

Small-sum pairs in abelian groups

Reza Akhtar

Dept. of Mathematics

Miami University, Oxford, OH 45056, USA

reza@calico.mth.muohio.edu

Paul Larson

Dept. of Mathematics

Miami University, Oxford, OH 45056, USA

larsonpb@muohio.edu

December 15, 2009

Abstract

Let G be an abelian group and A, B two subsets of equal size k such that $A + B$ and $A + A$ both have size $2k - 1$. Answering a question of Bihani and Jin, we prove that if $A + B$ is aperiodic or if there exist elements $a \in A$ and $b \in B$ such that $a + b$ has a unique expression as an element of $A + B$ and $a + a$ has a unique expression as an element of $A + A$, then A is a translate of B . We also give an explicit description of the various counterexamples which arise when neither condition holds.

1 Introduction

Let G be an abelian group, written additively. If A and B are subsets of G , we write $A + B$ to mean $\{a + b : a \in A, b \in B\}$, and similarly for $A - B$. We use $A \setminus B$ to denote set difference. In their study [1] of sets of natural numbers with small upper Banach density, Bihani and Jin asked the following in the context of cyclic groups:

Question 1. Let G be an abelian group. Given a pair (A, B) of subsets of G such that $|A| = |B| = k$ and $|A + A| = |A + B| = 2k - 1$, are A and B always translates of each other; that is, does there exist $h \in G$ such that $B = A + h$?

It is easily seen that this question cannot always be answered in the affirmative. To see this, let G be any abelian group of odd order $2k - 1 \geq 5$ and A, B any two subsets of G of order k . Since $|A| + |B| > |G|$, a rudimentary combinatorial result (cf. [7, Lemma 2.1] or Lemma 2.6 below) implies that $A + B = G$, regardless of whether or not A and B are translates of each other. It is far less obvious that all counterexamples are, in a suitable sense, based on this example.

The goal of this paper is to answer Question 1 in the affirmative under appropriate hypotheses and to provide explicit descriptions of counterexamples. We note that all our work is valid for arbitrary abelian groups G .

The key tool we use is the theory of *critical pairs*. A critical pair in an abelian group H is a pair (A, B) of subsets such that $|A + B| = |A| + |B| - 1$; an essentially complete description of all such pairs was given by Vosper [6] for groups of prime order and by Kemperman [5] (see also [2], [3], [4]) for general abelian groups. We show how to use Kemperman's results and Kneser's Theorem to give an essentially complete answer to Question 1. We will refer to the exposition of Kemperman's work in the paper of Grynkiewicz [2], as the definitions used there suit our purposes better than that of the original work [5]. For a detailed discussion of Kneser's Theorem, we refer the reader to Chapter 4 of [7].

2 Preliminaries

Let H be an abelian group. A *small-sum pair*, or *SS-pair* for short, is a pair (X, Y) of subsets of H such that $|X| = |Y| = k$ and $|X + X| = |X + Y| = 2k - 1$ for some k .

Given an abelian group H , subsets $A, B \subseteq H$, and $c \in H$, we define

$$\nu_c(A, B) = |\{(a, b) : a \in A, b \in B : a + b = c\}|.$$

We say that the pair (A, B) has the *unique expression property* (UEP) if there exist $a \in A$ and $b \in B$ such that $\nu_{a+b}(A, B) = 1$ and that (A, B) has the *strong unique expression property* (SUEP) if there exist $a \in A$ and $b \in B$ such that $\nu_{a+b}(A, B) = \nu_{a+a}(A, A) = 1$.

If $P \subseteq H$ is a subgroup, we denote by $\phi_P : H \rightarrow H/P$ the canonical quotient map.

The *stabilizer* of a subset $A \subseteq H$ is the subgroup of H defined by:

$$\text{Stab}(A) = \{h \in H : h + A = A\}$$

A subset $A \subseteq H$ is called *periodic* if $\text{Stab}(A) \neq 0$. For a nontrivial subgroup P , we say that A is *P -periodic* if A is a union of P -cosets; this is equivalent to the condition $P \subseteq \text{Stab}(A)$. We say that $A \subseteq H$ is *P -subperiodic* if there exists $h \in H - A$ such that $A \cup \{h\}$ is P -periodic.

Definition 2.1. *Let H be an abelian group and $P \subseteq H$ a nontrivial subgroup. A subset $A \subseteq H$ is said to have a quasi-periodic decomposition with respect to the quasi-period P if there exists a partition of A into two disjoint subsets $A_1 \cup A_0$ such that A_1 is either empty or P -periodic and A_0 is a subset of a P -coset.*

We refer to A_1 as the periodic part of A and to A_0 as the aperiodic part of A . We also say that A is quasi-periodic if A_1 is nonempty. This notation (with the above meaning) will be used for quasi-periodic decompositions for the remainder of this article.

Lemma 2.2. *Suppose H is finite, P is a subgroup of H and $A \subseteq H$ is any nonempty subset. If $A = A_1 \cup A_0$ is a quasi-periodic decomposition with respect to P and $|A_0| < |P|$, such a decomposition is unique.*

Proof.

With notation as above, suppose A has quasi-periodic decompositions $A = A_1 \cup A_0$ and $A = A'_1 \cup A'_0$ with respect to a common quasi-period P . Then A_1, A'_1 are unions of P -cosets, and each of A_0, A'_0 is a proper subset of a single P -coset. It follows that $A_0 = A'_0$ and hence $A_1 = A'_1$. \square

Lemma 2.3. *Suppose H is finite and A, B are subsets of H , and $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ are quasi-periodic decompositions with respect to a common quasi-period P . Suppose further that neither A nor B is P -periodic. If $A = h + B$, then $A_0 = h + B_0$ and $A_1 = h + B_1$.*

Proof.

If $A = h + B$, then $(h + B_1) \cup (h + B_0)$ is also a quasi-periodic decomposition for A . By Lemma 2.2, it follows that $A_1 = h + B_1$ and $A_0 = h + B_0$. \square

The following results are elementary:

Lemma 2.4. *Suppose H is an abelian group and $A \subseteq H$ is a nonempty subset such that $|A + A| = 2|A| - 1$. Then A is not periodic.*

Proof.

Let $k = |A|$. If A is periodic, then there is a nontrivial subgroup $P \subseteq H$ such that A is a disjoint union of P -cosets; in particular, $|P|$ divides k . However, $A + A$ is

also a union of P -cosets, so $|P|$ must divide $2k - 1$, which forces P to be the trivial subgroup. \square

Lemma 2.5. *Let H be an abelian group. If $A \subseteq H$ is P -periodic, then so is $A + B$ for any $B \subseteq H$.*

Finally, we mention a rudimentary but well-known result:

Lemma 2.6. *[7, Lemma 2.1] Let G be a finite abelian group and A, B subsets of G such that $|A| + |B| > |G|$. Then $A + B = G$.*

3 Kemperman pairs

In this section, we review the theory of critical pairs in abelian groups, following the exposition of Kemperman's work in [2], and prove various results that will help in the solution of our problem.

Definition 3.1. *Let H be an abelian group. A Kemperman pair in H is a pair (A, B) of subsets of H such that $A + B$ is not periodic or (A, B) has UEP.*

We now state Kemperman's Theorem [5, Theorem 5.1 and p. 82] in the form given by Gryniewicz [2].

Theorem 3.2. *([2], p. 563) Let G be an abelian group and (A, B) a Kemperman pair in G . Then $|A + B| = |A| + |B| - 1$ if and only if there exist quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ with nonempty aperiodic parts and common quasi-period P such that (A_0, B_0) is a Kemperman pair and:*

1. $\nu_c(\phi_P(A), \phi_P(B)) = 1$, where $c = \phi_P(A_0) + \phi_P(B_0)$;
2. $|\phi_P(A) + \phi_P(B)| = |\phi_P(A)| + |\phi_P(B)| - 1$, and
3. $|A_0 + B_0| = |A_0| + |B_0| - 1$ and the pair (A_0, B_0) is of one of the following (distinct) types:

- (a) $|A_0| = 1$ or $|B_0| = 1$.
- (b) $|A_0| \geq 2$, $|B_0| \geq 2$, and A_0, B_0 are arithmetic progressions with common difference $d \in H$ such that d has order at least $|A_0| + |B_0| - 1$. In this case, $\nu_c(A_0, B_0) = 1$ for exactly two values $c \in A_0 + B_0$.
- (c) $|A_0| + |B_0| = |P| + 1$, and there is exactly one element $g \in G$ such that $\nu_g(A_0, B_0) = 1$.

- (d) A_0 is aperiodic, B_0 is of the form $B_0 = g - [(G \setminus A_0) \cap (g' + P)]$ for some $g, g' \in A_0$, and $\nu_c(A_0, B_0) \neq 1$ for all c .

We say that a Kemperman pair (A, B) is *elementary* if there exists a decomposition as in Theorem 3.2 with $A_1 = B_1 = \emptyset$.

Remark.

We note (cf. [2], c.13 on p. 564) that if we select a different quasi-periodic decomposition for A or B , the type of the resulting pair of aperiodic parts does not change; hence we may speak of the type of (A, B) without reference to any choice of quasi-periodic decompositions.

If $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ are quasi-periodic decompositions of sets with respect to a common quasi-period P , we denote by $(A + B)_{per}$ the P -periodic set $(A_1 + B) \cup (A + B_1)$. Clearly $A + B = (A + B)_P \cup (A_0 + B_0)$.

Lemma 3.3. *Suppose (A, B) is a Kemperman SS-pair. With notation as in Theorem 3.2:*

1. $A + B$ is the disjoint union of $A_0 + B_0$ and $(A + B)_P$. In particular, $A + B$ is P -periodic if and only if $A_0 + B_0$ is P -periodic.
2. If (A, B) has type (a) or (d), then $A + B$ is not P -periodic. If (A, B) has type (c), then $A + B$ is P -periodic.

Proof.

For the first item, suppose $A_0 \subseteq g_1 + P$ and $B_0 \subseteq g_2 + P$ and let $h_1 = \phi_P(g_1)$, $h_2 = \phi_P(g_2)$. By Theorem 3.2, $\nu_{h_1+h_2}(\phi_P(A), \phi_P(B)) = 1$. Now if $x \in (A + B)_P \cap (A_0 + B_0)$, then $x = a + b$, where $a \in A$, $b \in B$ and $a \in A_1$ or $b \in B_1$. Thus, $\phi(x) = h_1 + h_2 = \phi(a) + \phi(b)$, contradicting $\nu_{h_1+h_2}(\phi_P(A), \phi_P(B)) = 1$. The second assertion now follows immediately. If (A, B) has type (a), then $|A_0| = |B_0| = 1$, so $|A_0 + B_0| = 1$. Since P is nontrivial, $A_0 + B_0$ is a strict subset of a P -coset and so $A_0 + B_0$ (and hence also $A + B$) is not P -periodic. If (A, B) has type (d), then, as noted in [2, p. 563], $A_0 + B_0$ is P -subperiodic, so again $A + B$ is not P -periodic. Finally, if (A, B) has type (c), then $|A_0 + B_0| = |A_0| + |B_0| - 1 = |P|$, so $A_0 + B_0$ is a (full) P -coset; thus, $A + B$ is P -periodic. \square

The proof of the following is immediate:

Lemma 3.4. *Suppose A, B are subsets of an abelian group H and that $A = A_1 \cup A_0$, $B = B_1 \cup B_0$ are quasi-periodic decompositions with respect to some common quasi-period P . If $A + B$ is P -periodic, then $|A + B| = |\phi_P(A + B)||P|$; otherwise, $|A + B| = (|\phi_P(A + B)| - 1)|P| + |A_0 + B_0|$.*

Lemma 3.5. *Suppose (A, B) is a Kemperman SS-pair of subsets of an abelian group H with corresponding quasi-periodic decompositions $A = A_0 \cup A_1$ and $B = B_0 \cup B_1$ with respect to some common quasi-period P . Then $|A_0| = |B_0|$, $|\phi_P(A)| = |\phi_P(B)|$, $|A_0 + B_0| = |A_0| + |B_0| - 1$, $|\phi_P(A + B)| = |\phi_P(A)| + |\phi_P(B)| - 1$, $|A_0 + A_0| = 2|A_0| - 1$, and $|\phi_P(A + A)| = 2|\phi_P(A)| - 1$.*

Proof.

Let $p = |P|$, and define x and y by $|A_1| = xp$ and $|B_1| = yp$. We have $|A| = xp + |A_0|$, $|B| = yp + |B_0|$; since A_0 and B_0 are nonempty, we have $1 \leq |A_0| \leq p$, $1 \leq |B_0| \leq p$. By properties of integer division, $|A_0| = |B_0| = k$ and $x = y$, so $|\phi_P(A)| = |\phi_P(A_1)| + 1 = x + 1 = y + 1 = |\phi_P(B_1)| + 1 = |\phi_P(B)|$; this establishes the first two formulas. The next two formulas follow from Theorem 3.2. If $A + B$ is not P -periodic, then $|A + A| = |A + B| \not\equiv 0 \pmod{|P|}$ so $A + A$ is not P -periodic, either. It follows that $A_0 + A_0$ is a strict subset of a single P -coset, and also that $|A_0 + A_0| = |A_0 + B_0| = |A_0| + |B_0| - 1 = 2|A_0| - 1$. If $A + B$ is P -periodic, then $|A + A| = |A + B| \equiv 0 \pmod{|P|}$, so $A + A$ is likewise P -periodic. Letting $c = |A + A|/p = |\phi_P(A + A)|$, we have $cp = |A + A| = 2|A| - 1 = 2(xp + k) - 1$. Thus, $p(c - 2x) = 2k - 1$. Since $1 \leq k \leq p$, it follows that $2k - 1 = p$, so $c = 2x + 1$; that is, $|\phi_P(A + A)| = 2|A_1|/p + 1 = 2(|\phi_P(A)| - 1) + 1 = 2|\phi_P(A)| - 1$, as desired. \square

Proposition 3.6. *Suppose (A, B) is a Kemperman SS-pair with quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ with respect to a common quasi-period P .*

- *If (A, B) has type (a) or (b), or (d) then A_0 is a translate of B_0 .*
- *If (A, B) has type (c), then $A + B$ is P -periodic, $|P| \geq 3$ is odd, and $|A_0| = |B_0| \geq 2$. Furthermore, if (A, B) has SUEP, then there exist $h_1, h_2 \in H$ and a set $S \subseteq P$ such that $A_0 = h_1 + S$, $B_0 = h_2 + S$, and $h_1 + h_2 \notin (A_1 + B_1) \cup (A_1 + A_1)$; in particular, A_0 is a translate of B_0 .*

Proof.

Since all properties mentioned in the proposition remain invariant when either A or B is replaced by a translate, we assume throughout this proof that A_0 and B_0 are subsets of P .

If (A, B) is of type (a) or (b), then clearly A_0 is a translate of B_0 . If (A, B) has type (c), $A + B$ is P -periodic by Lemma 3.3. Moreover, because $|A_0| = |B_0|$, it follows that $|P| = 2|A_0| - 1$ is odd. In particular, since P is nontrivial, $|P| \geq 3$, and so $|A_0| = |B_0| \geq 2$. Now suppose (A, B) has SUEP. By translating each appropriately,

we may assume that $\nu_0(A, B) = \nu_0(A, A) = 1$. Then $B_0 \cap -A_0 = A_0 \cap -A_0 = \{0\}$; hence $A_0 = B_0 \subseteq P$.

Finally, suppose (A, B) has type (d). As remarked in [2, p. 563], a pair of type (d) satisfies $A_0 + B_0 = (h_0 + P) - \{h_0\}$ for some $h_0 \in H$, so $|A + B| \equiv -1 \pmod{|P|}$. In particular, letting $k = |A_0|$, we have $|P| = |A_0 + B_0| + 1 = |A_0| + |B_0| = 2k$. Since (A, B) is an *SS*-pair, $A_0 + A_0$ is a subset of P of order $2k - 1$. Hence there exist $x, y \in P$ such that $A_0 + A_0 = P \setminus \{x\}$ and $A_0 + B_0 = P \setminus \{y\}$; setting $B'_0 = B_0 + x - y$, we have $A_0 + B'_0 = P \setminus \{x\}$. Thus, A_0 and B'_0 are subsets of P of order k , each disjoint from $-A_0 + x$. This forces $A_0 = B'_0$, and hence A_0 is a translate of B_0 . \square

Lemma 3.7. *Suppose (A, B) is a Kemperman *SS*-pair in H together with quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ with respect to a common quasi-period P . If $A + B$ is aperiodic or (A, B) has SUEP, then $(\phi_P(A), \phi_P(B))$ has SUEP.*

Proof.

For convenience, let $C = \phi_P(A)$ and $D = \phi_P(B)$. By translating A and B appropriately, we may assume that $A_0 \subseteq P$, $B_0 \subseteq P$, and hence that $\phi_P(A_0) = \phi_P(B_0) = 0 \in C \cap D$. Suppose (C, D) does not have SUEP. Since $\nu_0(C, D) = 1$ by statement 1 of Theorem 3.2, it follows that $\nu_0(C, C) > 1$; thus, we may select $0 \neq c \in C$ such that $-c \in C$. Writing $c = \phi_P(a)$ for some $a \in A_1$, observe that since $\phi(-a) = -c \neq 0 \in C$, $-a + P \subseteq A_1$, so $-a \in A_1$ also. Next, choose $p \in P$, $p \neq 0$. Since A_1 is P -periodic, $a - p, -a + p \in A_1$, and so $(a - p) + (-a + p) = 0$ witnesses that $\nu_0(A, A) \geq 2$; hence (A, B) does not have SUEP. Moreover, $A + A$ is the union of a P -periodic set with $A_0 + A_0$. Since the latter is a subset of P and $(a + P) + (-a + P) = P \subseteq A + A$, it follows that $A + A$ is P -periodic. Since $|A + A| = |A + B|$ and A, B both have quasi-periodic decompositions with respect to P , $A + B$ is also P -periodic. \square

Finally, we need the following “reconstruction lemma”:

Lemma 3.8. *Suppose (A, B) is a critical Kemperman pair in an abelian group H with $|A| = |B|$ and that $A = A_0 \cup A_1$, $B = B_0 \cup B_1$ are quasi-periodic decompositions with respect to a common quasi-period P . If A_0 is a translate of B_0 and $\phi_P(A)$ is a translate of $\phi_P(B)$ then A is a translate of B .*

Proof.

Note that the conclusion of Lemma 3.8 remains valid if we translate either A or B by any $h \in H$. Moreover, the assertion is automatically true if A_1 and B_1 are empty, so we assume henceforth that these are nonempty. Similarly, if A_0 (and hence also B_0)

is a full P -coset, the assertion is clear, so we assume otherwise. If $\phi_P(B) = \phi_P(A) + \bar{h}$ for some $\bar{h} \in H/P$, then picking $h \in G$ such that $\phi_P(h) = \bar{h}$, we may replace B by $B - h$ and assume henceforth that $\phi_P(B) = \phi_P(A)$. In particular, this means that there exist distinct cosets $h_1 + P, \dots, h_s + P$ of P in G and decompositions $A = \cup_{i=1}^s C_i$ and $B = \cup_{i=1}^s D_i$ where for every $i = 1, \dots, s$, $C_i \subseteq h_i + P$ and $D_i \subseteq h_i + P$ with $C_i = h_i + P$ if and only if $i \neq i_0$ and $D_j = h_j + P$ if and only if $j \neq j_0$. With this notation, $C_{i_0} = A_0$ and $D_{j_0} = B_0$. We claim that $i_0 = j_0$.

Note that $A+B$ is the union of a P -periodic set, together with $A_0+B_0 \subseteq (h_{i_0}+h_{j_0})+P$. If $i_0 \neq j_0$, then $A_1 + B_1 \supseteq C_{j_0} + D_{i_0} = (h_{i_0} + h_{j_0}) + P \supseteq A_0 + B_0$, contradicting Lemma 3.3. Thus $i_0 = j_0$, and so $A_1 = B_1$. Since $A_0 = p + B_0$ for some $p \in P$, we have that $A = p + B$, as desired. \square

4 Results

4.1 The Kemperman case

In this section, we answer our question in the case that our original SS -pair (A, B) is a Kemperman pair.

Theorem 4.1. *Let G be an abelian group and (A, B) an SS -pair in G . If $A + B$ is aperiodic or (A, B) has $SUEP$, then $A = x + B$ for some $x \in G$.*

Proof.

We prove the theorem by induction on $|A| + |B|$, the theorem being trivially true when $|A| = |B| = 1$. Since the hypothesis clearly implies that (A, B) is a Kemperman pair, fix quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ as in Theorem 3.2 with respect to some common quasi-period P . By Proposition 3.6, A_0 is a translate of B_0 . If either of A_1, B_1 is empty, the other is, too, so $A = A_0, B = B_0$ and the claim is proven. Suppose henceforth that A_1 and B_1 are nonempty. Lemma 3.5 implies that $(\phi_P(A), \phi_P(B))$ an SS -pair; thus, Lemma 3.7 implies that the hypotheses of the theorem are satisfied by $(\phi_P(A), \phi_P(B))$. Thus, by induction, $\phi_P(A)$ is a translate of $\phi_P(B)$. Finally, Lemma 3.8 implies that A is a translate of B . \square

Corollary 4.2. *Suppose G is a 2-group and (A, B) is an SS -pair of subsets of G . Then A is a translate of B .*

Proof.

Let $k = |A| = |B|$. First, note that $A+B$ cannot be periodic, because $|A+B| = 2k-1$, which is odd, so it cannot be the union of cosets of a nontrivial subgroup of G . Hence (A, B) is a Kemperman pair, and so A is translate of B by Theorem 4.1. \square

4.2 The periodic case

We now study SS -pairs (A, B) for which $A+B$ is periodic; in fact, all the results of this section apply even when (A, B) has SUEP. When (A, B) is not a Kemperman pair, we do not have Theorem 3.2 at our disposal, so we use Kneser's Theorem instead.

Theorem 4.3. (*Kneser, [7, Theorem 4.2]*)

Let G be an abelian group and A, B finite nonempty subsets of G ; set $H = \text{Stab}(A+B)$. If $|A+B| < |A| + |B|$, then

$$|A+B| = |A+H| + |B+H| - |H|$$

In particular, if $|A+B| < |A| + |B| - 1$, then H is nontrivial and so $A+B$ is periodic.

It is easy to see that SS -pairs (A, B) such that $\nu_c(A, B) > 1$ for all $c \in A+B$ exist. We describe how, starting with one such pair, one may construct SS -pairs (A, B') where B' is not a translate of A .

Lemma 4.4. *Let G be an abelian group, (A, B) an SS -pair in G , and $P = \text{Stab}(A+B)$. Let c_1+P, \dots, c_k+P be distinct cosets whose union is $A+P$ and d_1+P, \dots, d_l+P distinct cosets whose union is $B+P$.*

- $|P|$ is odd.
- $|A+P| - |A| = |B+P| - |B| = \frac{|P|-1}{2}$. In particular, $|(c_i+P) \cap A| \geq \frac{|P|+1}{2}$ and $|(d_j+P) \cap B| \geq \frac{|P|+1}{2}$ for all $i = 1, \dots, k$ and $j = 1, \dots, l$.
- Let (A', B') be any pair such that $A' \subseteq \cup_{i=1}^k (c_i+P)$, $B' \subseteq \cup_{j=1}^l (d_j+P)$, where $|(c'_i+P) \cap A'| \geq \frac{|P|+1}{2}$ and $|(d'_j+P) \cap B'| \geq \frac{|P|+1}{2}$ for all $i = 1, \dots, k$ and $j = 1, \dots, l$. Then $A' + B' = \cup_{i=1}^k \cup_{j=1}^l ((c'_i + d'_j) + P)$.

Proof.

For convenience of notation, let $C_i = c_i + P$, $D_j = d_j + P$ for $i = 1, \dots, k$, $j = 1, \dots, l$; hence $A+B = \cup_{i=1}^k \cup_{j=1}^l C_i + D_j$. Because $|A| = |B|$ and (A, B) is critical,

$|A + B| = |A| + |B| - 1 = 2|A| - 1$ is odd. Since $A + B$ is a disjoint union of P -cosets, $|P|$ must be odd. Now Kneser's Theorem gives $|A| + |B| - 1 = |A + B| = |A + P| + |B + P| - |P|$, or $(|A + P| - |A|) + (|B + P| - |B|) = |P| - 1$. Hence $|A + P|$ (respectively, $|B + P|$) is the smallest multiple of $|P|$ greater than or equal to $|A|$ (respectively $|B|$). However, since $|A| = |B|$, we must have $|A + P| = |B + P|$, so $2(|A + P| - |A|) = |P| - 1$. Reduction modulo $|P|$ gives $2|A| \equiv 1 \pmod{|P|}$, so since $|P|$ is odd, $|A| = |B| \equiv \frac{|P| + 1}{2} \pmod{|P|}$. Thus, $|A + P| - |A| = |B + P| - |B| = \frac{|P| - 1}{2}$. Since $|C_i \cap A| = |C_i| - |C_i \setminus A| \geq |C_i| - |(A + P) \setminus A| \geq |P| - \frac{|P| - 1}{2} = \frac{|P| + 1}{2}$. A similar argument shows that $|D_j \cap B| \geq \frac{|P| + 1}{2}$, thus establishing the first statement.

For the second statement, note that for every i and j , $((c'_i + P) \cap A') + ((d'_j + P) \cap B') \subseteq (c'_i + d'_j) + P$. Moreover, $|((c'_i + P) \cap A')| + |((d'_j + P) \cap B')| \geq |P| + 1 > |P|$, so by Lemma 2.6, $((c'_i + P) \cap A') + ((d'_j + P) \cap B') = (c'_i + d'_j) + P$. Thus, $A' + B' = \cup_{i=1}^k \cup_{j=1}^l (c'_i + d'_j) + P$. \square

Proposition 4.5. *If G is an abelian group and (A, B) a critical pair in G with $P = \text{Stab}(A + B)$, then $\phi_P(A + B)$ is aperiodic and $(\phi_P(A), \phi_P(B))$ is a critical Kemperman pair of subsets of G/P . In particular, if (A, B) is an SS -pair in G , then $(\phi_P(A), \phi_P(B))$ is a Kemperman SS -pair in G/P and $\phi_P(A)$ is a translate of $\phi_P(B)$.*

Proof.

Aperiodicity is clear in view of the definition of stabilizer. Let $A' = A + P$ and $B' = B + P$; then $\phi_P(A) = \phi_P(A')$, $\phi_P(B) = \phi_P(B')$ and $A' + B' = (A + B) + P = A + B$. By Kneser's Theorem, $|A + B| = |A' + B'| = |A'| + |B'| - |P|$. Dividing all terms by $|P|$, we have $|\phi_P(A + B)| = |\phi_P(A)| + |\phi_P(B)| - 1$, and so $(\phi_P(A), \phi_P(B))$ is a critical Kemperman pair. This proves the first part of the Proposition.

Now assume that (A, B) is an SS -pair. We wish to prove that $(\phi_P(A), \phi_P(B))$ is an SS -pair. Write $A' = \cup_{i=1}^k c_i + P$ and $B' = \cup_{j=1}^l d_j + P$ (as disjoint unions). By the second statement of Lemma 4.4, $|A \cap (c_i + P)| \geq \frac{|P| + 1}{2}$, $|B \cap (d_j + P)| \geq \frac{|P| + 1}{2}$, so by the third statement, $A + A$ is P -periodic; that is, $P \subseteq \text{Stab}(A + A)$. Furthermore, $A' + A' = (A + P) + (A + P) = (A + A) + P = A + A$. Now Kneser's Theorem implies $2|A| - 1 = |A + A| = |A' + A'| = 2|A'| - |\text{Stab}(A + A)|$, or $|A'| - |A| = \frac{|\text{Stab}(A + A)| - 1}{2}$. Because $|A'| - |A| = \frac{|P| - 1}{2}$ by Lemma 4.4, it follows that $P = \text{Stab}(A + A)$. Finally, dividing the equation $|A + A| = 2|A'| - |P|$ by $|P|$, we get $|\phi_P(A) + \phi_P(A)| = |\phi_P(A + A)| = 2|\phi_P(A)| - 1$. This establishes that $(\phi_P(A), \phi_P(B))$ is an SS -pair; hence $\phi_P(A)$ is a translate of $\phi_P(B)$ by Theorem 4.1. \square

Since Question 1 obviously has an affirmative answer if A and B have size 1 or 2, we assume henceforth without further mention that $|A| \geq 3$, $|B| \geq 3$. The next result shows that in general there are “many” SS -pairs (A, B) such that $A + B$ is periodic but A is *not* a translate of B . Since Proposition 4.5 implies that $\phi_P(A)$ is always a translate of $\phi_P(B)$, we assume $\phi_P(A) = \phi_P(B)$ in the following to simplify the discussion.

Theorem 4.6. *Suppose G is an abelian group and $A \subseteq G$ is a subset such that $|A + A| = 2|A| - 1$ and $P = \text{Stab}(A + A) \neq 0$. Write $A = \cup_{i=1}^k S_i$, where each S_i is a subset of (the P -coset) $c_i + P$. Consider the collection \mathcal{B} of all subsets $B \subseteq G$ such that $|A| = |B| = k$, $\phi_P(A) = \phi_P(B)$, and $|B \cap (c_i + P)| \geq \frac{|P|+1}{2}$ for all $i = 1, \dots, k$. Then each (A, B) is an SS -pair in G . Moreover, at most $|P|$ elements of \mathcal{B} are translates of A , and $|\mathcal{B}| > |P|$, so there is at least one $B \in \mathcal{B}$ which is not a translate of A .*

Proof.

Since $\phi_P(A) = \phi_P(B)$, any $B \in \mathcal{B}$ must satisfy $B \subseteq A + P$. Observe that by Lemma 2.4, A must be a strict subset of $A + P$. Clearly $P \subseteq \text{Stab}(A + P) = P'$; moreover, $A + A + P' = (A + A) + P + P' = (A + P) + (A + P) + P' = (A + P) + (A + P) = (A + A) + P = A + A$, so $P' \subseteq \text{Stab}(A + A) = P$ and hence $\text{Stab}(A + P) = P$. For any $B \in \mathcal{B}$, Lemma 4.4 shows that $A + B = A + A$, so (A, B) is an SS -pair. If $B = g + A$ for some $g \in G$, then (by definition) $A + P = B + P = g + (A + P)$, so $g \in \text{Stab}(A + P) = P$. Now $|P|$ is odd by Lemma 4.4, so $|P| \geq 3$. Since A is a strict subset of $A + P$, there exists i_0 , $1 \leq i_0 \leq k$ such that S_{i_0} is a strict subset of $c_{i_0} + P$. If $k \geq 2$, pick a nonzero element $p \in P$ and consider $B = \cup_{1 \leq i \leq k: i \neq i_0} S_i \cup (S_{i_0} + p)$. Then $B \in \mathcal{B}$, so (A, B) is an SS -pair, but B is not a translate of A . If $k = 1$, then $A \subseteq c_1 + P$ is a set of size $n = |A|$, and $A + A = 2c_1 + P$ has size $2n - 1$, so $|P| = 2n - 1$. There are $|P| = 2n - 1$ translates of A within $A + P = c_1 + P$ and $\binom{|P|}{|A|} = \binom{2n - 1}{n}$ subsets of $A + P$ of size n . If $n \geq 3$, $\binom{2n - 1}{n} > 2n - 1$, so one may choose B to be a subset of $A + P$ of size n which is not a translate of A . The case $n \leq 2$ is excluded from consideration since $|A| \geq 3$. \square

References

- [1] P. Bihani and R. Jin. Kneser's Theorem for Upper Banach Density. *Journal de Théorie des Nombres de Bordeaux*. **18** (2006), no. 2, 323-343.
- [2] D. Grynkiewicz. Quasi-periodic decompositions and the Kemperman structure theorem. *European Journal of Combinatorics*. **26** (2005), 559-575.
- [3] Y. O. Hamidoune. Subsets with small sums in abelian groups. I. The Vosper property. *European Journal of Combinatorics*. **18** (1997), no. 5, 541-556.
- [4] Y. O. Hamidoune. Subsets with a small sum. II. The critical pair problem. *European Journal of Combinatorics*. **21** (2000), no. 2, 231-239.
- [5] J. H. B. Kemperman. On small subsets of an abelian group. *Acta Mathematica*. **103** (1960), 63-88.
- [6] A. G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.* **31** (1956), 200-205 and 280-282.
- [7] M. Nathanson. *Additive Number Theory*. Springer, 1996.