ANNALES

DE

L'INSTITUT FOURIER

Yahya O. HAMIDOUNE

Some additive applications of the isoperimetric approach

Tome 58, n° 6 (2008), p. 2007-2036.

<http://aif.cedram.org/item?id=AIF_2008__58_6_2007_0>

Ann. Inst. Fourier, Grenoble
58, 6 (2008) 2007-2036

SOME ADDITIVE APPLICATIONS OF THE ISOPERIMETRIC APPROACH

by Yahya O. HAMIDOUNE

ABSTRACT. — Let G be a group and let X be a finite subset. The isoperimetric method investigates the objective function $|(XB) \setminus X|$, defined on the subsets X with $|X| \geqslant k$ and $|G \setminus (XB)| \geqslant k$, where XB is the product of X by B.

In this paper we present all the basic facts about the isoperimetric method. We improve some of our previous results and obtain generalizations and short proofs for several known results. We also give some new applications.

Some of the results obtained here will be used in coming papers to improve Kempermann structure Theory.

RÉSUMÉ. — Soient G un groupe et X un sous-ensemble fini de G. La méthode isopérimétrique étudie la fonction objective $|(XB) \setminus X|$, définie sur les parties X telles que $|X| \geqslant k$ et $|G \setminus (XB)| \geqslant k$, où XB est le produit de X par B. Les inégalités additives découlent de la structure des ensembles où cette fonction atteint sa valeur minimale.

Nous présentons dans ce mémoire les bases de cette méthode et certaines de ses applications. Nous obtenons quelques nouveaux résultats et des courtes preuves de résultats connus.

Certains des résultats obtenus dans ce travail seront appliqués dans un futur mémoire afin d'améliorer les théorèmes de structure de Kempermann.

1. Introduction

The starting point of set product estimation is the inequality $|AB| \geqslant \min(|G|, |A| + |B| - 1)$, where A, B are nonempty subsets of a group with a prime order, proved by Cauchy [4] and rediscovered by Davenport [6]. Some of the generalizations of this result are due to Chowla [5], Shepherdson [52], Mann [37] and Kemperman [33].

Kneser's generalization of the Cauchy-Davenport Theorem is a basic tool in Additive Number Theory:

Keywords: Addition theorem, Cayley graph, inverse additive theory.
Math. classification: 05C25,20D60,11B75,05C40.

Theorem 1.1 (Kneser [35]). — *Let G be an abelian group and let $A, B \subset G$ be finite nonempty subsets such that AB is aperiodic. Then* $|AB| \geqslant |A| + |B| - 1$.

In [35] Kneser gives hints for the proof of his theorem. A continuous generalization of this result is proved by Kneser in [36]. Other proofs of Kneser's Theorem may be found in [38, 40, 54]. Among the numerous applications of Kneser's Theorem, we mention a result of Dixmier on the Frobenius problem [10]. Several attempts were made to generalize Kneser's Theorem to non-abelian groups. The first result in this direction is due to Diderrich:

Theorem 1.2 (Diderrich [8]). — *Let G be a group and let $A, B \subset G$ be finite subsets such that AB is not the union of left cosets. Assume moreover that the elements of B commute. Then $|AB| \geqslant |A| + |B| - 1$.*

It was observed in [19] that this generalization is equivalent to Kneser's Theorem, *cf.* Corollary 6.5. More investigations and some examples, showing that the natural extension to the non-abelian case fails to hold, can be found in Olson [45].

The critical pair Theory is the description of the subsets A, B with $|AB| = |A| + |B| - 1$. Vosper's Theorem [56, 55] states that in a group with a prime order $|AB| = |A| + |B| - 1 \leqslant |G| - 2$ holds if and only if A and B are progressions with the same ratio, where $\min(|A|, |B|) \geqslant 2$. Other proofs of Vosper's Theorem may be found in [38, 40, 54]. More recently the authors of [26] obtained a description of sets A, B with $|AB| = |A| + |B| \leqslant |G| - 4$, if $|G|$ is a prime.

The last result was applied to sum-free sets in [46], and to show the existence rainbow solutions of linear equations in [31].

Kemperman's critical pair Theory [34] provides a generalization of Vosper's Theorem to general abelian groups.

In the non-abelian case only few results were known until recent years. These results are due to Kemperman [33], Olson [43, 44, 45] and Brailowski-Freiman [3].

The results described above were proved using the transformations introduced by Cauchy [4], Davenport [6], Dyson [11] and Kemperman [33].

The basic properties of the first three transformations are given in the books [38, 40, 54].

More recently Károlyi [32] used group extensions and the Feit-Thompson Theorem to obtain a generalization of Vosper's Theorem to the non-abelian case.

The exponential sums method in Additive Number Theory gives some sharp estimates for $|AB|$ in the abelian case if $|A|, |B|$ are relatively small. The reader may find applications of this method in the text books [40, 54] and the papers of Deshouillers-Freiman [7] and Green-Ruzsa [13].

Another method in Additive Number Theory based on Nonstandard Analysis was introduced by Jin. An example of the application of this method may be found in [30].

In this paper we are concerned with the isoperimetric method introduced by the author in [15, 18, 20, 22]. Let us present briefly some special cases of this method:

Let $\Gamma = (V, E)$ be a finite reflexive relation and consider the objective function $X \mapsto |\Gamma(X) \setminus X|$, defined on the subsets X with $|X| \geqslant k$ and $|V \setminus \Gamma(X)| \geqslant k$. The minimal value of this objective function is the *kth–connectivity* and a *k–atom* is a set with minimal cardinality where the objective function achieves its minimal value. The main result proved in [20] implies that distinct k–atoms of Γ intersect in at most $k-1$ elements or that distinct k–atoms of Γ^{-1} intersect in at most $k-1$ elements. This result, which generalizes some previous results of the author [15, 18, 22], has several applications in Additive Number Theory as we shall see in the present paper.

The strong connectivity, usually defined in Graph theory as the minimum cardinality of a cutset, coincides with our first connectivity. The *kth*–connectivity was introduced in [20] in connection with some additive problems.

Let B be a subset of a finite abelian group G with $1 \in B$ and $B \neq G$. As showed in [18], the main result proved in [15] implies that the objective function $X \mapsto |(XB) \setminus X|$, defined on the nonempty subsets X with $XB \neq G$, attains its minimal value on a subgroup. If $|G|$ is a prime this value is necessarily $|B| - 1$. The Cauchy-Davenport Theorem follows obviously from this fact.

In this paper we shall present basic facts about the isoperimetric method. We shall improve some of our previous results and obtain generalizations and short proofs for several known results. We also give some new applications.

The reader may find some applications of the isoperimetric method in Serra's survey [50]. Also, Balandraud [2] developed an isoperimetric approach to Kneser's Theorem.

The paper's organization is the following:

In Section 2, we present the terminology. In Section 3, we introduce the concepts of kth–connectivity, k–fragment and k–atom and prove some elementary properties of the k–fragments. In Section 4, we give some basic properties of the intersection of fragments. The main result of this section is Theorem 4.2 which gives conditions implying that the intersection of two k–fragments is a k–fragment. This theorem generalizes results contained in [15, 17, 18, 22, 20]. In Section 5, we obtain the structure of 1–atoms and give few applications. Most of the results of this section were proved in [18, 22]. We prove them since they are needed in several parts of this paper in order to make the present work self-contained. In Section 6, we investigate the inequality $|AB| \geqslant |A| + |B|/2$ and its critical pairs. In Section 7, Proposition 7.2 gives the value of κ_2 for a set with a small cardinality. As an application we generalize the result of Károlyi [32] mentioned above. In Section 8, we determine the structure of the 2–atoms in the abelian case if $\kappa_2(S) \leqslant |S|$. This result extends to the infinite case a previous result of the author [23]. The proof given here is much easier than our first proof. In Section 9, we give an upper bound for the size of a 2–atom. As an application we generalize to the infinite case a result proved in the finite case by Arad and Muzychuk [1]. In Section 10, we present a new basic tool: the strong isoperimetric property. This property will be used in a coming paper [24] to deduce Kemperman critical pair Theory from this property of the 2-atoms.

In the Appendix, we give a simple isoperimetric proof of Menger's Theorem in order to make the present work self-contained.

2. Terminology and preliminaries

2.1. Groups

Let G be a group and let S be a subset of G. The subgroup generated by S will be denoted by $\langle S\rangle$. Let A, B be subsets of G. The *Minkowski product* is defined as

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

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

Therefore a partition $A = \bigcup_{i\in I} A_i$ is a left H–decomposition if and only if A_i is a nonempty intersection of some left H–coset with A for every $i \in I$. A *right* H–decomposition is defined similarly.

Let X be a subset of a group G. We write

$$\Pi^r(X) = \{x \in G : Xx = X\} \text{ and } \Pi^{\mathrm{l}}(\mathrm{X}) = \{\mathrm{x} \in \mathrm{G} : \mathrm{xX} = \mathrm{X}\}.$$

Notice that

$$X = X\Pi^r(X) = \Pi^l(X)X. \tag{2.1}$$

We use the following well known fact:

Lemma 2.1 ([38], Theorem 1). — *Let G be a finite group and let A, B be subsets such that $|A| + |B| > |G|$. Then $AB = G$.*

2.2. Graphs

Let V be a set and let $E \subset V \times V$. The relation $\Gamma = (V, E)$ will be called a *graph*. The elements of V will be called *points* or *vertices*. The elements of E will be called *arcs* or *edges*.

The diagonal of V is by definition $\Delta_V = \{(x, x) : x \in V\}$. The graph Γ is said to be *reflexive* if $\Delta_V \subset E$. The *reverse* of Γ is by definition $\Gamma^{-1} = (V, E^{-1})$, where $E^{-1} = \{(x, y) : (y, x) \in E\}$.

Let $a \in V$ and let $A \subset V$. 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* of x is by definition $d_\Gamma(x) = |\Gamma(x)|$. We shall say that Γ is *locally finite* if $d_\Gamma(x)$ is finite for all x. We put $\delta(\Gamma) = \min\{d_\Gamma(x); x \in V\}$. The graph Γ will be called *regular* with valency r if the elements of V have the same valency r.

Let $\Gamma = (V, E)$ be a graph. For $X \subset V$, the *boundary* of X is by definition

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

When the context is clear the reference to Γ will be omitted. In this case we write

- $\partial_-(X) = \Gamma^{-1}(X) \setminus X$,
- $X^{\curlywedge} = V \setminus (X \cup \Gamma(X))$,
- $X^{\curlyvee} = V \setminus (X \cup \Gamma^{-1}(X))$.

Most of the time we shall work with reflexive graphs. In this case we have $\Gamma(X) = X \cup \Gamma(X)$.

Notice that there is no arc connecting X to $X^{\curlywedge}$, since any arc starting in X must end in $X \cup \partial(X)$. The reader should always have in mind this obvious fact.

Let $\Gamma = (V, E)$ be a reflexive graph. We shall say that a subset X induces a *k–separation* if $k \leqslant \min(|X|, |X^{\curlywedge}|) < \infty$. We shall say that Γ is k–separable if there is a subset X which induces a k–separation.

Observe that for every k, Γ is k–separable if V is infinite.

Notice that X induces a k–separation of Γ if and only if $X^{\curlywedge}$ induces a k–separation of Γ^{-1}. In particular Γ is k–separable if and only if Γ^{-1} is k-separable.

A subset X such that $\Gamma(X) \subset X$ is called a *sink* of the graph Γ. A subset X such that $\Gamma^{-1}(X) \subset X$ is called a *source* of the graph Γ.

A set T of the form $\partial(F)$, where $F \neq \emptyset$ and $F^{\curlywedge} \neq \emptyset$ is called a *cutset*. Notice that the deletion of T destroys all the arcs connecting F to $F^{\curlywedge}$.

Intuitively speaking Γ is k–separable if there is a cutset (namely $\partial(X)$) whose deletion creates a sink X of size $\geqslant k$ and a source (namely $X^{\curlywedge}$) of size $\geqslant k$.

2.3. Cayley graphs

Let $\Gamma = (V, E)$, $\Phi = (W, F)$ be two graphs. A map $f : V \mapsto W$ will be called a *homomorphism* if $(f(x), f(y)) \in F$ for all $x, y \in V$ such that $(x, y) \in E$.

The graph Γ will be called *point-transitive* if for all $x, y \in V$, there is an automorphism f such that $y = f(x)$. Clearly a point-transitive graph is regular.

Let G be a group and let $a \in G$. The permutation $\gamma_a : x \mapsto ax$ of G will be called *left- translation*. Let S be a subset of G. The graph (G, E), where $E = \{(x, y) : x^{-1}y \in S\}$ is called a *Cayley graph*. It will be denoted by $\mathrm{Cay}(G, S)$.

Let $\Gamma = \mathrm{Cay}(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = FS$. In the case of a Cayley graph, we shall write X^S instead of $X^{\curlywedge}$. More precisely we put

$$X^S = G \setminus (XS).$$

The following facts are easily seen:

- $(\mathrm{Cay}(G, S))^{-1} = \mathrm{Cay}(G, S^{-1})$;

- For every $a \in G$, γ_a is an automorphism of $\mathrm{Cay}(G,S)$, and hence $\mathrm{Cay}(G,S)$ is point-transitive.

3. The isoperimetric method revisited

In this section, we introduce the concepts of *kth*–connectivity, k–fragment and k–atom. We also prove some elementary properties of these objects.

Let $\Gamma = (V,E)$ be a locally finite k–separable reflexive graph. The *kth–connectivity* of Γ (called *kth–isoperimetric number* in [20]) is defined as

$$\kappa_k(\Gamma) = \min\{|\partial(X)| \ : \ \infty > |X| \geqslant k \text{ and } |V \setminus \Gamma(X)| \geqslant k\}. \tag{3.1}$$

A finite subset X of V such that $|X| \geqslant k$, $|V \setminus \Gamma(X)| \geqslant k$ and $|\partial(X)| = \kappa_k(\Gamma)$ is called a *k–fragment* of Γ. A k–fragment with minimum cardinality is called a *k–atom*. The cardinality of a k–atom of Γ will be denoted by $\alpha_k(\Gamma)$.

These notions, which generalize some concepts in [15, 17, 18, 22], were introduced in [20].

For non k–separable graphs, the notions of connectivity, fragments and atoms were not defined. In order to formulate logically correct statements without assuming k–separability, we shall now extend the above notions to non k–separable graphs by convention:

Let $\Gamma = (V,E)$ be a non k–separable graph with $|V| \geqslant 2k-1$. Then Γ is necessarily finite. We put in this case $\kappa_k(\Gamma) = |V| - 2k + 1$. In this case, any set with cardinality k will be called a *k–fragment* and a *k–atom*.

A k–fragment of Γ^{-1} will be called a *negative* k–fragment. We use the following notations, where the reference to Γ could be implicit:

- $\alpha_{-k}(\Gamma) = \alpha_k(\Gamma^{-1})$,
- $\kappa_{-k}(\Gamma) = \kappa_k(\Gamma^{-1})$.

Lemma 3.1. — *Let $\Gamma = (V,E)$ be a locally finite reflexive graph such that $|V| \geqslant 2k-1$. Then $\kappa_k(\Gamma)$ is the maximal integer j such that for every finite subset $X \subset V$ with $|X| \geqslant k$,*

$$|\Gamma(X)| \geqslant \min\Big(|V| - k + 1, |X| + j\Big). \tag{3.2}$$

Formulae (3.2) is an immediate consequence of the definitions. We shall call (3.2) the *isoperimetric inequality*. The reader may use the conclusion of this lemma as a definition of $\kappa_k(\Gamma)$.

Remark 3.2. — For any locally finite reflexive graph $\Gamma = (V,E)$ with $|V| \geqslant 1$, we have $\kappa_1(\Gamma) \leqslant \delta(\Gamma) - 1$.

Lemma 3.3. — *Let $\Gamma = (V, E)$ be a reflexive finite graph with $|V| \geqslant 2k - 1$. Then*

$$\kappa_k = \kappa_{-k}. \tag{3.3}$$

Proof. — As observed above, Γ is k-separable if and only if Γ^{-1} is k-separable. So (3.3) holds by convention if Γ is non k–separable. Suppose now that Γ is k–separable, and let X be a k–fragment of Γ. We have clearly $\partial_-(X^\curlywedge) \subset \partial(X)$. Therefore

$$\kappa_k(\Gamma) \geqslant |\partial(X)| \geqslant |\partial_-(X^\curlywedge)| \geqslant \kappa_{-k}.$$

The reverse inequality follows by applying this one to Γ^{-1}. □

Lemma 3.4. — *Let $\Gamma = (V, E)$ be a locally finite k–separable reflexive graph. Let X be a k–fragment. Then*

$$\partial_-(X^\curlywedge) = \partial(X), \tag{3.4}$$

$$(X^\curlywedge)^\curlyvee = X. \tag{3.5}$$

In particular $X^\curlywedge$ is a negative k–fragment, if V is finite.

Proof. — We have clearly $\partial_-(X^\curlywedge) \subset \partial(X)$.

We must have $\partial_-(X^\curlywedge) = \partial(X)$, since otherwise there is $y \in \partial(X) \setminus \partial_-(X^\curlywedge)$. It follows that $|\partial(X \cup \{y\})| \leqslant |\partial(X)| - 1$, contradicting the definition of κ_k. This proves (3.4).

We have $\Gamma^{-1}(X^\curlywedge) = X^\curlywedge \cup \partial_-(X^\curlywedge) = X^\curlywedge \cup \partial(X) = V \setminus X$. This implies obviously (3.5).

Assume now that V is finite. We have by Lemma 3.3, $|\partial_-(X^\curlywedge)| = |\partial(X)| = \kappa_k = \kappa_{-k}$.

This proves that $X^\curlywedge$ is a negative k–fragment. □

We conclude this section by introducing two important notions:

Let $\Gamma = (V, E)$ be a reflexive graph. We shall say that Γ is a *Cauchy graph* if Γ if $\kappa_1 = \delta - 1$. We shall say that Γ is a *Vosper graph* if Γ is non–2-separable or $\kappa_2 \geqslant \delta$.

Clearly Γ is a Vosper graph if and only if for every $X \subset V$ with $|X| \geqslant 2$,

$$|\Gamma(X)| \geqslant \min\big(|V| - 1, |X| + \delta\big).$$

4. The intersection of fragments

The main result of this section is Theorem 4.2 which gives conditions implying that the intersection of two k–fragments is a k–fragment. Theorem 4.2 implies that two distinct k–atoms intersect in at most $k-1$ elements if $\alpha_k \leqslant \alpha_{-k}$.

LEMMA 4.1 ([22]). — *Let $\Gamma = (V, E)$ be a locally finite reflexive graph. Let X, Y be finite nonempty subsets. Then*

$$|\partial(X \cup Y)| + |\partial(X \cap Y)| \leqslant |\partial(X)| + |\partial(Y)|. \tag{4.1}$$

Proof. — Observe that

$$\begin{aligned} |\Gamma(X \cup Y)| &= |\Gamma(X) \cup \Gamma(Y)| \\ &= |\Gamma(X)| + |\Gamma(Y)| - |\Gamma(X) \cap \Gamma(Y)| \\ &\leqslant |\Gamma(X)| + |\Gamma(Y)| - |\Gamma(X \cap Y)|. \end{aligned}$$

The result follows now by subtracting the equation $|X \cup Y| = |X| + |Y| - |X \cap Y|$. □

The following result is proved in [22] in the special case $\kappa_2 = \kappa_1$. Indeed the paper [22] was concerned only with Vosper graphs. The concept of κ_k was introduced two years later in [20].

THEOREM 4.2 ([22]). — *Let $\Gamma = (V, E)$ be a reflexive locally finite k–separable graph. Let X, Y be two fragments of Γ such that $|X \cap Y| \geqslant k$ and $|X| - |X \cap Y| + k \leqslant |Y^{\curlywedge}|$.*

Then $X \cap Y$ and $X \cup Y$ are k–fragments of Γ.

Proof. — Put $\kappa_k = \kappa_k(\Gamma)$. By the definition of κ_k, we have $|\partial(X \cap Y)| \geqslant \kappa_k$. Hence we have by (4.1), $\kappa_k + |\partial(X \cup Y)| \leqslant 2\kappa_k$. It follows that $|\Gamma(X \cup Y)| = |X \cup Y| + |\partial(X \cup Y)| \leqslant |V| - k$.

By (4.1),

$$2\kappa_k \leqslant |\partial(X \cup Y)| + |\Gamma(X \cup Y)| = |X \cap Y| \leqslant |\partial(X)| + |\partial(Y)| = 2\kappa_k.$$

It follows that $X \cap Y$ and $X \cup Y$ are k–fragments of Γ. □

The next consequence of Theorem 4.2 will be a main tool in this paper.

THEOREM 4.3 ([20]). — *Let $\Gamma = (V, E)$ be a reflexive locally finite k–separable graph. Also assume that either V is infinite or $\alpha_k \leqslant \alpha_{-k}$.*

Let A be a k–atom and let F be a k-fragment such that $|A \cap F| \geqslant k$. Then $A \subset F$.

In particular two distinct k-atoms intersect in at most $k-1$ elements.

Proof. — Let A' be a negative atom. We shall show that $|F^{\curlywedge}| \geqslant |A|$. This holds clearly if V is infinite. Suppose that $|V|$ is finite. We have now $|F^{\curlywedge}| \geqslant |A'| \geqslant |A|$, by Lemma 3.4. By Theorem 4.2, $A \cap F$ is a k–fragment. By the minimality of $|A|$, we must have $A \cap F = A$. $\square$

We shall prove a result concerning the intersection of a fragment with the dual of a negative fragment (a possibly infinite set). In the finite case this result follows by Theorem 4.2. We used above the submodularity of $|\partial(X)|$ to prove the intersection property of fragments as done in [22]. Here we shall use a intuitive language used in [20]. The two methods are basically the same.

Theorem 4.4. — *Let $\Gamma = (V, E)$ be a reflexive locally finite graph such that $|V| \geqslant 2k-1$. Let X be a k–fragment and let Y be a negative k-fragment such that $|Y| \geqslant |X|$ and $|X \cap Y^{\curlyvee}| \geqslant k$. Then $X \cap Y^{\curlyvee}$ is a k–fragment. In particular $X \subset Y^{\curlyvee}$ if X is a k–atom.*

Proof. — The result is obvious if Γ is non k–separable since a k–fragment is a k–subset in this case. So we may assume that Γ is k-separable.

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

By the definition of a k–fragment we have

$$\kappa_k = |\partial(X)| = |R_{21}| + |R_{22}| + |R_{23}|.$$

The following inclusion follows by an easy verification:

$$\partial(X \cap Y^{\curlyvee}) \subset R_{12} \cup R_{22} \cup R_{21}.$$

We have clearly $|V \setminus \Gamma(X \cap Y^{\curlyvee})| \geqslant |V \setminus \Gamma(X)| \geqslant k$. By the definition we have $|\partial(X \cap Y^{\curlyvee})| \geqslant \kappa_k$. It follows that

$$\begin{aligned} |R_{21}| + |R_{22}| + |R_{23}| &= \kappa_k \\ &\leqslant |\partial(X \cap Y^{\curlyvee})| \\ &\leqslant |R_{12}| + |R_{22}| + |R_{21}|. \end{aligned}$$

Therefore

$$|R_{12}| \geqslant |R_{23}|. \tag{4.2}$$

Now

$$\begin{array}{rcl} |X^{\curlywedge} \cap Y| = |R_{33}| & = & |Y| - |R_{23}| - |R_{13}| \\ & \geqslant & |X| - |R_{12}| - |R_{13}| \\ & = & |R_{11}| \geqslant k. \end{array}$$

By the definition of κ_{-k} we have

$$|\partial^-(X^{\curlywedge} \cap Y)| \geqslant \kappa_{-k}.$$

It follows that

$$\begin{array}{rcl} |R_{12}| + |R_{22}| + |R_{32}| & = & \kappa_{-k} \\ & \leqslant & |\partial - (X^{\curlywedge} \cap Y)| \\ & \leqslant & |R_{22}| + |R_{23}| + |R_{32}|. \end{array}$$

Therefore $|R_{12}| \leqslant |R_{23}|$. By (4.2) we have $|R_{12}| = |R_{23}|$.

It follows that the inequality $\kappa_k \leqslant |\partial(X \cap Y^{\curlyvee})|$, used in the proof of (4.2), is an equality and hence $X \cap Y^{\curlyvee}$ is a k-fragment of Γ. $\square$

One may define a *cofinite k–fragment* as a subset X with $|X| \geqslant k$, $|\partial(X)| = \kappa_k$ and $\infty > |V \setminus X| \geqslant k$. This notion allows give a common proof for Theorems 4.2 and 4.4. This approach was used in [22] in a special case and can be adapted very easily to the general case.

5. Estimation of the size of a set product

Most of the results in this section are proved in [18, 22]. We prove them here since they are needed in several parts of this paper in order to make the present work self-contained.

Let G be a group and let S be a subset of G with $1 \in S$. We put

- $\alpha_k(S) = \alpha_k(\mathrm{Cay}(\langle S\rangle, S))$;
- $\kappa_k(S) = \kappa_k(\mathrm{Cay}(\langle S\rangle, S))$.

We shall say that a subset S is *k–separable* if $\mathrm{Cay}(\langle S\rangle, S)$ is k–separable. By a fragment of S we shall mean a fragment of $\mathrm{Cay}(\langle S\rangle, S)$.

We shall say that a subset S is a *Cauchy subset* (resp. *Vosper subset*) if $\mathrm{Cay}(\langle S\rangle, S)$ is a Cauchy graph (resp. Vosper graph). We shall consider only generating subset containing 1 in order to avoid degenerate situations where $\kappa_k = 0$. Notice that $\kappa_k(\mathrm{Cay}(G, S)) = 0$, if S generates a finite proper subgroup. However $\kappa_k(S) > 0$ if $|\langle S\rangle| \geqslant 2k-1$. This easy fact was observed in [20].

Let us prove a lemma:

Lemma 5.1. — *Let S be a generating subset of a group G with $1 \in S$. Let H be a k-atom of S with $1 \in H$. Assume that either G is infinite or $\alpha_k \leqslant \alpha_{-k}$. If $|\Pi^r(H)| \geqslant k$ then H is a subgroup.*

Proof. — Put $Q = \Pi^r(H)$ and take $a \in H$. Since $HQ = H$, we have using the assumption $1 \in H$, $aQ \subset aH \cap H$. By Theorem 4.3, $aH = H$. Then $H^2 = H$ and hence H is a subgroup. □

The intersection property implies the following description of 1-atoms, obtained in [18] in the finite case. The general case was given later in [22].

Proposition 5.2 ([18, 22]). — *Let S be a finite generating subset of a group G with $1 \in S$. Let H be a 1–atom of S with $1 \in H$. Assume that either G is infinite or $\alpha_1 \leqslant \alpha_{-1}$. Then H is a subgroup generated by $S \cap H$.*

Proof. — Let $a \in H$. The set aH is a 1–atom, since any left-translation is an automorphism of the Cayley graph. Since $|(aH) \cap H| \geqslant 1$, we have by Theorem 4.3, $aH = H$. Then H is a subgroup.

Let $H_0 = \langle H \cap S \rangle$. We have clearly $H_0 S \cap H \subset H_0$. Therefore $\partial(H_0) \subset H_0 S \setminus H \subset HS \setminus H$. It follows that H_0 is a 1–fragment and hence $H_0 = H$. □

Corollary 5.3 ([18, 22]). — *Let S be a generating subset of a group G with $1 \in S$. Let H be a 1-atom such that $1 \in H$.*

If G is infinite or $\alpha_1 \leqslant \alpha_{-1}$, then H is a subgroup.

In particular there is a finite subgroup $L \neq G$ such that $\kappa_1 = \min(|LS| - |L|, |SL| - |L|)$.

Proof. — Let K be a negative 1-atom with $1 \in K$. Assume that either G is infinite or $|H| \leqslant |K|$. By Proposition 5.2, H is a subgroup. By the definition of a 1–atom we have $\kappa_1 = |HS| - |H|$.

Assume now $|H| > |K|$ and that $|G|$ is finite. By Proposition 5.2, K is a subgroup. By Lemma 3.3 and the definition of a negative 1–atom, we have $\kappa_1 = \kappa_{-1} = |KS^{-1}| - |K| = |SK| - |K|$. □

The next lemma could be useful when S generates a proper subgroup:

Lemma 5.4. — *Let G be group and let A, S be finite nonempty subsets of G with $1 \in S$. Put $K = \langle S \rangle$ and let $A = \bigcup_{i \in I} A_i$ be a left K–decomposition of A. Put $W = \{i : |A_i S| < |K|\}$. Then*

$$|W| \leqslant \frac{|AS| - |A|}{\kappa_1(S)}. \tag{5.1}$$

Proof. — Put $\kappa_1 = \kappa_1(S)$. For each i take $a_i \in {A_i}^{-1}$.

By the isoperimetric inequality, we have $|A_iS| = |a_iA_iS| \geqslant |A_i| + \kappa_1$ for all $i \in W$. Then

$$\begin{aligned} |AS| &= \sum_{i \in I} |A_iS| \\ &\geqslant \sum_{i \in I \setminus W} |A_i| + \sum_{i \in W} (|A_i| + \kappa_1) = |A| + |W|\kappa_1. \end{aligned}$$

□

6. A universal bound for κ_1

We give in this section a characterization of the sets S with $\kappa_1(S) = \frac{|S|}{2}$.

Proposition 6.1 ([17, 22]). — *Let S be a finite generating subset of a group G with $1 \in S$. Let H be a 1–atom and let K be a negative 1–atom such that $1 \in H \cap K$. Then*

$$\kappa_1(S) \geqslant \frac{|S|}{2}. \tag{6.1}$$

Moreover $\kappa_1(S) = \frac{|S|}{2}$ holds if and only if one of the following holds:

- *$|H| \leqslant |K|$ or G is infinite, and there is a u such that $S = H \cup Hu$;*
- *G is finite and $|H| \geqslant |K|$ and there is a u such that $S = K \cup uK$.*

Proof. — Assume first that $|H| \leqslant |K|$ or that G is infinite. By Corollary 5.3, H is a subgroup. We have $\kappa_1(S) = |HS| - |H| \geqslant \frac{|HS|}{2} \geqslant \frac{|S|}{2}$, observing that $|HS| \geqslant 2|H|$ since S is a generating subset with $1 \in S$. Suppose now that $\kappa_1(S) = \frac{|S|}{2}$. We see that $|HS| = 2|H|$, and hence there is a u such that $S = H \cup Hu$.

Assume now that $|H| \geqslant |K|$ and that G is finite. By Corollary 5.3, K is a subgroup. By Lemma 3.3, we have $\kappa_1 = \kappa_{-1} = |KS^{-1}| - |K| \geqslant \frac{|SK|}{2} \geqslant \frac{|S|}{2}$, observing that $|SK| \geqslant 2|K|$ since S is a generating subset with $1 \in S$. Suppose now that $\kappa_1(S) = \frac{|S|}{2}$. We see that $|SK| = 2$, and hence there is a u such that $S = K \cup uK$. □

Notice that the bound $\kappa_1(\Gamma) \geqslant \frac{\delta(\Gamma)}{2}$ holds for all point-transitive reflexive graphs. This was proved in [17] in the finite case. The general case is given in [22].

Zémor constructed in [57] a Cayley graph with $\alpha_1 > \alpha_{-1}$. The above result suggests more constructions of this type:

Example 6.2. — Consider a finite group G of odd order and consider a non normal subgroup H and an element u such that $uH \neq Hu$. Put $S = H \cup Hu$. By Proposition 6.1, H is a 1-atom of S. Let Q be a negative 1-atom. Q can not be a subgroup since otherwise $|QS^{-1}| = 2|Q| = \kappa_1 = 2|H|$, which is impossible.

Corollary 6.3 (Olson [43, 44]). — *Let A, B be finite nonempty subsets of a group G and put $K = \langle BB^{-1} \rangle$. Then*

$$|B^j| \geqslant \min\left(|K|, \frac{(j+1)|B|}{2}\right), \text{ and} \tag{6.2}$$

$$|AB| \geqslant \min\left(|AK|, |A| + \frac{|B|}{2}\right). \tag{6.3}$$

Proof. — It is enough to prove Formulae (6.3).

Take $b \in B^{-1}$ and put $S = Bb$. Since $BB^{-1} = SS^{-1} \subset \langle S \rangle$ and $S = Bb \subset BB^{-1}$ we have $K = \langle S \rangle$.

Take a left K–decomposition $A = \bigcup_{i \in I} A_i$. Suppose now that $AB \neq AK$. Then there is an s such that $|A_s B| < |K|$. Take a $u \in A_s^{-1}$. By the isoperimetric inequality and by (6.1), $|A_s B| = |uA_s B| \geqslant |A_s| + \frac{|B|}{2}$. Then

$$|AB| = \sum_{i \in I} |A_i B| \geqslant \sum_{i \in I \setminus \{s\}} |A_i| + |A_s B| \geqslant |A| + \frac{|B|}{2}.$$

□

Formulae (6.2) is proved by Olson in [43] as main tool in his proof that a subset of a finite group G with cardinality $\geqslant 3\sqrt{|G|}$ contains some nonempty subset $\{a_1, \cdots, a_k\}$ with $a_1 \cdots a_k = 1$, a result conjectured by Erdős and Heilbronn [12]. Olson's last result improves results by Erdős-Heilbronn [12] and Szemerédi [53].

Formulae (6.3) is proved by Olson in [44]. Notice that the bound $\kappa_1(\Gamma) \geqslant \frac{\delta(\Gamma)}{2}$ for all point-transitive reflexive graphs proved independently by the author in [17] implies easily Olson's result. Our isoperimetric proof looks much easier than the proof of Olson [44].

Applications of this formulae to σ–finite groups are given by the authors of [25] and by Hegyváry [29]. This result has the following easy consequence proved independently by Rødseth [48] and the author [16]:

Corollary 6.4 ([16, 48]). — *Let S be generating subset of a finite group G with $1 \in S$. Put $|G| = n$ and $|S| = k$. Then*

$$S^{\lfloor \frac{2n}{k} \rfloor - 1} = G.$$

Proof. — Put $j = \lfloor \frac{2n}{k} \rfloor - 1$ and suppose that $S^j \neq G$. By Lemma 2.1, $|S^{j-1}| + |S| \leqslant n$. By (6.3), we have $|S^i| \geqslant |S^{i-1}| + \frac{k}{2}$, for all $i \leqslant j-1$. By iterating we have

$$|S^{j-1}| \geqslant |S| + (j-2)\frac{k}{2} = j\frac{k}{2}.$$

Therefore $n \geqslant |S| + j\frac{k}{2}$. Hence $(j+2)k \leqslant 2n$ and $j \leqslant \frac{2n}{k} - 2$, a contradiction. □

Corollary 6.4 was proved independently by Rødseth [48] and the author [16]. Actually a more general result dealing with graphs having a transitive group of automorphisms is also proved in [16]. An application of Corollary 6.4 to the Frobenius problem is given by Rødseth [48]. Also this corollary is used in [47, 41, 42] in the investigation of finitely generated profinite groups.

Lemma 5.4 has the following consequence:

Corollary 6.5 ([19]). — *Diderrich Theorem 1.2 is equivalent to Kneser's Theorem 1.1.*

Proof. — Diderrich Theorem implies clearly Kneser's Theorem. Suppose now that any two elements of B commute and let K be the subgroup generated by B. Observe that K is abelian.

Without loss of generality we may assume that $1 \in B$. Take a left K–decomposition $A = \bigcup_{i \in I} A_i$. By Proposition 6.1 and Lemma 5.4, there is a $j \in I$ such that $A_iB = A_iK$ for all $i \neq j$. Since $\Pi^r(A_jB) \subset K$, we must have $|\Pi^r(A_jB)| = 1$. Take $a \in A_j$.

Since K is abelian we have by Kneser's Theorem 1.1, $|A_jB| = |a^{-1}A_jB| \geqslant |A_j| + |B| - 1$. Therefore $|AB| = \sum_{i \in I} |A_iB| \geqslant \sum_{i \in I \setminus \{j\}} |A_i| + |A_jB| \geqslant |A| + |B| - 1$. □

7. Some structural properties of the 2–atoms

In this section we obtain some results dealing with non necessarily abelian groups. Proposition 7.2 gives the value of κ_2 for sets with a small cardinality.

We shall define the *defect* of S as

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

The following lemma gives bound on the cardinality of a 2–atom. This bound allows to give some proofs by induction.

Lemma 7.1 ([20]). — *Let S be a finite generating subset of a group G with $1 \in S$ and $|S| \geqslant 3$. Also assume that either G is infinite or $\alpha_2 \leqslant \alpha_{-2}$. Let H be a 2–atom with $1 \in H$ and $|\Pi^l(H)| = 1$. Then $|H| \leqslant |S| - 1$.*

Proof. — Assume that $|H| \geqslant |S|$. Then $|H| \geqslant 3$. For each $x \in H$, there is an $a_x \in H$ such that $a_x^{-1}x \in S \setminus \{1\}$, since otherwise $\partial(H \setminus \{x\}) \subset \partial(H)$, and $H \setminus \{x\}$ would be a 2-fragment, a contradiction. By the pigeonhole principle there are $x, y \in H$ with $x \neq y$ and $a_x^{-1}x = a_y^{-1}y$. It follows that $a_y, y \in a_y a_x^{-1} H$. Therefore by Theorem 4.3, $H = a_y a_x^{-1} H$ and hence $|\Pi^l(H)| \geqslant 2$, a contradiction. □

Put $p(G) = \min\{|H| : H \text{ is a subgroup with } |H| \geqslant 2\}$.

The reader may define left and right progressions, *cf.* [22]. But these notions coincide if the progression contains 1. We shall mean by an r–progression a subset of the form $\{r^j, \cdots, r^{k+j}\}$.

Proposition 7.2. — *Let S be a generating subset of a group G with $1 \in S$ and $|S| \leqslant p(G)$. Then*

(i) *S is a Cauchy subset,*

(ii) *if $\kappa_2(S) = |S| - 1$, then S is a progression.*

Proof. — By Corollary 5.3, there is a finite subgroup N with $\kappa_1(S) = \min(|SN|, |NS|) - |N| \geqslant |N|$. We must have $|N| = 1$, since otherwise $\kappa_1(S) \geqslant |N| \geqslant p(G) \geqslant |S|$, a contradiction. Therefore $\kappa_1(S) = \min(|NS|, |SN|) - 1 = |S| - 1$, and hence (i) holds.

We shall now prove that $\alpha_2(S) = 2$ if $\kappa_2(S) = |S| - 1$, by induction on $|S|$. Take a 2-atom H of S and a 2-atom K of S^{-1} with $1 \in H \cap K$.

Case 1. $|H| \leqslant |K|$ or G is infinite.

We have $|\Pi^l(H)| = 1$, since otherwise, we would have $|S| - 1 = \kappa_2(S) = |\Pi^l(H)HS| - |\Pi^l(H)H| \geqslant |\Pi^l(H)| \geqslant p(G)$, a contradiction.

Put $L = \langle H^{-1} \rangle$. We have clearly $L = \langle H \rangle$.

By Lemma 7.1, $|H| \leqslant |S| - 1 \leqslant p(G) - 2$. By (i), H^{-1} is a Cauchy subset. Let $S = \bigcup_{i \in I} S_i$ be a right L–decomposition of A. Put $W = \{i : |HS_i| < |L|\}$. By Lemma 5.4, $|W| \leqslant 1$. Then $|I| = 1$, since otherwise $|HS| \geqslant p(G) + |H| > |H| + |S| - 1$, a contradiction. Hence $L = G$. Now we have $\kappa_2(H^{-1}) \leqslant |S^{-1}H^{-1}| - |S^{-1}| \leqslant |H| - 1$.

By the induction hypothesis there is a u such that $1 + |H| = |\{1, u\}H^{-1}| = 2|H| - |H \cap Hu^{-1}|$. Since $1 \in H$, we have $H \subset \langle u \rangle$. It follows that $|H \cap uH| = |H| - 1$. Since $|\Pi^l(H)| = 1$, we have by Theorem 4.3, $|H| = 2$.

Put $H = \{1, r\}$. It follows since $|S| \leqslant p(G) \leqslant |\langle r \rangle|$ that S is an r–progression.

Case 2. $|H| > |K|$ and G is finite. By Lemma 3.3, we have $\kappa_2(S) = \kappa_{-2}(S)$. The proof follows as in Case 1. $\square$

Corollary 7.3. — *Let G be a group and let A, B be subsets of G such that $|A|, |B| \geqslant 2$, $1 \in A \cap B$ and $|B| \leqslant p(G)$.*

Assume that $|AB| = |A| + |B| - 1 \leqslant |K| - 1$, where $K = \langle B \rangle$.

- *If $|A| + |B| = |K|$ then there is an a such that $A^{-1}a = K \setminus B$;*
- *If $|A| + |B| \leqslant |K| - 1$ then there is an r such that B and A are r–progressions.*

Proof. — By Proposition 7.2, $\kappa_1(B) = |B| - 1$. Take a left K-decomposition $A = A_1 \cup \cdots \cup A_j$. By Lemma 5.4, $|\{i : |A_i B| \neq |K|\}| \leqslant 1$. We have $|K| - 1 \geqslant |AB| > (j-1)|K|$, and hence $j = 1$.

Assume first $|A| + |B| = |K|$. By the isoperimetric inequality $|A| + |B| - 1 \geqslant |AB| \geqslant |A| + |B| - 1 = |K| - 1$. Take $\{a\} = K \setminus AB$. We have $A^{-1}a \subset K \setminus B$. Since these two sets have the same cardinality we must have $A^{-1}a = K \setminus B$.

Assume now $|A| + |B| \leqslant |K| - 1$.

Then B is 2-separable and $\kappa_2(B) \leqslant |B| - 1 < p(G)$. By Proposition 7.2, B is a r–progression, for some r. Now r generates K, and hence K is a cyclic group. It follows that $|X\{1, r\}| \geqslant |X| + 1$ for every subset $X \subset K$ with $X\{1, r\} \neq K$. Moreover equality holds only if X is an r–progression. Now $|AB| = |A\{1, r\}^k|$, where $k = |B| - 1$. The above observation shows that $|A\{1, r\}| = |A| + 1$, and hence A is an r–progression. $\square$

Corollary 7.3 implies a result due to Brailowski-Freiman [3] since $p(G) = \infty$ for a torsion free group. Corollary 7.3 implies the validity of Károlyi's Theorem 4 [32] for infinite groups. In the finite case Károlyi's condition $|A| + |B| \leqslant p(G)$ is relaxed in Corollary 7.3 to the weaker one $|B| \leqslant p(G)$ and $|A| + |B| \leqslant |\langle B \rangle| - 1$. Notice that Corollary 7.3 implies Vosper's Theorem.

8. 2–atoms in abelian groups

In this section we determine the structure of the 2–atoms in the abelian case if $\mu \leqslant 0$. This result extends to the infinite case a previous result [23]. The proof given here is much easier than our first proof.

Lemma 8.1. — *Let S be a finite subset of an abelian group G with $1 \in S$. Then $\kappa_k(S) = \kappa_{-k}(S)$ and $\alpha_k(S) = \alpha_{-k}(S)$.*

Proof. — This follows since the map "$x \mapsto x^{-1}$" is an isomorphism from $\mathrm{Cay}(G,S)$ onto its reverse $\mathrm{Cay}(G,S^{-1})$, in the abelian case. $\square$

Lemma 8.2. — *Let S be a finite generating subset of an abelian group G with $1 \in S$ and $\mu(S) \leqslant 0$. Let H be a 2–atom of S with $1 \in H$. Also assume that $|H| \neq 2$ and that H is not a subgroup. Then*

- $|H| \leqslant \kappa_2(H)$.
- *If H generates G then $|H| = 3$.*

Proof. — By Lemma 5.1, H is aperiodic. By Lemma 8.1 and Theorem 4.3, for every $a \in H \setminus \{1\}$, we have

$$|aH \cap H| = 1. \tag{8.1}$$

Let K be a 2–atom of H with $1 \in K$. Put $K = \{1, a_1, \cdots, a_{k-1}\}$. Assume first that $|K| > |H|$. By Lemma 7.1, K is periodic. Hence K is a subgroup by Lemma 5.1 and hence $|\kappa_2(H) = |KH| - |K| \geqslant |K| > |H|$.

Assume now that $|K| \leqslant |H|$.

We have using (8.1)

$$\begin{aligned}
\kappa_2(H) + |K| &\geqslant |KH| \\
&\geqslant |\{1, a_1, \cdots, a_{k-1}\}H| \\
&\geqslant |H| + |a_1H \setminus H| + \cdots + a_{k-1}H \setminus (H \cup a_1H \cup \cdots, a_{k-2}H) \\
&\geqslant |H| + |H| - 1 + \cdots |H| - k + 1 = k|H| - \frac{k(k-1)}{2} \qquad (8.2)
\end{aligned}$$

and hence $\kappa_2(H) \geqslant k|H| - \frac{k(k-1)}{2} - |K|$. If $k = 2$, then $\kappa_2(H) \geqslant 2|H| - 1 - |K| \geqslant |H|$. If $k \geqslant 3$, then $\kappa_2(H) \geqslant (k-1)|H| - \frac{k(k-1)}{2} \geqslant 2|H| - 3 \geqslant |H|$.

Assume now that H generates G. The inequality $|HS| \leqslant |H| + |S| \leqslant |G| - 2$ implies that $\kappa_2(H) \leqslant |H|$. Then we have since $|K| \leqslant |H|$ and by (8.2), $|H| + |K| \geqslant k|H| - \frac{k(k-1)}{2}$.

Case 1. $k \leqslant |H| - 1$. Then $(k-1)(k+1) \leqslant (k-1)|H| \leqslant k + \frac{k(k-1)}{2}$, and hence $|H| = k + 1 = 3$.

Case 2. $k = |H|$. Then $(k-2)k \leqslant \frac{k(k-1)}{2}$, and hence $|H| = k = 3$. $\square$

The next result describes the 2–atoms if $\mu(S) \leqslant 0$.

Theorem 8.3 ([21, 23]). — *Let S be a finite generating 2–separable subset of an abelian group G with $1 \in S$ and $\mu(S) \leqslant 0$. Also assume that $|S| \neq |G| - 6$ if $\mu(S) = 0$. Let $1 \in M$ be a 2–atom which is not a subgroup. Then $|M| = 2$.*

Proof. — We shall write $o(y) = |\langle y \rangle|$, for any $y \in G$. Put $L = \langle H \rangle$ and $t = \mu(S)$. Let H denotes a translate of M with the form $\{1, a, b\}$

maximizing $o(a^{-1}b)$. Clearly H is not a subgroup. We have $\kappa_2(S) \geqslant |S|-1$, by Lemma 8.1 and Proposition 5.2, since in this case a 2-atom is a 1-atom. Therefore

$$-1 \leqslant t \leqslant 0.$$

Suppose to the contrary that $|H| \geqslant 3$.

Case 1. $L = G$. By Lemma 8.2, $|H| = 3$ and $\kappa_2(H) \geqslant |H|$. Then $|HS| \geqslant |S| + |H|$, and hence $t = 0$. Consider the case $|S| > |G| - 6$. Then $|H^S| \leqslant |G| - |H| - (|G| - 5) \leqslant 2$. It follows by Lemma 3.4 that H^S is a negative 2–fragment with $|H^S| = 2$ and hence $-H^S$ is a 2–atom, a contradiction. So we have $|S| \leqslant |G| - 7$.

Put $U = \{a^{-1}, b^{-1}\}$. Put $N = (H^2S) \setminus HS$. By the definition of κ_2, we have $|HS| + |N| \geqslant \min(|G| - 1, |HS| + 3) = |HS| + 3$. Notice that xH^{-1} is a negative 2–atom. Take $x \in N$, then $(xH^{-1}) \cap (HS) \neq \emptyset$. Since $(xH^{-1}) \not\subset (X^S)$, we have by Theorem 4.4, $(xH^{-1}) \cap (X^S) = \{x\}$. Therefore $(NU) \subset (HS) \setminus S$. Since $|(HS) \setminus S| = 3$, we have $NU = (HS) \setminus S$ and $|N| = 3$. It follows also that $ab^{-1}N = N$. In particular $o(ab^{-1}) = 3$. Since $\{1, a^{-1}, ba^{-1}\}$, $\{1, b^{-1}a, ab^{-1}\}$ are translates of M, we must have $\max(o(a), o(b)) \leqslant 3$. It follows that $|G| \leqslant 9$, contradicting the relation $3 \leqslant |S| < |G| - 6$.

Case 2. $L \neq G$. By Lemma 8.2, $\kappa_2(H) \geqslant |H|$. This implies obviously that $\kappa_1(H) = |H| - 1$.

Put $L = \langle H \rangle$ and take an L–decomposition $S = S_1 \cup \cdots \cup S_j$. Without loss of generality we may assume $1 \in S_1$ and $|HS_1| \leqslant \cdots \leqslant |HS_j|$. Put $W = \{i : |HS_i| < |L|\}$.

By Lemma 5.4, $|W| \leqslant \frac{|HS|-|S|}{\kappa_1(H)} \leqslant \frac{|H|}{|H|-1} < 2$. Then we must have $|HS_i| = |L|$, for all $i \geqslant 2$. We must have

$$LS = G,$$

since otherwise

$$\begin{aligned} |S| - 1 \leqslant \kappa_2(S) &\leqslant |LS| - |L| \\ &= (j-1)|L| = |HS| - |HS_1| \leqslant |S| - 3, \end{aligned}$$

a contradiction. In particular

$$S = (G \setminus L) \cup S_1. \tag{8.3}$$

Using (8.3) we see that any 2– fragment of S containing 1 is a 2-fragment of S_1. In particular H is a 2-atom of S_1.

We have $|S_1| \neq |L| - 6$, otherwise we have by (8.3), $|S| = |G| - 6$.

We have also $|S_1| \geqslant 2$, since otherwise

$$|HS| = (j-1)|L| + |H| \geqslant |S| - |S_1| + 3 = |S| + 2,$$

a contradiction. Now we apply Case 1 to get a contradiction. □

The above result was proved for $\kappa_2 = |S| - 1$ in [21], and for finite groups in [23]. In the case where $|G|$ is a prime, a proof of Theorem 8.3 using the Davenport's transform was obtained by the authors of [26]. In [51], Serra and Zémor proved that a 2–atom of S has size $= 2$, if $|G|$ is a prime and $|S| < \binom{4+\kappa_2-|S|}{2}$. A short proof of the last result was given by the authors of [28]. A generalization of this result to arbitrary finite abelian groups was obtained by the authors of [27] when $\mu(S) \leqslant 4$.

An example given by Serra and Zémor in [51] shows that in the prime case the 2-atom may have size $= 3$ if $\mu = 0$ and $|S| = |G| - 6$.

9. An upper bound for the size of a 2–atom

In this section we prove more results on the intersection of fragments that we shall need in the next section.

Lemma 9.1. — *Let $\Gamma = (V, E)$ be a locally finite k–separable reflexive graph. Let X and Y be k–fragments. Then $X \subset Y$ if and only if $Y^{\curlywedge} \subset X^{\curlywedge}$.*

Proof. — Assume first that $X \subset Y$. Then

$$X^{\curlyvee} = V \setminus \Gamma(X) \supset V \setminus \Gamma(Y) = Y^{\curlyvee}.$$

Assume now that $Y^{\curlyvee} \subset X^{\curlyvee}$. Then

$$X = V \setminus \Gamma^{-1}(X^{\curlyvee}) \subset V \setminus \Gamma^{-1}(Y^{\curlyvee}) = Y.$$

□

Lemma 9.2. — *Let $\Gamma = (V, E)$ be a reflexive locally finite k–separable graph with $k \geqslant 2$. Let A, F be k–fragments such that $|A| \leqslant |F^{\curlywedge}|$ and $|A \cap F| \geqslant k - 1$. Then*

$$|A \cap \partial(F)| \leqslant |\partial(A) \cap F^{\curlywedge}|, \tag{9.1}$$

$$|\Gamma(A) \cap \Gamma(F)| \leqslant |A \cap F| + \kappa_k \text{ and} \tag{9.2}$$

$$|F^{\curlywedge} \setminus A^{\curlywedge}| \leqslant |A \setminus F| + \kappa_k - \kappa_{k-1}. \tag{9.3}$$

Proof.

$\cap$	F	$\partial(F)$	$F^{\curlywedge}$
A	R_{11}	R_{12}	R_{13}
$\partial(A)$	R_{21}	R_{22}	R_{23}
$A^{\curlywedge}$	R_{31}	R_{32}	R_{33}

Suppose that (9.1) is false. Then

$$|R_{12}| > |R_{23}|.$$

It follows that

$$\begin{aligned} |F^{\curlywedge} \cap A^{\curlywedge}| &= |F^{\curlywedge}| - |R_{23}| - |R_{13}| \\ &> |A| - |R_{12}| - |R_{13}| \\ &= |R_{11}| \geqslant k-1. \end{aligned}$$

Now we have

$$\begin{aligned} |R_{32}| + |R_{22}| + |R_{23}| &\geqslant |\partial(A \cup F)| \geqslant \kappa_k \\ &= |R_{12}| + |R_{22}| + |R_{32}|, \end{aligned}$$

and hence $|R_{23}| \geqslant |R_{21}|$ a contradiction proving (9.1). Now we have

$$\begin{aligned} |\Gamma(A) \cap \Gamma(F)| &= |A \cap F| + |R_{12}| + |R_{21}| + |R_{22}| \\ &\leqslant |A \cap F| + |R_{23}| + |R_{21}| + |R_{22} \\ &= |A \cap F| + \kappa_k. \end{aligned}$$

This proves (9.2).

Since $|A \cap F| \geqslant k-1$, we have

$$\begin{aligned} |R_{12}| + |R_{22}| + |R_{21}| &\geqslant \kappa_{k-1} \\ &= \kappa_k - (\kappa_k - \kappa_{k-1}) \\ &= |R_{21}| + |R_{22}| + |R_{23}| - (\kappa_k - \kappa_{k-1}). \end{aligned}$$

It follows that

$$|R_{23}| \leqslant |R_{12}| + \kappa_k - \kappa_{k-1}.$$

Hence

$$\begin{aligned} |F^{\curlywedge} \setminus A^{\curlywedge}| &= |R_{13}| + |R_{23}| \\ &\leqslant |R_{13}| + |R_{12}| + \kappa_k - \kappa_{k-1} \\ &= |A \setminus F| + \kappa_k - \kappa_{k-1}. \end{aligned}$$

This proves (9.3). □

We shall now investigate the number of 2–atoms containing a given element and obtain an upper bound for the size of a 2–atom.

We obtain some applications including a generalization to the infinite case a result proved in the finite case by Arad and Muzychuk [1].

The smallest number j (possibly null) such that every element $x \in V$ belongs to j pairwise distinct k–atoms will be denoted by $\omega_k(\Gamma)$. We shall write $\omega_k(\Gamma^{-1}) = \omega_{-k}(\Gamma)$. We also write $\omega_k(S) = \omega_k(\mathrm{Cay}(\langle S \rangle, S))$. The next result is a basic tool in the investigation of the 2-atoms structure. The case $\kappa_2 = \kappa_1$ of this result is proved in [22]. Also the finite case of this result is proved in [23].

Theorem 9.3. — *Let $\Gamma = (V, E)$ be a reflexive locally finite graph. Let H be a 2–atom and let K be a negative 2–atom with $|K| \geqslant |H| \geqslant 3$. Also assume that V is infinite or $\alpha_2 \leqslant \alpha_{-2}$. Then one of the following holds:*

(i) $\min(\omega_2, \omega_{-2}) \leqslant 2$.

(ii) $|H| \leqslant 3 + \max(\kappa_2 - \delta, \kappa_{-2} - \delta_-)$.

Proof. — Suppose contrary to (i) that $\omega_2 \geqslant 3$ and $\omega_{-2} \geqslant 3$. We have $\alpha_1 = \alpha_{-1} = 1$, since otherwise a 2–atom containing x is a 1–atom containing x and it is unique by Theorem 4.3, contradicting $\min(\omega_2, \omega_{-2}) \geqslant 3$.

Take $v \in V$ and choose two distinct 2–atoms M_1, M_2 such that $v \in M_1 \cap M_2$. By Theorem 4.3, we have $M_1 \cap M_2 = \{v\}$.

We have $M_1^{\curlywedge} \not\subset M_2^{\curlywedge}$, by Lemma 9.1.

Take $w \in {M_1}^{\curlywedge} \setminus M_2^{\curlywedge}$, and take three pairwise distinct negative 2-atoms L_1, L_2, L_3 such that $w \in L_1 \cap L_2 \cap L_3$.

Assume first that for some $i \neq j$ we have $L_i \cup L_j \subset M_1^{\curlywedge}$.

By Theorem 4.4, $|L_i \cap M_2^{\curlywedge}| \leqslant 1$, for every i.

Then we have using (9.3), the fact that $\kappa_1 = \delta - 1$ and the intersection property of atoms

$$\begin{aligned} |H| + \kappa_2 - \delta &= |H| + \kappa_2 - \kappa_1 - 1 \\ &= |M_1 \setminus M_2| + \kappa_2 - \kappa_1 \\ &\geqslant |({M_1}^{\curlywedge} \setminus M_2^{\curlywedge}) \cap (L_i \cup L_j)| \\ &= |L_i \cup L_j| - |(L_i \cup L_j) \cap M_2^{\curlywedge}| \\ &\geqslant |L_i \cup L_j| - 2 \\ &= 2|K| - 3 \geqslant 2|H| - 3, \end{aligned}$$

and hence (ii) holds.

We can now assume without loss of generality that

$$L_1, L_2 \not\subset M_1^{\curlywedge}.$$

By Lemma 9.1, we have $M_1 \not\subset L_i^{\curlyvee}$ for $1 \leqslant i \leqslant 2$. By Theorem 4.4, $|M_1 \cap (L_1^{\curlyvee} \cup L_2^{\curlyvee})| \leqslant 2$. Then $|M_1 \cap \Gamma^{-1}(L_1) \cap \Gamma^{-1}(L_2)| \geqslant |M_1| - 2$.

Now $\Gamma^{-1}(L_1) \cap \Gamma^{-1}(L_2) \supset (\Gamma^{-1}(L_1) \cap \Gamma^{-1}(L_2) \cap M_1) \cup \Gamma^{-1}(w)$. Notice that $\Gamma^{-1}(w) \cap M_1 = \emptyset$.

Then we have by (9.2)

$$\begin{aligned} \delta_- + |H| - 2 &\leqslant |\Gamma^{-1}(w)| + |M_1 \cap \Gamma^{-1}(L_1) \cap \Gamma^{-1}(L_2)| \\ &\leqslant |\Gamma^{-1}(L_1) \cap \Gamma^{-1}(L_2)| \\ &\leqslant 1 + \kappa_{-2}. \end{aligned}$$

Therefore $|H| \leqslant 3 + \kappa_{-2} - \delta_-$. □

Let us apply this result in the symmetric case.

Corollary 9.4. — *Let S be a finite generating subset of a group G with $1 \in S$ and $S = S^{-1}$. Let H be a 2-atom of S such that $1 \in H$. If $|H| \geqslant \kappa_2 - |S| + 4$, then $|\Pi^l(H)| \geqslant 2$.*

Proof. — Since $S = S^{-1}$, H is also a negative 2–atom. Also $\kappa_2 = \kappa_{-2}$. Take a 3–subset $\{a_1, a_2, a_3\}$ contained in H.

By Theorem 9.3, $\omega_2 \leqslant 2$. Hence two of the 2–atoms $a_1^{-1}H, a_2^{-1}H, a_3^{-1}H$ must be equal and hence $|\Pi^l(H)| \geqslant 2$. □

Let G be group and let S be a finite subset with $1 \in S$. One may have $\alpha_1 > \alpha_{-1}$ [57]. We may even have $\kappa_1 > \kappa_{-1}$ if G is infinite. We have seen that $\kappa_k = \kappa_{-k}$ and that $\alpha_k = \alpha_{-k}$ if G is abelian since the Cayley graph defined by S is isomorphic to its reverse. We shall define subsets having this property:

The set S is said to be *normal* if $xSx^{-1} = S$, for every $x \in G$.

It would be too restrictive to deal only with normal subsets, since the isopermetric results are valid for translate copies of some set. We consider the following more general notion:

We shall say that S is *semi-normal* if there is $a \in G$ such that for $xSx^{-1} = Sa^{-1}xax^{-1}$, for every $x \in G$.

In this case we have

$$x(Sa^{-1})x^{-1} = Sa^{-1}xax^{-1}xa^{-1}x^{-1} = Sa^{-1}.$$

In particular Sa^{-1} is normal. On the other side it is an easy exercise to see that Xa is *semi-normal* if X is normal.

Lemma 9.5. — *Let S be a finite generating semi-normal subset of a group G with $1 \in S$. Then the map $Y \mapsto a^{-1}Y^{-1}a$ is a bijection from the set of k–fragments of S onto the set of k–fragments of S^{-1}. In particular $\kappa_k = \kappa_{-k}$, $\alpha_k = \alpha_{-k}$ and $\omega_k = \omega{-}k$.*

Proof. — By the definition of a semi-normal subset we have $XS = Sa^{-1}Xa$, for every subset a. Let X be a subset with $\min(|X|, |G|-|XS^{-1}|) \geqslant k$. Then $|XS^{-1}|-|X| = |SX^{-1}|-|X| = |aX^{-1}a^{-1}S|-|X| \geqslant \kappa_k(S)$. It follows that $\kappa_k \leqslant \kappa_{-k}$.

Similarly for every subset Y with $\min(|Y|, |G|-|YS|) \geqslant k$. Then $|YS|-|Y| = |Sa^{-1}Ya|-|Y| = |Y^{-1}aS^{-1}|-|Y| \geqslant \kappa_{-k}(S)$. It follows also that the map $Y \mapsto a^{-1}Y^{-1}a$ is a bijection from the set of k–fragments of S onto the set of k–fragments of S^{-1}. Therefore $\alpha_k = \alpha_{-k}$ and $\omega_k = \omega_{-k}$. □

The next result extends to the infinite case Arad-Muzychuk Theorem 3.1 of [1]. Our terminologies differ slightly.

Corollary 9.6. — *Let S be a finite generating semi-normal subset of a group G with $1 \in S$. Let H be a 2-atom of S such that $1 \in H$. If $|H| \geqslant \kappa_2 - |S| + 4$, then H is subgroup of G and $[G : N_G(H)] \leqslant 2$.*

Proof. — By Lemma 9.5, $\alpha_2 = \alpha_{-2}$, $\kappa_2 = \kappa_{-2}$ and $\omega_2 = \omega_{-2}$. By Theorem 9.3, $\omega_2 \leqslant 2$.

Take a 3–subset $\{a_1, a_2, a_3\}$ contained in H. Then two of the 2–atoms $a_1^{-1}H, a_2^{-1}H, a_3^{-1}H$ must be equal and hence $2 \leqslant |\Pi^l(H)| = |\Pi^r(H^{-1})|$. By Lemma 9.5, H^{-1} is a negative 2–atom. By Lemma 5.1, H^{-1} is a subgroup. Therefore H is a subgroup and $xS = Sa^{-1}xa$. Clearly $|xHx^{-1}S| = |xHSa^{-1}x^{-1}a| = |HS|$. Therefore xHx^{-1} is a 2–atom for every x. If $xHx^{-1} = H$, for every x then $N_G(H) = G$. Suppose that there is a such that $aHa^{-1} \neq H$.

We have $[G : N_G(H)] \leqslant 2$, since for every $x \in G$, we have $xHx^{-1} = H$ or $xHx^{-1} = aH$, otherwise $\omega_2 \geqslant 3$, a contradiction. □

10. The strong isoperimetric property

In this section, we prove the strong ioperimetric property which allows to use the structure of atoms to calculate all the fragments in some important cases. The strong isoperimetric methodology will be used in a coming papers [24, 14] to extend Kemperman's critical pair Theory using Theorem 8.3.

We shall use a mi-max result proved by Menger [39] for symmetric graphs and generalized to arbitrary graphs by Dirac [9]. The Dirac-Menger Theorem is now a basic tool in Additive number Theory [40, 54]. In particular it was used by Ruzsa [49] to give a simple proof of the Pluünnecke inequalities. We need it to prove the strong isoperimetric property. In the Appendix, we give a simple isoperimetric proof of this result.

Let $\Gamma = (V, E)$ be graph and let $a, b \in V$. A *path* from a to b is a sequence of arcs $\sigma = \{(x_1, y_1), \cdots, (x_k, y_k)\}$ with $x_i = y_{i+1}$ for all $1 \leqslant i \leqslant k-1$, $x_1 = a$ and $y_k = b$. We put $V(\sigma) = \{x_1, \cdots, x_k, y_k\}$. Two paths σ, τ from a to b will be said to be *openly* disjoint if $V(\sigma) \cap V(\tau) \subset \{a, b\}$.

Let x, y be elements of V. We shall say that x is *k–connected* to y in Γ if $|\partial(A)| \geqslant k$, for every subset A with $x \in A$ and $y \notin A \cup \Gamma(A)$.

Theorem 10.1 (Dirac-Menger). — *Let $\Gamma = (V, E)$ be a finite reflexive graph Let k be a nonnegative integer. Let $x, y \in V$ such that x is k–connected y, and $(x, y) \notin E$. Then there are k openly disjoint paths from x to y.*

One may formulate Menger's Theorem for non reflexive graphs. Such a formulation follows easily from the reflexive case.

We need the following consequence of Menger's Theorem.

Corollary 10.2. — *Let Γ be a locally finite reflexive graph and let k be a nonnegative integer with $k \leqslant \kappa_1$. Let X a finite subset of V such that* $\min(|V| - |X|, |X|) \geqslant k$. *Then there are pairwise distinct elements $x_1, x_2, \cdots, x_k \in X$ and pairwise distinct elements $y_1, y_2, \cdots, y_k \notin X$ such that*

$$(x_1, y_1), \cdots, (x_k, y_k) \in E.$$

Proof. — By the definition of κ_1, we have $|\partial(Y)| \geqslant \min(|V| - |Y|, \kappa_1) \geqslant k$, for every $Y \subset V$. Let $\Phi = (\Gamma(X), E')$ be the restriction of Γ to $\Gamma(X)$ (observe that $X \subset \Gamma(X)$). Choose two elements $a, b \notin V$. Let Ψ be the reflexive graph obtained by connecting a to $X \cup \{a\}$ and $\partial(X) \cup \{b\}$ to b. We shall show that a is k–connected to b in Ψ. Take $a \in T$ such that $b \notin \Psi(T)$. Then clearly $T \subset X \cup \{a\}$. Assume first $T = \{a\}$. Then $|\Psi(T)| - |T| = |X \cup \{a\}| - 1 \geqslant k$. Assume now $T \cap X \neq \emptyset$. We have $\Psi(T) = X \cup \{a\} \cup \Gamma(T \cap X)$. Therefore

$$|\Psi(T)| \geqslant 1 + |X| + |\Gamma(T \cap X) \setminus X| \geqslant 1 + |X| + (|T \cap X| + \kappa_1(\Gamma) - |X|) > k.$$

By Menger's Theorem there are $P_1, \cdots, P_k$ openly disjoint paths from a to b. Choose x_i as the last point of the path P_i belonging to X and let y_i the successor of x_i on the path P_i. This choice satisfies the requirements of the proposition. $\square$

We call the property given in Corollary 10.2 the *strong isoperimetric property.*

We shall use this property in the special case:

Proposition 10.3. — *Let G be an abelian group and let S be a finite subset of G with $1 \in S$. Let H be a subgroup of G which is a 2–fragment of S. Let $S = S_0 \cup \cdots \cup S_u$ and $X = X_1 \cup \cdots \cup X_t$ be H-decompositions. Also assume that $|G| - (t+1)|H| \geqslant u|H|$. Then there are pairwise distinct elements $n_1, n_2, \cdots, n_r \in [0, t]$ and elements $y_1, y_2, \cdots, y_r \in S \setminus H$ such that*

$$|\phi(X \cup (X_{n_1} y_1) \cup \cdots \cup (X_{n_r} y_r)| = t + 1 + u.$$

Proof. — Let ϕ denotes the canonical morphism from G onto G/H. Let us show that $\kappa_1(\phi(S)) \geqslant u$.

Let $Y \subset G/H$ be such that $Y + \phi(S) \neq G$. By the definition we

$$\begin{aligned} |\phi^{-1}(Y) + S| &\geqslant |\phi^{-1}(Y)| + \kappa_2(S) \\ &= |\phi^{-1}(Y)| + u|H|. \end{aligned}$$

Therefore $|Y + \phi(S)| \geqslant |Y| + u$.

The result follows now by applying Corollary 10.2 to $\phi(X)$ and $\phi(S)$. $\square$

Proposition 10.3 follows easily by Hall marriage Lemma if $X = S$.

11. Appendix: An isoperimetric proof of Menger's Theorem

We present here an isoperimetric proof of Menger's Theorem. Let $E \subset V \times V$ and let $\Gamma = (V, E)$ be a reflexive graph. Let x, y be elements of V. The graph Γ will be called *(x, y)–k–critical* if x is k–connected to y in Γ, and if this property is destroyed by the deletion of every arc (u, v) with $u \neq v$.

A subset A with $x \in A$ and $y \notin \Gamma(A)$ and $|\partial(A)| = k$ will be called a *k–part* with respect to (x, y, Γ).

The reference to (x, y) will be omitted.

Lemma 11.1. — *Assume that $\Gamma = (V, E)$ is k–critical and let $(u, v) \in E$ be an arc with $u \neq v$. Then Γ has k–part F with $u \in F$ and $v \in \partial(F)$.*

Proof. — Consider the graph $\Psi = (V, E \setminus \{(u, v)\})$. There is an F with $x \in F$ and $y \notin \Psi(F)$ such that $|\partial_\Psi(F)| < k$. This forces that $u \in F$ and that $v \in \partial(F)$, since otherwise $\partial_\Psi(F) = \partial_\Gamma(F)$.

Since $\partial_\Psi(F) \cup \{v\} \supset \partial_\Gamma(F)$, we have $|\partial_\Gamma(F)| \leqslant k$. We must have $|\partial_\Gamma(F)| = k$, since u is k–connected to v in Γ. This shows that F is a k-part. $\square$

Lemma 11.2. — *Let F be a k–part with respect to (x, y, Γ). Then $F^{\curlywedge}$ is a k–part a with respect to (y, x, Γ^{-1}). Moreover $\partial_-(F^{\curlywedge}) = \partial(F)$.*

In particular y is k–connected to x in Γ^{-1}, if x is k–connected to y in Γ.

Proof. — We have clearly $\partial_-(F^{\curlywedge}) \subset \partial(F)$. Put $C = \partial(F) \setminus \partial_-(F^{\curlywedge})$. Since $y \notin \Gamma(F \cup C)$, we have $k \leqslant |\partial(F \cup C)| \leqslant |\partial_-(F^{\curlywedge})| \leqslant |\partial(F)| = k$. □

The above lemma is a local version of the isoperimetric duality given in Lemma 3.4.

Lemma 11.3. — *Assume that $\Gamma = (V, E)$ is k–critical and that $\Gamma(x) \cap \Gamma^{-1}(y) = \emptyset$. There is a k–part F of Γ such that* $\min(|F|, |F^{\curlywedge}|) \geqslant 2$.

Proof. — Take a path $[x, a, b, \cdots, c, y]$ of minimal length from x to y. By Lemma 11.1, there is a k-part F, with $a \in F$ and $b \in \partial(F)$. We have $\{x, a\} \subset F$. We have $|F^{\curlywedge}| \geqslant 2$ since otherwise $F^{\curlywedge} = \{y\}$. Hence by Lemma 11.2, $b \in \partial(F) = \partial^-(\{y\})$. Therefore $b \in \Gamma(x) \cap \Gamma^{-1}(y)$, a contradiction. □

Let x be an element of V and let $T = \{y_1, \cdots, y_k\}$ be a subset of $V \setminus \{v\}$. A family of k–openly disjoint paths $P_1, \cdots, P_k$, where P_i is a path from x to y_i will be called an *(x, T)–fan*.

Proof of Theorem 10.1. — The proof is by induction, the result being obvious for $|V|$ small. Assume first that there $z \in \Gamma(x) \cap \Gamma^{-1}(y)$. Consider the restriction Ψ of Γ to $V \setminus \{z\}$. Clearly x is $(k-1)$–connected to y in Ψ. By the induction hypothesis there are $(k-1)$–openly disjoint paths from x to y in Ψ. We adjoin the path $[x, z, y]$ to these paths and we are done. So we may assume that $\Gamma(x) \cap \Gamma^{-1}(y) = \emptyset$.

By Lemma 11.3 there is a part F with $\min(|F|, |F^{\curlywedge}|) \geqslant 2$. Consider the reflexive graph $\Theta = (V', E')$ obtained by contracting $F^{\curlywedge}$ to a single vertex y_0. We have $V' = (V \setminus F^{\curlywedge}) \cup \{y_0\}$. Since $|V'| < |V|$, by the induction hypothesis there are k openly disjoint paths form x yo y_0. By deleting y_0 we obtain an $(x, \partial(F))$–fan. Similarly by contracting F and applying induction, we form a $(\partial(F), y)$–fan.

By composing these two fans, we form k openly disjoint paths from x to y. □

Acknowledgement. This paper was revised while the author is visiting Centre de Recerca Matemàtica, Barcelona, Catalonia, Spain. The author would like to thank this Institute and Professor Oriol Serra for their hospitality. Many thanks also for an anonymous referee for many valuable comments.

BIBLIOGRAPHY

[1] Z. Arad & M. Muzychuk, "Order evaluation of products of subsets in finite groups and its applications. II.", *Trans. Amer. Math. Soc.* **349** (1997), no. 11, p. 4401-4414.

[2] E. Balandraud, "Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser", december 2005, Preprint.

[3] L. V. Brailowski & G. A. Freiman, "On a product of finite subsets in a torsion free group", *J. Algebra* **130** (1990), p. 462-476.

[4] A. Cauchy, "Recherches sur les nombres", *J. École polytechnique* **9** (1813), p. 99-116.

[5] S. Chowla, "A theorem on the addition of residue classes: applications to the number $\Gamma(k)$ in Waring's problem", *Proc. Indian Acad. Sc.* **2** (1935), p. 242-243.

[6] H. Davenport, "On the addition of residue classes", *J. London Math. Soc.* **10** (1935), p. 30-32.

[7] J. M. Deshouillers & G. A. Freiman, "A step beyond Kneser's Theorem", *Proc. London Math. Soc.* **86** (2003), no. 3, p. 1-28.

[8] G. T. Diderrich, "On Kneser's addition theorem in groups", *Proc. Amer. Math. Soc.* (1973), p. 443-451.

[9] G. A. Dirac, "Extensions of Menger's theorem", *J. Lond. Math. Soc.* **38** (1963), p. 148161.

[10] J. Dixmier, "Proof of a conjecture by Erdös, Graham concerning the problem of Frobenius", *J. number Theory* **34** (1990), p. 198-209.

[11] F. J. Dyson, "A theorem on the densities of sets of integers", *J. London Math. Soc.* **20** (1945), p. 8-14.

[12] P. Erdős & H. Heilbronn, "On the Addition of residue classes mod p", *Acta Arith.* **9** (1964), p. 149-159.

[13] B. Green & I. Z. Ruzsa, "Sets with small sumset and rectification", *Bull. London Math. Soc.* **38** (2006), no. 1, p. 43-52.

[14] Y. O. Hamidoune, "Beyond Kemperman's Structure Theory: The isoperimetric approach", In preparation.

[15] ———, "Sur les atomes d'un graphe orienté", *C.R. Acad. Sc. Paris A* **284** (1977), p. 1253-1256.

[16] ———, "An application of connectivity theory in graphs to factorizations of elements in groups", *Europ. J. of Combinatorics* **2** (1981), p. 349-355.

[17] ———, "Quelques problèmes de connexité dans les graphes orientés", *J. Comb. Theory* **B 30** (1981), p. 1-10.

[18] ———, "On the connectivity of Cayley digraphs", *Europ. J. Combinatorics* **5** (1984), p. 309-312.

[19] ———, "On a subgroup contained in words with a bounded length", *Discrete Math.* **103** (1992), p. 171-176.

[20] ———, "An isoperimetric method in additive theory", *J. Algebra* **179** (1996), no. 2, p. 622-630.

[21] ———, "On subsets with a small sum in abelian groups I: The Vosper property", *Europ. J. of Combinatorics* **18** (1997), p. 541-556.

[22] ———, "On small subset product in a group. Structure Theory of set-addition", *Astérisque* **258** (1999), p. 281-308, xiv-xv.

[23] ———, "Some results in Additive number Theory I: The critical pair Theory", *Acta Arith.* **96** (2000), no. 2, p. 97-119.

[24] ———, "Hyper-atoms and the Kemperman's critical pair Theory", September 2007, Preprint.

[25] Y. O. Hamidoune & Ø. J. Rødseth, “On bases for σ-finite groups”, *Math. Sc.* **78** (1996), no. 2, p. 246-254.

[26] ———, “An inverse theorem modulo p”, *Acta Arithmetica* **92** (2000), p. 251-262.

[27] Y. O. Hamidoune, O. Serra & G. Zémor, “On the critical pair theory in Abelian groups: Beyond Chowla’s Theorem”, September 2006, Preprint.

[28] ———, “On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$”, *Acta Arith.* **121** (2006), no. 2, p. 99-115.

[29] N. Hegyvári, “On iterated difference sets in groups”, *Period. Math. Hungar.* **43** (2001), no. 1-2, p. 105-110.

[30] R. Jin, “Solution to the inverse problem for upper asymptotic density”, *J. Reine Angew. Math.* **595** (2006), p. 121-165.

[31] V. Jungić, J. Licht, M. Mahdian, J. Nešetřil, R. Jaroslav & R. Radoičić, “Rainbow arithmetic progressions and anti-Ramsey results. Special issue on Ramsey theory”, *Combin. Probab. Comput.* **12** (2003), no. 5-6, p. 599-620.

[32] G. Károlyi, “Cauchy-Davenport theorem in group extensions”, *Enseign. Math.* **(2)51** (2005), no. 3-4, p. 239-254.

[33] J. H. B. Kemperman, “On complexes in a semigroup”, *Nederl. Akad. Wetensch. Proc. Ser. A* **59** (1956), no. 18, p. 247-254, Indag. Math.

[34] ———, “On small sumsets in Abelian groups”, *Acta Math.* **103** (1960), p. 66-88.

[35] M. Kneser, “Abschätzung der asymptotischen Dichte von Summenmengen”, *Math. Z.* **58** (1953), p. 459-484.

[36] ———, “Summenmengen in lokalkompakten abelesche Gruppen”, *Math. Zeit.* **66** (1956), p. 88-110.

[37] H. B. Mann, “An addition theorem for sets of elements of an Abelian group”, *Proc. Amer. Math. Soc.* **4** (1953), p. 423.

[38] ———, *Addition Theorems*, R.E. Krieger, New York, 1976.

[39] K. Menger, “Zur allgemeinen Kurventhoerie”, *Fund. Math.* **10 Karl** (1927), p. 96-115.

[40] M. B. Nathanson, “Additive Number Theory. Inverse problems and the geometry of sumsets”, in *Grad. Texts in Math.* (Springer, ed.), vol. 165, 1996.

[41] N. Nikolov & D. Segal, “On finitely generated profinite groups. I. Strong completeness and uniform bounds”, *Ann. of Math.* **(2) 165** (2007), no. 1, p. 171-238.

[42] ———, “On finitely generated profinite groups. II. Products in quasisimple groups”, *Ann. of Math.* **(2) 165** (2007), no. 1, p. 239-273.

[43] J. E. Olson, “Sums of sets of group elements”, *Acta Arith.* **28** (1975/76), no. 2, p. 147-156.

[44] ———, “On the sum of two sets in a group”, *J. Number Theory* **18** (1984), p. 110-120.

[45] ———, “On the symmetric difference of two sets in a group”, *Europ. J. Combinatorics* (1986), p. 43-54.

[46] A. Plagne, “(k, l)-free sets in $\mathbb{Z}/p\mathbb{Z}$ are arithmetic progressions”, *Bull. Austral. Math. Soc.* **65** (2002), no. 1, p. 137-144.

[47] L. Pyber, “Bounded generation and subgroup growth”, *Bull. London Math. Soc.* **34** (2002), no. 1, p. 55-60.

[48] Ø. J. Rødseth, “Two remarks on linear forms in non-negative integers”, *Math. Scand.* **51** (1982), p. 193-198.

[49] I. Ruzsa, “An application of graph theory to additive number theory”, *Scientia, Ser. A* **3** (1989), p. 97109.

[50] O. Serra, "An isoperimetric method for the small sumset problem", in *Surveys in combinatorics*, London Math. Soc. Lecture Note Ser., vol. 327, Cambridge Univ. Press, Cambridge, 2005, p. 119-152.

[51] O. Serra & G. Zémor, "On a generalization of a theorem by Vosper", Integers, 2000, 0, A10, (electronic).

[52] J. C. Shepherdson, "On the addition of elements of a sequence", *J. London Math Soc.* **22** (1947), p. 85-88.

[53] E. Szemerédi, "On a conjecture of Erdös and Heilbronn", *Acta Arithmetica* **17** (1970), p. 227-229.

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

[55] G. Vosper, "Addendum to: The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956), p. 280-282.

[56] ———, "The critical pairs of subsets of a group of prime order", *J. London Math. Soc.* **31** (1956), p. 200-205.

[57] G. Zémor, "On positive and negative atoms of Cayley digraphs", *Discrete Appl. Math.* **23** (1989), no. 2, p. 193-195.

Manuscrit reçu le 4 juin 2007,
accepté le 11 janvier 2008.

Yahya O. HAMIDOUNE
Université Paris 06
UPMC
E. Combinatoire
4, place Jussieu
75005 Paris (France)
hamidoune@math.jussieu.fr