Quasi-periodic Decompositions and the Kemperman Structure Theorem

David J. Grynkiewicz

Mathematics 253-37,
Caltech,
Pasadena, CA 91125

diambri@hotmail.com

December 11, 2008

Abstract

The Kemperman Structure Theorem (KST) yields a recursive description of the structure of a pair of finite subsets A and B of an abelian group satisfying $|A+B| \leq |A|+|B|-1$. In this paper, we introduce a notion of quasi-periodic decompositions and develop their basic properties in relation to KST. This yields a fuller understanding of KST, and gives a way to more effectively use KST in practice. As an illustration, we first use these methods to (a) give conditions on finite sets A and B of an abelian group so that there exists $b \in B$ such that $|A+(B\setminus\{b\})| \geq |A|+|B|-1$, and to (b) give conditions on finite sets $A, B, C_1, \ldots, C_r$ of an abelian group so that there exists $b \in B$ such that $|A+(B\setminus\{b\})| \geq |A|+|B|-1$ and $|A+(B\setminus\{b\})+\sum_{i=1}^{r} C_i| \geq |A|+|B|+\sum_{i=1}^{r}|C_i|-(r+2)+1$. Additionally, we simplify two results of Hamidoune, by (a) giving a new and simple proof of a characterization of those finite subsets B of an abelian group G for which $|A+B| \geq \min\{|G|-1,\, |A|+|B|\}$ holds for every finite subset $A \subseteq G$ with $|A| \geq 2$, and (b) giving, for a finite subset $B \subseteq G$ for which $|A+B| \geq \min\{|G|,\, |A|+|B|-1\}$ holds for every finite subset $A \subseteq G$, a nonrecursive description of the structure of those finite subsets $A \subseteq G$ such that $|A+B| = |A|+|B|-1$.

1 Introduction

Let $(G, +, 0)$ be an abelian group. If $A, B \subseteq G$, then their *sumset*, $A + B$, is the set of all possible pairwise sums, i.e. $\{a + b \mid a \in A, b \in B\}$. We denote by $\nu_c(A, B)$ the number of representations of $c = a + b$ with $a \in A$ and $b \in B$. We denote by $\eta_b(A, B)$ the number of $c \in A + b$ such that $\nu_c(A, B) = 1$, and denote by $\overline{A}$ the compliment of A. A set $A \subseteq G$ is said to be H_a*-periodic*, if it is the union of H_a-cosets for some nontrivial subgroup H_a of G, and otherwise A is *aperiodic*. We use $\phi_a : G \to G/H_a$ to denote the natural homomorphism. If $A + B$ is H_a-periodic, then an H_a*-hole* of A (where the subgroup H_a is usually understood) is an element $\alpha \in (A + H_a) \setminus A$. Finally, a subset $B \subseteq G$ is *Cauchy* if B is finite and nonempty and $|A + B| \geq \min\{|G|, |A| + |B| - 1\}$ for every finite, nonempty subset $A \subseteq G$.

For finite subsets A and B of an abelian group, the estimation of $|A+B|$ began with Cauchy, who showed that $|A + B| \geq \min\{|G|, |A| + |B| - 1\}$ for $|G|$ prime [5]. Nearly 100 years later the result (now known as the Cauchy-Davenport Theorem) was independently rediscovered by Davenport [7] [23]. Subsequently, Kneser proved the following foundational generalization for an arbitrary abelian group [18] [15] [19] [16] [23] [11].

Kneser's Theorem. *Let G be an abelian group, and let $A_1, A_2, \ldots, A_n$ be a collection of finite, nonempty subsets of G. If $\sum_{i=1}^{n} A_i$ is maximally H_a-periodic, then*

$$\left|\sum_{i=1}^{n} \phi_a(A_i)\right| \geq \sum_{i=1}^{n} |\phi_a(A_i)| - n + 1, \tag{1}$$

and otherwise the above inequality holds with ϕ_a the identity.

Note that if A is maximally H_a-periodic, then $\phi_a(A)$ is aperiodic. Also, if $A+B$ is maximally H_a-periodic and $\rho = |A + H_a| - |A| + |B + H_a| - |B|$ is the number of holes in A and B, then Kneser's Theorem implies $|A+B| \geq |A|+|B|-|H_a|+\rho$. Consequently, if either A or B contains a unique element from some H_a-coset, then $|A + B| \geq |A| + |B| - 1$. Furthermore, it is also easily derived from Kneser's Theorem that if $|A + B| < |A| + |B| - 1$, then $A + B$ is periodic, and if $|A + B| \leq |A| + |B| - 1$, then equality holds in (1).

The problems of describing the structure of sets A and B for which $A + B$ is small and of estimating the size of $A + B$ are important in many applications ranging from analysis to zero-sum Ramsey theory (e.g. [3] [17] [16] [10] [2] [1] [4] [23] [8] [24] [6] [12]). Sets such that $|A + B| \leq |A| + |B| - 1$ are called *critical pairs* and, despite some confusion to the contrary, a complete recursive description of their structure was first given by Kemperman [16] (we refrain from stating the theorem until we have developed further notation). However, the description is somewhat complicated and seemingly unwieldy to use. Owing to this fact, several attempts were made to obtain more readily usable theorems related to KST [20] [13] [14]. In [20], Lev gave a weaker but simpler necessary condition for a pair (A, B) to be critical. In [13] [14], Hamidoune used his isoperimetric method—a sophisticated method, applicable to a wide range of additive problems, that uses global properties to infer results about local structure—to (a) determine the structure of those finite, nonempty subsets $B \subseteq G$ for which $|A + B| \geq \min\{|G| - 1, |A| + |B|\}$ holds for every finite subset $A \subseteq G$ with $|A| \geq 2$, and to (b) give for a fixed Cauchy subset $B \subseteq G$ a recursive description of the structure of those finite, nonempty subsets $A \subseteq G$ such that $|A + B| = |A| + |B| - 1$.

Another unfortunate effect of the complicated nature of Kemperman's result and its decentralized statement in the original paper of Kemperman (the full recursive description was spread across two separate theorems, Theorems 3.4 and 5.1, and some remarks at the end of Section 5), is that the result of Kemperman has been misportrayed in several later papers as a limited result that does not completely characterize all critical pairs [12] [13] [14], which misleadingly gives the impression that the critical pair problem for abelian groups is still not fully solved [pp. 130, 23].

The aim of this paper is to introduce the geometrically intuitive concept of quasi-periodic decompositions and develop their basic properties in relation to KST. This yields a fuller understanding of KST, and gives a way to more effectively use KST. As one consequence, we will give a centralized and (relatively) compact statement of the full recursive version of KST. As additional illustration, we then use these methods in Section 3 to prove the following single element draining results, which are crucial base steps in a multiple element draining theorem for a collection of sets motivated by applications in zero-sum Ramsey Theory [9].

Theorem 1.1. *Let G be an abelian group, and let A, $B \subseteq G$ be finite subsets such that $|A| \geq 2$, and $|B| \geq 3$. If $|A + B| \geq |A| + |B| - 1$, then either:*

(i) there exists $b \in B$ such that $|A + (B \setminus \{b\})| \geq |A| + |B| - 1$, or

(ii) (a) $|A + B| = |A| + |B| - 1$, (b) there exists $a \in A$ such that $A \setminus \{a\}$ is H_a-periodic, and (c) there exists $\alpha \in G$ such that $B \subseteq \alpha + H_a$.

Theorem 1.2. *Let G be an abelian group, and let A, B, $C_1, \ldots, C_r \subseteq G$ be finite subsets with $|B| \geq 3$. If $|A + B| > |A| + |B| - 1$, $|A + B + \sum_{i=1}^{r} C_i| \geq |A| + |B| + \sum_{i=1}^{r} |C_i| - (r + 2) + 1$, and $|A + \sum_{i=1}^{r} C_i| \geq |A| + \sum_{i=1}^{r} |C_i| - (r + 1) + 1$, then there exists $b \in B$ such that $|A + (B \setminus \{b\})| \geq |A| + |B| - 1$ and $|A + (B \setminus \{b\}) + \sum_{i=1}^{r} C_i| \geq |A| + |B| + \sum_{i=1}^{r} |C_i| - (r + 2) + 1$.*

Finally, to illustrate how, for questions involving critical pairs, our results can often be used as an alternative to the isoperimetric method, we will subsequently in Section 3 use our results to simplify and generalize the previously mentioned results of Hamidoune [13] [14]. Specifically, we will (a) give a new and simple proof of the description of the structure of those finite, nonempty subsets $B \subseteq G$ for which $|A+B| \geq \min\{|G|-1,\ |A|+|B|\}$ holds for every finite subset $A \subseteq G$ with $|A| \geq 2$, and will (b) give for a Cauchy subset $B \subseteq G$ a *nonrecursive* description of the structure of those finite, nonempty subsets $A \subseteq G$ such that $|A+B| = |A|+|B|-1$. We will accomplish (b) by showing that the recursive description given by Kemperman terminates after one or two iterations, provided one of the two subsets is Cauchy.

In what follows, we will need the following two basic theorems [16] [23].

Theorem 1.3. *Let G be an abelian group, and let A, $B \subseteq G$ be finite subsets. If $|A+B| = |A|+|B|-\rho$, then $\nu_c(A,B) \geq \rho$ for all $c \in A+B$.*

Theorem 1.4. *Let G be a finite abelian group, and let A, $B \subseteq G$. If $|A|+|B| > |G|$, then $A+B = G$.*

2 Quasi-periodic Decompositions and KST

This section contains many comments and observations concerning quasi-periodic decompositions and KST, which while important are also straightforward to verify. Thus we will generally state the simpler observations, attaching to the ends of the corresponding sentences labels of the form (c.x) with $x \in \mathbb{Z}$ for ease of future reference, and will provide proofs and explanations for the more involved statements.

Let G be an abelian group, and let H_a be a nontrivial subgroup. If $A \subseteq G$, then a *quasi-periodic decomposition* of A with *quasi-period* H_a is a partition $A = A_1 \cup A_0$ of A into two disjoint (each possibly empty) subsets such that A_1 is H_a-periodic or empty and A_0 is a subset of an H_a-coset. A set $A \subseteq G$ is *quasi-periodic* if A has a quasi-periodic decomposition $A = A_1 \cup A_0$ with A_1 nonempty. Given a quasi-periodic decomposition $A_1 \cup A_0$ with quasi-period H_a, we refer to A_1 as the *H_a-periodic part*, and refer to A_0 as the *aperiodic part* (although it may be periodic if A is periodic). Such a decomposition is *reduced* if A_0 is not quasi-periodic. Note that if A is finite and has a quasi-periodic decomposition $A_1 \cup A_0$ with quasi-period H, then A has a reduced quasi-periodic decomposition $A'_1 \cup A'_0$ with quasi-period $H' \leq H$ and $A'_0 \subseteq A_0$ (c.1). Additionally, a pair of quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ with common quasi-period H_a induce a quasi-periodic decomposition of $A+B = C$ with quasi-period H_a given by $(C \setminus (A_0+B_0)) \cup (A_0+B_0)$ (c.2). Useful examples of non-quasi-periodic sets include arithmetic progressions with difference d and at most $|\langle d \rangle|-2$ terms (c.3). A *punctured periodic set*, i.e. a set A for which there exists $\alpha \in G \setminus A$ such that $A \cup \{\alpha\}$ is maximally H_a-periodic, has a reduced quasi-periodic decomposition for each prime order subgroup of H_a (c.4). However, as the following proposition shows, reduced quasi-periodic decompositions are otherwise canonical.

Proposition 2.1. *If $A_1 \cup A_0$ and $A_1' \cup A_0'$ are both reduced quasi-periodic decompositions of a subset A of an abelian group G, with A_1 maximally H-periodic and A_1' maximally L-periodic, then either (i) $A_1 = A_1'$ and $A_0 = A_0'$ or (ii) $H \cap L$ is trivial, $A_0 \cap A_0' = \emptyset$, $|H|$ and $|L|$ are prime, and there exists $\alpha \in G \setminus A$ such that $A_0 \cup \{\alpha\}$ is an H-coset, $A_0' \cup \{\alpha\}$ is an L-coset, and $A \cup \{\alpha\}$ is $(H+L)$-periodic.*

Proof. To show (i) it suffices to show $A_1 = A_1'$. We may assume A_1 and A_1' are nonempty, since if w.l.o.g. $A_1 = \emptyset$ and $A_1' \neq \emptyset$, then $A_0 = A = A_1' \cup A_0'$ is quasi-periodic, contradicting that $A_1 \cup A_0$ is reduced. Note that $H \cap L$ is trivial, since otherwise $(A_0' \cap A_1) \cup (A_0' \cap A_0) = A_0'$ and $(A_0 \cap A_1') \cup (A_0 \cap A_0') = A_0$ imply either $A_1 = A_1'$, or that one of A_0' or A_0 is quasi-periodic with quasi-period $H \cap L$, a contradiction.

Suppose $A_1' \subseteq A_1$. Then each L-coset of A_1' is contained in an $(H+L)$-coset contained in A_1. Hence, since $H \cap L$ is trivial, it follows that there must be an entire L-coset, say $\gamma + L$, contained in one of these $(H+L)$-cosets contained in A_1, such that $\gamma + L$ is not in A_1', since otherwise A_1' will be $(H+L)$-periodic, contradicting the maximality of L. But then A_0' must contain $\gamma + L$, implying $A_0' = \gamma + L$, which contradicts that A_0' is not quasi-periodic. So $A_1' \cap A_0 \neq \emptyset$.

By repeating the above argument for A_1, it follows that $A_1 \cap A_0' \neq \emptyset$ as well. Now A_0' is contained in an $(H+L)$-coset, and this $(H+L)$-coset decomposes as a union of H-cosets. Since $A_1 \cap A_0' \neq \emptyset$, one of these H-cosets, say $\gamma + H$, is contained in A_1. Hence, since $H \cap L$ is trivial, it follows that part of $\gamma + H$ is contained in A_1'. Let $\beta + L$ be an L-coset in A_1' that intersects $\gamma + H$. If every H-coset that meets $\beta + L$ is in A_1, then this implies that the entire $(H+L)$-coset, which contains the L-coset in which A_0' is contained, is in A_1. Hence A_0' is periodic, contradicting that A_0' is not quasi-periodic. So there exists an H-coset, say $\gamma' + H$, that meets $\beta + L$, and which is not contained in A_1. Then $\gamma' + H$ must be the H-coset containing A_0, and hence also the unique H-coset that meets $\beta + L$ not in A_1. Thus the entire $(H+L)$-coset containing A_0' is contained in A_1 except for (possibly) elements in $\gamma' + H$. Hence, if $\beta' + L$ is the L-coset containing A_0', then the only elements that can be missing from $\beta' + L$ in A are those in $(\beta' + L) \cap (\gamma' + H)$. Hence, since $H \cap L$ is trivial, and since A_0' is not periodic, it follows that A_0' is obtained from $\beta' + L$ by deleting the single element α in $(\beta' + L) \cap (\gamma' + H)$. The same is true of A_0, and (ii) immediately follows. $\square$

In view of Proposition 2.1 and (c.1), it follows that a punctured H-periodic set A is aperiodic and, if $|H| > 2$, has a unique $\alpha \notin A$ such that $A \cup \{\alpha\}$ is periodic (c.5). Hence the compliment of a puncture periodic set, i.e. a set A such that $A \setminus \{\beta\}$ is maximally H_a-periodic for some $\beta \in A$, is also aperiodic, and either has a unique $\beta \in A$ such that $A \setminus \{\beta\}$ is periodic, or else there is a unique $\alpha \notin A$ such that $A \cup \{\alpha\}$ is K-periodic, where K is isomorphic to the Klein four group (c.6). We can now state the structure theorem for critical pairs proved by Kemperman [Theorem 5.1 and comments on pp. 82, 14].

Kemperman Structure Theorem I (KST). *Let A and B be finite subsets of an abelian group G. Then $|A+B| = |A| + |B| - 1$, and, moreover, if $A+B$ is periodic then $\nu_c(A,B) = 1$ for some c, 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 H_a, such that:*
(i) $\nu_c(\phi_a(A), \phi_a(B)) = 1$, where $c = \phi_a(A_0) + \phi_a(B_0)$
(ii) $|\phi_a(A) + \phi_a(B)| = |\phi_a(A)| + |\phi_a(B)| - 1$, and
(iii) the pair (A_0, B_0) is of one of the following types (all of which imply $|A_0 + B_0| = |A_0| + |B_0| - 1$):

(I) $|A_0| = 1$ or $|B_0| = 1$;

(II) A_0 and B_0 are arithmetic progressions with common difference d, where the order of d is at least $|A_0| + |B_0| - 1$, and $|A_0| \geq 2$, $|B_0| \geq 2$ (hence, $A_0 + B_0$ is an arithmetic progression with difference d, while $\nu_c(A_0, B_0) = 1$ for exactly two $c \in A_0 + B_0$);

(III) $|A_0| + |B_0| = |H_a| + 1$, and precisely one element g_0 satisfies $\nu_{g_0}(A_0, B_0) = 1$ (hence, B_0 has the form $B_0 = (g_0 - \overline{A_0} \cap (g_1 + H_a)) \cup \{g_0 - g_1\}$, where $g_1 \in A_0$);

(IV) A_0 is aperiodic, B_0 is of the form $B_0 = g_0 - \overline{A_0} \cap (g_1 + H_a)$, with $g_1 \in A_0$ (hence, $A_0 + B_0 = (g_0 + H_a) \setminus \{g_0\})$, and $\nu_c(A_0, B_0) \neq 1$ for all c.

Note that KST(i) and KST(ii) insure that we can apply KST modulo H_a (c.7). Next observe that (II) implies that $|\{c \in A+B \mid \nu_c(A,B) = 1\}| = 2$, that (III) implies $A+B$ is periodic and $|\{c \in A+B \mid \nu_c(A,B) = 1\}| = 1$, and that (IV) implies $|\{c \in A+B \mid \nu_c(A,B) = 1\}| = 0$ (c.8). Hence if $|\{c \in A+B \mid \nu_c(A,B) = 1\}| > 2$, then (A,B) must be of type (I) (c.9). Also if $\nu_c(A,B) = 1$ for $c = a+b$ with $a \in A$ and $b \in B_1$, or if $\eta_b(B,A) \geq 2$ for some $b \in A$, then (A,B) must have type (I) with $|A_0| = 1$ (c.10).

In view of Proposition 2.1, (c.1), (c.3), the characterization of type (IV) given in KST(iii), and a simple counting argument, it follows that the subsets A_0 and B_0 from KST can always be taken to be the respective aperiodic parts of (some) reduced quasi-periodic decompositions of A and B, provided $A+B$ is aperiodic, and furthermore, assuming A_0 and B_0 have been chosen such, then $A_0 + B_0$ will be non-quasi-periodic, provided $A+B$ is not a punctured periodic set (c.11).

Note that an arithmetic progression with at least two terms, difference d and at most $|\langle d \rangle| - 2$

terms union a disjoint nonempty $\langle d\rangle$-periodic set cannot satisfy KST(iii) as in view of Proposition 2.1 and (c.1) it is no longer an arithmetic progression and hence not of type (II), nor a set with a single element and hence not of type (I), nor since $|\{c \in A+B \mid \nu_c(A,B)=1\}| = 2 \neq 0, 1$ of type (III) or (IV). Hence in view of Proposition 2.1 and (c.1) it follows that if (A,B) has type (II), then $A_1 \cup A_0$ and $B_1 \cup B_0$ must be taken to be the reduced quasi-periodic decompositions of A and B (c.12). Hence in view of (c.8), since (A,B) of type (I) implies $|\{c \in A+B \mid \nu_c(A,B)=1\}| > 0$ so that (A,B) cannot be type (IV), and since (A,B) of type (I) with $A+B$ H_a-periodic implies $|\{c \in A+B \mid \nu_c(A,B)=1\}| \geq |H_a| \geq 2$ so that (A,B) cannot have type (III), it follows that the type of a pair (A,B) is unique and depends only on (A,B) and not the choice of quasi-periodic decompositions that satisfy KST (c.13). If $A+B$ is maximally H_a-periodic, then from Kneser's Theorem it follows that KST(ii) holds with H_a, and that there are exactly $|H_a|-1$ holes in A and B. If there does not exist a pair of subsets $A_0 \subseteq A$ and $B_0 \subseteq B$, each contained in an H_a-coset, such that all $|H_a|-1$ holes in A and B are contained in $(A_0+H_a) \setminus A_0$ and $(B_0+H_a) \setminus B_0$, then from Theorems 1.3 and 1.4 it follows that there will not be a unique expression element in $A+B$. Hence if (A,B) has type (III) with $A+B$ maximally H_a-periodic, then it follows from the previous two sentences that there will be quasi-periodic decompositions of A and B that satisfy KST with quasi-period H_a (c.14). The following proposition gives a canonical decomposition for (A,B) of type (I).

Proposition 2.2. *Let A and B be finite subsets of an abelian group G such that $|A+B| = |A|+|B|-1$, and let $A_0 = \{b \in A \mid \eta_b(B,A) > 0\}$, $A_1 = \{b \in A \mid \eta_b(B,A) = 0\}$, $B_0 = \{b \in B \mid \eta_b(A,B) > 0\}$, and $B_1 = \{b \in B \mid \eta_b(A,B) = 0\}$. If (A,B) has type (I), then $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ are a pair of quasi-periodic decompositions that satisfy KST.*

Proof. Since A and B are finite, we may w.l.o.g. assume G is finitely generated. Let $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ be quasi-periodic decompositions that satisfy KST with quasi-period H_a maximal. Since (A,B) has type (I), then w.l.o.g. $|A_0| = 1$. If $|A| = 1$ or $|B| = 1$, then the proof is trivial. So we may assume $|A| > 1$ and $|B| > 1$. If $\eta_b(A,B) = 0$ for all $b \in B_1$, and $\eta_b(B,A) = 0$ for all $b \in A_1$, then the proof is complete. Hence in view of (c.10) we may w.l.o.g. assume $\eta_{b'}(A,B) > 0$ for some $b' \in B_1'$. In view of (c.7), apply KST modulo H_a, and let $\phi_a(A) = \phi_a(A_1') \cup \phi_a(A_0')$ and $\phi_a(B) = \phi_a(B_1') \cup \phi_a(B_0')$, with $A = A_1' \cup A_0'$ and $B = B_1' \cup B_0'$, be corresponding quasi-periodic decompositions that satisfy KST with quasi-period $H_{a'}/H_a$ maximal. Note that $\eta_b(A,B) > 0$ for $b \in B$ implies $\eta_{\phi_a(b)}(\phi_a(A), \phi_a(B)) > 0$. Hence, in view of KST(i), and since $\eta_{b'}(A,B) > 0$ for some $b' \in B_1$, it follows that $\eta_{\phi_a(a_0)}(\phi_a(B), \phi_a(A)) \geq 2$, where $A_0 = \{a_0\}$. Hence from (c.10) it follows that $\phi_a(A)$ must have type (I) with $A_0' = A_0$, implying that $A_1' = A_1$. Thus since $|A| > 1$, it follows that A_1' is $H_{a'}$-periodic and nonempty.

Suppose that $\eta_{\phi_a(b)}(\phi_a(A), \phi_a(B)) = 0$ for all $b \in B'_1$. Hence from KST(i) it follows that $B_0 \subseteq B'_0$. Hence B'_1 is $H_{a'}$-periodic. Thus, since $A'_0 = A_0 = \{a_0\}$, it follows that $A = A_1 \cup A_0$ and $B = B'_1 \cup B'_0$ are a pair of quasi-periodic decompositions that satisfies KST with quasi-period $H_{a'}$, contradicting the maximality of H_a. So we may assume that $\eta_{\phi_a(b'')}(\phi_a(A), \phi_a(B)) > 0$ for some $b'' \in B'_1$. Hence we can iterate the above arguments indefinitely, yielding an infinite chain of strictly increasing subgroups $H_a < H_{a'} < \ldots$, which is impossible in a finitely generated abelian group. □

We will refer to the pair of quasi-periodic decompositions that satisfy KST with quasi-period H_a maximal as the *Kemperman decompositions* of A and B. Note in view of (c.2) that the decompositions mentioned in Proposition 2.2, (c.12) and (c.14) are those that satisfy KST with H_a maximal, for types (I), (II) and (III), respectively, and that they are each unique (c.15). We proceed to show the following proposition that in view of (c.2) and (c.5) will characterize the Kemperman decomposition for (A, B) of type (IV).

Proposition 2.3. *Let A and B be finite subsets of an abelian group. If (A, B) has type (IV), $A + B$ is a punctured maximally H_a-periodic set, and $|A + B| = |A| + |B| - 1$, then there exist quasi-periodic decompositions of A and B that satisfy KST with quasi-period H_a.*

Proof. From KST(iii) and Theorem 1.4 it follows that there exists an element $b \notin A$, from the coset containing the aperiodic part of the Kemperman decomposition of A, such that $|A \cup \{b\} + B| = |A \cup \{b\}| + |B| - 1$. Hence, since the inclusion of b increased the cardinality of the sumset by one, it follows that $\eta_b(B, A \cup \{b\}) = 1$, and hence, since (A, B) has (IV), that $(A \cup \{b\}, B)$ has type (III). Hence, let $A \cup \{b\} = A_1 \cup A_0$ and $B = B_1 \cup B_0$ be the Kemperman decompositions with quasi-period H_a. Since $\eta_b(B, A \cup \{b\}) = 1$, and since $(A \cup \{b\}, B)$ has type (III), it follows that $b \in A_0$. Hence, since $A + B$ is aperiodic from (c.5), it follows that $|A_0| > 1$. Thus from the characterizations of sets satisfying (III) and (IV) found in KST(iii), it follows that $A_0 \setminus \{b\}$ and B_0 have type (IV) and hence $A = A_1 \cup (A_0 \setminus \{b\})$ and $B = B_1 \cup B_0$ are a pair of quasi-periodic decompositions that satisfy KST with quasi-period H_a, completing the proof. □

In view of Propositions 2.2 and 2.3, (c.11) and (c.15), it follows, for (A, B) of type (I) or (IV) with $A+B$ aperiodic, that there are two main choices for the quasi-periodic decompositions that satisfy KST. The first being to take reduced quasi-period decompositions of A and B, which from Proposition 2.1 will be unique provided $A + B$ is not a punctured periodic set, and the second being to take the Kemperman decompositions.

In view of Proposition 2.2, (c.10) and KST(iii), it follows that either $\eta_b(A, B) \le 1$ for all $b \in B$ or $\eta_b(B, A) \le 1$ for all $b \in A$ (c.16). Hence, if $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ are quasi-periodic decompositions that satisfy KST with quasi-period H_a, and if $A+B=C_1\cup C_0$ is the corresponding induced quasi-periodic decomposition, then applying (c.16) modulo H_a, it follows from KST(i) that either $A_1+B=C_1$ or $A+B_1=C_1$ (c.17). Note too that if $A=A_1\cup A_0$ and $B=B_1\cup B_0$ are the Kemperman decompositions, then $\eta_b(A,B)=0$ for all $b\in B_1$ and $\eta_b(B,A)=0$ for all $b\in A_1$ (c.18).

A recursive description for all (A,B) with $A+B$ aperiodic or $A+B$ containing a unique expression element, is obtained from KST by repeatedly applying KST modulo the quasi-period H_a. In view of KST(i), it follows that type (IV) can never occur in one of the recursive iterations other than in the initial pair of quasi-periodic decompositions (c.19). If $A+B$ is maximally H_a-periodic, then in view of Kneser's it follows that $\phi_a(A+B)$ is aperiodic and that $|\phi_a(A)+\phi_a(B)|=|\phi_a(A)|+|\phi_a(B)|-1$. Hence the recursive description given by KST can be used to describe the mod H_a skeletons of A and B. From Kneser's Theorem it follows that A and B must satisfy $|A|+|B|=|A+H_a|+|B+H_a|-|H_a|+1$, while in view of Theorem 1.4 and Kneser's Theorem it follows that any pair of subsets $A'\subset A+H_a$ and $B'\subset B+H_a$ with $|A'|+|B'|=|A+H_a|+|B+H_a|-|H_a|+1$ satisfies $A'+B'=A+B$ and $|A'+B'|=|A'|+|B'|-1$. Combining the last two sentences we obtain a complete recursive characterization for sets A and B with $A+B$ periodic and $|A+B|=|A|+|B|-1$. As noted by Kemperman [16], to describe A and B for which $|A+B|=|A|+|B|-1-\rho$ with $\rho\geq 1$, we simply use Kneser's Theorem to conclude $A+B$ is maximally H_a-periodic and that $|\phi_a(A)+\phi_a(B)|=|\phi_a(A)|+|\phi_a(B)|-1$, and then use the recursive description given by KST for $A+B$ aperiodic or containing a unique expression element. This gives us the mod H_a skeletons for A and B. To complete the description we simply take $A+H_a$ and $B+H_a$ (well defined since both these sets depend only on the H_a skeleton) and delete any $|H_a|-1-\rho$ total elements from $A+H_a$ and $B+H_a$ collectively. In view of KST(i) and (c.18), it follows that by choosing the Kemperman decompositions at each step of the recursion we are assured that if $A=A_1\cup A_0$ and $B=B_1\cup B_0$ are the Kemperman decompositions with quasi-period H_a, and if $\phi_a(A)=\phi_a(A'_1)\cup\phi_a(A'_0)$ and $\phi_a(B)=\phi_a(B'_1)\cup\phi_a(B'_0)$ with $A=A'_1\cup A'_0$ and $B=B'_1\cup B'_0$ are the Kemperman decompositions modulo H_a, then $A_0\subseteq A'_0$ and $B_0\subseteq B'_0$. To put all this in more rigorous summary, we restate the Kemperman Structure Theorem with the described recursive aspects included.

Kemperman Structure Theorem II (with Recursion). *Let A and B be finite subsets of an abelian group G. Then $|A+B|=|A|+|B|-1$, and, moreover, if $A+B$ is periodic then $\nu_c(A,B)=1$ for some c, if and only if there exist an integer $r\geq 1$, partitions $A=A_r\cup\ldots\cup A_1\cup A_0$ and $B=B_r\cup\ldots\cup B_1\cup B_0$ of A and B into disjoint (possibly empty) subsets, and a sequence of subgroups $H_{a_r}>\ldots>H_{a_1}>H_{a_0}=0$, such that A_0 and B_0 are nonempty, $A_r=B_r=\emptyset$, and* *for each* $l \in \{1, \ldots, r\}$*:*

(i) $\phi_{a_{l-1}}(A) = \phi_{a_{l-1}}(A_r \cup \ldots \cup A_l) \cup \phi_{a_{l-1}}(A_{l-1} \cup \ldots \cup A_0)$ *and* $\phi_{a_{l-1}}(B) = \phi_{a_{l-1}}(B_r \cup \ldots \cup B_l) \cup \phi_{a_{l-1}}(B_{l-1} \cup \ldots \cup B_0)$ *are the Kemperman decompositions with common quasi-period* $H_{a_l}/H_{a_{l-1}}$*,*

(ii) $\nu_{c_l}(\phi_{a_l}(A), \phi_{a_l}(B)) = 1$*, where* $c_l = \phi_{a_l}(A_{l-1} \cup \ldots \cup A_0) + \phi_{a_l}(B_{l-1} \cup \ldots \cup B_0)$

(iii) $|\phi_{a_l}(A) + \phi_{a_l}(B)| = |\phi_{a_l}(A)| + |\phi_{a_l}(B)| - 1$*,*

(iv) $\eta_b(\phi_{a_{l-1}}(A), \phi_{a_{l-1}}(B)) = 0$ *for all* $b \in \phi_{a_{l-1}}(B_r \cup \ldots \cup B_l)$ *and* $\eta_b(\phi_{a_{l-1}}(B), \phi_{a_{l-1}}(A)) = 0$ *for all* $b \in \phi_{a_{l-1}}(A_r \cup \ldots \cup A_l)$*,*

(v) the pair (A'_l, B'_l)*, where* $A'_l = \phi_{a_{l-1}}(A_{l-1} \cup \ldots \cup A_0)$ *and* $B'_l = \phi_{a_{l-1}}(B_{l-1} \cup \ldots \cup B_0)$*, is of one of the below types, with type (IV) possible only for* $l = 1$*;*

(I) $|A'_l| = 1$ *or* $|B'_l| = 1$*,*

(II) A'_l *and* B'_l *are arithmetic progressions with common difference d, where the order of d is at least* $|A'_l| + |B'_l| - 1$*, and* $|A'_l| \geq 2$*,* $|B'_l| \geq 2$ *(hence,* $A'_l + B'_l$ *is an arithmetic progression with difference d, while* $\nu_c(A'_l, B'_l) = 1$ *for exactly two* $c \in A'_l + B'_l$*),*

(III) $|A'_l| + |B'_l| = |H_{a_l}/H_{a_{l-1}}| + 1$*, and precisely one element* g_0 *satisfies* $\nu_{g_0}(A'_l, B'_l) = 1$ *(hence,* B'_l *has the form* $B'_l = (g_0 - \overline{A'_l} \cap (g_1 + (H_{a_l}/H_{a_{l-1}}))) \cup \{g_0 - g_1\}$*, where* $g_1 \in A'_l$*);*

(IV) A'_l *is aperiodic,* B'_l *is of the form* $B'_l = g_0 - \overline{A'_l} \cap (g_1 + (H_{a_l}/H_{a_{l-1}}))$*, with* $g_1 \in A'_l$ *(hence,* $A'_l + B'_l = (g_0 + (H_{a_l}/H_{a_{l-1}})) \setminus \{g_0\}$*), and* $\nu_c(A'_l, B'_l) \neq 1$ *for all c.*

Furthermore, $|A+B| < |A| + |B| - 1$ *or* $|A+B| = |A| + |B| - 1$ *with* $A + B$ *periodic, if and only if* $A + B$ *is maximally* H_a*-periodic, the pair* $(\phi_a(A), \phi_a(B))$ *satisfies the conditions from the above paragraph, and* $|A + H_a| + |B + H_a| = |A + B| + |H_a|$*.*

However, in many applications it suffices to deal only with single level quasi-periodic decompositions and use KST without the above recursive aspects included. The following proposition, like Proposition 2.3, gives conditions when a quasi-periodic decomposition of $A+B$ can be realized as the induced decomposition of a pair of decompositions that satisfy the conditions of KST, and hence can be used to pull back a quasi-periodic decomposition from sum to components, an ability that can sometimes be quite useful.

Proposition 2.4. *Let A, B, C be finite subsets of an abelian group G, such that* $A + B = C$ *and* $|A+B| = |A| + |B| - 1$*. Suppose C is neither periodic nor a punctured periodic set, and let* $C = C_1 \cup C_0$ *be the reduced quasi-periodic decomposition. If* C_1 *is maximally* H_a*-periodic, then there exist quasi-periodic decompositions* $A = A_1 \cup A_0$ *and* $B = B_1 \cup B_0$ *that satisfy KST with quasi-period* H_a *such that* $A_0 + B_0 = C_0$*.*

Proof. From Proposition 2.1, (c.2) and (c.11), it follows that there exist reduced quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ that satisfy KST with quasi-period $H_{a'} \leq H_a$

such that $A_0 + B_0 = C_0$. Hence C_0 is contained in an $H_{a'}$-coset, and the proof is complete unless C_1 is nonempty. Let A'_0 be the maximal subset of A containing A_0 that is contained in an H_a-coset. Define B'_0 likewise. Since C_0 is contained in an $H_{a'}$-coset, since C_1 is maximally H_a-periodic, and since $H_{a'} \leq H_a$, it follows that $A'_0 + B'_0 = A_0 + B_0 = C_0$. Hence $A'_0 = A_0$ and $B'_0 = B_0$, since otherwise $|\phi_{a'}(C_0)| = |\phi_{a'}(A'_0 + B'_0)| > 1$, contradicting that C_0 is contained in an $H_{a'}$-coset. Since in view of KST(i) $A_0 + B_0 = C_0$ is a unique expression element modulo $H_{a'}$, since $H_{a'} \leq H_a$, and since C_1 is H_a-periodic, it follows that $A_0 + B_0 = C_0$ is a unique expression element modulo H_a. Hence it remains to show that KST(ii) holds with H_a and that A_1 and B_1 are H_a-periodic.

Suppose that $|\phi_a(A) + \phi_a(B)| > |\phi_a(A)| + |\phi_a(B)| - 1$. Hence, since C_1 is H_a-periodic, it follows that $|\phi_{a'}(C)| \geq (|\phi_a(A)| + |\phi_a(B)| - 1)|H_a/H_{a'}| + 1$. However, since $A_0 = A'_0$ and $B_0 = B'_0$ are each a subset of an $H_{a'}$-coset, it follows from KST(ii) that $|\phi_{a'}(C)| \leq ((|\phi_a(A)| - 1)|H_a/H_{a'}| + 1) + ((|\phi_a(B)| - 1)|H_a/H_{a'}| + 1) - 1$, contradicting the bound from the previous sentence. So we may assume that $|\phi_a(A) + \phi_a(B)| \leq |\phi_a(A)| + |\phi_a(B)| - 1$.

Suppose that $|\phi_a(A) + \phi_a(B)| < |\phi_a(A)| + |\phi_a(B)| - 1$. Hence, since $A'_0 = A_0$, $B'_0 = B_0$ and $A_0 + B_0 = C_0$ are each a subset of an $H_{a'}$-coset, since C_1 is H_a-periodic, and in view of KST(i) with $H_{a'}$, it follows that $|\phi_a(A_1) + \phi_a(B)| < |\phi_a(A_1)| + |\phi_a(B)| - 1$ and $|\phi_a(A) + \phi_a(B_1)| < |\phi_a(A)| + |\phi_a(B_1)| - 1$. Since $A_0 + B_0 = C_0$, it follows from (c.17) that w.l.o.g. $A_1 + B = C_1$. Thus from the conclusions of the previous two sentences, and in view of Kneser's Theorem, it follows that $\phi_a(C_1)$ is periodic, contradicting that C_1 is maximally H_a-periodic. So in view of the previous paragraph we may assume that KST(ii) holds with H_a. Hence, since C_1 is H_a-periodic, it then follows from a simple counting argument that A_1 and B_1 are H_a-periodic, completing the proof. □

3 Some Illustrative Examples

Having developed the machinery of Section 2, we can now give the proofs of Theorems 1.1 and 1.2, which should also serve to illustrate the ideas of the previous section.

Proof Theorem 1.1. Suppose (i) does not hold. Hence $\eta_b(A, B) \geq 1$ for all $b \in B$. Furthermore, if $|A + B| > |A| + |B| - 1$, then $\eta_b(A, B) \geq 2$ for all $b \in B$, whence $|A + (B \setminus \{b\})| \geq |A| + 2(|B| - 2) \geq |A| + |B| - 1$ for any $b \in B$. So we may assume $|A + B| = |A| + |B| - 1$. Hence apply KST to (A, B) and let $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ be the Kemperman decompositions with quasi-period H_a. Since $|B| \geq 3$, and since $\eta_b(A, B) \geq 1$ for each $b \in B$, it follows from (c.9) that (A, B) has type (I) with $|A_0| = 1$, whence the remainder of the theorem follows from the characterization of the Kemperman decomposition for type (I) given in Proposition 2.2. $\Box$

Proof Theorem 1.2. Let $b_1, \ldots, b_k$ be those $b_i \in B$ such that $|A + (B \setminus \{b\})| \geq |A| + |B| - 1$, and let $b_{k+1}, \ldots, b_n$ be the remaining elements of B. Note $\eta_{b_i}(A, B) \geq 1$ for all i, else the proof is complete with $b = b_i$. Since $|A + B| > |A| + |B| - 1$, then for each b_j with $j > k$, it follows that $\eta_{b_j}(A, B) \geq 2$. Thus, if $k \leq n - 2$, then for $j > k$ it follows, in view of $\eta_{b_i}(A, B) \geq 1$ for all i, that $|A + (B \setminus \{b_j\})| \geq \min\{|A| + 2(n - k - 1) + k - 1, |A| + 2n - 4\} \geq |A| + |B| - 1$, contradicting that $j > k$. So $k \geq n - 1$.

Let $C = \sum_{i=1}^{r} C_i$. If $|A + C + B| < |A + C| + |B| - 1$, then it follows from Theorem 1.3 that the proof is complete with $b = b_1$. Thus $|A + C + B| \geq |A + C| + |B| - 1$. Suppose $|A + C + B| > |A + C| + |B| - 1$. Hence, since $|A + \sum_{i=1}^{r} C_i| \geq |A| + \sum_{i=1}^{r} |C_i| - (r + 1) + 1$, it follows that $\eta_{b_j}(A + C, B) \geq 2$ for all $j \leq k$, else the proof is complete with $b = b_j$. Hence, since $k \geq n - 1$, it follows that $|A + C + (B \setminus \{b_1\})| \geq |A + C| + 2n - 4 \geq |A + C| + |B| - 1$. Thus in view of $|A + \sum_{i=1}^{r} C_i| \geq |A| + \sum_{i=1}^{r} |C_i| - (r + 1) + 1$ it follows that the proof is complete with $b = b_1$. So we may assume

$$|A + C + B| = |A + C| + |B| - 1. \tag{2}$$

Since $|A + \sum_{i=1}^{r} C_i| \geq |A| + \sum_{i=1}^{r} |C_i| - (r + 1) + 1$, it follows that the proof will be complete with $b = b_j$, $j \leq k$, unless

$$|A + C + (B \setminus \{b_j\})| \leq |A + C| + |B| - 2. \tag{3}$$

However, since $k \geq 2$, if the inequality in (3) is sharp for some $j \leq k$, then from (2) and Theorem 1.3, it follows for $j' \leq k$, $j' \neq j$, that $|A + C + (B \setminus \{b_{j'}\})| \geq |A + C| + |B| - 1$, contradicting (3). Hence, for $j \leq k$, it follows that

$$|A + C + (B \setminus \{b_j\})| = |A + C| + |B| - 2. \tag{4}$$

If $A + C$ is H_a-periodic, then $|A + C + B| - |A + C + (B \setminus \{b_j\})|$ must be a multiple of $|H_a|$, contradicting (4) and (2). So we may assume $A + C$ is aperiodic. Hence C is aperiodic, whence from Kneser's Theorem it follows that $|C| \geq \sum_{i=1}^{r} |C_i| - r + 1$. Hence if $|A + C| > |A| + |C| - 1$, then $|A + C| > |A| + \sum_{i=1}^{r} |C_i| - (r + 1) + 1$, whence in view of (4) the proof is complete with $b = b_1$. So

$$|A + C| = |A| + |C| - 1. \tag{5}$$

Note that $\eta_{b_j}(A + C, B) \geq 1$ for b_j with $j \leq k$ else the proof is complete. Suppose $\eta_{b_n}(A + C, B) \geq 1$. Hence, since $k \geq n - 1$ and since $\eta_{b_j}(A + C, B) \geq 1$ for b_j with $j \leq k$, then from Theorem 1.1 and (2) it follows that $A + C$ has quasi-periodic decomposition $C_1 \cup C_0$, where

$C_0 = \{c_0\}$ and C_1 is maximally H_a-periodic, and that B is a subset of an H_a-coset. Since B is a subset of an H_a-coset, and since $|B| \geq 3$, it follows that $|H_a| \geq 3$. Hence, from (5) and Proposition 2.4 applied to $A + C$, it follows that A has a quasi-periodic decomposition $A_1 \cup A_0$ where A_1 is H_a-periodic and $|A_0| = 1$. Hence, since B is a subset of an H_a-coset, it follows that $|A + B| = |A| + |B| - 1$, a contradiction. So we may assume that $\eta_{b_n}(A + C, B) = 0$ and, since $\eta_{b_j}(A + C, B) \geq 1$ for b_j with $j \leq k$, that $k = n - 1$.

Since $k \geq 2$, it follows from (4) and (2) that we can apply KST to $(A + C, B)$. Hence, let $A + C = C_1 \cup C_0$ and $B = B_1 \cup B_0$ be the Kemperman decompositions with quasi-period H_a. Since b_n is the unique $b \in B$ with $\eta_b(A + C, B) = 0$, it follows in view of (c.18) that $|B_1| \leq 1$ and hence, since B_1 is periodic, that $|B_1| = 0$. Hence B_0 is a subset of an H_a-coset, and since $\eta_{b_n}(A + C, B) = 0$, it follow in view of Proposition 2.2 that $(A + C, B)$ cannot have has type (I) with $|C_0| = 1$. Hence, in view of (c.9) and since $\eta_{b_j}(A + C, B) \geq 1$ for b_j with $j \leq k = n-1$, it follows that we may assume $n = 3$; furthermore $|\{c \in A+B \mid \nu_c(A, B) > 0\}| = 2$, implying $(A + C, B)$ has type (II) with (b_1, b_3, b_2) an arithmetic progression with difference $d = b_1 - b_3 = b_3 - b_2$. Since $|B_0| = 3$, and since $|A_0 + B_0| = |A_0| + |B_0| - 1$ (follows from KST(iii)), it follows in view of Proposition 2.1 and (c.1) that $A + C$ is not a punctured periodic set. Thus, in view of (c.12), Proposition 2.1, and the previous two sentences, and since $A + C$ is aperiodic, it follows that $2 \leq |C_0| \leq |\langle d\rangle| - 2$, that $C_1 \cup C_0$ is the unique reduced quasi-periodic decomposition of $A + C$, and that C_0 is an arithmetic progression with difference d. Hence from (5) and Proposition 2.4 it follows that A has a quasi-periodic decomposition $A_1 \cup A_0$ with quasi-period H_a, and that C has a quasi-periodic decomposition $C = C_1' \cup C_0'$, such that $A_0 + C_0' = C_0$. If $|A_0| = 1$, then since B is a subset of an H_a-coset it follows that $|A + B| = |A| + |B| - 1$, a contradiction. So we may assume $|A_0| \geq 2$. Thus, since $A_0 + C_0' = C_0$, and since $|C_0| \leq |\langle d\rangle| - 2$, it follows that $2 \leq |A_0| \leq |\langle d\rangle| - 2$. Hence $|\langle d\rangle| \geq 4$. Since C_0 is an arithmetic progression with difference d, and since $|A_0| \geq 2$, then if (A, B) has type (I) it follows that A_0 is an arithmetic progression with difference d. Otherwise, since $A + C$ is aperiodic and not a punctured periodic set, it follows that (A, C) has type (II). Thus A_0 and C_0' are arithmetic progressions with $A_0 + C_0' = C_0$ an arithmetic progression with difference d and at most $|\langle d\rangle| - 2$ terms. Since C_0 has at most $|\langle d\rangle| - 2$ terms, it follows that the difference of the arithmetic progression C_0 is unique up to sign. Hence A_0 must be an arithmetic progression with difference d in this case as well. Thus A_0 is an arithmetic progression with difference d regardless of the type of (A, C). Hence, since $2 \leq |A_0| \leq |\langle d\rangle| - 2$, then it follows from Proposition 2.1 that $A_1 \cup A_0$ is the unique reduced quasi-periodic decomposition of A.

Since $k = n - 1 = 2$, it follows from the definition of k that $|A + \{b_1, b_2\}| \leq |A| + |\{b_1, b_2\}| - 1$;

furthermore, in view of Theorem 1.3 it follows that the proof is complete with $b = b_2$, unless $|A + \{b_1, b_2\}| = |A| + |\{b_1, b_2\}| - 1$. Hence, since $\eta_{b_1}(A, B) \geq 1$, it follows that we can apply KST to the pair $(A, \{b_1, b_2\})$. Let $A = A'_1 \cup A'_0$ and $\{b_1, b_2\} = B'_1 \cup B'_0$ be the Kemperman decompositions. Since B'_0 is nonempty, and since B'_1 periodic implies $|B'_1| \geq 2$ or $|B'_1| = 0$, it follows that $B'_0 = \{b_1, b_2\}$. Hence, since $\eta_{b_i}(A, B) \geq 1$ for $i = 1, 2$, then it follows from KST(iii) that A'_0 is an arithmetic progression with difference $b_1 - b_2$, and that $(A, \{b_1, b_2\})$ has type (I) or (II). However from the conclusion of the last paragraph it follows that $A = A_1 \cup A_0$ is the unique reduced quasi-periodic decomposition of A, and that $|A_0| \geq 2$. Hence $(A, \{b_1, b_2\})$ must be of type (II), whence from (c.12) it follows that $A'_1 = A_1$ and $A'_0 = A_0$. Thus $A_0 = A'_0$ is an arithmetic progression with difference $d = b_1 - b_3 = b_3 - b_2$ as well as an arithmetic progression with difference $b_1 - b_2$. Hence, since $2 \leq |A_0| \leq |\langle d \rangle| - 2$ so that the difference of A_0 is unique up to sign, it follows that $\pm(b_2 - b_1) = b_1 - b_3 = b_3 - b_2$, which either contradicts that the b_i are distinct or that $|\langle d \rangle| \geq 4$. $\square$

Next we proceed to give some examples relating our results with similar results obtained using the isoperimetric method. However, we first note that it is a result of Mann, or an easily derived consequence of Kneser's Theorem, that a finite, nonempty subset $B \subseteq G$ being Cauchy is equivalent to there not existing a finite subgroup H of G such that $|H + B| < \min\{|G|, |H| + |B| - 1\}$ (c.20) [21] [22], i.e B cannot have too few H-holes for any subgroup H such that $H + B \neq G$.

The following is a simple proof of Theorem 4.6 from [14].

Theorem 3.1. *Let G be an abelian group, let $B \subseteq G$ be a Cauchy subset, and let $B = B_1 \cup B_0$ be a reduced quasi-periodic decomposition of B. Then a necessary and sufficient condition for there to exist a finite, nonempty subset $A \subseteq G$ such that $|A + B| \leq \min\{|G| - 2, |A| + |B| - 1\}$ and $|A| \geq 2$, is that $|B| < |G| - 2$ and one of the following conditions hold:*

(i) B_0 is an arithmetic progression and either B is not quasi-periodic or $\overline{B}$ is an arithmetic progression of finite length,

(ii) $|B_0| = 1$,

(iii) for any $b \in B$, there exists a finite subgroup H generated by $(B - b) \cap H$ such that $|H + B| = |H| + |B| - 1 < |G|$ and $|H| \geq 3$.

Proof. To show sufficiency, in case (i) let $A = \{0, d\}$, where d is the difference of the arithmetic progression B_0, in case (ii) let $A = \{0, h\}$, where h is any nonzero element of a quasi-period of $B = B_1 \cup B_0$, and in case (iii) let $A = H$. We next show necessariness.

If $|B| \geq |G| - 1$, then $|A + B| \geq |G| - 1$. Furthermore, if $|B| = |G| - 2$, then since B is Cauchy, it follows that $|A + B| \geq \min\{|G|, |A| + |B| - 1\} \geq |B| + 1 = |G| - 1$ for any finite subset $A \subseteq G$ with $|A| \geq 2$. Thus it follows that $|B| < |G| - 2$. If B does not have a unique reduced quasi-periodic decomposition, then, since B is Cauchy, it follow in view of Proposition 2.1 and (c.20) that $B = G \setminus \{g\}$ for some $g \in G$, contradicting that $|B| < |G| - 2$. Thus we may assume B has a unique reduced quasi-periodic decomposition.

Since A is Cauchy, it follows from hypothesis that $|A + B| = |A| + |B| - 1 < |G|$. Suppose that $A+B$ is maximally H_a-periodic. Hence $A' = A + H_a$ satisfies $|A'+B| \leq |A|+|B|-1 < |G|$, whence $A' = A$, since otherwise $|A' + B| < |A'| + |B| - 1$, contradicting that B is Cauchy. Thus, since $|A + B| = |A| + |B| - 1$, then from Kneser's Theorem it follows that

$$|H_a + B| - |B| = |H_a| - 1. \tag{6}$$

Let $b \in B$ and let H be the subgroup generated by $H_a \cap (B - b)$.

First suppose that $|H| = 1$. Hence $|H_a \cap (B - b)| = 1$, whence (ii) follows in view of (6) and the uniqueness of the reduced quasi-periodic decomposition for B. Next suppose that $|H| = 2$. Hence $|H_a \cap (B - b)| = 2$, and from (6) it then follows that B has a reduced quasi-periodic decomposition with quasi-period H and with its aperiodic part having cardinality one. Thus, as in previous sentence, it follows that (ii) holds. So may assume that $|H| \geq 3$.

Since $H + B \subset H_a + B \subset (A - a_0) + B \neq G$, where $a_0 \in A$, it follows that $|H + B| < |G|$. In view of (6) and the definition of H, it follows by counting holes that

$$\begin{aligned}&|H + B| - |B| \leq |H_a + B| - |B| - (l - 1)|H| = \\ &\qquad\qquad |H_a| - 1 - (l - 1)|H| = l|H| - 1 - (l - 1)|H| = |H| - 1,\end{aligned}$$

where $l = [H_a, H]$. Since B is Cauchy, and since $|H + B| < |G|$, then in view of (c.20) it follows that we must have equality in the above inequality, and (iii) follows. So we may assume that there does not exist a subset A satisfying the hypothesis of the theorem with the additional property that $A + B$ is periodic.

Since $A+B$ is aperiodic, apply KST to the pair (A, B) and let $A = A_1' \cup A_0'$ and $B = B_1' \cup B_0'$ be the Kemperman decomposition of (A, B) with quasi-period H_a. Since $A + B$ is aperiodic, it follows in view of (c.8) that (A, B) cannot have type (III). If (A, B) has type (IV), then from the characterization of type (IV) it follows that we can find an element $a_0 \in G \setminus A$ such that $(A \cup \{a_0\}, B)$ will be a type (III) pair. Furthermore, since $|A + B| < |G| - 1$, and since $|A + B|$ is congruent to -1 modulo $|H_a|$ for type (IV), it follows that $|A + B| \leq |G| - |H_a| - 1 \leq |G| - 3$, implying $|(A \cup \{a_0\}) + B| = |A + B| + 1 \leq |G| - 2$. Hence this reduces to the previously handled case. If (A, B) has type (I) with $|B_0'| = 1$, then (ii) follows by the uniqueness of a reduced quasi-periodic decomposition for B.

Suppose (A, B) has type (I) with $|B_0'| \geq 2$ and $|A_0'| = 1$. Since B is Cauchy, it follows that if $B = B_1'' \cup B_0''$ is a quasi-periodic decomposition with quasi-period H, then either $H + B = G$ or $|B_0''| = 1$. Hence, since $|B_0'| \geq 2$, it follows that $\phi_a(B) = G/H_a$, implying from KST(ii) that $\phi_a(A) = 1$, whence $A = A_0'$. However, since $|A_0'| = 1$ and since $|A| \geq 2$, this is a contradiction. So we may assume that (A, B) has type (II), implying that B_0' is an arithmetic progression with $|B_0'| \geq 2$ and also, by the characterization of the type (II) Kemperman decomposition, that $B = B_1' \cup B_0'$ is reduced. Since B is Cauchy, then the remainder of conclusion (i) follows easily from (c.20) and the uniqueness of the reduced quasi-periodic decomposition for B. □

The following is the (corrected) Theorem 6.6 from [12], which we will derive as a basic corollary to Theorem 3.1 (there is a typo in the original statement of Theorem 6.6; namely the inequality in Theorem 6.6(iii) should not be strict, as is easily seen by the example $G = \mathbb{Z}_6$, $B = \{0, 3, 1\}$).

Theorem 3.2. *Let B be a finite, nonempty subset of an abelian group G. If $|B| \leq |G|/2$, then one of the following conditions holds:*

(i) $|A + B| \geq \min\{|G| - 1,\ |A| + |B|\}$, for all finite subsets $A \subseteq G$ with $|A| \geq 2$,

(ii) B is an arithmetic progression,

(iii) there is a finite, nontrivial subgroup H, such that $|H + B| \leq \min\{|G| - 1,\ |H| + |B| - 1\}$.

Proof. We may assume B is not Cauchy, else (iii) follows in view of (c.20). We may also assume that the hypothesis of Theorem 3.1 holds for B, else (i) follows. Apply Theorem 3.1 to B. If Theorem 3.1(iii) holds, then (iii) follows. Since B is not Cauchy, we may assume $|B| > 1$. Hence, if Theorem 3.1(ii) holds, then we may assume $B = B_1 \cup B_0$ is quasi-periodic with quasi-period H. Hence (iii) follows unless $H + B = G$, in which case $|B| > |G|/2$, a contradiction. So we may assume that Theorem 3.1(i) holds. However, $|B| \leq |G|/2$ and B being Cauchy prevent B from being quasi-periodic, whence $B = B_0$ is an arithmetic progression, and (ii) follows. □

The following theorem gives a nonrecursive description of those finite, nonempty subsets A for which $|A+B| = |A|+|B|-1$, where B is a fixed Cauchy subset. This shows that additionally assuming one of the sets from a critical pair is Cauchy allows for a significant simplification of the structure of the pair.

Theorem 3.3. *Let G be an abelian group, let A, $B \subseteq G$ be finite, nonempty subsets, and let $B = B_1 \cup B_0$ be a reduced quasi-periodic decomposition of B. Suppose that B is Cauchy. Then $|A + B| = |A| + |B| - 1$, and, moreover, if $A + B$ is periodic then $\nu_c(A, B) = 1$ for some c, if and only if one of the following conditions holds:*

(i) A is aperiodic and $A = g_0 - \overline{B}$, for some $g_0 \in G$ (in which case $A + B = G \setminus \{g_0\}$),

(ii) $A = (g_0 - \overline{B}) \cup \{g_1\}$, for some $g_0 \in G$ and $g_1 \notin g_0 - \overline{B}$, (in which case $A + B = G$),

(iii) $|A| = 1$ or $|B| = 1$,

(iv) A and B_0 are arithmetic progressions with common difference d, where the order of d is at least $|A| + |B_0| - 1$, and either B is not quasi-periodic (in which case $B = B_0$) or $\overline{B}$ is an arithmetic progression with difference d and finite length,

(v) $|B_0| = 1$, and there exists a quasi-period H_a of $B = B_1 \cup B_0$ (namely the maximal quasi-period of the type (I) Kemperman decomposition of (A, B)) such that A has a quasi-periodic decomposition $A = A_1' \cup A_0'$ with quasi-period H_a and $A_0' \neq \emptyset$, such that $\nu_c(\phi_a(A), \phi_a(B)) = 1$, where $c = \phi_a(A_0') + \phi_a(B_0)$, such that $\phi_a(B)$ is Cauchy, and such that the pair $(\phi_a(A), \phi_a(B))$ satisfies one of (ii), (iii) or (iv) with $G = G/H_a$.

Furthermore, $|A+B| = |A|+|B|-1 < |G|$ with $A+B$ maximally H_k-periodic, if and only if A is maximally H_k-periodic, $A+B \neq G$, $|B+H_k|-|B| = |H_k|-1$, and the pair $(\phi_k(A), \phi_k(B))$ satisfies the hypotheses from the above paragraph with $G = G/H_k$; and $|A+B| = |A|+|B|-1 = |G|$ if and only if $|A| = |G| - |B| + 1$.

Proof. We first show that the furthermore statement of the theorem follows from the first part of the theorem. Note that the last part of the furthermore statement is a consequence of Theorem 1.4.

Suppose A is maximally H_k-periodic, $A + B \neq G$, B is Cauchy, $|B + H_k| - |B| = |H_k| - 1$, and the pair $(\phi_k(A), \phi_k(B))$ satisfies the hypotheses from the first part of the theorem with $G = G/H_k$. Then by the first part of the theorem it follows that $|\phi_k(A) + \phi_k(B)| = |\phi_k(A)| + |\phi_k(B)| - 1$. Hence, since A is H_k-periodic, and since $|B + H_k| - |B| = |H_k| - 1$, it follows that $|A+B| = |A|+|B|-1$ with $A+B$ being H_k-periodic. Furthermore, since $|A+B| = |A|+|B|-1$, since A is maximally H_k-periodic, and since $A + B \neq G$, it follows that $A + B$ is maximally H_k-periodic, since otherwise $A+H$ will contradict that B is Cauchy, where $A+B$ is maximally H-periodic.

Next suppose that B is Cauchy and that $|A+B| = |A|+|B|-1 < |G|$ with $A+B$ maximally H_k-periodic. Hence, by the reasoning from the previous paragraph, it follows that A must be maximally H_k-periodic and $A + B \neq G$. Thus, since $|A + B| = |A| + |B| - 1$, then in view of Kneser's Theorem it follows that $|B + H_k| - |B| = |H_k| - 1$, and that $|\phi_k(A) + \phi_k(B)| = |\phi_k(A)| + |\phi_k(B)| - 1$. Also, by the maximality of H_k it follows that $\phi_k(A) + \phi_k(B)$ is aperiodic. Finally, since B is Cauchy and since $|B + H_k| - |B| = |H_k| - 1$, then in view of (c.20) it follows by counting holes that $\phi_k(B)$ is Cauchy. Thus the pair $(\phi_k(A), \phi_k(B))$ satisfies the hypotheses of the first part of the theorem with $G = G/H_k$, and the proof of the furthermore statement of the theorem is complete.

Sufficiency of the first part of the theorem follows directly from KST-II. Thus it remains to show necessariness. Assume B is Cauchy, $|A+B| = |A|+|B|-1$, and, moreover, if $A+B$ is periodic, then $\nu_c(A,B)=1$ for some c. Apply KST to the pair (A,B) and let $A = A_1' \cup A_0'$ and $B = B_1' \cup B_0'$ be the corresponding Kemperman decompositions with maximal quasi-period H_a.

Since B is Cauchy, it follows that if $B = B_1'' \cup B_0''$ is a quasi-periodic decomposition with quasi-period H, then either $H+B = G$ or $|B_0''| = 1$ (c.21). Hence from KST it follows that (i) or (ii) holds provided (A,B) has type (IV) or (III), respectively.

Suppose B does not have a unique reduced quasi-periodic decomposition. Hence, since B is Cauchy, it follow in view of Proposition 2.1 and (c.20) that $B = G \setminus \{g\}$ for some $g \in G$. Thus $|A+B| = |A|+|B|-1$ implies $|A| \leq 2$, and it easily seen that (ii) or (iii) holds. So we may assume B has a unique reduced quasi-periodic decomposition (c.22).

Suppose (A,B) has type (II). Hence in view of KST, the characterization of the Kemperman decomposition for type (II), and (c.22), it follows that $B_0 = B_0'$ and A_0' are arithmetic progressions with common difference d, where the order of d is at least $|A_0'|+|B_0|-1$, that $|A_0'| \geq 2$ and that $|B_0| \geq 2$. Hence, in view of (c.21) it follows that $\phi_a(B) = G/H_a$. Thus from KST(ii) it follows that $\phi_a(A) = 1$, implying $A = A_0'$. Furthermore, since B_0 is an arithmetic progression with difference d, then it follows from (c.21) that if B is quasi-periodic, then $\overline{B}$ is also a finite arithmetic progression with difference d. Thus (iv) follows. So we may assume (A,B) has type (I).

Suppose $|B_0'| > 1$. Hence from (c.21) it follows that $|\phi_a(A)| = 1$, whence $A = A_0'$. Hence, since (A,B) has type (I) with $|B_0'| > 1$, it follow that $|A| = |A_0'| = 1$ and (iii) follows. So we may assume $|B_0'| = 1$. Thus in view of (c.22) it follows that $B_0' = B_0$, whence we may assume $B_1 \neq 0$, else (iii) follows with $|B| = 1$.

Since $|B_0| = 1$, then in view of KST and the above work, it follows that (v) will hold, provided we can additionally show that $\phi_a(B)$ is Cauchy, and also that $(\phi_a(A), \phi_a(B))$ does not have type (I) with $|B''| = 1$, where B'' is the aperiodic part of the corresponding Kemperman decomposition of $\phi_a(B)$.

Suppose $\phi_a(B)$ is not Cauchy. Hence by (c.20) it follows that there exists a finite subgroup H of G such that $|H/H_a + \phi_a(B)| < |G/H_a|$ and $|H/H_a + \phi_a(B)| < |H/H_a| + |\phi_a(B)| - 1$. Hence, since B has exactly $|H_a|-1$ H_a-holes, it follows by multiplying the previous inequality by H_a that $|H+B| < |H| + (|B|+|H_a|-1) - |H_a| = |H|+|B|-1$. Also, $|H/H_a + \phi_a(B)| < |G/H_a|$ implies that $|H+B| < |G|$, whence in view of (c.20) and the last sentence it follows that B is not Cauchy, a contradiction. So we may assume $\phi_a(B)$ is Cauchy.

Let $\phi_a(B) = \phi_a(B_1'') \cup \phi_a(B_0'')$ and $\phi_a(A) = \phi_a(A_1'') \cup \phi_a(A_0'')$, with $B = B_1'' \cup B_0''$ and $A = A_1'' \cup A_0''$, be the corresponding modulo H_a Kemperman decompositions with maximal quasi-period H/H_a. Suppose $(\phi_a(A), \phi_a(B))$ has type (I) with $|\phi_a(B_0'')| = 1$. Hence, $B_0'' = B_0$ and $B_1'' = B_1$. Thus, since $|B_1| > 0$, it follows that H/H_a is nontrivial. Since $B_0'' = B_0$, it follows for $a_0 \in A$, in view of the characterization of the type (I) Kemperman decomposition and KST, that $\eta_{a_0}(B, A) > 0$ if and only if $\eta_{\phi_a(a_0)}(\phi_a(B), \phi_a(A)) > 0$, whence the characterization of the type (I) Kemperman decomposition implies that $A_0'' = A_0'$ and $A_1'' = A_1'$. Thus $A = A_1' \cup A_0'$ and $B = B_1 \cup B_0$ are a quasi-periodic decomposition that satisfies KST with quasi-period H, whence by the maximality of H_a it follows that $H = H_a$. Hence H/H_a is trivial, a final contradiction. $\square$

Acknowledgements. I would like to thank my advisor R. Wilson for his understanding. I would also like to the thank the referees for their useful suggestions, particularly that of the one referee that I include material relating the results of the paper with the isoperimetric method of Hamidoune.

References

[1] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, *Combinatorics, Paul Erdős is eighty*, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., (Budapest, 1993), 33–50.

[2] A. Bialostocki, P. Dierker, D. Grynkiewicz, and M. Lotspiech, On some developments of the Erdős-Ginzburg-Ziv Theorem II, *Acta. Arith.*, 110 (2003), no. 2, 173–184.

[3] J. Bourgain, N. Katz and T. Tao, A sum-product estimate for finite fields, and applications, to appear in *GAFA*.

[4] Y. Caro, Zero-sum problems—a survey, *Discrete Math.*, 152 (1996), no. 1–3, 93–113.

[5] A. L. Cauchy, Recherches sur les nombres, *J. École polytech.*, 9 (1813), 99–116.

[6] S. Chowla, H. B. Mann, and E. G. Strauss, Some applications of the Cauchy-Davenport Theorem, *Norske Vid. Selsk. Forh.* (Trondheim) 32 (1959), 74–80.

[7] H. Davenport, On the addition of residue classes, *J. London Math. Society* 10 (1935), 30–32.

[8] W. D. Gao, On the Erdős-Ginzburg-Ziv theorem—a survey, *Paul Erdős and his mathematics*, János Bolyai Math. Soc., (Budapest, 1999), 76–78.

[9] D. Grynkiewicz, An extension of the Erdős-Ginzburg-Ziv Theorem to Hypergraphs, Preprint.

[10] D. Grynkiewicz, On four colored sets with nondcecreasing diameter and the Erdős-Ginzburg-Ziv Theorem. *J. Combin. Theory, Ser. A*, 100 (2002), no. 1, 44–60.

[11] H. Halberstam and K. F. Roth, *Sequences*, Springer-Verlag, (New York, 1983).

[12] Y. O. Hamidoune, Some results in additive number theory I, The critical pair theory, *Acta Arith.* 96 (2000), no. 2, 97–119.

[13] Y. O. Hamidoune, Subsets with a small sum II: The critical pair problem. *European J. Combin.* 21 (2000), no. 2, 231–239.

[14] Y. O. Hamidoune, Subsets with small sums in abelian groups I: The Vosper property. *European J. Combin.* 18 (1997), no. 5, 541–556.

[15] X. Hou, K. Leung, and Q. Xiang, A generalization of an addition theorem of Kneser, *Journal of Number Theory*, 97 (2002), 1–9.

[16] J. H. B. Kemperman, On small sumsets in an abelian group. *Acta Math.*, 103 (1960), 63–88.

[17] M. Kneser, Summenmengen in lokalkompakten abelschen gruppen, *Math. Z.*, 66 (1956), 88–110.

[18] M. Kneser, Ein satz über abelsche gruppen mit anwendungen auf die geometrie der zahlen, *Math. Z.* 64 (1955), 429–434.

[19] M. Kneser, Abschätzung der asymptotischen dichte von summenmengen, *Math. Z.*, 58 (1953), 459–484.

[20] V. Lev, On small sumsets in abelian groups. *Structure theory of set addition. Asterisque*, No. 258 (1999), xv, 317321.

[21] H. B. Mann, An addition theorem for sets of elements of an abelian group, *Proc. Am. Math. Soc.*, 4 (1953), 423.

[22] H. B. Mann, *Addition theorems: the addition theorems of group theory and number theory*, Interscience, New York, 1965.

[23] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics, 165, Springer-Verlag, (New York, 1996).

[24] A. Tietäväinen, On diagonal forms over finite fields, *Ann. Univ. Turku Ser. A I* 118 (1968), 10pp.