applied to inverse additive problems

Yahya Ould Hamidoune (invited speaker)
Université Pierre and Marie Curie, Paris 06
Paris

Dedicated to M. A. Fiol

Abstract

We present the basic isopermetric structure theory, obtaining some new simplified proofs. Let $1 \le r \le k$ be integers. As an application, we obtain simple descriptions for the subsets S of an abelian group with $|kS| \le k|S|-k+1$ or $|kS-rS|-(k+r)|S|$, where where ℓS denotes as usual the Minkowski sum of ℓ copies of S. These results may be applied to several questions in Combinatorics and Additive Combinatorics including the Frobenius Problem, Waring's problem in finite fields and the structure of abelian Cayley graphs with a big diameter.

1 Introduction

The connectivity of a graph is just the smallest number of vertices disconnecting the graph. In order investigate more sophisticated properties of graphs, several authors proposed generalizations of connectivity. The reader may find details on this investigation in the chapter [2]. Investigating the isoperimetric connectivity in Cayley graphs is just one of the many facets of Additive Combinatorics. It is also one of the many facets of Network topology. For space limitation, we concentrate on Additive Combinatorics, but the reader may find details and a bibliography in the recent paper [15] concerning the other aspect.

Let $\Gamma = (V, E)$ be a reflexive graph. The minimum of the objective function $|\Gamma(X)|-|X|$, restricted to subsets X with $|X| \ge k$ and $|V \setminus \Gamma(X)| \ge$

k, the k-isoperimetric connectivity. Subsets achieving the above minimum are called k-fragments. k-fragments with smallest cardinality are called k-atoms. It was proved by the author in [7], that distinct k-atoms of Γ intersect in at most $k-1$ elements, if the size of the k-atom of Γ is not greater than the size of the k-atom of Γ^{-1}. Let $1 \in S$ be a finite generating subset of a group G such that the cardinality 1-atom of the Cayley graph defined by S is not greater than the cardinality 1-atom of the Cayley graph defined by S^{-1}. Then a 1-atom H containing 1 is a subgroup. The last result applied to a group with a prime order is just the Cauchy-Davenport Theorem. It has several other implications and leads to few lines proof for result having very tedious proof using the classical transformations. In particular, it was applied recently by the author [14] to a problem of Tao [19].

In the abelian case, things are much easier. Assume that G is abelian and let $1 \in H$ be a k-atom of the Cayley graph defined by S. If $k = 1$, then H a subgroup (the condition involving S^{-1} is automatically verified). In particular, there is a subgroup which is a 1-fragment. A maximal such a group is called an hyper-atom. Assuming now that $k = 2$ and that $\kappa_2 \leq |S| - 1$. It was proved in [8] that either $|H| = 2$ or H is a subgroup. It was proved also in [8] that either S is an arithmetic progression or there is a non-zero subgroup which is a 1-fragment, if $|S| \leq (|G|+1)/2$. Let Q be a hyper-atom of S and let $\phi : G \mapsto G/Q$ denotes the canonical morphism. The author proved in [12] that $\phi(S)$ is either an arithmetic progression or satisfies the sharp Vosper property (to be defined later) if $|S| \leq (|G|+1)/2$.

Let G be an abelian group and let A, B be finite non-empty subsets of G, with $|A+B| = |A| + |B| - 1 - \mu$. Kneser's Theorem states that $\pi(A+B) \neq \{0\}$, where $\pi(A+B) = \{x : x + A + B = A + B\}$. The hard Kemperman Theorem, which needs around half a page to be formulated, describes recursively the subsets A and B if $\mu = 1$. Its classical proof requires around 30 pages. It was applied by Lev [18] to propose a dual description, that looks easier to implement than Kemperman's description.

The above structure isoperimetric results were used in [12, 13] to explain the topological nature of Kemperman Theory and to give a shorter proof of it. Our method involve few technical steps and use some duality arguments and the strong isoperimetric property. We suspect that it could be drastically simplified. In this paper, we shall verify this hypothesis for Minkowski sums of the form $rS - sS$, obtaining very simple proofs and tight descriptions. This case covers almost all the known applications. Also, Modern Additive Combinatorics deals almost exclusively with $rS - sS$, c.f. [20].

The organization of the paper is the following:

Section 2 presents the isoperimetric tools, with complete proofs in order to make the paper self-contained. In particular, this section contains a proof of the fundamental property of k-atoms. In Section 3, we start by showing the structure of 1-atoms of arbitrary Cayley graphs. We then restrict ourselves to the abelian case. We give in this section an new simplified proof for the structure theorem of 2-atoms. We deduce from it the structure of hyper-atoms. In Section 4, we give easy properties of the decomposition modulo a subgroup which is a fragment. Easy proofs of the Kneser's theorem and a Kemperman type result for kA are then presented.

In Section 5, we investigate universal periods for kS introducing a new object: the sub-atom. It follows from a result by Balandraud [1] that $|TS| \leq |T| + |S| - 2$ implies that $T + S + K = T + S$, where K is the final kernel of S (a subgroup contained in the atom of S described in [1]). We shall prove that the $kS + M = kS$, if $|kS| \leq k|S| - k$, where M is the sub-atom. Clearly $K \subset M$. The case $rS - sS$, where $r \geq s \geq 1$, is solved easily in Section 5, by showing that one of the following holds

- S is an arithmetic progression,
- $|sS - rS| \geq \min(|G| - 1, (r + s)|S|)$,
- $|H| \geq 2$ and $sS - rS + H = sS - rS$, where H is an hyper-atom of S.

Readers familiar with Kemperman Theory could appreciate the simplicity of this result. In Section 6, we obtain the following description:

Let $k \geq 3$ be an integer and let $0 \in S$ be a finite generating subset of an abelian group G such that S is not an arithmetic progression, kS is aperiodic and $|kS| = k|S| - k + 1$. Let H be a hyper-atom of S and let S_0 be a smaller H-component of S. Then $(S \setminus S_0) + H = (S \setminus S_0)$ and $|kS_0| = k|S_0| - k + 1$. Moreover $\phi(S)$ is an arithmetic progression, where $\phi : G \mapsto G/H$ denotes the canonical morphism.

Necessarily $|H| \geq 2$, since S is not an arithmetic progression.

2 Basic notions

Recall a well known fact:

Lemma 1 *(folklore) Let a, b be elements of a group G and let H be a finite subgroup of G. Let A, B be subsets of G such that $A \subset aH$ and $B \subset Hb$. If $|A| + |B| > |H|$, then $AB = aHb$.*

Let H be a subgroup of an abelian group G. Recall that a H*–coset* is a set of the $a + H$ for some $a \in G$. The family $\{a + H; a \in G\}$ induces a partition of G. The trace of this partition on a subset A will be called an H*–decomposition* of A.

By a graph, we shall mean a directed graph, identified with its underlying relation. Undirected graphs are identified with symmetric graphs. We recall the definitions in this context.

An ordered pair $\Gamma = (V, E)$, where V is a set and $E \subset V \times V$, will be called a *graph* or a *relation* on V. Let $\Gamma = (V, E)$ be a graph and let $X \subset V$. The *reverse* graph of Γ is the graph $\Gamma^- = (V, E^-)$, where $E^- = \{(x, y) : (y, x) \in E\}$. The *degree* (called also outdegree) of a vertex x is

$$d(x) = |\Gamma(x)|.$$

The graph Γ will be called *locally-finite* if for all $x \in V$, $|\Gamma(x)|$ and $|\Gamma^-(x)|$ are finite. The graph Γ is said to be r*-regular* if $|\Gamma(x)| = r$, for every $x \in V$. The graph Γ is said to be r*-reverse-regular* if $|\Gamma^-(x)| = r$, for every $x \in V$. The graph Γ is said to be r*-bi-regular* if it is r*-regular* and r*-reverse-regular*.

- The minimal degree of Γ is defined as $\delta(\Gamma) = \min\{|\Gamma(x)| : x \in V\}$.
- We write $\delta_{\Gamma^-} = \delta_-(\Gamma)$.
- The boundary of X is defined as $\partial_\Gamma(X) = \Gamma(X) \setminus X$.
- The exterior of X is defined as $\nabla_\Gamma(X) = V \setminus \Gamma(X)$.
- We shall write $\partial^-_\Gamma = \partial_{\Gamma^-}$. This subset will be called the *reverse-boundary* of X.
- We shall write $\nabla^-_\Gamma = \nabla_{\Gamma^-}$.

In our approach, $\Gamma(v)$ is just the image of v by the relation Γ and $\Gamma^-(v)$ requires no definition since Γ^- is defined in Set Theory as the reverse of Γ.

An automorphism of a graph $\Gamma = (V, E)$ is a permutation f of V such that $f(\Gamma(v)) = \Gamma(f(v))$, for any vertex v. A graph $\Gamma = (V, E)$ is said to be *vertex-transitive* if for any ordered pair of vertices there is an automorphism mapping the first one to the second.

Let A, B be subsets of a group G. The *Minkowski product* of A with B is defined as

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

Let S be a subset of G. The subgroup generated by S will be denoted by $\langle S\rangle$. The graph (G, E), where $E = \{(x, y) : x^{-1}y \ \in S\}$ is called a *Cayley graph*. It will be denoted by $\mathrm{Cay}(G, S)$. Put $\Gamma = \mathrm{Cay}(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = FS$. One may check easily that left-translations are automorphisms of Cayley graphs. In particular, Cayley graphs are vertex-transitive.

Let $\Gamma = (V, E)$ be a reflexive graph. We shall investigate the *boundary operator* $\partial_\Gamma : 2^V \to 2^V$. When the context is clear, the reference to Γ will be omitted. Since Γ is reflexive, we have in this case $|\partial(X)| = |\Gamma(X)| - |X|$.

Let $\mathcal{A} \subset 2^V$ be a family of finite subsets of V. We define the *connectivity* of $\mathcal{A}$ as

$$\kappa(\mathcal{A}) = \min\{|\partial(X)| \ : \ \ X \in \mathcal{A}\}.$$

An $X \in \mathcal{A}$ with $\kappa(\mathcal{A}) = |\partial(X)|$ will be called a *fragment*.

A fragment with a minimal cardinality will be called an *atom*.

Put

$$\mathcal{S}_k(\Gamma) = \{X : k \leq |X| < \infty \text{ and } |\Gamma(X)| \leq |V| - k \ \}.$$

We shall say that Γ is *k-separable* if $\mathcal{S}_k(\Gamma) \neq \emptyset$. In this case, we write

$$\kappa_k(\Gamma) = \kappa(\mathcal{S}_k).$$

By a *k-fragment* (resp. *k-atom*), we shall mean a fragment (resp. atom) of $\mathcal{S}_k$. A k-fragment of Γ^{-1} is sometimes called a *k-negative*) fragment. This notion was introduced by the author in [7]. A relation Γ will be called *k-faithful* if $|A| \leq |V \setminus \Gamma(A)|$, where A is a k-atom of Γ. By a *fragment* (resp. *atom*), we shall mean a 1-fragment (resp. 1- atom).

The following lemma is immediate from the definitions:

Lemma 2 [7] *Let $k \geq 2$ be an integer. A reflexive locally finite k-separable graph $\Gamma = (V, E)$ is a $k-1$-separable graph, and moreover $\kappa_{k-1} \leq \kappa_k$.*

Recall the following easy fact:

Lemma 3 [7] *Let $\Gamma = (V, E)$ be a locally-finite k-separable graph and let A be a k-atom with $|A| > k$. Then $\Gamma^-(x) \cap A \neq \{x\}$, for every $x \in A$.*

Proof: We can not have $\Gamma^-(x) \cap A = \{x\}$, otherwise $A \setminus \{x\}$ would be a k-fragment. $\square$

The next lemma contains useful duality relations:

Lemma 4 [9] *Let X and Y be k-fragments of a reflexive locally finite k-separable graph $\Gamma = (V, E)$. Then*

$$\partial^-(\nabla(X)) = \partial(X), \tag{1}$$
$$\nabla^-(\nabla(X)) = X, \tag{2}$$

Proof: Clearly, $\partial(X) \subset \partial^-(\nabla(X))$

We must have $\partial(X) = \partial^-(\nabla(X))$, since otherwise there is a $y \in \partial^-(\nabla(X)) \setminus \partial(X)$. It follows that $|\partial(X \cup \{y\})| \leq |\partial(X)| - 1$, contradicting the definition of κ_k. This proves (1).

Thus $\Gamma^-(\nabla(X)) = \nabla(X) \cup \partial^-(\nabla(X)) = \nabla(X) \cup \partial(X) = V \setminus X$, and hence (2) holds.

Let $\Gamma = (V, E)$ be a reflexive graph. We shall say that Γ is a *Cauchy graph* if Γ is non-1-separable or if $\kappa_1(\Gamma) = \delta - 1$. h We shall say that Γ is a *reverse-Cauchy graph* if Γ^- is a Cauchy graph.

Clearly, Γ is a Cauchy graph if and only if for every $X \subset V$ with $|X| \geq 1$,

$$|\Gamma(X)| \geq \min\Big(|V|, |X| + \delta - 1\Big). \quad \square$$

Lemma 5 [7] *Let $\Gamma = (V, E)$ be a reflexive finite k-separable graph and let X be a subset of V. Then*

$$\kappa_k = \kappa_{-k}. \tag{3}$$

Moreover,

(i) *X is a k-fragment if and only if $\nabla(X)$ is a k-reverse-fragment,*

(ii) *Γ is a Cauchy graph if and only if it is a reverse-Cauchy graph.*

Proof: Observe that a finite graph is k-separable if and only if its reverse is k-separable. Take a k-fragment X of Γ. We have clearly $\partial_-(\nabla(X)) \subset \partial(X)$. Therefore

$$\kappa_k(\Gamma) \geq |\partial(X)| \geq |\partial^-(\nabla(X))| \geq \kappa_{-k}.$$

The reverse inequality of (3) follows similarly or by duality.

Suppose that X is a k-fragment. By (1) and (3), $|\partial_-(\nabla(X))| = |\partial(X)| = \kappa_k = \kappa_{-k}$, and hence $\nabla(X)$ is a revere k-fragment. The other implication of (i) follows easily. Now (ii) follows directly from the definitions. $\square$

Theorem 6 [7] *Let $\Gamma = (V, E)$ be a reflexive locally-finite k-faithful k-separable graph. Then the intersection of two distinct k-atoms X and Y has a cardinality less than k. Moreover, any locally-finite k-separable graph is either k-faithful or reverse k-faithful.*

Proof:

$\cap$	Y	$\partial(Y)$	$\nabla(Y)$
X	R_{11}	R_{12}	R_{13}
$\partial(X)$	R_{21}	R_{22}	R_{23}
$\nabla(X)$	R_{31}	R_{32}	R_{33}

Assume that $|X \cap Y| \geq k$. By the definition of κ_k,

$$\begin{aligned} |R_{21}| + |R_{22}| + |R_{23}| &= \kappa_k \\ &\leq |\partial(X \cap Y)| \\ &= |R_{12}| + |R_{22}| + |R_{21}|, \end{aligned}$$

and hence

$$|R_{23}| \leq |R_{12}|. \tag{4}$$

Thus,

$$\begin{aligned} |\nabla(X) \cap \nabla(Y)| &= |\nabla(Y)| - |R_{13}| - |R_{23}| \\ &\geq |Y| - |R_{13}| - |R_{12}| \\ &= |X| - |R_{13}| - |R_{12}| = |R_{11}| \geq k. \end{aligned}$$

Thus,

$$\begin{aligned} |R_{12}| + |R_{22}| + |R_{32}| &= \kappa_k \\ &\leq |\partial(X \cup Y)| \\ &\leq |R_{22}| + |R_{23}| + |R_{32}|, \end{aligned}$$

and hence $|R_{12}| \leq |R_{23}|$, showing that $|R_{12}| = |R_{23}|$.

It follows that

$$\kappa_k \leq |\partial(X \cap Y)| \leq |R_{12}| + |R_{22}| + |R_{21}| \leq |R_{12}| \leq |R_{23}| + |R_{22}| + |R_{21}| = \kappa_k,$$

showing that $X \cap Y$ is a k-fragment, a contradiction.

The fact that a locally-finite k-separable graph is either k-faithful or reverse k-faithful follows by Lemma 5. □

3 A structure Theory for atoms

In the sequel, we identify $\mathrm{Cay}(\langle S\rangle, S)$ with S, if $0 \in S$. We shall even work with subsets not containing 1. By $\kappa_k(S)$ we shall mean $\kappa_k(S - a) = \kappa_k(\mathrm{Cay}(\langle S-\rangle, S - a))$, for some $a \in S$. As an exercise, the reader may check that this notion does not depend on a particular choice of $a \in S$.

Theorem 7 *[6] Let $1 \in S$ be a finite proper generating subset of a group G. Let $1 \in H$ be a 1-atom of S.*

(i) *If S is 1–faithful, then H is a subgroup. Moreover $|H|$ divides $\kappa_1(S)$.*

(ii) *If G is abelian and if S is k-separable, then S is k-faithful.*

(iii) *If G is abelian, then H is a subgroup.*

Proof: Take an element $x \in H$. Clearly xH is a 1-atom. Since $(xH) \cap H \neq \emptyset$, we have by Theorem 6, $xH = H$. Since H is finite, H is a subgroup. Now $\kappa_1(S) = |HS| - |H|$, showing the last part of (i).

If G is abelian, then $\mathrm{Cay}(G, S)$ is isomorphic to $\mathrm{Cay}(G, -S)$, and hence S is k-faithful if S is k-separable. Now (iii) follows by combining (i) and (ii). □

Theorem 8 [8] *Let S be a finite generating 2–separable subset of an abelian group G with $0 \in S$ and $\kappa_2(S) \leq |S|-1$. If $0 \in H$ is a 2–atom with $|H| \geq 3$, then H is a subgroup.*

Proof: The proof is by induction. Assume first that $H+Q=H$, where Q is a non-zero subgroup. For every, $x \in H$, we have $|(H+x)\cap H| \geq |x+Q| \geq 2$. By Theorems 7 and 6, $H+x=H$. It follows that H is a subgroup. Assume now that H is aperiodic. Let us first show that $\kappa_1(H)=|H|-1$. Suppose the contrary and take a 1-atom L of H with $0 \in L$. By Theorem 7, L is a subgroup and $|L| \leq \kappa_1(H)$. Take a nonzero element $y \in L$. We have $|H \cup (y+H)| \leq |L+H| = |L| + \kappa_1(H) \leq 2\kappa_1(H) \leq 2|H|-4$. Thus, $|H \cap (y+H)| \geq 2$, and hence $y+H=H$, by Theorem 6.

Take an N-decomposition $S = \bigcup_{1 \leq i \leq s} S_i$, with $|S_1+H| \leq \cdots \leq |S_s+H|$. Without loss of generality, we may take $0 \in S_1$. We have necessarily $s \geq 2$. We must have $|S_i|=|N|$, for all $i \geq 2$. Suppose the contrary. By the definition of κ_1, we have $|S_1+H| \geq |S_1|+\kappa_1(H)=|S_1|+|H|-1$. We have also, since H generates N, $|S_i+H| \geq |S_1|+1$. Thus, $|S+H| \geq |S|+|H|-1+1 \geq |S|+|H|$, a contradiction. Now we have $|X+S| = |S \setminus S_1| + |X+S_1$, for any subset X of N. In particular, H is a 2-atom of S_1. If $|S_1| < |S|$, the result holds by Induction. It remains to consider the case $s=1$.

The relation $|H+S|-|H| \leq |S|-1$ implies that $\kappa_2(H) \leq |H|-1$. By Lemma 3, for every $x \in H$, there $s_x \in S \setminus \{0\}$, with $x - s_x \in H$. We must have

$$|H| \leq |S|-1,$$

otherwise there are distinct elements $x, y \in H$ and an element $s \in S \setminus \{0\}$ such that $x-s, y-s \in H$. It follows that $|(H+s) \cap H| \geq 2$. By Theorem 6, $H+s=H$, a contradiction.

Let $0 \in M$ be a 2-atom of H. Take a non-zero element $a \in M$. Since $\kappa_2(H) = |M+H|-|M|$, $|M|$ divides $\kappa_2(H)$ if M is a subgroup. Thus, the Induction hypothesis implies that $|M| \leq |H|-1$. Since $|M+H| \leq |M|+\kappa_2(H) \leq 2|H|-2$, we have $|H \cap (H+a)| \geq 2$. By Theorem 6, $H+a=H$, a contradiction. □

Theorem 9 ([8],Theorem 4.6) *Let S be a 2–separable finite subset of an abelian group G such that $0 \in S$, $|S| \leq (|G|+1)/2$ and $\kappa_2(S) \leq |S|-1$. If S is not an arithmetic progression, then there is a subgroup which is a 2–fragment of S.*

Proof: Suppose that S is not an arithmetic progression.

Let H be a 2–atom such that $0 \in H$. If $\kappa_2 \le |S| - 2$, then clearly $\kappa_2 = \kappa_1$ and H is also a 1–atom. By Theorem 7, H is a subgroup. Then we may assume

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

By Theorem 8, it would be enough to consider the case $|H| = 2$, say $H = \{0, x\}$. Put $N = \langle x \rangle$.

Decompose $S = S_0 \cup \cdots \cup S_j$ modulo N, where $|S_0 + H| \le |S_1 + H| \le \cdots \le |S_j + H|$. We have $|S| + 1 = |S + H| = \sum_{0 \le i \le j} |S_i + \{0, x\}|$.

Then $|S_i| = |N|$, for all $i \ge 1$. We have $j \ge 1$, since otherwise S would be an arithmetic progression. In particular, N is finite. We have $|N + S| < |G|$, since otherwise $|S| \ge |G| - |N| + 1 \ge \frac{|G|+2}{2}$, a contradiction.

Now

$$\begin{aligned} |N| + |S| - 1 &= |N| + \kappa_2(S) \\ &\le |S + N| = (j+1)|N| \\ &\le |S| + |N| - 1, \end{aligned}$$

and hence N is a 2-fragment. □

Theorem 9 was used to solve Lewin's Conjecture on the Frobenius number [10].

A H–decomposition $A = \bigcup_{i \in I} A_i$ will be called a *H–modular-progression* if it is an arithmetic progression modulo H.

Recall that S is a Vosper subset if and only if S is non 2–separable or if $\kappa_2(S) \ge |S|$.

Theorem 10 [12] *Let S be a finite generating subset of an abelian group G such that $0 \in S$, $|S| \le (|G|+1)/2$ and $\kappa_2(S) \le |S| - 1$. Let H be a hyperatom of S. Then $\phi(S)$ is either an arithmetic progression or a Vosper subset, where ϕ is the canonical morphism from G onto G/H.*

Proof: Let us show that

$$2|\phi(S)| - 1 \le \frac{|G|}{|H|}. \tag{5}$$

Clearly we may assume that G is finite.

Observe that $2|S+H| - 2|H| \leq 2|S| - 2 < |G|$. It follows, since$|S+H|$ is a multiple of $|H|$, that $2|S+H| \leq |G| + |H|$, and hence (5) holds.

Suppose now that $\phi(S)$ is not a Vosper subset. By the definition of a Vosper subset, $\phi(S)$ is 2–separable and $\kappa_2(\phi(S)) \leq |\phi(S)| - 1$.

Let us show that $\phi(S)$ has no 1–fragment M which is a non-zero subgroup. Assuming the contrary. We have $|\phi(\phi^{-1}(M) + S)| = |M + \phi(S)| \leq |M| + |\phi(S)| - 1$. Thus, $|\phi^{-1}(M) + S| \leq |\phi^{-1}(M)| + |H|(|\phi(S)| - 1) = |\phi^{-1}(M)| + \kappa_1(S)$. It follows that $\phi^{-1}(M)$ is a 1-fragment. By the maximality of H, we have $|M| = 1$, a contradiction. By (5) and Theorem 9, $\phi(S)$ is an arithmetic progression. □

4 Decomposition modulo a fragment

Let H be a subgroup of an abelian group G. Recall that a H*–coset* is a set of the $a + H$ for some $a \in G$. The family $\{a + H; a \in G\}$ induces a partition of G. A non-empty set of the form $A \cap (x + H)$ will be called a H*-component* of A. The partition of A into its H-components will be called a H*-decomposition* of A. By a *smaller* component, we shall mean a component with a smallest cardinality.

Assume now that H is 1-fragment and take a H-decomposition $S = S_0 \cup \cdots \cup S_u$, with $|S_0| \leq \cdots \leq |S_u|$.

We have $|S| - 1 \geq \kappa(S) = |H + S| - |H|$.

It follows that for $i \geq 1$, we have

$$2|H| - |S_0| - |S_i| \leq |H + S| - |S| \leq |H| - 1,$$

and hence $|S_0| + |S_i| \geq |H| + 1$. In particular,

for all $(i, j) \neq (0, 0)$, $|S_i| + |S_j| \geq |H| + 1$, hence

$$S_i + S_j + H = S_i + S_j,$$

by Lemma 1.

Thus

$$(S \setminus S_0) + S = (S \setminus S_0) + H + S.$$

Similarly

$$((S \setminus S_0)) - S = (S \setminus S_0) + H - S.$$

Since $S_0 - S_0 \subset S_1 - S_1 = H$, we have

$$S - S + H = S - S.$$

In particular, $(kS \setminus kS_0) + H = kS \setminus kS_0$.

Proposition 11 *Let S_0 denotes a smaller H-component of S, where H is a non-zero subgroup fragment. We have $S - S + H = S - S$. Let $2 \leq k$ be an integer. Then $(S \setminus S_0) + (k-1)S$ is H-periodic subset with cardinality at least* $\min(|G|, k|S+H| - k|H|)$. *If $kS + H \neq kS$, then $|S_1| > |H|/2 \geq |S_0|$, and $|kS| \geq k|S+H| - k|H| + |kS_0|$. Moreover kS_0 is aperiodic if kS is aperiodic.*

Proof: The first part was proved above. By the definition of κ, we have $|(S \setminus S_0) + (k-1)S| = |(S \setminus S_0)H + (k-1)S| \geq u|H| + (k-1)\kappa = k|S+H| - k|H|$.

Assume now that $kS + H \neq kS$. we have $kS_0 \neq kS_0 + H$, and hence $2S_0 \neq 2S_0 + H$, since $(S \setminus S_0) + (k-1)S$ is H-periodic. By Lemma 1, $|H|/2 \geq |S_0|$. We have now $|S_1| \geq |H| + 1 - |S_0| \geq |H|/2 + 1$. We must also have $kS_0 \cap ((S \setminus S_0) + (k-1)S) = \emptyset$. Thus, $|kS| \geq |(S \setminus S_0) + (k-1)S| + |kS_0| \geq k|S+H| - k|H| + |kS_0|$.

Assume now that kS is aperiodic. Since $(S \setminus S_0) + (k-1)S$ is H-periodic and since the period of kS_0 is a subgroup of H, necessarily kS_0 is aperiodic.
□

Corollary 12 (Kneser, [17]) *Let k be a non-negative integer and let S be a finite subset of an abelian group G. If kS is aperiodic, then $|kS| \geq k|S| - k + 1$*

Proof: Let H be a 1-atom containing 0. By Theorem 7, H is subgroup. Let S_0 denotes a smaller H-component of S. Without loss of generality we may assume that $0 \in S_0$. We may assume $\kappa(S) \leq |S| - 2$, since otherwise $|kS| \geq |S| + (k-1)\kappa(S) = k|S| - k + 1$, and the result holds.

By Proposition 11, kS_0 is aperiodic. By the Induction hypothesis and Proposition 11, $|kS| = |kS_0| + (k-1)(|S+H| - |H|) \geq k|S_0| - k + 1 + (k-1)(|S+H| - |H|) \geq k|S| - k + 1$. □

We shall now complete Proposition 11 in order to deal with the critical pair Theory.

Proposition 13 *Let $2 \leq k$ be an integer. Let S_0 denotes a smaller H-component of S, where H is a non-zero subgroup fragment $kS + H \neq kS$. Assume moreover that kS is aperiodic and $|kS| = k|S| - k + 1$. Then*

(i) *kS_0 is aperiodic,*

(ii) $|kS_0| = k|S_0| - k + 1$,

(iii) $(S \setminus S_0) + H = S \setminus S_0$ *and*

(iv) $|k(S + H)| = k|S + H| - k|H| + |H|$.

Proof: (i) follows by Proposition 11. By Kneser Theorem and Proposition 11,

$$\begin{aligned} k|S| - k + 1 = |kS| &\geq |kS_0| + |(k-1)S + (S \setminus S_0)| \\ &\geq |kS_0| + k|S + H| - k|H| \\ &\geq k|S_0| - k + 1 + k|S + H| - k|H| \geq k|S| - k + 1. \end{aligned}$$

In particular, the inequalities used are equalities and hence (ii) holds and $|S| = |S + H| - |H| + |S_0|$, proving (iii). Also, it follows that $|kS + H| = |(k-1)S + (S \setminus S_0)| + |H| = k|S + H| - k|H| + |H|$, proving (iii). □

We can deduce now a Kemperman type result for kS.

Corollary 14 *Let $k \geq 2$ be an integer and let S be a finite subset of an abelian group G such that kS is aperiodic and $|kS| = k|S| - k + 1$. There is a non-zero subgroup H such $(S \setminus S_0) + H = (S \setminus S_0)$, where S_0 is an H-component of S. Also, $|kS_0| = k|S_0| - k + 1$ and $|k\phi(S)| = k|\phi(S)| - k + 1$, where $\phi : G \mapsto G/H$ denotes the canonical morphism. Moreover one of the following holds:*

- *S_0 is an arithmetic progression,*
- *$k = 2$ and $S_0 = x - ((S_0 + H) \setminus S_0)$, for some x.*

Proof: Take a non-zero subgroup H with minimal cardinality such $k(S + H) = k|S + H| - k|H| + |H|$ and $(S \setminus S_0) + H = (S \setminus S_0)$, where S_0 is an

H-component of S. Notice that G is such a group. Since the period of kS_0 is a subgroup of H, kS_0 is aperiodic and hence

$$|kS_0| = k|S_0| - k + 1,$$

using the relation $|kS| = k|S| - k + 1$.

Observe that S_0 can not have a fragment non-zero subgroup Q. Otherwise we have by Proposition 11, $k(S_0 + Q) = k|S_0 + Q| - k|Q| + |Q|$ and $(S_0 \setminus T_0) + Q = (S_0 \setminus T_0)$, where T_0 is a Q-component of S_0. It would follow that $k(S + Q) = k|S + Q| - k|Q| + |Q|$ and $(S \setminus T_0) + Q = (S \setminus T_0)$, a contradiction. Let H_0 be the subgroup generated by $S_0 - S_0$. By Theorem 9, either (i) holds or one of the following holds:

- S_0 is non 2-separable. We have necessarily $|2S_0| = |H_0| - 1$. Take $a \in S_0$ and put $\{b - a\} = H_0 \setminus (2(S_0 - a))$. Necessarily $b - (S_0 - a) = H_0 \setminus (S_0 - a)$, and thus $b - S_0 = H_0 + a \setminus (S_0) = (S_0 + H_0) \setminus S_0$.

- S_0 is a 2-separable Vopser subset. We must have $k = 2$, otherwise The condition $|2S_0| \geq \min(|H_0| - 1, 2|S_0|)$. But $|H_0| \geq |kS_0| \geq 2|S_0| + |S_0| - 1 \geq 2|S_0| + 1$, observing that S_0 is not an arithmetic progression. By Kneser's Theorem, $|kS_0| \geq k|S_0| - k + 2$, a contradiction. Since $|2S_0| = 2|S_0| - 1$ and since S_0 is a Vosper subset, we have necessarily $|2S_0| = |H_0| - 1$. Take $a \in S_0$ and put $\{b - a\} = H_0 \setminus (2(S_0 - a))$. Thus, $b - (S_0 - a) = H_0 \setminus (S_0 - a)$, and hence

$$b + a - S_0 = (H_0 + a) \setminus S_0 = (S_0 + H_0) \setminus S_0. \quad \square$$

In the above result, the structure of S is completely determined by the structure of S_0 and by the structure of $\phi(S)$. Unfortunately $k\phi(S)$ is sometimes periodic. In order transform the last result, we investigate the S, where kS is periodic and where one element has a unique expressible element. The methods of Kemperman solve very easily this question, as shown in [12].

The hyper-atomic approach avoids the last difficulty and lead to a simpler description, as we shall see later.

5 Universal periods

Let T and S be finite subsets of an abelian group. It follows from a result by Balandraud that $|TS| \leq |T| + |S| - 2$ implies that $T + S$ has a universal period contained in the atom of S. We shall construct a universal period for kS which is bigger in general.

We shall first prove that $S-S$ has a universal period containing the atom if S is not an arithmetic progression and if $|S-S|$ is not very big.

Theorem 15 *Let $r \geq s \geq 1$ be integers and let S be a finite subset of an abelian group G and let H be a hyper-atom of S. One of the following holds:*

(i) *S is an arithmetic progression,*

(ii) $|sS-rS| \geq \min(|G|-1,(r+s)|S|)$,

(iii) *The hyper-atom H is a non-zero-subgroup and $sS-rS+H=sS-rS$.*

Proof: Assume that (i) and (ii) do not hold. It follows that S is 2-separable and non-vosperian. Let H be a hyper-atom of S. By Theorem 9, $|H| \geq 2$. By Proposition 11, $S-S+H=S-S$. Therefore, $sS-rS+H=sS-rS$. □

Proposition 11 suggests a very simple method giving another universal period for kS containing necessarily Balandraud period.

Let H be a subgroup fragment of S. An H-component S_0 of S will be called *desertic* component if $|S_0| \leq |H|/2$. By Proposition 11, the desertic component is unique if it exists. We shall say that S is a *desert* if it has a desertic component.

Given a subset A, with $\kappa(A) \leq |A|-2$. We define a *desert* sequence $A_0, \cdots, A_\ell$, verifying the following conditions:

- $A_0 = A$,
- A_{i+1} is a desert for $0 \leq i \leq \ell-1$,
- A_ℓ is not a desert.

Such a sequence exists and is unique, since Proposition 11 asserts that A_i is unique for $1 \leq i \leq \ell$. The sequence must end since H_i is a finite group with size $< |H_{i-1}|/2$. The *sub-atom* M of A is defied as $M=H_\ell$ if H_ℓ is non-zero. Otherwise $M=H_{\ell-1}$. In particular, the sub-atom is a non-zero subgroup.

Theorem 16 *Let k be a non-negative integer and let S be a finite subset of an abelian group G. If $|kS| \leq k|S| - k$, then*

$$kS + M = kS,$$

where M is the sub-atom of S.

Proof: We use the last notations. The proof is by induction on ℓ. We have $\kappa_1(S) \leq |S|-2$, and hence $|H_0| \geq 2$. By Proposition 11, $(S \setminus S_0)+(k-1)S$ is H-periodic. We may assume that $kS_0 \cap ((S \setminus S_0)+(k-1)S) = \emptyset$, otherwise kS is H_0-periodic. Proposition 11, $|kS| = |kS_0| + |(S \setminus S_0) + (k-1)S| \geq k|S_0| - k + 1 + ku|H| \geq k|S| - k + 1$. In particular, $|kS_0| \leq k|S_0| - k$. Notice that S and S_0 have the same sub-atom. By the induction hypothesis $kS_0 + M = kS_0$. It follows that $kS + M = kS$. □

6 Hyper-atoms and the critical pair Theory

Applications of hyper-atoms to the critical pair theory where first obtained in [12]. A more delicate notion of hyper-atoms was introduced in [13].

Theorem 17 *Let $k \geq 2$ be an integer and let S be a finite subset of an abelian group G such that S is not an arithmetic progression, kS is aperiodic and $|kS| = k|S| - k + 1$. Let H be a hyper-atom of S and let S_0 be a smaller H-component of S. If $|2S| \neq |G| - 1$, then $|H| \geq 2$. Moreover, $(S \setminus S_0) + H = (S \setminus S_0)$ and $|kS_0| = k|S_0| - k + 1$. Also, either $\phi(S)$ is an arithmetic progression or $k = 2$ and one of the following holds:*

1. *$S = x - (G \setminus S)$, for some x.*
2. *$(\phi(S)-\phi(S_0)) \cap (\phi(S_0)-\phi(S)) = \{\phi(0)\}$, where $\phi : G \mapsto G/H$ denotes the canonical morphism.*

Proof: By Kneser's Theorem and since $2S$ is aperiodic, we have $|2S| = 2|S| - 1$. Take an H-decomposition $S = S_0 \cup \cdots \cup S_u$.

Assume first that S is non-2-separable. This forces $|2S| = |G|-1$. Then necessarily $k = 2$, otherwise $3S = G$, by Lemma 1. Put $2S = G \setminus \{x\}$. We have clearly $(x - S) \cap S = \emptyset$. Clearly (1) holds. Assume now that S is 2-separable. By Theorem 9, $|H| \geq 2$.

By Proposition 13, $(S \setminus S_0) + H = (S \setminus S_0)$ and $|kS_0| = k|S_0| - k + 1$.

Assume now that $\phi(S)$ is not an arithmetic progression. By Theorem 10, $\phi(S)$ is a Vosper subset.

Thus, $|\phi(G)| - 1 < 2|\phi(S)| - 1$, otherwise $|\phi((S \setminus S_0) + S)| \geq 2|\phi(S)| - 1$, and hence $|(S \setminus S_0) + S| \geq 2u|H| + |H| \geq 2|S|$, a contradiction. Thus, $|\phi(G)| = 2|\phi(S)| - 1$. In this case, $k = 2$ and $2\phi(S) = \phi(G)$. Necessarily, $2\phi(S_0)$ is uniquely expressible in $2\phi(S)$. In other words $(\phi(S) - \phi(S_0)) \cap (\phi(S_0) - \phi(S)) = \{\phi(0)\}$. □

Corollary 18 *Let $k \geq 3$ be an integer and let S be a finite subset of an abelian group G such that S is not an arithmetic progression, kS is aperiodic and $|kS| = k|S| - k + 1$. Let H be a hyper-atom of S and let S_0 be a smaller H-component of S. Then $(S \setminus S_0) + H = (S \setminus S_0)$ and $|kS_0| = k|S_0| - k + 1$. Moreover $\phi(S)$ is an arithmetic progression, where $\phi : G \mapsto G/H$ denotes the canonical morphism.*

Acknowledgement

The author would like to thank M.A. Fiol for stimulating discussions on connectivity extra-connectivity

References

[1] E. Balandraud. Une variante de la méthode isopérimétrique de Hamidoune, appliquée au théorème de Kneser. *Ann. Inst. Fourier* (Grenoble), 58(3):915–943, 2008.

[2] J. Fàbrega and M. A. Fiol. Futher Topics in Connectivity, in *Handbook of Graph Theory,* (J.L. Gross and Y.Yellen Eds.), CRC Press, Boca Raton, 300–329, 2004.

[3] M. A. Fiol. The superconnectivity of large digraphs and graphs. *Discrete Math.*, 124(1–3):67–78, 1994.

[4] D. Grynkiewicz. A step beyond Kemperman's structure theorem, *Mathematika*, 55(1–2):67–114, 2009.

[5] Y.O. Hamidoune. Sur les atomes d'un graphe orienté. *C.R. Acad. Sc. Paris A*, 284:1253–1256, 1977.

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

[7] Y. O. Hamidoune. An isoperimetric method in additive theory. *J. Algebra* 179(2):622–630, 1986.

[8] Y. O. Hamidoune. Subsets with small sums in Abelian groups I: The Vosper property. *European J. Combin.*, 18(5):541–556, 1997.

[9] Y. O. Hamidoune. On small subset product in a group. Structure Theory of set-addition. *Astérisque*, 258:281–308, 1999.

[10] Y. O. Hamidoune. Some results in Additive number Theory I: The critical pair Theory. *Acta Arith.*, 96(2):97–119, 2000.

[11] Y. O. Hamidoune. Some additive applications of the isoperimetric approach. *Annals Institute Fourier* (Grenoble)m, 58(6):2007–2036, 2008.

[12] Y. O. Hamidoune. Hyper-atoms and the critical pair Theory. *Combinatorica*, accepted. arXiv:0805.3522v1.

[13] Y. O. Hamidoune. A Structure Theory for Small Sum Subsets. Preprint, 2009.

[14] Y. O. Hamidoune. Two Inverse results related to a question of Tao. Preprint 2010.

[15] Y. O. Hamidoune, A. Lladó and S. C. López. Vertex-transitive graphs that remain connected after failure of a vertex and its neighbors. *J. Graph Theory*, accepted.

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

[17] M. Kneser. Summenmengen in lokalkompakten abelesche Gruppen, *Math. Zeit.*, 66:88–110, 1956.

[18] V. F. Lev. Critical pairs in abelian groups and Kemperman's structure theorem. *Int. J. Number Theory*, 2(3): 379–396, 2006.

[19] T. Tao. An elementary non-commutative Freiman theorem. `http://terrytao.wordpress.com/2009/11/10/an-elementary-non-commutative-freiman-theorem.`

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

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