HYPER-ATOMS APPLIED TO THE CRITICAL PAIR THEORY

YAHYA O. HAMIDOUNE

Abstract. The isoperimetric method is very useful for proving many results regarding sumsets. Here, we introduce the notion of a hyper-atom into the method, which overcomes a previous weakness when dealing with atoms that are cosets. To show the utility of this new object, we give a new isoperimetric proof of the cornerstone of classical critical pair theory: The Kemperman Structure Theorem, proved in its so-called "dual" formulation.

1. Introduction

Let G be an abelian group and let A and B be subsets of G. The subgroup generated by A will be denoted by $\langle A\rangle$. The *sumset* $A+B$ is defined as

$$A+B=\{x+y\ :\ x\in A \text{ and } y\in B\}.$$

Let H be a subgroup of G. We shall say that H is a *proper* subgroup if $H\neq G$. We shall denote by ϕ_H the canonical homomorphism from G onto G/H. We shall say that A is H-periodic if $A+H=A$, which is equivalent to A being a union of H-cosets. The *stabilizer* of A is the subgroup $\mathsf{H}(A)=\{x\in G : A+x=A\}\leq G$. A set having a nontrivial stabilizer is said to be *periodic*. Sets with trivial stabilizer are called *aperiodic*. A basic tool in Additive Number Theory is the following generalization of the Cauchy-Davenport Theorem due to Kneser.

Theorem A (Kneser [5] [18] [17])**.** *Let $A,B\subseteq G$ be finite, nonempty subsets of an abelian group. If $A+B$ is aperiodic, then $|A+B|\geq |A|+|B|-1$.*

The description of the subsets A and B with $|A+B|\leq |A|+|B|-1$, obtained by Kemperman in [13] (see also [5]), is a deep result in classical critical pair theory. A further step in this direction was accomplished by Grynkiewicz in [4].

The present work is essentially self-contained. We assume only Kneser's Theorem, Menger's Theorem (for directed graphs in the finite vertex case), Theorem 5 and Theorem 8. The last two results, at least in the special cases we need, are proved in around two pages in [11]. We give a more general result in Theorem 8 proved using the basic isoperimetric machinery developed in [5, Ch. 21]. One of our aims is to present a methodology leading to an entirely new proof of Kemperman's result. This will be done by introducing the notion of a *hyper-atom* into the

Yahya O. Hamidoune passed away on March 11, 2011 before the final revisions for the already submitted manuscript could be completed. Final revisions have been made post mortem by David J. Gynkiewicz, Department of Mathematical Sciences, University of Memphis, Memphis TN, 38152, USA.

standard isoperimetric machinery. The isoperimetric method is one of the main tools for proving sumset results [5, Ch. 21]. For instance, Theorem A can be proved via these means [2] [14]. The idea of the method is to study a set S via certain auxiliary sets, called k-atoms and k-fragments. Having control over the size of a k-atom is often important for the method. Unfortunately, while there are good upper bounds for the size of k-atoms that are *not* cosets [5, Proposition 21.6], there are only trivial ones possible when the k-atom is itself a coset. We will see an instance of this dichotomy in Theorem 8. However, it is precisely in this latter setting that one can define a notion of hyper-atom, giving a new tool for dealing with sets having cosets for k-atoms.

Let S be a finite subset of an abelian group G. For $k \geq 1$, let

$$\mathcal{S}_k(S) = \{X \subseteq G : \infty > |X| \geq k \text{ and } |G \setminus (X+S)| \geq k\}.$$

We shall write

$$\kappa_k(S) = \min\{|X+S| - |X| : \ X \in \mathcal{S}_k\}.$$

A maximal cardinality subgroup $H \in \mathcal{S}_k$ with $\kappa_k(S) = |H+S|-|H|$ will be called a *k-hyper-atom*. When $k=1$, we talk simply of *hyper-atoms*. In Section 3, we will see that hyper-atoms exist and obtain the following result, which will be one of the first main steps towards our proof of the Kemperman Structure Theorem: Assume that $|S| \leq (|G|+1)/2$ and $\kappa_2(S) \leq |S|-1$ and let H be a hyper-atom of S. Then $\phi_H(S)$ is either an arithmetic progression or $\kappa_2(\phi_H(S)) \geq |\phi_H(S)|$.

Let H be a subgroup of an abelian group G and A a subset of G. Given an H-coset $\alpha + H$ that intersects A, where $\alpha \in G$, we call $A_\alpha = (\alpha+H) \cap A \neq \emptyset$ an *H-component* of A. The H-components naturally form a disjoint partition

$$A = \biguplus_{\alpha \in I} A_\alpha, \qquad \text{where each } A_\alpha = (\alpha+H) \cap A \neq \emptyset$$

and $I \subseteq G$ is a set of representatives for A modulo H. The notation $\uplus$ is used in place of $\cup$ to convey the additional information that sets in the union are disjoint. We refer to this decomposition as the *H-coset decomposition* of A. An H-component $A_\alpha \neq \alpha + H$ is called *partially filled*, and when $A_\alpha = \alpha + H$ it is instead called *full*.

- The set A is said to have an *H-quasi-periodic decomposition* if A is the union of an H-component $A_\emptyset \subseteq A$ and an H-periodic (possibly empty) subset $A \setminus A_\emptyset$. In such case, $A_\emptyset \subseteq A$ is called a *partial component* of the decomposition. It is uniquely determined when A is not H-periodic.
- The set A is said to be *H-quasi-periodic* if either A is the union of an H-component $A_\emptyset \subseteq A$ and a *nonempty* H-periodic subset $A \setminus A_\emptyset$ or if A is an H-coset. If A is H-quasi-periodic for some nontrivial $H \leq G$, then A is called *quasi-periodic*.

Kemperman's Structure Theorem is a precise if and only if characterization of all finite, nonempty subset S and T of an abelian group satisfying $|T+S| \leq |S| + |T| - 1$. The exact description of Kemperman is quite complex, meaning there are several ways to state the theorem that all imply the complete characterization. First, it is well-known that Theorem A implies

$|\phi_H(T)+\phi_H(S)| = |\phi_H(T)|+|\phi_H(S)|-1$ with $\phi_H(T)+\phi_H(S)$ aperiodic, where $H = \mathsf{H}(T+S)$ [5, Ch. 6]. Thus, to characterize such subsets, it suffices to consider the case when $T+S$ is aperiodic with $|T+S| = |T|+|S|-1$. If $|T+S| = |G|-1$, it is relatively easy to characterize the possibilities for S and T [5, pp. 122]. This case (corresponding to the fourth elementary structure in the discussion below) has been excluded below solely to simplify the statement of Theorem 1. Next, it is a standard normalization assumption to assume $0 \in S \cap T$ with $\langle T+S\rangle = G$. Kemperman's Structure Theorem shows that all such pairs are recursively constructed using quasi-periodic decompositions and certain precisely described elementary pairs. In essence, it says that S and T have H-quasi-periodic decompositions and either

(i) gives the precise elementary structure of $\phi_H(S)$ and $\phi_H(T)$ along with conditions that ensure the theorem can be recursively applied to $S_\emptyset + T_\emptyset$, or

(ii) gives the precise elementary structure of $S_\emptyset$ and $T_\emptyset$ along with conditions that ensure the theorem can be recursively applied to $\phi_H(S) + \phi_H(T)$.

Formulation (ii) was that originally given by Kemperman. Formulation (i) is the so-called "dual" formulation. It first appears in [16] and is equivalent to the formulation of Kemperman via a simple consequence of the original first observed in [3]. See [5, Ch. 9] for a fuller discussion. As such, one is at liberty to prove either the original or dual version of Kemperman's Structure Theorem. We will provide a proof of the dual version, given in Theorem 1 below.

Regarding the nature of the "elementary structure," the structure given in Theorem 1 below may at first seem weaker than the version of Kemperman's Structure Theorem given in [5, Theorem 9.2]. This is because there are two possible choices of how to define the four elementary structures of Kemperman, and his theorem is valid using either set of definitions. One set of definitions is more stringent, imposing additional conditions involving the number of unique expression elements, and the other is more lax, not requiring this additional information. The more stringent version provides more information at the expense of being more complicated to work with, requiring potentially more iterations in the recursive process, while the less stringent version is often sufficient in practice and is simply less refined in the iteration process. That there are two alternative versions was already noted in Kemperman's original paper. However, as explained both in [5, pp. 120] and in the original paper of Kemperman [13], this seemingly weaker version implies the stronger version in a couple pages. Since this is well-known and standard, we do not repeat the argument here.

Theorem 1 will follow easily from Theorem 17 in Section 5, which will be proved using the global isoperimetric methodology introduced in [11].

Theorem 1 (Kemperman [13] [5] [16] [3])**.** *Let S and T be finite, nonempty subsets of the nontrivial abelian group G with $0 \in S \cap T$, $\langle T + S\rangle = G$ and $|S| \le |T|$. Suppose $T + S$ is aperiodic and*

$$|T + S| = |T| + |S| - 1 \le |G| - 2.$$

Then there exists a finite and proper subgroup $H < G$ such that T and S both have H-quasi-periodic decompositions with partial components $T_\emptyset \subseteq T$ and $S_\emptyset \subseteq S$ and one of the following holds:

(I) $\phi_H(S) = \{0\}$,

(II) $\phi_H(T)$ *and* $\phi_H(S)$ *are arithmetic progressions of common difference with both* $\phi_H(T_\emptyset)$ *and* $\phi_H(S_\emptyset)$ *initial terms in their respective progressions, or*

(III) $\phi_H(T) + \phi_H(S) = G/H$ *with* $|\phi_H(T)| + |\phi_H(S)| - 1 = |G/H|$

Moreover, the above conditions imply that $T_\emptyset + S_\emptyset$ is aperiodic, that $|T_\emptyset + S_\emptyset| = |T_\emptyset| + |S_\emptyset| - 1$, and that $\phi_H(T_\emptyset) + \phi_H(S_\emptyset)$ is a unique expression element in $\phi_H(T) + \phi_H(S)$.

The organization of the paper is the following. Section 2 develops the preliminaries, including the strong isoperimetric property. In Section 3, we prove a basic property of hyper-atoms. In Section 4, we describe T when S is H-quasi-periodic with $\phi_H(S)$ an arithmetic progression. In Section 5, we prove the $\frac{2n}{3}$-Theorem, which is the main isoperimetric consequence used to prove Theorem 1. In Section 6, we complete the proof of Theorem 1. In the last section, we investigate the strong isoperimetric property in more detail. In particular, we will give a variation valid in the non-abelian setting and with the hypothesis $|T| \geq k$ removed from Theorem 10.

2. Terminology and preliminaries

We recall the following result, which is a simple application of the pigeonhole principle.

Lemma B (Folklore [17] [5])**.** *Let G be a finite group and let A and B be subsets of G such that $|A| + |B| \geq |G| + t$, where $t \geq 1$ is a positive integer. Then every element of G has t distinct representations of the form $x + y$ with $x \in A$ and $x \in B$.*

We continue with an easy lemma.

Lemma 2. *Let G be a cyclic group generated by an element $d \in G$ and let $P \subseteq G$ be a finite arithmetic progression with difference d. Let X be a finite, nonempty subset of G. Then*

$$|X + P| \geq \min\{|G|, |X| + |P| - 1\}. \tag{1}$$

If $|X + P| = |X| + |P| - 1$ and $|P| \geq 2$, then X is an arithmetic progression with difference d if one of following holds:

(i) $|X + P| \leq |G| - 1$,

(ii) $|P| = 2$,

(iii) $X + P$ *contains a unique expression element $z = x + y$ with $x \in X$ and y either the first or last term of P, or*

(iv) $|X| \geq 3$ *and $X + P$ contains two unique expression elements.*

Proof. To prove (1), we may w.l.o.g. translate P so that its first term is 0. Then note that, if there is some $x \in X$ such that $x + id \notin X$ for $i \in [1, |P| - 1]$, then it follows that $|X + P| \geq$

$|(X+0)\cup(x+P)| = |X|+|P|-1$, while if this fails, then $X+P=G$ easily follows. Now assume that $|X+P| = |X|+|P|-1$ and $|P|\geq 2$.

Assume first that $|G| > |X+P|$. Since $|P|\geq 2$, we may w.l.o.g. take $P = \underbrace{\{0,d\}+\ldots+\{0,d\}}_{k}$, where $k = |P|-1 \geq 1$. In order to have $|X+P| = |X|+k$, we must have $|X+\{0,d\}| = |X|+1$ in view of (1). Hence X is an arithmetic progression with difference d.

Assume now that $X+P=G$, so that $|G| = |X+P| = |X|+|P|-1$. We may assume $|X|\geq 2$, else X is trivially an arithmetic progression with difference d, and now $|P| = |G|-|X|+1 \leq |G|-1$. If $|P| = 2$, then $|X| = |G|-1$, and hence X is an arithmetic progression with difference d. So we may assume $|P|\geq 3$. Now consider the case when $X+P$ contains a unique expression element $z = x+y$ with $x\in X$ and y either the first or last term of P. Then $P^* = P\setminus\{y\}$ is also an arithmetic progression with difference d and $|P^*| = |P|-1 \geq 2$. Moreover, $|X|+|P^*|-1 \leq |X+P^*| \leq |X+P|-1 = |X|+|P^*|-1 < |G|$, with the first inequality form (1), and now applying case (i) to $X+P^*$ completes the proof.

Finally, assume $|X|\geq 3$ and that $X+P$ contains two unique expression elements. Let $z=x+y$ with $x\in X$ and $y\in P$ be one of these unique expression elements. Letting $X^* = X\setminus\{x\}$, we see that $|X^*|+|P|-1 \leq |X^*+P| \leq |X+P|-1 = |X^*|+|P|-1 = |G|-1$. Thus $X^*+P = G\setminus\{z\}$ and, by case (i), we conclude that $X^* = X\setminus\{x\}$ is an arithmetic progression with difference d. Moreover, $|X^*| = |X|-1 \geq 2$. But now, since $|P|\geq 2$, it is easily seen that only unique expression elements in $X^*+P = G\setminus\{z\}$ are the first term of X^* added to the first term of P and the last term of X^* added to the last term of P. Since $X+P$ contains two unique expression elements, one of the unique expression elements from $X^*+P = G\setminus\{z\}$ must remain disjoint from $x+P$. However, it is easily seen that the only way this can be is if x either follows directly after the last term in X^* or directly before the first term in X^*. In either case, X is an arithmetic progression with difference d. □

The isoperimetric method is a global approach introduced by the author which derives additive inequalities from the properties of fragments and atoms. The reader may refer to the recent paper [11] for an introduction to the applications of this method as well as [5, Ch. 21].

Let S be a finite generating subset of an abelian group G with $0\in S$. For a subset $X\subseteq G$, we define the *boundary* of X as

$$\partial_S(X) = (X+S)\setminus X.$$

The boundary of X with respect to $-S$ will be written $\partial_S^-(X)$. We define the *co-image* of X as

$$\nabla_S(X) = G\setminus(X+S).$$

The co-image of X with respect to $-S$ will be written $\nabla_S^-(X)$. The references to S will often be omitted. A subset X with $|\nabla(X)|\geq|X|$ will be called *faithful* with respect to S. We remark that faithful subsets play an important role in the non-abelian case.

The next lemma is related to the notion of dual pairs and saturation (see [5, Exercise 7.3] [4] [2]), used in more rudimentary form by Vosper [19] and also Lee [15].

Lemma C. *Let S be a finite generating subset of an abelian group G with $0 \in S$. Let X be a subset of G. Then $\nabla_S^-(\nabla_S(X)) + S = X + S$.*

Proof. To show $X + S \subseteq \nabla^-(\nabla(X)) + S$, it suffices to show $X \subseteq \nabla^-(\nabla(X))$. However, if this fails, then there is some $x \in X$ with $x \notin G \setminus (\nabla(X) - S)$, which implies $x \in \nabla(X) - S$. Thus $x = d - s$ with $s \in S$ and $d \in \nabla(X) = G \setminus (X + S)$. But then $d = x + s \in X + S$, contradicting the definition of d. This establishes the inclusion

$$X + S \subseteq \nabla^-(\nabla(X)) + S.$$

If $\Big(\nabla^-(\nabla(X)) + S\Big) \cap \nabla(X) \neq \emptyset$, then there would be some $x \in \nabla(X)$ with $x = d + s$, where $s \in S$ and $d \in G \setminus (\nabla(X) - S)$. But then $d = x - s \in \nabla(X) - S$, contradicting the definition of d. Therefore

$$\Big(\nabla^-(\nabla(X)) + S\Big) \cap \Big(G \setminus (X + S)\Big) = \Big(\nabla^-(\nabla(X)) + S\Big) \cap \nabla(X) = \emptyset,$$

implying the reverse inclusion. □

We shall say that a finite subset $X \subseteq G$ induces a *k-separation* if $|X| \geq k$ and $|\nabla(X)| \geq k$, that is, $X \in \mathcal{S}_k(S)$. We shall say that S is k-separable if some finite $X \subseteq G$ induces a k-separation, that is, $\mathcal{S}_k(S) \neq \emptyset$.

Suppose that S is k-separable. The *k-th connectivity* of S is defined as

$$\kappa_k(S) = \min\{|\partial(X)| \ : \ \infty > |X| \geq k \text{ and } |\nabla(X)| \geq k\}.$$

Clearly $\kappa_1(S) \leq \ldots \leq \kappa_k(S)$.

- A finite subset $X \subseteq G$ such that $|X| \geq k$, $|\nabla(X)| \geq k$ and $|\partial(X)| = \kappa_k(S)$ is called a *k-fragment* of S.
- A k-fragment with minimum cardinality is called a *k-atom*.

It will be helpful to have in mind the following well-known lemma implicit in [9]. See also [5, Ch. 21].

Lemma 3. *Let S be a finite generating subset of an abelian group G with $0 \in S$. Suppose that S is k-separable and let F be a k-fragment of S. Then $-S$ is k-separable. Moreover, the following hold:*

(i) $\kappa_k(S) = \kappa_k(-S)$.
(ii) *If G is finite, then $\nabla(F)$ is a k-fragment of $-S$.*
(iii) *Any k-atom is faithful.*

Proof. Let $X \subseteq G$ be a nonempty subset. The inclusion $-S + G \setminus (X + S) \subseteq G \setminus X$ is readily verified by arguments similar to those used in Lemma C. But this implies

$$\partial^-(\nabla(X)) = \Big(-S+G\backslash(X+S)\Big)\backslash\Big(G\backslash(X+S)\Big) \subseteq \Big(G\backslash X\Big)\backslash\Big(G\backslash(X+S)\Big) = (X+S)\backslash X = \partial(X).$$

In particular, $-S$ is k-separable. Notice that we needed G to be abelian for the inclusion in the above argument. It is easily noted that if X is a k-fragment of S, then $-X$ will be a k-fragment of $-S$. Thus (i) follows.

Since F is a k-fragment, we have $|\nabla(F)| = |G\backslash(F+S)| \geq k$ and $|G\backslash\nabla(F)| = |F+S| \geq |F| \geq k$. As a result, it follows that

$$\kappa_k(S) = |\partial(F)| \geq |\partial^-(\nabla(F))| \geq \kappa_k(-S) = \kappa_k(S),$$

where the first equality and the second inequality follow from the definitions involved (since G finite implies $\nabla(F)$ is finite), the first inequality from the displayed equation above, and the final equality from part (i). Thus (ii) holds.

In order to show (iii), we may assume that G is finite. Let A be a k-atom of S and let A' be a k-atom of $-S$. It follows from the definitions that $-F$ is a k-fragment of $-S$ if F is a k-fragment of S. Thus $|A| = |A'| \leq |\nabla(A)|$, with the inequality following from (ii). □

Notice that (i) can fail for infinite non-abelian groups and that (iii) can fail for finite non-abelian groups.

We shall say that S is a *Vosper subset* if, for all finite $X \subseteq G$ with $|X| \geq 2$, we have $|X + S| \geq \min\{|G| - 1, |X| + |S|\}$.

Let S be a k-separable subset. Notice that $\kappa_k(S)$ is the maximal integer such that, for every finite subset $X \subseteq G$ with $|X| \geq k$, we have

$$|X + S| \geq \min\Big(|G| - k + 1, |X| + \kappa_k(S)\Big). \tag{2}$$

Formula (2) is an immediate consequence of the definitions. We shall call (2) the *isoperimetric inequality*. The reader may use this formula as a definition of $\kappa_k(S)$.

Let us point out that S is 1-separable if and only if $S \neq G$. The following lemma, implicit in some previous papers, describes useful relations between κ_1 and κ_2.

Lemma 4. *Let S be a finite generating subset of an abelian group G with $0 \in S$ and let X be a subset of G. The following hold.*

(i) *If $S \neq G$, then $\kappa_1(S) \leq |\partial(\{0\})| = |S| - 1$.*
(ii) *If S is 2-separable and $\kappa_2 \leq |S| - 1$, then $\kappa_2 = \kappa_1$.*
(iii) *Suppose that S is 1-separable and $\kappa_1 \leq |S| - 2$. Then S is 2-separable. Moreover X is a 1-fragment (resp. 1-atom) of S if and only if X is a 2-fragment (resp. 2-atom) of S.*

Proof. Note that (i) is obvious. Assume that $\kappa_2 > \kappa_1$ and take a 1-atom A of S. Then $|S| - 1 \geq \kappa_2 > \kappa_1 = |A + S| - |A|$. It follows that $|A| \geq 2$. Since A is faithful by Lemma 3(iii), we have $|\nabla(A)| \geq |A| \geq 2$. Thus $\kappa_2 \leq |A + S| - |A| = \kappa_1$, a contradiction. The proof

of (iii) follows by a similar argument. The only potential difficulty is in showing there is no 1-fragment F with $\kappa_1(S)+|F|=|F+S|=|G|-1$. However, if this were the case, then $|S|+|F|-1\geq \kappa_1(S)+|F|+1=|G|$, whence Lemma B give $F+S=G$, which is not possible for a 1-fragment F. □

The basic intersection theorem is the following.

Theorem 5. [9] [11] [5, Theorem 21.1] *Let S be a finite generating subset of an abelian group G with $0\in S$. Let A be a k-atom of S and let F be a k-fragment of S such that $|A\cap F|\geq k$. Then $A\subseteq F$. In particular, distinct k-atoms intersect in at most $k-1$ elements.*

The structure of 1-atoms is the following.

Proposition 6. [7] [6] *Let S be a finite generating subset of an abelian group G with $0\in S$ and $S\neq G$. Let H be a 1-atom of S with $0\in H$. Then H is a subgroup. Moreover, $\kappa_1(S)\geq \frac{|S|}{2}$.*

Proof. Take $x\in H$. Since $x\in (H+x)\cap H$ and since $H+x$ is a 1-atom, we have $H+x=H$ by Theorem 5. Therefore H is a subgroup, which must be proper in view of $|H+S|<|G|$ (from the definition of a 1-atom). Thus, since S generates G, we have $|H+S|\geq 2|H|$, and hence $\kappa_1(S)=|H+S|-|H|\geq \frac{|H+S|}{2}\geq \frac{|S|}{2}$. □

Recently, Balandraud introduced some isoperimetric objects and proved a strong form of Kneser's Theorem using Proposition 7.

Proposition 7. [7] [6] *Let S be a finite subset of an abelian group G with $0\in S$. Suppose $H=\langle S\rangle$. Let T be a subset of G, let $T=\biguplus_{\alpha\in I}T_\alpha$ be the H-coset decomposition of T, and let $\mathcal{V}\subseteq I$ be those $\alpha\in I$ with $|T_\alpha+S|<|H|$. Then*

$$\begin{aligned}|T+S| &\geq (|\phi_H(T)|-|\mathcal{V}|)|H|+\sum_{\alpha\in\mathcal{V}}|T_\alpha|+|\mathcal{V}|\frac{|S|}{2} \\ &\geq |T|+|\mathcal{V}|\frac{|S|}{2}.\end{aligned} \tag{3}$$

Proof. For every $\alpha\in\mathcal{V}$, Proposition 6 gives

$$|T_\alpha+S|=|(T_\alpha-\alpha)+S|\geq |T_\alpha-\alpha|+\kappa_1\geq |T_\alpha|+\frac{|S|}{2}.$$

Now (3) follows since $T+S=\bigcup_{\alpha\in I}(T_\alpha+S)$ is the H-coset decomposition of $T+S$ and $|\phi_H(T)|=|I|$. □

We will only need the following theorem in the case when $\kappa_2(S)\leq |S|-1$, for which it may be found (in various forms) in [8] [10] [11]. We give a more general result here using the results from [5, Ch. 21].

Theorem 8 (Grynkiewicz)**.** *Let S be a finite generating subset of an abelian group G with $0 \in S$. Suppose that S is 2-separable and let X be a 2-atom with $0 \in X$. Then either X is a subgroup or*

$$|X| \le \kappa_2(S) - |S| + 3.$$

In particular, if $\kappa_2(S) \le |S| - 2$, then X is a subgroup, and if $\kappa_2(S) \le |S| - 1$, then either X is a subgroup or $|X| = 2$.

Proof. If $\kappa_2(S) \le |S| - 2$, then $\kappa_1(S) \le |S| - 2$ in view of $\kappa_1(S) \le \kappa_2(S)$. Thus Lemma 4 implies that any 2-atom X is also a 1-atom, and now Proposition 6 implies that X is a subgroup. Therefore we now assume $\kappa_2(S) \ge |S| - 1$, so that $\kappa_2(S) - |S| + 3 \ge 2$. In particular, we may also assume $|X| \ge 3$, else the proof is complete.

Assume X is not a subgroup. Then [5, Proposition 21.8] implies that X is a Sidon set: $|X - X| = |X|^2 - |X| + 1$. Let $H = \langle X \rangle$ and observe that

$$|H| \ge |X - X| = |X|^2 - |X| + 1 \ge 2|X| + 1 \ge |X| + 4, \tag{4}$$

where we have made free use of $|X| \ge 3$ above. Let $S = \biguplus_{\alpha \in I} S_\alpha$ be the H-coset decomposition of S. If $|S_\alpha| = 1$ for some $\alpha \in I$, then all elements of $X + S_\alpha$ are unique expression elements. In this case, letting $X^* = X \setminus \{x\}$ for some $x \in X$, we have $\kappa_2(S) = |X + S| - |X| \ge |X^* + S| - |X^*|$ with $|X^*| = |X| - 1 \ge 2$. Hence $|X^*|$ contradicts the minimality of $|X|$ for the 2-atom X. Therefore, we instead assume $|S_\alpha| \ge 2$ for every $\alpha \in I$, in which case [5, Corollary 21.1] implies

$$|X + S_\alpha| \ge \min\{|H| - 1,\, |S_\alpha| + 2|X| - 3\}$$

for all $\alpha \in I$.

If $|X + S_\alpha| \ge |S_\alpha| + 2|X| - 3$ for some $\alpha \in I$, then

$$|X + S| = \sum_{\beta \in I \setminus \{\alpha\}} |X + S_\beta| + |X_\alpha + S| \ge \sum_{\beta \in I \setminus \{\alpha\}} |S_\beta| + |S_\alpha| + 2|X| - 3 = |S| + 2|X| - 3.$$

Since $|X + S| - |X| = \kappa_2(S)$, the above inequality yields $|X| \le \kappa_2(S) - |S| + 3$, as desired. Therefore we may instead assume $|X + S_\alpha| \ge |H| - 1$ for every $\alpha \in I$.

If $|X + S_\alpha| = |H| - 1$ and $|X + S_{\alpha'}| = |H| - 1$ for some distinct α', $\alpha \in I$, then Lemma B implies that $|S_\alpha| + |X| \le |H|$ and $|S_{\alpha'}| + |X| \le |H|$. It follows that

$$|X + S| = \sum_{\beta \in I \setminus \{\alpha, \alpha'\}} |X + S_\beta| + |X_\alpha + S| + |X_{\alpha'} + S| \ge \sum_{\beta \in I \setminus \{\alpha, \alpha'\}} |S_\beta| + 2|H| - 2 \ge |S| + 2|X| - 2,$$

and the proof is complete as before. Therefore we can assume there is at most one $\alpha \in I$ with $|X + S_\alpha| = |H| - 1$, while $|X + S_\alpha| = |H|$ for all other $\beta \in I \setminus \{\alpha\}$. In particular,

$$|H + S| = |H + X + S| \le |X + S| + 1. \tag{5}$$

As a result, since $|X+S| \leq |G|-2$ (as X is a 2-fragment), there must be some H-coset disjoint from $H+S$, whence $|H+S| \leq |G|-|H| \leq |G|-2$. We also have $|H| \geq 2$ and

$$|H+S|-|H| \leq |X+S|+1-|H| \leq |X+S|-|X|-3 = \kappa_2(S)-3,$$

with the first inequality from (5) and the second from (4), which contradicts that X is a 2-fragment of S, completing the proof. □

Corollary 9 ([8] Theorem 4.6)**.** *Let S be a finite generating subset of an abelian group G with $0 \in S$. Suppose that S is 2-separable, $|S| \leq (|G|+1)/2$ and $\kappa_2(S) \leq |S|-1$.*

If S is not an arithmetic progression, then there is a subgroup H which is a 2-fragment of S.

Proof. Suppose that S is not an arithmetic progression and let H be a 2-atom with $0 \in H$. If $\kappa_2(S) \leq |S|-2$, then Theorem 8 implies that H is a subgroup, and the result holds. Assume now that

$$\kappa_2(S) = |S|-1.$$

In view of Theorem 8, it is enough to consider the case $|H|=2$, say $H=\{0,x\}$. Then $\kappa_2(S) = |S|-1$ implies that $|S+H| = |S|+|H|-1 = |S|+1$, which is only possible if $S = S_0 \uplus S_\emptyset$ with S_0 an N-periodic subset and $S_\emptyset \neq \emptyset$ an arithmetic progression with difference x, where $N=\langle x\rangle$. We must have $S_0 \neq \emptyset$, since otherwise S would be an arithmetic progression. In particular, N is finite and proper. There must an N-coset disjoint from S, as otherwise $|S| \geq (|G/N|-1)|N|+|S_\emptyset| \geq |G|-|N|+1 \geq \frac{1}{2}|G|+1$, contrary to hypothesis. Thus $|N+S| \leq |G|-|N| \leq |G|-2$. Consequently, by the definition of κ_2 and the structure of S, we have

$$\begin{aligned} |S|-1 = \kappa_2(S) &\leq |N+S|-|N| \\ &= |S|+|N|-|S_\emptyset|-|N| \\ &\leq |S|-1, \end{aligned}$$

and hence N is a 2-fragment. □

Corollary 9 was used to solve Lewin's Conjecture on the Frobenius number [10]. Corollary 9 coincides with [8, Theorem 4.6]. A special case of this result is Theorem 6.6 of [10]. As mentioned in [12], there was a misprint in this last statement. Indeed $|H|+|B|-1$ should be replaced by $|H|+|B|$ in case (iii) of [10, Theorem 6.6].

Alternative proofs of Corollary 9 using Kermperman's Structure Theorem (with $|S| \leq |G|/2$ replacing $|S| \leq (|G|+1)/2$) were obtained by Grynkiewicz in [3] and Lev in [16]. In the present paper, Corollary 9 will be one of the pieces leading to the proof of Kemperman's Theorem.

We need the following consequence of Menger's Theorem proved in [11]. Proposition 10 follows from [11, Corollary 32] by the same argument used to prove [11, Proposition 33]. In fact, it is simply an immediate consequence of [11, Corollary 32] and should be compared with [11, Proposition 33]. We remark that the condition $|\phi_H(T)| \geq |\phi_H(S)|-1$ is missing from the hypotheses of [11, Proposition 33]. Just like the condition $|T| \geq k$ in Proposition 10, it is clearly

needed. It was left off the statement of [11, Proposition 33] as an oversight, and it should be $X = X_0 \cup \ldots \cup X_t$ as well in the statement of [11, Proposition 33].

Proposition 10. [11] *Let $k \geq 0$ be an integer and let S and T be finite, nonempty subsets of the abelian group G such that $0 \in S$,*

$$\kappa_1(S) \geq k, \quad k + |T| \leq |G| \qquad \text{and} \qquad |T| \geq k.$$

Then there is a subset $X \subseteq T$ with $|X| = k$ and $s_x \in S$ for each $x \in X$ such that

$$\{x + s_x : x \in X\} \subseteq (T + S) \setminus T$$

is a set of $|X| = k$ distinct elements.

Note the s_x need not be distinct in Proposition 10 and that the proposition is rather trivial unless $\langle S \rangle = G$ (as otherwise $\kappa_1(S) = 0$). We call the property given in Proposition 10 the *strong isoperimetric property*. Let $H \leq G$ be a subgroup and let $T = \biguplus_{\alpha \in I_T} T_\alpha$, $S = \biguplus_{\beta \in I_S} S_\beta$ and $T + S = \biguplus_{\gamma \in J} C_\gamma$ be the corresponding H-coset decompositions of T, S and $T + S$. If $|\phi_H(T) + \phi_H(S)| = |J|$ is large, then the number of H-components in $T + S$ is large, but this may not be enough to show that $|T + S|$ is large. It is conceivably possible that T and S have a small number of H-components that are each very small in size (for instance, of size 1), while at the same time many H-components in $T + S$ are simply of the from $T_\alpha + S_\beta$ with both T_α and S_α one of these small components. Then, even though $T + S$ has many H-components, too many of these components would be unreasonably small, un-naturally reducing the size of $T + S$ due to this skewed distribution of sums in $\phi_H(T) + \phi_H(S)$. Applying the strong isoperimetric property in G/H to $\phi_H(S)$ and $\phi_H(T)$ shows that this is not possible.

We will investigate the strong isoperimetric property in more detail in Section 7 with additional details given there, including a proof of a more general version of Proposition 10 as well as a version valid without the restriction $|T| \geq k$.

3. Hyper-atoms

In this section, we investigate the new notion of a hyper-atom. Let S be a generating subset of an abelian group G with $0 \in S$. Recall that, in view of the isoperimetric inequality (2), S is a Vosper subset if and only if S is not 2-separable or $\kappa_2(S) \geq |S|$.

Lemma 11. *Let S be a finite generating subset of an abelian group G with $0 \in S$. Suppose S is Vosper and let $X \subseteq G$ be a subset with $|X| \geq |S|$ and $|X + S| = |X| + |S| - 1$. Then, for every $y \in S$, we have $|X + (S \setminus \{y\})| \geq |X| + |S| - 2$.*

Proof. The result clearly holds if $|S| \leq 2$. So we may assume that $|S| \geq 3$. By the definition of a Vosper subset, we have $|X + S| \geq |G| - 1$. Assume first that $|X| = 3$ and hence $|S| = 3$. Then the result holds unless $|X + S \setminus \{y\}| = |X|$. Assuming the last equality, then X is a coset of some subgroup H of order $|H| = |X| = 3$. Now either S is also an H-coset, in which case

$X+S\setminus\{y\}=X+S$ follows trivially, or else $|\phi_H(S)|\geq 2$, in which case $|X+S|\geq 2|X|=6$, contradicting that $|X+S|=|X|+|S|-1=5$. So we may assume that $|X|\geq 4$.

Suppose that $|X+S\setminus\{y\}|\leq |X|+|S|-3$ and take a 2-subset R of $(X+S)\setminus(X+S\setminus\{y\})$. We have $R-y\subseteq X$. Also $X\setminus(R-y)+S\subseteq (X+S)\setminus R$. Thus $|X\setminus(R-y)+S|\leq |X|+|S|-3\leq |G|-2$, contradicting the definition of a Vosper subset in view of $|X|\geq 4$. □

Let us prove a lemma about fragments in quotient groups. See also [5, Proposition 21.5].

Lemma 12. *Let G be an abelian group and let S be a finite generating subset with $0\in S$ and $S\neq G$. Let H be a subgroup which is a 1-fragment. Then H is faithful and*

$$\kappa_1(\phi_H(S))=|\phi_H(S)|-1. \tag{6}$$

Let K/H be a subgroup which is a 1-fragment of $\phi_H(S)$, where $H\leq K\leq G$, and assume that K is a nontrivial subgroup. Then K is a 2-fragment of S.

Proof. Since $|G|>|H+S|$, so that $|G|-|H|\geq |H+S|$, we have $|\nabla(H)|=|G|-|H+S|\geq |H|$. Hence H is faithful. Since $|H+S|<|G|$ with $H+S$ being H-periodic, we have $\phi_H(S)\neq G/H$, and hence $\phi_H(S)$ is 1-separable. Put $|\phi_H(S)|=u+1$, so $\kappa_1(S)=u|H|$.

Let $\phi_H(X)\subseteq G/H$, where $X\subseteq G$ with $H+X=X$, be such that $\phi_H(X)+\phi_H(S)\neq G/H$. Clearly $H+X+S=X+S\neq G$. Then

$$|\phi_H(X)+\phi_H(S)||H|=|X+S|\geq |X|+\kappa_1(S)=|X|+u|H|=|\phi_H(X)||H|+u|H|.$$

Hence $\kappa_1(\phi_H(S))\geq u=|\phi_H(S)|-1$. The reverse inequality is obvious and follows by Lemma 4(i). This proves (6).

Let K/H be a subgroup which is a 1-fragment of $\phi_H(S)$, where $H\leq K\leq G$. Then (6) implies $|G/H|-|K/H|\geq |K/H+\phi_H(S)|=|K/H|+\kappa_1(\phi_H(S))=|K/H|+u$. Thus

$$|G|-|K|\geq |K+S|=|H+K+S|=|H|(|K/H+\phi_H(S)|)=|K|+u|H|=|K|+\kappa_1(S).$$

Hence the nontrivial subgroup K shows that S is 2-separable with $\kappa_2(S)\leq\kappa_1(S)$. As $\kappa_1(S)\leq\kappa_2(S)$ holds trivially, it follows that $\kappa_2(S)=\kappa_1(S)$ with K a 2-fragment. □

Let S be a finite generating subset of an abelian group G with $0\in S$ and $S\neq G$. Proposition 6 states that there is a 1-atom of S which is a subgroup. A maximal cardinality subgroup which is a 1-fragment will be called a *hyper-atom* of S. This definition may be adapted to non-abelian groups. As we shall see, the hyper-atom is more closely related to the critical pair theory than the 2-atom.

Theorem 13. *Let S be a finite generating subset of an abelian group G with $0\in S$. Suppose S is 2-separable,*

$$|S|\leq (|G|+1)/2 \qquad \textit{and} \qquad \kappa_2(S)\leq |S|-1.$$

Let H be a hyper-atom of S. Then $\phi_H(S)$ is either an arithmetic progression or a Vosper subset.

Proof. By Lemma 4, $\kappa_2(S) = \kappa_1(S)$. Let us show that

$$2|\phi_H(S)| - 1 \le |G/H|. \tag{7}$$

Clearly, we may assume that G is finite. Observe that $2|S+H| - 2|H| = 2\kappa_1 \le 2|S| - 2 < |G|$, with the first inequality from Lemma 4(i) and the second by hypothesis. It follows, since $|S+H|$ is a multiple of $|H|$, that $2|S+H| \le |G| + |H|$, and hence (7) holds.

Suppose now that $\phi_H(S)$ is not a Vosper subset. By the definition of a Vosper subset, it follows that $\phi_H(S)$ is 2-separable and $\kappa_2(\phi_H(S)) \le |\phi_H(S)| - 1$. Thus Lemma 4 implies that $\kappa_2(\phi_H(S)) = \kappa_1(\phi_H(S))$.

Observe that $\phi_H(S)$ cannot have a 2-fragment M/H which is a nontrivial subgroup, where $H < M \le G$. Otherwise, M/H will be a 1-fragment of $\phi_H(S)$ in view of $\kappa_2(\phi_H(S)) = \kappa_1(\phi_H(S))$, whence Lemma 12 implies that M is a 2-fragment of S strictly containing H, and thus also a 1-atom of S in view of $\kappa_1 = \kappa_2$, contradicting the maximality of H. In consequence, (7) and Corollary 9 imply that $\phi_H(S)$ is an arithmetic progression. □

Theorem 13 implies a result proved by Plagne and the author [12] and some extensions of it, proved using Kermperman's Theory, obtained by Grynkiewicz in [3] and Lev in [16]. The two main new facts in Theorem 13 are the following:

- The subgroup H in Theorem 13 is well described as a hyper-atom.
- The equality $|H+S|-|H| = \kappa_1$ is more precise than the inequality $|H+S| \le |H|+|S|-1$ in the previous results. This equality will be needed later.

4. Pairs involving a quasi-periodic modular progression

We shall deal with sets not necessarily containing 0. The important group in the isoperimetric approach is

$$\langle S\rangle_* := \langle S - S\rangle,$$

which is the minimal subgroup $H \le G$ such that S is contained in an H-coset. It is easy to show that $\langle S\rangle = \langle S\rangle_*$ when S contains 0.

Lemma 14. *Let S and T be finite, nonempty subsets of an abelian group G such that*

$$T + S \text{ is aperiodic} \qquad \text{and} \qquad |T+S| = |T| + |S| - 1.$$

Then T has a $\langle S\rangle_*$-quasi-periodic decomposition with partial component $T_\emptyset \subseteq T$. Moreover, $T_\emptyset + S$ is aperiodic and $|T_\emptyset + S| = |T_\emptyset| + |S| - 1$.

Proof. By translation, we may w.l.o.g. assume $0 \in S \cap T$. The case $|S| = 1$ is trivial. Assume that $|S| \ge 2$ and put $H = \langle S\rangle_* = \langle S\rangle$. Let $T = \biguplus_{\alpha\in I} T_\alpha$ be the H-coset decomposition of T and let $\mathcal{V} \subseteq I$ be all those $\alpha \in I$ with $|T_\alpha + S| < |H|$. By (3),

$$|T+S| \ge |T| + |\mathcal{V}|\frac{|S|}{2}.$$

Consequently, since $T+S$ is aperiodic with H nontrivial, it follows that $|\mathcal{V}|=1$. Let $T_\emptyset \subseteq T$ be the H-component corresponding to $\mathcal{V}$. Since $T+S$ is aperiodic, $T_\emptyset + S$ must be aperiodic (as all other H-components are full by definition of $\mathcal{V}$). By Theorem A, $|T_\emptyset+S| \geq |T_\emptyset|+|S|-1$. Therefore,

$$|T|+|S|-1=|T+S|=\sum_{\alpha\in I\setminus\mathcal{V}}|T_\alpha+S|+|T_\emptyset+S|\geq \sum_{\alpha\in I\setminus\mathcal{V}}|T_\alpha|+|T_\emptyset|+|S|-1=|T|+|S|-1.$$

Thus we must have equality in all the above estimates. In particular, $|T_\emptyset+S|=|T_\emptyset|+|S|-1$ and $|T_\alpha+S|=|T_\alpha|$ for all $\alpha\in I\setminus\mathcal{V}$. However, by definition of $\mathcal{V}$, we have $|T_\alpha+S|=|H|$ for all $\alpha\in I\setminus\mathcal{V}$, and the result is now obvious. □

Lemma 15. *Let S be a finite generating subset of an abelian group G with $0\in S$. Let T be a finite, nonempty subset of G such that*

$$T+S \text{ is aperiodic} \qquad \text{and} \qquad |T+S|=|S|+|T|-1.$$

Suppose that S has an H-quasi-periodic decomposition with partial component $S_\emptyset\subseteq S$ such that $\phi_H(S)$ is an arithmetic progression with $\phi_H(S_\emptyset)$ the first term in $\phi_H(S)$. Then T also has an H-quasi-periodic decomposition with partial component $T_\emptyset\subseteq T$ such that

- *$\phi_H(S)$ and $\phi_H(T)$ are arithmetic progressions of common difference and*
- *$\phi_H(T_\emptyset)$ and $\phi_H(S_\emptyset)$ are each the first term in their respective arithmetic progression.*

Proof. If $|\phi_H(S)|=1$, then $S=S_\emptyset$ and $H=G$ (since $\langle S\rangle_*=G$ by hypothesis), and now the result is trivial. Therefore we may assume $|\phi_H(S)|\geq 2$, so that $S\setminus S_\emptyset\neq\emptyset$ with G nontrivial.

If H is trivial, then $T+S$ aperiodic implies that $|T+S|<|G|$, in which case the result follows from Lemma 2. Therefore we may assume H is nontrivial. Since $T+S\setminus S_\emptyset$ is H-periodic but $T+S$ is aperiodic, there must be at least one unique expression element in $\phi_H(T)+\phi_H(S)$ of the form $\phi_H(T_\emptyset)+\phi_H(S_\emptyset)$ with $T_\emptyset\subseteq T$ an H-component of T.

Let $|\phi_H(T)+\phi_H(S\setminus S_\emptyset)|=|\phi_H(T)|+|\phi_H(S\setminus S_\emptyset)|+u$ with $u\in\mathbb{Z}$. Then

$$\begin{aligned}(8)\qquad |T+S| &\geq |T+S\setminus S_\emptyset|+|T_\emptyset+S_\emptyset| = |H||\phi_H(T)+\phi_H(S\setminus S_\emptyset)|+|T_\emptyset+S_\emptyset|\\ &= |T+H|+|S\setminus S_\emptyset|+u|H|+|T_\emptyset+S_\emptyset|\\ &\geq |T+H|+|S\setminus S_\emptyset|+u|H|+|S_\emptyset|\end{aligned}$$

Since $|T+S|=|T|+|S|-1$, it follows that $u\leq -1$. However, since $\phi_H(S\setminus S_\emptyset)$ is an arithmetic progression—as $\phi_H(S_\emptyset)$ is the first term in the progression $\phi_H(S)$—Lemma 2 implies that $u\geq -1$. Thus

$$u=-1.$$

Suppose there is another H-component $T'_\emptyset\subseteq T$ such that $\phi_H(T'_\emptyset)+\phi_H(S_\emptyset)$ is a unique expression element in $\phi_H(T)+\phi_H(S)$. Then the estimate (8) can be improved by $|T'_\emptyset+S_\emptyset|$.

Moreover, we trivially have $|T'_\emptyset + S_\emptyset| \geq |T'_\emptyset| \geq |H| - (|T+H| - |T|)$. Thus we obtain

$$\begin{aligned} |T+S| &\geq |T+H| + |S \setminus S_\emptyset| - |H| + |T_\emptyset + S_\emptyset| + |T'_\emptyset + S_\emptyset| \\ &\geq |T+H| + |S \setminus S_\emptyset| - |H| + |S_\emptyset| + |H| - |T+H| + |T| = |T| + |S|, \end{aligned}$$

contrary to hypothesis. So we instead conclude that

$$T + S = (T + S \setminus S_\emptyset) \uplus (T_\emptyset + S_\emptyset).$$

In particular,

$$\begin{aligned} |\phi_H(T) + \phi_H(S)| &= |\phi_H(T) + \phi_H(S \setminus S_\emptyset)| + 1 = |\phi_H(T)| + |\phi_H(S \setminus S_\emptyset)| + u + 1 \\ &= |\phi_H(T)| + |\phi_H(S)| - 1. \end{aligned} \tag{9}$$

Also, since $T + S$ is aperiodic and $T + S \setminus S_\emptyset$ is H-periodic with H nontrivial, it follows that $T_\emptyset + S_\emptyset$ is aperiodic. Hence Theorem A implies $|T_\emptyset + S_\emptyset| \geq |T_\emptyset| + |S_\emptyset| - 1$, and now (8) yields

$$\begin{aligned} |T+S| &\geq |T+H| + |S \setminus S_\emptyset| - |H| + |T_\emptyset + S_\emptyset| \\ &\geq |T+H| + |S \setminus S_\emptyset| - |H| + |T_\emptyset| + |S_\emptyset| - 1 \\ &\geq |T \setminus T_\emptyset + H| + |T_\emptyset| + |S| - 1 \geq |T| + |S| - 1. \end{aligned}$$

In view of $|T + S| = |T| + |S| - 1$, we must have equality in all estimates used above. In particular, $|T \setminus T_\emptyset + H| = |T \setminus T_\emptyset|$, implying T has an H-quasi-periodic decomposition with partial component $T_\emptyset$. In view of (9), applying Lemma 2(iii) to $\phi_H(T) + \phi_H(S)$ implies that $\phi_H(T)$ is an arithmetic progression of the same difference. Moreover, since $|\phi_H(S)| \geq 2$, the only way $\phi_H(T_\emptyset) + \phi_H(S_\emptyset)$ can be a unique expression element in $\phi_H(T) + \phi_H(S)$ is if $\phi_H(T_\emptyset)$ is also the first term in $\phi_H(T)$, completing the proof. □

Lemma 16. *Let S and T be subsets of a finite abelian group G with $0 \in S \cap T$ and $\langle S \rangle = G$. Suppose*

$$T + S \text{ is aperiodic} \quad \text{and} \quad |T + S| = |S| + |T| - 1.$$

Then $\nabla_S(T) - S$ is aperiodic and $|\nabla_S(T) - S| = |\nabla_S(T)| + |S| - 1$.

Proof. Lemma C implies that $T + S = \nabla^-(\nabla(T)) + S = G \setminus (\nabla(T) - S) + S$ is aperiodic, whence the summand $G \setminus (\nabla(T) - S)$ is also aperiodic, and thus its complement $\nabla(T) - S$ too. Clearly $\nabla(T) - S = G \setminus (T + S) - S \subseteq G \setminus T$. Thus,

$$|\nabla(T) - S| \leq |G| - |T| = |G \setminus (T+S)| + |T+S| - |T| = |\nabla(T)| + |T| + |S| - 1 - |T| = |\nabla(T)| + |S| - 1.$$

On the other hand, since $\nabla(T) - S$ is aperiodic, Theorem A implies $|\nabla(T) - S| \geq |\nabla(T)| + |S| - 1$, so that equality must hold. □

5. The $\frac{2n}{3}$-Theorem

The following result encodes efficiently the critical pair theory.

Theorem 17. *Let S and T be finite subsets of a nontrivial abelian group G with $0 \in T \cap S$ and $\langle S\rangle = G$. Suppose $|S| \le |T|$, $T+S$ is aperiodic, and*

$$\frac{2|G|+2}{3} \ge |T+S| = |S|+|T|-1.$$

Let H be a hyper-atom of S. Then S and T have H-quasi-periodic decompositions with partial components $T_\emptyset \subseteq T$ and $S_\emptyset \subseteq S$ such that

- *$\phi_H(S)$ and $\phi_H(T)$ are both arithmetic progressions of common difference and*
- *$\phi_H(S_\emptyset)$ and $\phi_H(T_\emptyset)$ are each the first term in their respective progression.*

Furthermore, $T_\emptyset + S_\emptyset$ is aperiodic, $|T_\emptyset + S_\emptyset| = |T_\emptyset| + |S_\emptyset| - 1$, and $\phi_H(T_\emptyset) + \phi_H(S_\emptyset)$ is a unique expression element in $\phi_H(T) + \phi_H(S)$.

Proof. Since G is nontrivial with $\langle S\rangle_* = G$, we have

$$2 \le |S| \le \frac{|S|+|T|}{2} \le \lfloor \frac{2|G|+5}{6} \rfloor < \frac{|G|}{3}+1,$$

whence $|G| \ge 4$. Thus $|T| \ge |S| \ge 2$ with $|T+S| \le \frac{2|G|+2}{3} < |G|$.

Suppose S is an arithmetic progression. Then Lemma 2(i) implies that S and T are both arithmetic progressions of common difference. It remains to show that a hyper-atom for S must be trivial. Let H be a hyper-atom of S. Then, since $\langle S\rangle_* = G$ with S an arithmetic progression, and since $H+S \ne G$, we have $\kappa_1 = |H+S| - |H| = |H|(|\phi_H(S)|-1) = |H|(|S|-1)$. Thus Lemma 4(i) implies $|H| = 1$, as desired. So we now assume S is not an arithmetic progression. In particular, $|S| \ge 3$, so that $3 \le |S| < \frac{|G|}{3}+1 \le \frac{|G|+1}{2}$. Hence $|G| \ge 7$ and $|T+S| \le \frac{2|G|+2}{3} < |G|-1$. Thus the set $T \subseteq G$ shows that S is 2-separable with

$$\kappa_2(S) \le |S|-1.$$

By Theorem 13, we find that either $\phi_H(S)$ is an arithmetic progression or a Vosper subset. As a result, since S is not an arithmetic progression, and since S is 2-separable with $\kappa_2 \le |S|-1$, so that S is not a Vosper subset, we conclude that $|H| \ge 2$ with H also a 2-fragment of S. Since H must be proper (as $H+S \ne G$) and since $\langle S\rangle_* = G$, it follows that $|\phi_H(S)| \ge 2$. Let $\mathcal{C}_S$ be the set of H-components of S and let $\mathcal{C}_T$ be the set of H-components of T.

Choose an H-component S_+ of S with a maximal cardinality and an H-component S_- of $S \setminus S_+$ with minimal cardinality. If $|\phi_H(S)| \ge 3$, we also choose an H-component S_{+-} of $S \setminus (S_+ \cup S_-)$ with minimal cardinality. Without loss of generality, we shall assume that $0 \in S_+$.

From the definitions involved, we have

$$(|\phi_H(S)|-1)|H| = |H+S| - |H| = \kappa_1 = \kappa_2 \le |S|-1, \tag{10}$$

where the equality $\kappa_1 = \kappa_2$ follows as H is both a 1-fragment and a 2-fragment. In consequence, for any subset $\mathcal{X} \subseteq \mathcal{C}_S$, we have $\sum_{C\in\mathcal{X}}(|H| - |C|) \leq |H + S| - |S| \leq |H| - 1$. Thus

$$|\mathcal{X}| \max_{C\in\mathcal{X}} |C| \geq \sum_{C\in\mathcal{X}} |C| \geq |\mathcal{X}||H| - (|H| - 1) = (|\mathcal{X}| - 1)|H| + 1. \tag{11}$$

By an *internal* component, we shall mean an H-component of $T + S$ contained in $T + H$. The set of internal components of $T + S$ will denoted by $\mathcal{I}$. Note $|\mathcal{I}| = |\phi_H(T)|$. By an *external* component, we shall mean an H-component of $T + S$ disjoint from $T + H$. The set of external components of $T + S$ will denoted by $\mathcal{E}$. Let $\mathcal{F}$ denote the set of full internal components and let $\mathcal{V}$ denote the set of partially filled internal components. Clearly, we have

$$\mathcal{I} = \mathcal{V} \uplus \mathcal{F}.$$

Let $\mathcal{V}_T = \{C \cap T : C \in \mathcal{V}\}$. Observe that $\mathcal{V}_T$ is a subset of H-components of T, that $|\mathcal{V}| = |\mathcal{V}_T|$, and that $C + S_+$, for $C \in \mathcal{V}_T$, is a subset of some component of $T + S$ from $\mathcal{V}$. We shall use the following trivial observation without reference:

$$|C + S_+| < |H| \quad \text{for } C \in \mathcal{V}_T.$$

By (11), $|S_+| > \frac{|\mathcal{C}_S|-1}{|\mathcal{C}_S|}|H| \geq \frac{1}{2}|H|$, with the latter inequality in view of $|\mathcal{C}_S| = |\phi_H(S)| \geq 2$. Thus $\langle S_+\rangle_* = \langle S\rangle = H$. By (3),

$$|T + S| \geq \sum_{C\in\mathcal{F}} |H| + \sum_{C\in\mathcal{V}_T} |C + S_+| + \sum_{C\in\mathcal{E}} |C| \tag{12}$$

$$\geq |\mathcal{F}||H| + \sum_{C\in\mathcal{V}_T} |C| + |\mathcal{V}_T|\frac{|S_+|}{2} + \sum_{C\in\mathcal{E}} |C|. \tag{13}$$

From (10), we have $|\phi_H(T)||H| \geq |T| \geq |S| > \kappa_2(S) = (|\phi_H(S)| - 1)|H|$. Hence

$$|\phi_H(T)| \geq |\phi_H(S)|. \tag{14}$$

Since $\frac{|G|}{3} > |S| - 1 \geq \kappa_1 = |H + S| - |H| \geq |H|$, we must have

$$|G/H| \geq 4. \tag{15}$$

Claim 0: $|\phi_H(T)| + |\phi_H(S)| - 1 \leq |G/H|$.

Suppose the contrary:

$$|\phi_H(T)| + |\phi_H(S)| \geq |G/H| + 2.$$

Then, in view of Lemma B, every element of G/H has two distinct expressions as a sum from $\phi_H(T) + \phi_H(S)$. In particular,

$$|C| \geq |S_{+-}| \quad \text{for every } C \in \mathcal{E} \text{ when } |\phi_H(S)| \geq 3.$$

Observe that any internal component $C \in \mathcal{I}$ contains a set of the form $C_0 + S_+$ with $C_0 \in \mathcal{C}_T$ a component of T. In particular,

$$|C| \geq |S_+| \quad \text{for every } C \in \mathcal{I}.$$

Assume first that $|\phi_H(S)| = |\mathcal{C}_S| \geq 3$. Then (11) gives $|S_+| > \frac{|\mathcal{C}_S|-1}{|\mathcal{C}_S|}|H| \geq \frac{2|H|}{3}$. Also, (14) gives $2|\phi_H(T)| \geq |\phi_H(S)| + |\phi_H(T)| \geq |G/H| + 2$. By (11),

$$2|S_+| \geq |S_+| + |S_{+-}| \geq \frac{2(|S_+| + |S_{+-}| + |S_-|)}{3} \geq \frac{2(2|H|+1)}{3}.$$

Putting all the above estimates together, we have

$$\begin{aligned}
\frac{2|G|+2}{3} &\geq |T+S| = \sum_{C\in\mathcal{I}} |C| + \sum_{C\in\mathcal{E}} |C| \\
&\geq |\phi_H(T)|\,|S_+| + \big(|G/H| - |\phi_H(T)|\big)\,|S_{+-}| \\
&= \big(2|\phi_H(T)| - |G/H|\big)\,|S_+| + \big(|G/H| - |\phi_H(T)|\big)\,\big(|S_+| + |S_{+-}|\big) \\
&\geq \big(2|\phi_H(T)| - |G/H|\big)\frac{2|H|+1}{3} + 2\frac{2|H|+1}{3}\big(|G/H| - |\phi_H(T)|\big) \\
&= |G/H|\frac{2|H|+1}{3} = \frac{2|G|}{3} + \frac{1}{3}|G/H|.
\end{aligned}$$

Thus $|G/H| \leq 2$, contrary to (15).

Assume now that $|\phi_H(S)| = 2$. Then $|\phi_H(T)| + |\phi_H(S)| \geq |G/H| + 2$ forces

$$|\phi_H(T)| = |G/H|$$

and $\mathcal{E} = \emptyset$. Also, (11) gives $|S_+| > \frac{|\mathcal{C}_S|-1}{|\mathcal{C}_S|}|H| = \frac{1}{2}|H|$.

We must have $|\mathcal{V}_T| \leq 3$, since otherwise (13) gives $|T+S| \geq |T| + |\mathcal{V}_T|\frac{|S_+|}{2} \geq |T| + |S|$, a contradiction. We must have $|\mathcal{V}_T| \geq 3$, since otherwise (12) and (15) give

$$|T+S| \geq (|G/H|-2)|H| + 2|S_+| \geq (|G/H|-1)|H| + 1 = |G| - |H| + 1 \geq \frac{3|G|}{4} + 1,$$

contradicting that $|T+S| \leq \frac{2|G|+2}{3}$. Thus $|\mathcal{V}_T| = 3$. In particular, since $|\phi_H(T)| = |G/H| \geq 4$ by (15), we have $|\mathcal{C}_T| > |\mathcal{V}_T|$.

Since $|\phi_H(S)| = 2$, we have $S = S_+ \uplus S_-$. Since $|\phi_H(T)| = |G/H|$, since $G/H = \langle \phi_H(S)\rangle_* = \langle \phi_H(S_-)\rangle$, and since $|\mathcal{C}_T| > |\mathcal{V}_T|$, there is a component $T_0 \in \mathcal{C}_T \setminus \mathcal{V}_T$ such that $T_0 + S_- \subseteq V$ for some $V \in \mathcal{V}$. Consequently, Lemma B and the definition of $\mathcal{V}$ ensure that $|T_0| + |S_-| \leq |H|$. Moreover, since $T_0 \in \mathcal{C}_T \setminus \mathcal{V}_T$, we have $(|\mathcal{F}|-1)|H| + \sum_{C\in\mathcal{V}_T} |C| \geq |T| - |T_0|$. Thus (13) now gives

$$\begin{aligned}
|T+S| &\geq (|\mathcal{F}|-1)|H| + |H| + \sum_{C\in\mathcal{V}_T} |C| + \frac{3|S_+|}{2} \\
&\geq (|T| - |T_0|) + (|T_0| + |S_-|) + \frac{3|S_+|}{2} > |T| + |S|,
\end{aligned}$$

contradicting the hypothesis $|T+S| = |T| + |S| - 1$. The claim is proved.

Claim 1: $|\phi_H(T)+\phi_H(S)| = |\phi_H(T)|+|\phi_H(S)|-1$.

By Claim 0, (6) and (2), we have

$$|\phi_H(T)+\phi_H(S)| \ge \min\{|G/H|, |\phi_H(T)|+|\phi_H(S)|-1\} = |\phi_H(T)|+|\phi_H(S)|-1$$

and $\kappa_1(\phi_H(S)) = |\phi_H(S)|-1$.

Apply Proposition 10 to $\phi_H(S)$ and $\phi_H(T)$ in G/H using $k = |\phi_H(S)|-1$. Then there exists a subset of H-components $\mathcal{X} \subseteq \mathcal{C}_T$ with

$$|\mathcal{X}| = |\phi_H(S)|-1$$

and $S_X \in \mathcal{C}_S$ for each $X \in \mathcal{X}$ such that the $X+S_X \subseteq T+S$, for $X \in \mathcal{X}$, are all disjoint from each other and $T+H$ (as they are distinct modulo H and not contained in $\phi_H(T)$), i.e., with each

$$X+S_X \subseteq E_X$$

for some external H-component $E_X \in \mathcal{E}$. Define $u = |\phi_H(T)+\phi_H(S)|-|\phi_H(S)|-|\phi_H(T)|+1$. Then there are precisely u H-components $C \in \mathcal{E}$ besides those E_X with $X \in \mathcal{X}$. For each such H-component C of $T+S$, we have the trivial estimate $|C| \ge |S_-|$. Thus

$$\begin{aligned}
|T+S| &= \sum_{C\in\mathcal{I}}|C| + \sum_{C\in\mathcal{E}}|C| \ge \sum_{C\in\mathcal{C}_T}|C+S_+| + \sum_{X\in\mathcal{X}}|X+S_X| + u|S_-| \\
&= \sum_{C\in\mathcal{C}_T\setminus\mathcal{X}}|C+S_+| + \sum_{X\in\mathcal{X}}|X+S_X| + \sum_{X\in\mathcal{X}}|X+S_+| + u|S_-| \\
&\ge \sum_{C\in\mathcal{C}_T\setminus\mathcal{X}}|C| + \sum_{X\in\mathcal{X}}|X| + \sum_{X\in\mathcal{X}}|S_+| + u|S_-| \\
&= |T| + |\mathcal{X}||S_+| + u|S_-| = |T| + (|\phi_H(S)|-1)|S_+| + u|S_-|.
\end{aligned}$$

We must have $u \le 0$, since otherwise $|T+S| \ge |T|+(|\phi_H(S)|-1)|S_+|+|S_-| \ge |T|+|S|$, contrary to hypothesis. Thus $|\phi_H(T)+\phi_H(S)| \le |\phi_H(S)|+|\phi_H(T)|-1$, and as the other direction was already established, the claim follows.

Claim 2: If $|\phi_H(S)| \ge 3$, then there is at most one H-component $C \in \mathcal{E}$ with $|C| < |S_{+-}|$. In particular, $\sum_{C\in\mathcal{E}}|C| \ge |S_-| + \big(|\phi_H(S)|-2\big)|S_{+-}|$.

By Theorem 13, $\phi_H(S)$ is an arithmetic progression or a Vosper subset. In view of Claim 1, it suffices to show

$$|\phi_H(T)+\phi_H(S\setminus S_-)| \ge |\phi_H(T)|+|\phi_H(S)|-2. \tag{16}$$

In view of (14) and Claim 1, (16) follows by Lemma 11 if $\phi_H(S)$ is a Vosper subset. So suppose $\phi_H(S)$ is an arithmetic progression. If (16) fails, then Theorem A implies that $\phi_H(T)+\phi_H(S\setminus S_-)$ is periodic, so $K/H = \mathsf{H}\big(\phi_H(T)+\phi_H(S\setminus S_-)\big)$ is nontrivial, where $H \le K \le G$. Moreover, applying Theorem A modulo K yields

$$|G/H| > |\phi_H(T)+\phi_H(S\setminus S_-)| \ge |\phi_H(T)+K/H| + |\phi_H(S\setminus S_-)+K/H| - |K/H|, \tag{17}$$

with the first inequality from Claim 0 since (16) is assumed to fail. Thus, since $\phi_H(S)$ is an arithmetic progression with $\langle \phi_H(S)\rangle_* = G/H$, it follows that K/H is proper with either $|\phi_H(S\setminus S_-)+K/H| = |K/H||\phi_H(S\setminus S_-)|$ or $|\phi_H(S\setminus S_-)+K/H| = |G/H|-|K/H|$. In the former case, we have

$$|\phi_H(S\setminus S_-)+K/H| = |\phi_H(S\setminus S_-)| + \big(|K/H|-1\big)|\phi_H(S\setminus S_-)| \geq |\phi_H(S\setminus S_-)| + |K/H| - 1$$

in which case (17) yields (16). So instead assume $|\phi_H(S\setminus S_-)+K/H| = |G/H|-|K/H|$. Then (17) implies $\phi_H(T)$ is contained in a K/H-coset. In particular,

$$|K/H| \geq |\phi_H(T)| \geq |\phi_H(S)|$$

follows from (14). Recall that $\phi_H(T)+\phi_H(S\setminus S_-)$ is K/H-periodic. Thus, in view of (17), either $|\phi_H(T)+\phi_H(S\setminus S_-)| \geq 2|K/H| \geq |\phi_H(T)|+|\phi_H(S)|$ or $|\phi_K(T)| = |\phi_K(S\setminus S_-)| = |\phi_K(T+S\setminus S_-)| = 1$. The former case yields (16), as desired. In the latter case, since $\phi_H(S)$ is an arithmetic progression generating G/H with $K/H < G/H$ proper, it follows that $\phi_H(S_-)$ must be contained in a disjoint K/H-coset. In this case, we have $|\phi_H(T)+\phi_H(S)| = |\phi_H(T)+\phi_H(S_-)| + |\phi_H(T)+\phi_H(S\setminus S_-)| \geq 2|\phi_H(T)| \geq |\phi_H(T)|+|\phi_H(S)|$, with the final inequality from (14). Since this is contrary to Claim 1, the claim is complete.

Claim 3: If $|\phi_H(S)| \geq 3$, then $|\phi_H(T)|+|\phi_H(S)| \leq |G/H|-1$.

Assume that $|\phi_H(S)| \geq 3$. Let us begin by showing that

$$|\mathcal{F}| \geq 2. \tag{18}$$

Now

$$\sum_{C\in\mathcal{E}} |C| \geq |S_{+-}| + |S_-|$$

follows from Claim 2. By (11), we have

$$3|S_+| \geq |S_+| + |S_{+-}| + |S_-| \geq 2|H|+1,$$

and thus

$$|S_+| > \frac{2}{3}|H|.$$

By (11), we also have

$$|S_{+-}| + |S_-| \geq |H| + 1.$$

Since $|C+S_+| < |H|$ for $C \in \mathcal{V}_T$, Lemma B implies that $|C|+|S_+| \leq |H|$ for every $C \in \mathcal{V}_T$, in turn implying

$$|C| \leq |H| - |S_+| < |H| - \frac{2}{3}|H| = \frac{1}{3}|H| < \frac{1}{2}|S_+| \leq \frac{1}{2}|C+S_+| \quad \text{for every } C \in \mathcal{V}_T.$$

Combining the above estimates, we see that

$$\begin{aligned} 2|T| > |T+S| &\geq \sum_{C\in\mathcal{V}_T}|C+S_+| + \sum_{C\in\mathcal{F}}|C| + \sum_{C\in\mathcal{E}}|C| \\ &\geq \sum_{C\in\mathcal{V}_T} 2|C| + |\mathcal{F}||H| + |S_{+-}| + |S_-| \\ &\geq \sum_{C\in\mathcal{V}_T} 2|C| + (|\mathcal{F}|+1)|H| + 1 \end{aligned}$$

If $|\mathcal{C}_T \setminus \mathcal{V}_T| = |\mathcal{F}| \leq 1$, then $(|\mathcal{F}|+1)|H| \geq \sum_{C\in\mathcal{C}_T\setminus\mathcal{V}_T} 2|C|$ holds trivially, in which case the above estimate yields $2|T| > 2|T|$, a contradiction. Thus (18) is established.

We have, using (11),

$$|S_+| + |S_{+-}| \geq \frac{2}{3}(|S_-| + |S_{+-}| + |S_-|) \geq \frac{4|H|+2}{3}. \tag{19}$$

Recall that $|C| \geq |S_+|$ for any $C \in \mathcal{I}$. Consequently, it follows from (18) that $|\phi_H(T)| = |\mathcal{C}_T| = |\mathcal{I}| \geq |\mathcal{F}| \geq 2$ with

$$\sum_{C\in\mathcal{I}}|C| \geq 2|H| + \big(|\phi_H(T)|-2\big)|S_+|.$$

Combining the above estimates along with Claim 2, (14) and $|\phi_H(T)| \geq |\phi_H(S)| \geq 3$ (so that $|\phi_H(T)| + |\phi_H(S)| \geq 6$), it follows that

$$\begin{aligned} |T+S| &= \sum_{C\in\mathcal{I}}|C| + \sum_{C\in\mathcal{E}}|C| \\ &\geq 2|H| + \big(|\phi_H(T)|-2\big)|S_+| + \big(|\phi_H(S)|-2\big)|S_{+-}| + |S_-| \\ &= 2|H| + \big(|\phi_H(T)| - |\phi_H(S)|\big)|S_+| + \big(|\phi_H(S)|-3\big)\big(|S_+| + |S_{+-}|\big) \\ &\quad + \big(|S_+| + |S_{+-}| + |S_-|\big) \\ &\geq 2|H| + \big(|\phi_H(T)| - |\phi_H(S)|\big)\frac{2|H|+1}{3} + \frac{(4|H|+2)(|\phi_H(S)|-3)}{3} + 2|H| + 1 \\ &= \big(|\phi_H(T)| + |\phi_H(S)|\big)\frac{2|H|+1}{3} - 1 \geq \big(|\phi_H(T)| + |\phi_H(S)|\big)\frac{2|H|}{3} + 1, \end{aligned}$$

If the claim is false, we have $|\phi_H(T)| + |\phi_H(S)| \geq |G/H|$, in which case the above estimate yields $|T+S| \geq \frac{2|G|}{3} + 1$, contrary to hypothesis. This completes the claim.

Suppose that $\phi_H(S)$ is not an arithmetic progression. Then $|\phi_H(T)| \geq |\phi_H(S)| \geq 3$ (in view of (14)), and Theorem 13 implies that $\phi_H(S)$ is a Vosper subset. By Claim 1 and Claim 3, we have $|G/H| - 2 \geq |\phi_H(T) + \phi_H(S)| = |\phi_H(T)| + |\phi_H(S)| - 1$, contradicting the definition of a Vosper subset. So we instead conclude that $\phi_H(S)$ is an arithmetic progression with difference $\phi_H(d)$ for some $d \in S$. Consequently, by Lemma 2(i)(ii) and Claims 1 and 3, $\phi_H(T)$ is also an arithmetic progression with difference $\phi_H(d)$. Let

$$|\phi_H(S)| = s+1 \qquad \text{and} \qquad |\phi_H(T)| = t+1.$$

In view of Claim 1, let $S = \biguplus_{i=0}^{s} S_i$, $T = \biguplus_{i=0}^{t} T_i$ and $T+S = \biguplus_{i=0}^{s+t} E_i$ be the H-coset decompositions of T, S and $T+S$. Since $\phi_H(-d)$ is also a difference of $\phi_H(S)$, we may replace $\phi_H(d)$ by $\phi_H(-d)$ if need be, retranslate S to w.l.o.g. assume $0 \in S_0$, and choose an indexing such that

(1) $\phi_H(S_0), \cdots, \phi_H(S_s)$ is an arithmetic progression with difference $\phi_H(d)$ and $|S_0| \geq |S_s|$,
(2) $\phi_H(T_0), \cdots, \phi_H(T_t)$ is an arithmetic progression with difference $\phi_H(d)$, and
(3) $T_i + S_j \subseteq E_{i+j}$ for all $i \in [0,t]$ and $j \in [0,s]$.

Note that we no longer know $0 \in S_+$ as we have retranslated so that the first term S_0 now contains zero. The sets S_+, S_{+-} and S_- will no longer be needed. Let

$$I_{\mathcal{V}} = \{i \in [0,t] : |E_i| < |H|\} \qquad \text{and} \qquad I_{\mathcal{F}} = \{i \in [0,t] : |E_i| = |H|\}.$$

Since $|S_0| \geq |S_s|$, (11) implies that $|S_0| > \frac{1}{2}|H|$. Thus $\langle S_0 \rangle = \langle S_0 \rangle_* = H$, and now (3) yields

$$\begin{aligned} |T+S| &\geq \sum_{i \in I_{\mathcal{F}}} |E_i| + \sum_{i \in I_{\mathcal{V}}} |T_i + S_0| + \sum_{j=1}^{s} |T_t + S_j| \\ &\geq |T| + |I_{\mathcal{V}}| \frac{|S_0|}{2} + \sum_{j=1}^{s} |T_t + S_i|. \end{aligned}$$

Thus $|T| + |S| - 1 \geq |T+S| \geq |T| + |I_{\mathcal{V}}| \frac{|S_0|}{2} + |S \setminus S_0|$, implying

$$|I_{\mathcal{V}}| \leq 1.$$

Claim 4: $I_{\mathcal{V}} = \emptyset$.

Assume by contradiction that $I_{\mathcal{V}} = \{r\}$ for some $r \in [0,t]$. Observe that $|E_i| = |H|$ for $i \in [0,t] \setminus \{r\}$. Suppose first that $r < t$. Since $T_r + S_0 \subseteq E_r$ with $|E_r| < H$ by definition of $I_{\mathcal{V}}$, Lemma B implies that $|H| \geq |T_r| + |S_0|$. Since $T_r + S_0 \subseteq E_r$, we have $|E_r| \geq |S_0|$. Combining these estimates together yields

$$\begin{aligned} |T+S| &= \sum_{i=0}^{t} |E_i| + \sum_{j=t+1}^{s+t} |E_j| \geq \sum_{i=0}^{t} |E_i| + \sum_{j=1}^{s} |T_t + S_j| \\ &\geq |E_r| + t|H| + \sum_{j=1}^{s} |T_t + S_j| \\ &\geq |S_0| + |T_r| + |S_0| + (t-1)|H| + |T_t| + \sum_{j=1}^{s-1} |S_j| \\ &\geq |T| + |S| - |S_s| + |S_0| \geq |T| + |S|, \end{aligned}$$

where the final inequality follows in view of $|S_0| \geq |S_s|$ and the penultimate one in view of $r < t$ and $t = |\phi_H(T)| - 1$. However, this contradicts the hypothesis $|T+S| = |T| + |S| - 1$. So we now assume $r = t$.

Since $T_t + S_0 \subseteq E_t = E_r$ with $|E_r| < |H|$, Lemma B implies that $|H| \geq |T_t| + |S_0|$. Also, $|E_t| \geq |T_{t-1} + S_1| \geq |T_{t-1}|$ since (14) ensures that $t \geq s = |\phi_H(S)| - 1 \geq 1$. Hence

$$\begin{aligned} |T+S| &= \sum_{i=0}^{t} |E_i| + \sum_{j=t+1}^{s+t} |E_j| \geq \sum_{i=0}^{t} |E_i| + \sum_{j=1}^{s} |T_t + S_j| \\ &\geq t|H| + |E_t| + \sum_{j=1}^{s} |T_t + S_j| \\ &\geq |T_t| + |S_0| + (t-1)|H| + |T_{t-1}| + \sum_{j=1}^{s} |S_j|. \end{aligned}$$

However, in view $t = |\phi_H(T)| - 1$, the above estimate yields $|T+S| \geq |T| + |S|$, contrary to hypothesis. This completes Claim 4.

Claim 5: $|E_i| = |H|$ for all $i \leq s + t - 1$.

By Claim 4, we know $|E_i| = |H|$ for all $i \leq t$. Suppose to the contrary that there is some r with $|E_r| < |H|$ and $t + 1 \leq r \leq s + t - 1$. Since $(T_t + S_{r-t}) \cup (T_{t-1} + S_{r-t+1}) \subseteq E_r$ with $|E_r| < |H|$, Lemma B implies that $|H| \geq |T_t| + |S_{r-t}|$ and $|H| \geq |T_{t-1}| + |S_{r-t+1}|$. But now (11) yields

$$2|H| \geq |T_t| + |S_{r-t}| + |T_{t-1}| + |S_{r-t+1}| \geq |T_t| + |T_{t-1}| + |H| + 1.$$

Thus $|T + H| - |T| \geq 2|H| - (|T_t| + |T_{t-1}|) \geq |H| + 1$, implying

$$\begin{aligned} |T+S| &\geq \sum_{i=0}^{t} |E_i| + \sum_{j=1}^{s} |T_t + S_j| = |T+H| + \sum_{j=1}^{s} |T_t + S_j| \geq |T+H| + \sum_{j=1}^{s} |S_j| \\ &\geq |T| + |H| + 1 + |S| - |S_0| > |T| + |S|, \end{aligned}$$

where the equality follows from Claim 4. Since this contradicts the hypothesis $|T + S| = |T| + |S| - 1$, the claim is complete. Note we needed $r \leq s + t - 1$ to ensure S_{r-t+1} is a well-defined component of S (as S_j for $j \geq s + 1$ is not defined).

By Claim 5, E_{s+t} is the only H-component of $T + S$ that is not a full H-coset. Since $T + S$ is aperiodic with H nontrivial, this forces E_{s+t} to be aperiodic. Since $\phi_H(S)$ and $\phi_H(T)$ are arithmetic progressions with common difference generating G/H, it follows from Claim 1 that $T_t + S_s = E_{s+t}$. Since this sumset is aperiodic, Theorem A yields $|T_t + S_s| \geq |T_t| + |S_s| - 1$. Now we have

$$\begin{aligned} |S| + |T| - 1 = |T+S| &= \sum_{i=0}^{s+t-1} |E_i| + |E_{s+t}| = (t+s)|H| + |T_t + S_s| \\ &\geq t|H| + |T_t| + s|H| + |S_s| - 1 \\ &= (|\phi_H(T)| - 1)|H| + |T_t| + (|\phi_H(S)| - 1)|H| + |S_s| - 1 \\ &\geq |T| + |S| - 1. \end{aligned}$$

As a result, all estimates used above must be exact. In particular, $|T_t + S_s| = |T_t| + |S_s| - 1$, $|S \setminus S_s| = |\phi_H(S \setminus S_s)||H|$ and $|T \setminus T_t| = |\phi_H(T \setminus T_t)||H|$. The latter two estimates imply $S \setminus S_s + H = S \setminus S_s$ and $T \setminus T_t + H = T \setminus T_t$, meaning S and T are H-quasi-periodic with partial components $T_t \subseteq T$ and $S_s \subseteq S$. Also, $\phi_H(S)$ and $\phi_H(T)$ are arithmetic progressions with common difference such that $\phi_H(S_s)$ and $\phi_H(T_t)$ are the first term of their respective progression (replacing the difference $\phi_H(d)$ by $\phi_H(-d)$), and $\phi_H(T_t)+\phi_H(S_s)$ is a unique expression element in $\phi_H(T) + \phi_H(S)$ (as seen above or by noting that, otherwise, $T + S$ will be H-periodic with H nontrivial, contrary to assumption). This completes the proof. □

Notice that the subgroup in Theorem 17 depends only on the smaller set S, while the subgroup in Kemperman's Structure Theorem depends on S and T.

6. The Kemperman Structure Theorem

We now proceed to prove Kemperman's Structure Theorem.

Proof of Theorem 1. If $T \not\subseteq \langle S\rangle$, then $H = \langle S\rangle < G$ is a proper subgroup and Theorem 1 follows from Lemma 14 with $H = \langle S\rangle$ and condition (I) holding. Note $T \not\subseteq \langle S\rangle = H$ forces $|\phi_H(T)| \geq 2$ so that T having an H-quasi-periodic decomposition implies that T has some full H-component, which is only possible, since $|T|$ is finite, if $|H|$ is finite. This ensures that H is finite and proper, which is required in Theorem 1. Therefore we now assume $T \subseteq \langle S\rangle$ and thus $\langle S\rangle = \langle T+S\rangle = G$.

If $\langle T\rangle < G$ is a proper subgroup, then Lemma 14 implies that S is $\langle T\rangle$-quasi-periodic with necessarily two components (since $\langle T\rangle < G = \langle S\rangle$). Thus $|S| \geq |\langle T\rangle| + 1 \geq |T| + 1$, contrary to hypothesis. Therefore we may assume $\langle T\rangle = G$ as well.

Let $L = \langle \nabla_S(T)\rangle_*$. If G is finite and $L < G$ is a proper subgroup, then, since $\langle S\rangle = G$, Lemmas 16 and 14 imply that $-S$, and thus also S, is L-quasi-periodic, say with partial component $S_\emptyset \subseteq S$. Observing that $\nabla_T(S) = \nabla_S(T)$, we can repeat this argument using $\nabla_T(S)$ to find that T is also L-quasi-periodic with partial component $T_\emptyset \subseteq T$. It follows that $T + S$ is L-quasi-periodic. Our hypotheses ensure that $|L| \geq |\nabla_S(T)| = |G \setminus (T + S)| \geq 2$, so L is nontrivial. Consequently, since $T + S$ is aperiodic, it follows that $\phi_L(T_\emptyset) + \phi_L(S_\emptyset)$ is a unique expression element in $\phi_L(T_\emptyset)+\phi_L(S_\emptyset)$ and that $|T_\emptyset + S_\emptyset| < |L|$ with $T_\emptyset + S_\emptyset$ aperiodic. Thus, if $\phi_L(T)+\phi_L(S) \neq G/L$, then $\nabla_S(T) = G \setminus (T + S)$ will contain elements from two distinct L-cosets, contradicting that $L = \langle \nabla_T(S)\rangle_*$. Therefore $\phi_L(T)+\phi_L(S) = G/L$. If $|\phi_L(T)|+|\phi_L(S)| \geq |G/L|+2$, then Lemma B implies that all elements of $\phi_L(T) + \phi_L(S)$ have at least two representations, contradicting that $\phi_L(T_\emptyset) + \phi_L(S_\emptyset)$ is a unique expression element. Therefore $|\phi_L(T)| + |\phi_L(S)| \leq |G/L| + 1$. If this inequality is strict, then $|G/L| \geq |\phi_L(T)| + |\phi_L(S)|$, in turn implying $|\phi_L(T) + \phi_L(S)| = |G/L| \geq |\phi_L(T)| + |\phi_L(S)|$. Then, since $T + S$ is L-quasi-periodic, it follows that

$$\begin{aligned} |T + S| &= \big(|\phi_L(T) + \phi_L(S)| - 1\big)|L| + |T_\emptyset + S_\emptyset| \\ &\geq \big(|\phi_L(T)| + |\phi_L(S)| - 2\big)|L| + |L| + |T_\emptyset| + |S_\emptyset| - 1 \\ &\geq |T| + |S| + |L| - 1, \end{aligned} \tag{20}$$

where the second inequality makes use of Theorem A. Since this contradicts that $|T+S| = |T|+|S|-1$, we instead conclude that equality holds in the estimate: $|\phi_L(T)|+|\phi_L(S)| = |G/L|+1$. In this case, the calculation used to derive (20) instead yields $|T+S| \geq |T|+|S|-1$. As this estimate holds with equality, all estimates used in (20) must also hold with equality. In particular, $|T_\emptyset+S_\emptyset| = |T_\emptyset|+|S_\emptyset|-1$, and now Theorem 1 follows with $H = L < G$ and condition (III) holding (note L must be finite as T and S are finite L-quasi-periodic sets). So we may now assume

$$L = \langle \nabla_S(T) \rangle_* = G \quad \text{when } G \text{ is finite.} \tag{21}$$

Notice that $|S|+|T|+|\nabla_S(T)| = |S|+|T|+(|G|-|T+S|) = |G|+1$. We consider two cases.

Case 1: $|S| \leq |\nabla_S(T)|$.

Let $H \leq G$ denote a hyper-atom of S. Then $H < G$ is a finite, proper subgroup of G. Assume first that $|T| \leq |\nabla_S(T)|$. Then $|S|+|T| \leq \frac{2(|S|+|T|+|\nabla_S(T)|)}{3} = \frac{2|G|+2}{3}$. Applying Theorem 17 yields the desired conclusions of Theorem 1 with (II) holding.

Assume now $|T| > |\nabla_S(T)|$, and hence $|S|+|\nabla_S(T)| \leq \frac{2(|S|+|T|+|\nabla_S(T)|)}{3} = \frac{2|G|+2}{3}$ with $\nabla_S(T)$ and G finite. Applying Theorem 17 to $-\nabla_S(T)+S$ via Lemma 16, it follows that S has an H-quasi-periodic decomposition with partial component $S_\emptyset \subseteq S$ such that $\phi_H(S)$ is an arithmetic progression having $\phi_H(S_\emptyset)$ as its first term. By Lemma 15, T also has an H-quasi-periodic decomposition with partial component $T_\emptyset \subseteq T$ such that $\phi_H(T)$ is an arithmetic progression of the same difference with $\phi_H(T_\emptyset)$ the first term in the progression. The remaining conclusions of Theorem 1 with (II) holding are now all routinely verified, completing the case.

Case 2: $|S| > |\nabla_S(T)|$.

In this case, $|\nabla_S(T)|$ and G are finite. Let $x \in \nabla_S(T)$ and let $H \leq L = G$ denote a hyper-atom of $\nabla_S(T)-x$. Then $H < G$ is a finite, proper subgroup of G. We have $|\nabla_S(T)|+|S| \leq \frac{2(|S|+|T|+|\nabla_S(T)|)}{3} = \frac{2|G|+2}{3}$. Applying Theorem 17 to $-\nabla_S(T)+S$ via Lemma 16 and (21) (with $-\nabla_S(T)$ playing the role of S), it follows that S has an H-quasi-periodic decomposition with partial component $S_\emptyset \subseteq S$ such that $\phi_H(S)$ is an arithmetic progression having $\phi_H(S_\emptyset)$ as its first term. Now Theorem 1 follows with (II) holding as argued at the end of Case 1, completing the case and proof. □

Our proof of Theorem 1 sheds some light on the quasi-period H occurring in dual formulation of Kemperman's Structure Theorem. As the proof above shows, if $X \in \{S, T, \nabla_S(T)\}$ is a set with minimal cardinality, then the quasi-period H in the dual form of Kemperman's Theorem is either equal to $\langle X \rangle_*$ (if this is a proper subgroup of G) or to a hyper-atom of X (when $\langle X \rangle_* = G$).

7. The strong isoperimetric property

In this section, we shall assume some familiarity with digraphs. We shall also assume that the reader is aware of the definition of κ_1 in the non-abelian case and its relation with the corresponding notion in Cayley digraphs. These questions are explained in [11]. The reader not interested in non-abelian groups can restrict themselves to the abelian case, where all notions are defined in the present paper.

Let V be a set and let $E \subseteq V \times V$. The relation $\Gamma = (V, E)$ will be called a *digraph*. The elements of V are called *vertices*. The elements of E are called *arcs*. The digraph Γ is said to be *reflexive* if $\{(x, x) : x \in V\} \subseteq E$. Let $a \in V$ and let $A \subseteq V$. The image of a is by definition

$$\Gamma(a) = \{x : \ (a, x) \in E\}.$$

The image of A is by definition

$$\Gamma(A) = \bigcup_{x \in A} \Gamma(x).$$

The *valency* or *out-degree* of x is by definition $\mathsf{d}_\Gamma(x) = |\Gamma(x)|$. We shall say that Γ is *locally finite* if $\mathsf{d}_\Gamma(x)$ is finite for all $x \in V$.

For $X \subseteq V$, the *boundary* of X is by definition

$$\partial_\Gamma(X) = \Gamma(X) \setminus X.$$

For an integer $k \geq 1$, the *k-th connectivity* of Γ is defined as

$$\kappa_k(\Gamma) = \min\{|\partial(X)| : \quad \infty > |X| \geq k \quad \text{and} \quad |V \setminus \Gamma(X)| \geq k\}. \tag{22}$$

The digraph Γ is said to be *k-separable* if the set that the minimum is take over in (22) is nonempty.

Given a multiplicatively written group G and a finite subset $S \subseteq G$ with $1 \in S$, we define the Cayley digraph Γ_S by letting G be the vertices of Γ_S with $(x, y) \in G \times G$ an arc when $y \in xS$. Then Γ_S is a locally finite, reflexive digraph. Moreover, if $T \subseteq G$, then

$$\Gamma_S(T) = TS = \{ts : \ t \in T, \ s \in S\} \qquad \text{and} \qquad \partial(T) = TS \setminus T.$$

With these definitions, it becomes clear that all isoperimetric notions defined for the set $S \subseteq G$ coincide with the those for the Cayley digraph defined by S, e.g., $\kappa_k(S) = \kappa_k(\Gamma_S)$. The digraph setting is the more general one. The reader may refer to [11] for a further discussion. By a directed path from a vertex x to a vertex y, we shall mean a finite sequence of arcs $(x, y_1), (y_1, y_2), \ldots, (y_k, y)$ with the vertices encountered all distinct. Let $\Gamma = (V, E)$ be a digraph. Two directed paths from x to y are said to be disjoint if their only common vertices are x and y: more formally, if $y_i = y'_j$ implies either $y_i = y'_j = x$ or $y_i = y'_j = y$, where $(x, y'_1), (y'_1, y'_2), \ldots, (y'_{k'}, y)$ is the second path. The following is a special case of the Erdős-Menger Conjecture, resolved recently in [1]. We only need the much simpler case when $|V|$ is finite [18].

Theorem 18 (Erdős-Menger Conjecture [1])**.** *Let $\Gamma = (V, E)$ be a digraph and let k be a nonnegative integer. Let $x, y \in V$ be vertices such that $(x, y) \notin E$ and*

$$|\partial(X)| \geq k \quad \text{for every subset } X \subseteq V \text{ with } x \in X \text{ and } y \notin X \cup \Gamma(X).$$

Then there are k disjoint directed paths from x to y.

Proposition 19 (The Strong Isoperimetric Property for Graphs I)**.** *Let $\Gamma = (V, E)$ be a locally finite digraph, let $X \subseteq V$ be a finite, nonempty subset, and let k and s be positive integers such that*

$$\kappa_k(\Gamma) \geq s, \quad |V| \geq |X| + s + k - 1, \qquad \text{and} \qquad |X| \geq s + k - 1.$$

Then there are distinct vertices $x_1, \ldots, x_s \in X$ and distinct vertices $y_1, \ldots, y_s \in \partial(X)$ such that

$$(x_i, y_i) \in E \quad \text{for every } i \in [1, s].$$

Proof. Take elements α and β not contained in V and set $\hat{V} = X \cup \partial(X) \cup \{\alpha, \beta\}$, which is finite since Γ is locally finite and X is finite. We define a digraph $\hat{\Gamma}$ on $\hat{V}$ as follows:

- $\hat{\Gamma}(\alpha) = X$ and $\hat{\Gamma}(\beta) = \emptyset$,
- $\hat{\Gamma}(x) = \Gamma(x)$ for every $x \in X$,
- $\hat{\Gamma}(x) = \beta$ for every $x \in \partial(X)$.

Take a subset Y with $\alpha \in Y$ and $\beta \notin Y \cup \hat{\Gamma}(Y)$. It follows that $Y \cap (\partial(X) \cup \{\beta\}) = \emptyset$, whence $Y \subseteq X \cup \{\alpha\}$. Put $Y_0 = Y \setminus \{\alpha\}$. We have

$$\hat{\Gamma}(Y) = \hat{\Gamma}(\alpha) \cup \hat{\Gamma}(Y_0) = X \cup \Gamma(Y_0).$$

Thus $\hat{\partial}(Y) = (X \setminus Y_0) \cup \partial(Y_0)$. If $|Y_0| \leq k - 1$, then

$$|\hat{\partial}(Y)| \geq |X \setminus Y_0| \geq |X| - |Y_0| \geq |X| - k + 1 \geq s.$$

If $|Y_0| \geq k$, then

$$|\hat{\partial}(Y)| \geq |\partial(Y_0)| \geq \min\{|V| - k + 1 - |Y_0|,\, \kappa_k(\Gamma)\} \geq \min\{|V| - k + 1 - |X|,\, \kappa_k(\Gamma)\} \geq s$$

follows by the isoperimetric inequality and our hypotheses. In consequence, by the finite case in Theorem 18, there are s disjoint directed paths from α to β. Each such path P_i, for $i \in [1, s]$, must pass through X and then into $\partial(X)$, meaning at some point there is an edge $(x_i, y_i) \in E$ with $x_i \in X$ and $y_i \in \partial(X)$. Since the paths are disjoint, it follows that all the x_i are distinct as are all the y_i, completing the proof. □

Proposition 20 (The Strong Isoperimetric Property for Graphs II)**.** *Let $\Gamma = (V, E)$ be a locally finite digraph, let $X \subseteq V$ be a finite, nonempty subset, let $x \in X$, and let s be a positive integer such that*

$$\kappa_1(\Gamma) \geq s, \quad |V| \geq |X| + s, \qquad \text{and} \qquad |X| \leq s.$$

Then there are vertices $x_1, \dots, x_s \in X$ and distinct vertices $y_1, \dots, y_s \in \partial(X)$ such that

$$(x_i, y_i) \in E \quad \text{for every } i \in [1, s],$$
$$X = \{x_1, \dots, x_{|X|}\} \quad \text{and} \quad x_i = x \quad \text{for every } i \geq |X|.$$

Proof. Take elements α and β not contained in V and, for $i \in [|X|+1, s]$, let $\tilde{x}_i$ be an element not contained in $V \cup \{\alpha, \beta\}$. Set $\hat{V} = X \cup \partial(X) \cup \{\alpha, \beta\} \cup \{\tilde{x}_{|X|+1}, \dots, \tilde{x}_s\}$, which is finite since Γ is locally finite and X is finite. Let $\widetilde{X} = X \cup \{\tilde{x}_{|X|+1}, \dots, \tilde{x}_s\}$. We define a digraph $\hat{\Gamma}$ on $\hat{V}$ as follows:

- $\hat{\Gamma}(\alpha) = \widetilde{X}$ and $\hat{\Gamma}(\beta) = \emptyset$,
- $\hat{\Gamma}(y) = \Gamma(y)$ for every $y \in X$,
- $\hat{\Gamma}(\tilde{x}_i) = \Gamma(x)$ for every $i \in [|X|+1, s]$.
- $\hat{\Gamma}(y) = \beta$ for every $y \in \partial(X)$.

Take a subset Y with $\alpha \in Y$ and $\beta \notin Y \cup \hat{\Gamma}(Y)$. It follows that $Y \cap (\partial(X) \cup \{\beta\}) = \emptyset$, whence $Y \subseteq \widetilde{X} \cup \{\alpha\}$. Put $\widetilde{Y}_0 = Y \setminus \{\alpha\}$. If $\tilde{x}_i \in \widetilde{Y}_0$ for some $i \in [|X|+1, s]$, let $Y_0 = Y \setminus \{\tilde{x}_{|X|+1}, \dots, \tilde{x}_s\} \cup \{x\}$, and otherwise let $Y_0 = \widetilde{Y}_0$. Observe that $Y_0 \subseteq X$. We have

$$\hat{\Gamma}(Y) = \hat{\Gamma}(\alpha) \cup \hat{\Gamma}(\widetilde{Y}_0) = \widetilde{X} \cup \Gamma(Y_0).$$

Thus $\hat{\partial}(Y) = (\widetilde{X} \setminus \widetilde{Y}_0) \cup \partial(Y_0)$. If $\widetilde{Y}_0 = \emptyset$, then $|\hat{\partial}(Y)| = |\widetilde{X} \setminus \widetilde{Y}_0| = |\widetilde{X}| = s$. If $\widetilde{Y}_0 \neq \emptyset$, then

$$|\hat{\partial}(Y)| \geq |\partial(Y_0)| \geq \min\{|V| - |Y_0|, \kappa_1(\Gamma)\} \geq \min\{|V| - |X|, \kappa_1(\Gamma)\} \geq s$$

follows by the isoperimetric inequality and our hypotheses. In consequence, by the finite case in Theorem 18, there are s disjoint directed paths from α to β. Each such path P_i, for $i \in [1, s]$, must pass through $\widetilde{X}$ and then into $\partial(\widetilde{X}) = \partial(X)$, meaning at some point there is an edge $(x_i, y_i) \in \hat{E}$ with $x_i \in \widetilde{X}$ and $y_i \in \partial(X)$. Since the paths are disjoint, it follows that all the x_i are distinct as are all the y_i. Since $|\widetilde{X}| = s$, this is only possible if every vertex of $\widetilde{X}$ occurs as an x_i in some P_i. Hence, by re-indexing the paths P_i as need be, we may assume $x_1, \dots, x_{|X|} \in X$ are the distinct elements of X with $x_{|X|} = x$ and that $x_i = \tilde{x}_i$ for $i \in [|X|+1, s]$. Finally, by definition of $\hat{\Gamma}$, any time $(\tilde{x}_i, y_i)$ is an edge in $\hat{\Gamma}$, (x, y_i) is an edge in Γ, while $(x_i, y_i) \in \hat{E}$ implies $(x_i, y_i) \in E$ for $x_i \in X$, and the proof is complete. □

As explained above, the Strong Isoperimetric Property for graphs includes the case of sumsets via Cayley digraphs. We conclude the paper by formulating these special cases in the language of sumsets. Note that Proposition 21 is a mild generalization of Proposition 10. We again remark that it is usually applied modulo H as explained after Proposition 10.

Proposition 21 (The Strong Isoperimetric Property for Sumsets I)**.** *let S and T be finite, nonempty subsets of the multiplicative group G such that $1 \in S$ and let k and s be positive integers such that*

$$\kappa_k(S) \geq s, \quad |G| \geq |T| + s + k - 1, \qquad \text{and} \qquad |T| \geq s + k - 1.$$

Then there is a subset $X \subseteq T$ with $|X| = s$ and $s_x \in S$ for each $x \in X$ (not necessarily distinct) such that

$$\{xs_x : x \in X\} \subseteq (TS) \setminus T$$

is a set of $|X| = s$ distinct elements.

Proposition 22 (The Strong Isoperimetric Property for Sumsets II)**.** *let S and T be finite, nonempty subsets of the multiplicative group G such that $1 \in S$, let $x \in T$, and let s be a positive integer such that*

$$\kappa_1(S) \geq s, \quad |G| \geq |T| + s, \qquad \text{and} \qquad |T| \leq s.$$

Then there are elements $x_1, \ldots, x_s \in T$ and $y_1, \ldots, y_s \in S$ such that

$$\{x_i y_i : i \in [1, s]\} \subseteq (TS) \setminus T \text{ is a subset of } s \text{ distinct elements},$$
$$T = \{x_1, \ldots, x_{|T|}\} \qquad \text{and} \qquad x_i = x \quad \text{for every } i \geq |T|.$$

References

[1] R. Aharoni and E. Berger, Menger's Theorem for Infinite Graphs, *Invent. Math.* 176 (2009), 1–62.

[2] E. Balandraud, Un nouveau point de vue isopérimetrique appliqué au théorème de Kneser, *Ann. Inst. Fourier* 58 (2008), 915–943.

[3] D. Grynkiewicz, Quasi-periodic decompositions and the Kemperman's structure theorem, European J. Combin. 26 (2005), no. 5, 559–575.

[4] D. Grynkiewicz, A step beyond Kemperman's structure theorem, *Mathematika* 55 (2009), no. 1-2, 67–114.

[5] D. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30, Springer (2013), 426 pp.

[6] Y.O. Hamidoune, Quelques problèmes de connexité dans les graphes orientés, *J. Comb. Theory* B 30 (1981), 1-10.

[7] Y.O. Hamidoune, On the connectivity of Cayley digraphs, *Europ. J. Combinatorics*, 5 (1984), 309-312.

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

[9] Y.O. Hamidoune, An isoperimetric method in additive theory. *J. Algebra* 179 (1996), no. 2, 622–630.

[10] Y.O. Hamidoune, Some results in Additive number Theory I: The critical pair Theory, Acta Arith. 96, no. 2(2000), 97-119.

[11] Y.O. Hamidoune, Some additive applications of the isopermetric approach, Annales de l' Institut Fourier 58(2008), fasc. 6, 2007-2036.

[12] Y. O. Hamidoune, A. Plagne. A new critical pair theorem applied to sum-free sets. *Comment. Math. Helv.* 79 (2004), no. 1, 183–207.

[13] J. H. B. Kemperman, On small sumsets in Abelian groups, *Acta Math.* 103 (1960), 66–88.

[14] Y. O. Hamidone, O. Serra and G. Zémor, One some subgroup chains related to Kneser's Theorem, *J. Théor. Nr. Bordx.* 20 (2008), no. 1, 125–130.

[15] R. A. Lee, Proving Kneser's theorem for finite groups by another e-transform *Proc. Amer. Math. Soc.* **44** (1974), 255–258.

[16] V. F. Lev, Critical pairs in abelian groups and Kemperman's structure theorem. *Int. J. Number Theory* 2 (2006), no. 3, 379–396.

[17] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[18] T. Tao, V.H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (2006), Cambridge University Press.

[19] G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* 31 (1956), 200–205.

Acknowledgement. The author is grateful to an anonymous referee for many valuable comments on the first two drafts.

UPMC Univ Paris 06, E. Combinatoire, Case 189, 4 Place Jussieu, 75005 Paris, France
E-mail address: hamidoune@math.jussieu.fr