the other hand, for every $B$, $m(B) > 0$, we can find $A$ such that $A \oplus B = I$ and $m(A) = 0$.

**Proof of (A).** Every $x \in [0, 1)$ can be written $x = \sum_{k=1}^{\infty} a_k/n^k$, $0 \leq a_k < n$, $n \geq 2$. Let $X_n$ be the class of numbers $x = \sum_{k=1}^{\infty} a_k/n^k$, $0 \leq a_k < n - 1$, $n \geq 2$. Clearly $m(X_n) = 0$. Define $B' = \bigcup_{n=2}^{\infty} X_n$. From this it follows that $m(B) = 1$. Since $X_n$ is perfect and nowhere dense, $B' \in \text{Cat. I}$ and hence $B$ is a residual set.

Suppose $B$ and any 2 shifts of $B$ fail to cover $I$. Then for any pair $x_1, x_2 \in I$ we can find $d_1, d_2, d_3 \in B'$ such that

$$x_1 + d_1 = d_3, \quad x_2 + d_2 = d_3.$$

It is also clear that this condition is sufficient to guarantee that $B$ and any 2 shifts of $B$ fail to cover $I$.

We can generalize this by stating the following: a necessary and sufficient condition that $B$ and any $m$ shifts of $B$ fail to cover $I$ is that for any $m$ elements of $I$: $x_1, \ldots, x_m$, there exist $m + 1$ elements in $B'$: $d_1, \ldots, d_{m+1}$, such that

$$x_1 + d_1 = d_{m+1}, \quad x_2 + d_2 = d_{m+1}, \ldots, \quad x_m + d_m = d_{m+1}.$$

In fact we can already find these $m + 1$ elements: $d_1, \ldots, d_{m+1}$, in $X_n$ if only $n > m + 1$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
If we denote by \( x_{j,1} x_{j,2} \cdots x_{j,k} \cdots \) the number
\[
x_j = \sum_{q=1}^{\infty} x_{j,q}/n^q,
\]
and denote by \( d_{k,1} d_{k,2} \cdots d_{k,r} \cdots \) the number
\[
d_k = \sum_{q=1}^{\infty} d_{k,q}/n^q,
\]
then the above claim is equivalent to stating that the congruences:
\[
\begin{align*}
  x_{1,i} + d_{1,i} + p_{1,i} & \equiv d_{m+1,i} \pmod{n} \\
  x_{2,i} + d_{2,i} + p_{2,i} & \equiv d_{m+1,i} \pmod{n} \\
  & \vdots \\
  x_{m,i} + d_{m,i} + p_{m,i} & \equiv d_{m+1,i} \pmod{n}
\end{align*}
\]
are solvable subject to the constraints \( 0 < d_{k,i} < n - 1, 1 \leq k \leq m + 1, i = 1, 2, \cdots \).

Recall that \( 0 < x_{k,i} < n \). Now \( p_{j,i} = 1 \) if \( x_{j,i+1} + d_{j,i+1} + p_{j,i+1} \geq n \); \( p_{j,i} = 0 \) otherwise.

Assume that \( p_{j,i}, j = 1, \ldots, m, \) have been determined. Then for \( x_{1,i} \) there are at least \( n - 2 \) possible values for \( d_{m+1,i} \). Only the values of \( d_{m+1,i} \) such that \( x_{1,i} + (n - 1) + p_{1,i} \equiv d_{m+1,i} \pmod{n} \) and \( d_{m+1,i} = (n - 1) \) are inadmissible. Of these \( n - 2 \) possible values exactly \( n - 3 \) are still possible solutions for \( x_{2,i} \) and so, by the time we reach \( x_{m,i} \) there are still \( n - m - 1 \) possible values for \( d_{m+1,i} \). Since we assumed \( n > m + 1 \) the assertion is proved.

We have shown that no finite set of shifts of \( B \) covers \( I \). Since \( B \) is a residual set, and therefore of Cat. II, the theorem is proved.

**Proof of (B).** By Theorem 5(B) we can find \( F \) such that \( m(F \oplus B) = 1 \) and \( F \) is denumerable. We can also add one element to \( F \), if necessary, so that \( 0 \in C = F \oplus B \). Then \( m(C') = 0 \) and we define \( \overline{C} = C' \cup \{0\} \). Then \( I = \overline{C} \oplus C = \overline{C} \oplus F \oplus B = A \oplus B \) if we define \( A = \overline{C} \oplus F \). Since \( F \) is denumerable and \( m(A) = 0 \) we have \( m(A) = 0 \).

**Note.** P. Erdös asks [4] whether, in Theorem 6(A), infinite can be changed to nondenumerable.

**Acknowledgment.** This paper is part of the author's doctoral dissertation, completed at Yeshiva University under the direction of Professor D. J. Newman. The author expresses his appreciation to Professor Newman for his advice and encouragement during the preparation of this paper.
REFERENCES

4. P. Erdős, Private communication.

DEPARTMENT OF MATHEMATICS, CITY COLLEGE (CUNY), NEW YORK, NEW YORK 10031