Astérisque

YAHYA OULD HAMIDOUNE

On small subset product in a group

Astérisque, tome 258 (1999), p. 281-308

<http://www.numdam.org/item?id=AST_1999__258__281_0>

Astérisque **258**, 1999, p. 281–308

ON SMALL SUBSET PRODUCT IN A GROUP

by

Yahya Ould Hamidoune

Abstract. — We generalise some known addition theorems to non abelian groups and to the most general case of relations having a transitive group of automorphisms.

The classical proofs of addition theorems use local transformations due to Davenport, Dyson and Kempermann. We present a completely different method based on the study of some blocks of imprimitivity with respect to the automorphism group of a relation.

Several addition theorems including the finite $\alpha + \beta$-Theorem of Mann and a formula proved by Davenport and Lewis will be generalised to relations having a transitive group of automorphisms.

We study the critical pair theory in the case of finite groups. We generalise Vosper Theorem to finite not necessarily abelian groups.

Chowla, Mann and Straus obtained in 1959 a lower bound for the size of the image of a diagonal form on a prime field. This result was generalised by Tietäväienen to finite fields with odd characteristics. We use our results on the critical pair theory to generalise this lower bound to an arbitrary division ring.

Our results apply to the superconnectivity problems in networks. In particular we show that a loopless Cayley graph with optimal connectivity has only trivial minimum cuts when the degree and the order are coprime.

1. Introduction

Let p be a prime number, and let A and B be two subsets of $\mathbf{Z}_p$, such that $|A|$, $|B| \geq 2$. The Cauchy-Davenport Theorem states that

$$|A + B| \geq \min(p, |A| + |B| - 1),$$

cf. [2,5]. Vosper Theorem states that

$$|A + B| \geq \min(p - 1, |A| + |B|),$$

unless A and B form arithmetic progressions, cf. [31,32]. Freiman obtained a structure theorem for all $A \subset \mathbf{Z}_p$ such that $|2A| < 12|A|/5 - 3$, cf. [26].

1991 ***Mathematics Subject Classification.*** — Primary: 20D60, Secondary: 20K01, 11B13, 11B75, 05C25.

Key words and phrases. — Addition theorems, blocks of imprimitivity, network reliability.

Let A and B be finite subsets of an abelian group G. We shall say that B a Cauchy subset if for every finite non-empty subset X,

$$|X+B| \geq \min(|G|, |X|+|B|-1).$$

Mann proved in [24] that B is a Cauchy subset if and only if for every finite subgroup H, $|H+B| \geq \min(|G|, |H|+|B|-1)$. Kneser Theorem states that $|A+B| < |A|+|B|-1$ only if there is a finite non-null subgroup H such that $A+H+B = A+B$. Some progress toward the determination of all pairs A, B such that $|A+B| \leq |A|+|B|-1$ is obtained by Kempermann in [20]. In [14], we could classify all the pairs, $\{A, B\}$ with $|A+B| = |A|+|B|-1$, if B is a Cauchy subset.

Less results are know in the non-abelian case. The classical basic tools in this case are two nice results proved by Kempermann in [19]. No generalisation of Kneser Theorem is known in the non-abelian case. The natural one is false in general, cf. [28,33]. Diderrich obtained in [7] a generalisation of Kneser Theorem in the case where the elements of B commute. But this result is an easy corollary of Kneser Theorem as showed in [13]. Brailowski and Freiman obtained a Vosper Theorem in free torsion groups, cf. [1]. It was observed recently that some results involving the connectivity of Cayley graphs are strongly related to addition theorems. This connection will be explained below.

A natural question consists of asking how addition Theorems generalise to a group acting on a set. The connectivity of Cayley graphs belongs to this kind of problems. The connectivity of a reflexive relation $\Gamma = (V, E)$ is

$$\kappa(\Gamma) = \min\{|\Gamma(F)| - |F| : 1 \leq |\Gamma(F)| < |V|\}.$$

Let B be a finite subset of a group G containing 1 and let Γ be the Cayley relation $x^{-1}y \in B$. In this case, $\kappa(\Gamma)$ is the best possible lower bound for $|AB^{-1}| - |A|$, where $AB \neq G$. The Cauchy-Davenport Theorem may be expressed using this language as $\kappa(\Gamma) = |B| - 1$, for $|G|$ prime. Under this formulation, this result was rediscovered in [9]. The method used in [9] is based on the study of blocks of imprimitivity with respect to the group of automorphisms. The same method is used in [12] to prove a local generalisation of Mann Theorem for finite groups. Zemor used the same method in [33] to obtain a global one. More complicated blocks are studied in [14] to calculate the critical pairs in Mann Theorem in the abelian case.

The connection between connectivity problems and addition theorems were observed only recently.

The results obtained in [14] are strongly based on the well known fact that an abelian Cayley relation is isomorphic to its reverse. We generalise some of the results to the non abelian case. The organisation of the paper is as follows. In section 2, we study the connectivity of relations. We give also lemmas allowing to translate connectivity bounds into addition theorems. We improve some results contained in [9,10,11,12,14]. In section 3, we generalise several basic additive inequalities. In particular, we give a generalisation of Mann Theorem to non-abelian groups and to relations with a transitive group of automorphisms. We generalise also a formula proved by Davenport and Lewis for finite fields to division rings and to arc-transitive

relations. We generalise also a result proved by Olson [27] to point transitive relations. This generalisation in the finite case was proved in [10, Proposition 3.4]. In section 4, we study the superatoms. They form the main tool for the critical pair problem in our approach. The main result of section 5 is the following result which characterizes the equality cases in Mann Theorem. We state it below.

Let B be a subset of a finite group G such that $1 \in B$. Then the following conditions are equivalent.

(i) For all $A \subset G$ such that $2 \leq |A|$,

$$|AB| \geq \min(|G| - 1, |A| + |B|).$$

(ii) For every subgroup H of G and for every $a \in G$ such that $|H \cup Ha| \geq 2$,

$$\min(|B(H \cup aH)|, |(H \cup Ha)B|) \geq \min(|G| - 1, |H \cup Ha| + |B|).$$

The main result of section 6 is a critical pair theorem which generalises Vosper Theorem. We state it below.

Let G be a finite group and let B be a Cauchy subset of G such that $(|G|, |B|-1) = 1$. Let $A \subset G$ such that

$$|AB| = |A| + |B| - 1 \leq |G| - 1.$$

Then one of the following conditions holds.

(i) $|A| = 1$ or $A = G \setminus aB^{-1}$, for some $a \in G$.

(ii) There are $a, b, r \in G$, $k, s \in \mathbf{N}$ such that

$$A = \{a, ar, ar^2, \ldots, ar^{k-1}\} \quad \text{and} \quad B = (G \setminus \langle r \rangle b) \cup \{b, rb, r^2b, \ldots, r^{s-1}b\}.$$

(iii) There are $a, b, r \in G$, $k, s \in \mathbf{N}$ such that

$$A = \{ab^{-1}, arb^{-1}, ar^2b^{-1}, \ldots, ar^{k-1}b^{-1}\} \quad \text{and} \quad B = (G \setminus b\langle r \rangle) \cup \{b, rb, r^2b, \ldots, r^{s-1}b\}.$$

One of the classical applications of the critical pair theory is the estimation of the range of a diagonal form. Using Vosper's Theorem, Chowla, Mann and Straus obtained in [4] an estimation of the range of a diagonal form over $\mathbf{Z}_p$. Tietäväinen obtained in [30] the same bound in the case of finite fields with odd characteristics. We gave in [14] a proof for all finite fields based on the method of superatoms. We generalise this bound to all division rings in this paper as follows.

Let R be a division ring and let P be a finite subset of R such that $0 \in P$ and $P \setminus 0$ is multiplicative subgroup. Let R_0 be the additive subgroup generated by P. Suppose that $|P| \geq 4$ and let $a_1, a_2, \ldots, a_n$ be non-zero elements of R. Then

$$|a_1P + a_2P + \cdots + a_nP| \geq \min(|R_0|, (2n - 1)(|P| - 1) + 1).$$

In section 8, we apply our results to solve some problems raised in network Theory. We also explain the connections between Cayley graphs reliability and Additive group Theory. In particular we show that a loopless Cayley graph with optimal connectivity has only trivial minimum cuts when the degree and the order are coprime.

2. The connectivity of a relation

In this section we study subsets with a small image with respect to a given relation. Restricted to Cayley relations defined on a group, this problem becomes the study of subsets with a small product. The results obtained in this section improve slightly our previous results obtained in [9,10,11,12,14].

The cardinality of a finite set V will be denoted by $|V|$. For an infinite set V, we write $|V| = \infty$. By a *relation* we mean an ordered pair $\Gamma = (V, E)$, where V is a set and E is a subset of $V \times V$. A permutation σ of V is said to be an automorphism of Γ if $E = \{(\sigma(x), \sigma(y)) : (x, y) \in E\}$. The group of automorphisms of Γ will be denoted by $\mathrm{Aut}(\Gamma)$. A relation will be called *point transitive* if its group of automorphisms acts transitively on V. Let $A \subset V$. The *subrelation induced* on A is $\Gamma[A] = (A, E \cap (A \times A))$.

We introduce some notations. Let $\Gamma = (V, E)$ be a relation and let F be a subset of V. The *image* of F will be denoted by $\Gamma(F)$. We recall that

$$\Gamma(F) = \{y \in V : \text{ there is } x \in F \text{ such that } (x, y) \in E\}.$$

We write $\partial_\Gamma(F) = \Gamma(F) \setminus F$ and $\delta_\Gamma(F) = V \setminus (F \cup \Gamma(F))$. The reference to Γ will be omitted when the meaning is clear from the context. In particular we shall write $\partial_{\Gamma^-}(F) = \partial^-(F)$ and $\delta_{\Gamma^-}(F) = \delta^-(F)$. The *degree* of a point $x \in V$ is by definition $d_\Gamma(x) = |\Gamma(x)|$. A relation Γ is said to be *locally finite* if both Γ and Γ^- have only finite degrees. A relation $\Gamma = (V, E)$ is said to be *regular* if Γ is locally finite and if all $x, y \in V$, $|\Gamma(x)| = |\Gamma(y)|$ and $|\Gamma^-(x)| = |\Gamma^-(y)|$. Let Γ be a regular relation. The degree of every point with respect to Γ will be called the degree of Γ and denoted by $d(\Gamma)$.

A relation Γ on a set V is said to be *connected* if $\Gamma(A) \not\subset A$ for every finite proper subset A of V. A subset C of V is said to be *connected* if $\Gamma[C]$ is connected. A *block* of Γ is a subset B of V such that for every automorphism f of Γ, either $f(B) = B$ or $f(B) \cap B = \varnothing$.

The following remark is easy to show and well known.

Remark 2.a. — If Γ is regular and if V is finite then $d(\Gamma) = d(\Gamma^-)$.

Let Γ be a reflexive relation on V. The *connectivity* of Γ is by definition:

$$\kappa(\Gamma) = \min\{|\partial(F)| : 1 \leq |\Gamma(F)| < |V| \text{ or } |F| = 1\}.$$

The inequality $1 \leq |\Gamma(F)| < |V|$ is never satisfied if $V \times V = \Gamma$. In the other cases,

$$\kappa(\Gamma) = \min\{|\partial(F)| : 1 \leq |\Gamma(F)| < |V|\}.$$

Remark 2.b. — The connectivity of a relation coincides with the connectivity of its reflexive closure. For this reason we restrict ourselves to reflexive relations. This choice simplifies the proofs and the notations. In some previous papers [9,10,11,12] we adopted the opposite choice, where a relation is assumed to be disjoint from its diagonal. These two choices are essentially equivalent.

Lemma 2.1. — *Let Γ be a locally finite reflexive relation. Then $\kappa(\Gamma)$ is the maximal k such that for every non-empty finite subset A, $|\Gamma(A)| \geq \min(|V|, |A| + k)$.*

Proof. — The Lemma follows easily from the definitions. □

One see easily that a locally finite reflexive relation Γ on a set V is connected if and only if $\kappa(\Gamma) \geq 1$.

Let Γ be a locally finite reflexive relation on V and let F be a subset of V. We say that F is a *fragment* of Γ if the following conditions are satisfied.

(i) $\kappa(\Gamma) = |\partial(F)|$ and $\Gamma(F) \neq V$.
(ii) F is finite or $V \setminus F$ is finite.

A fragment with minimal cardinality will be called an *atom*. The cardinality of an atom of Γ will be denoted by $\mu(\Gamma)$. We see easily that an atom is always finite. We write $\rho(\Gamma) = \min(d(x); x \in V)$. Observe that $\rho(\Gamma)$ is the minimal degree.

***Lemma 2.2* ([9]).** — *Let Γ be a locally finite reflexive relation on a set V and let A be an atom of Γ. Then $\Gamma[A]$ is connected. Moreover $\kappa(\Gamma) \leq \rho(\Gamma) - 1$ and equality holds if and only if $\mu(\Gamma) = 1$ or $\Gamma = V \times V$.*

Proof. — Lemma 2.2 follows easily from the definitions. □

***Lemma 2.3* ([9]).** — *Let Γ be a reflexive relation on a finite set V. Then $\kappa(\Gamma) = \kappa(\Gamma^-)$.*

Proof. — The equality is obvious if $\Gamma = V \times V$. Suppose the contrary and let F be a fragment of Γ. We have clearly $\partial^-(\delta(F)) = \partial^-(V \setminus \Gamma(F)) \subset \partial(F)$. By the definition we have

$$\kappa(\Gamma^-) \leq |\partial^-(\delta(F))| \leq |\partial(F)| = \kappa(\Gamma).$$

The other inequality follows by duality. □

We use the following result.

***Lemma 2.4* ([9]).** — *Let Γ be a locally finite reflexive relation on a set V such that $\kappa(\Gamma) = \kappa(\Gamma^-)$. Let F and M be two fragments of Γ. Then*

(i) $\partial^-(\delta(F)) = \partial(F)$ and $\delta^-(\delta(F)) = F$.
(ii) $\delta(F)$ is a fragment of Γ^-.
(iii) $F \subset M$ if and only if $\delta(F) \supset \delta(M)$.

Proof. — We have clearly

$$\partial^-(\delta(F)) = \partial^-(V \setminus \Gamma(F)) \subset \partial(F).$$

If $\delta(F)$ is finite, then

$$|\partial^-(\delta(F))| \geq \kappa(\Gamma^-) = \kappa(\Gamma) = |\partial(F)|.$$

Therefore $\partial^-(\delta(F)) = \partial(F)$. Assume now that $\delta(F)$ is infinite. Hence F is finite. We shall prove that $\partial(F) \subset \partial^-(\delta(F))$. Suppose on the contrary that there exists $x \in \partial(F) \setminus \partial^-(\delta(F))$. It follows that $\Gamma(F \cup \{x\}) \subset \Gamma(F)$. Therefore

$$|\partial(F \cup \{x\})| \leq |\partial(F)| - 1 = \kappa(\Gamma) - 1.$$

It follows by the definition of κ that $|\Gamma(F \cup \{x\})| = \infty$, a contradiction. The first equality in (i) is proved. It follows that

$$\delta^-(\delta(F)) = V \setminus (\partial^-(\delta(F)) \cup \delta(F)) = V \setminus (\partial(F) \cup \delta(F)) = F.$$

Hence (i) holds. It follows that

$$|\partial^-(\delta(F))| = |\partial(F)| = \kappa(\Gamma) = \kappa(\Gamma^-).$$

Since $F \cap \Gamma^-(\delta(F)) = \varnothing$, $\delta(F)$ is a fragment of Γ^-. Thus (ii) is proved.

Suppose that $F \subset M$. We have $\delta(F) = V \setminus \Gamma(F) \supset V \setminus \Gamma(M) = \delta(M)$.

Suppose that $\delta(F) \supset \delta(M)$. We see as above that $\delta^-(\delta(F)) \subset \delta^-(\delta(M))$. Using (i) we obtain, $F \subset M$. □

We shall use the following lemma.

Lemma 2.5. — *Let Γ be reflexive relation on a set V. Let M be a finite fragment and let F be a fragment of Γ such that $M \cap F \neq \varnothing$. Then $|\delta(F) \setminus \delta(M)| \leq |M \setminus F|$.*

Suppose that $\kappa(\Gamma) = \kappa(\Gamma^-)$ or that F is finite. Then one of the following conditions holds.

(i) $\delta(F) \cap \delta(M) = \varnothing$.

(ii) $F \cap M$ is a fragment of Γ and $\Gamma(M \cap F) = \Gamma(M) \cap \Gamma(F)$.

Proof. — We have clearly

$$\Gamma(M \cap F) \subset \Gamma(M) \cap \Gamma(F) = M \cup \partial(M) \cap (F \cup \partial(F)).$$

Therefore

$$\partial(F \cap M) \subset (\partial(M) \setminus \delta(F)) \cup (M \cap \partial(F)). \tag{1}$$

Clearly $\Gamma(M \cap F) \neq V$. By the definition of the connectivity and since $|\partial(M)| = \kappa(\Gamma)$, we have $|\partial(M)| \leq |\partial(M \cap F)|$. Using (1), we have

$$|\delta(F) \cap \partial(M)| \leq |\partial(F) \cap M|. \tag{2}$$

It follows that

$$|\delta(F) \setminus \delta(M)| = |\delta(F) \cap M| + |\delta(F) \cap \partial(M)| \leq |\delta(F) \cap M| + |M \cap \partial(F)| = |M \setminus F|.$$

This proves the first part of the lemma.

We have clearly $\partial(M \cup F) \subset \partial(M) \cup \partial(F)$. Therefore

$$\partial(F \cup M) \subset (\partial(F) \setminus M) \cup (\delta(F) \cap \partial(M)). \tag{3}$$

Assume now $\delta(F) \cap \delta(M) \neq \varnothing$. It follows that $\Gamma(M \cup F) \neq V$. We shall show the following inequality.

$$|\partial(F) \cap M| \leq |\delta(F) \cap \partial(M)|. \tag{4}$$

Consider first the case where F is finite. By the definition of the connectivity and since $\Gamma(M \cup F) \neq V$ and $|\partial(F)| = \kappa(\Gamma)$, we have $|\partial(F)| \leq |\partial(M \cup F)|$. Using (3), we obtain (4). Assume now that $\kappa(\Gamma) = \kappa(\Gamma^-)$ and that F is infinite. By the definitions $\delta(F)$ is finite. By Lemma 2.4, $\delta(F)$ and $\delta(M)$ are fragments of Γ. By applying (2) to Γ^-, with M replaced by $\delta(F)$ and F replaced by $\delta(M)$, we obtain

$$|\delta^-\delta(M) \cap \partial^-(\delta(F))| \leq |\partial^-(\delta(M)) \cap \delta(F)|.$$

(4) follows now using Lemma 2.4.

By (2) and (4) we have

$$|M \cap \partial(F)| = |\partial(M) \cap \delta(F)|. \tag{5}$$

Since $\Gamma(F \cap M) \neq \varnothing$ and $\Gamma(F \cap M) \neq V$, we have $|\partial(F \cap M)| \geq \kappa(\Gamma)$. By (1) and (5) we have

$$\kappa(\Gamma) \leq |\partial(F \cap M)| \leq |(\partial(F) \setminus \delta(M)) \cup (K \cap \partial(M))| \leq |\partial(M)| = \kappa(\Gamma).$$

It follows that $F \cap M$ is a fragment of Γ. It follows also that

$$\partial(F \cap M) = (\partial(F) \setminus \delta(M)) \cup (F \cap \partial(M)).$$

Therefore

$$\Gamma(F \cap M) = (F \cap M) \cup (\partial(F) \setminus \delta(M)) \cup (F \cap \partial(M)) = \Gamma(F) \cap \Gamma(M).$$

□

Remark 2.c. — If A and B be two finite fragments such that $|A| = |B|$ then $|\delta(A)| = |\delta(B)|$.

Clearly we have $|\delta(B)| = |V| - (|B| + \kappa(\Gamma)) = |\delta(A)|$. □

The fundamental property of atoms is the following.

Proposition 2.6. — *Let A and B be two distinct atoms of a locally finite reflexive relation Γ and let F be a fragment of Γ. Suppose that $\kappa(\Gamma) = \kappa(\Gamma^-)$ or that F is finite.*

(i) Assume that $|A| \leq |\delta(F)|$. Then either $A \subset F$ or $A \cap F = \varnothing$.
(ii) Assume that $|A| \leq |\delta(A)|$. Then $A \cap B = \varnothing$.
(iii) Assume that $|A| \geq |\delta(A)| + 1$. Then $\delta(A) \cap \delta(B) = \varnothing$.

Proof. — Assume that $|A| \leq |\delta(F)|$ and suppose that $A \cap F \neq \varnothing$. By Lemma 2.5, we have

$$|\delta(F) \setminus \delta(A)| \leq |A \setminus F| < |A|.$$

Hence $\delta(F) \cap \delta(A) \neq \varnothing$. By Lemma 2.5, $A \cap F$ is a fragment of Γ. By the minimality of $|A|$, we have $A \cap F = A$. Therefore $A \subset F$. This proves (i).

Assume that $|A| \leq |\delta(A)|$ and that $A \cap B \neq \varnothing$. By Remark 2.c and (i), we have $A \cap B = \varnothing$, a contradiction. Hence (ii) is proved.

Assume that $|A| \geq |\delta(A)| + 1$ and that $\delta(A) \cap \delta(B) \neq \varnothing$. Clearly $|V|$ is finite.

By Lemma 2.5, we have

$$|A \setminus B| = |B \setminus A| \leq |\delta(A) \setminus \delta(B)|.$$

Therefore $A \cap B \neq \varnothing$. By Lemma 2.5, $A \cap B$ is a fragment. Hence $A = B$, a contradiction. □

Corollary 2.7. — *Let Γ be a locally finite reflexive relation such that either V is infinite or $\mu(\Gamma) \leq \mu(\Gamma^-)$. Let A be an atom of Γ and let F be a finite fragment of Γ. Then either $A \subset F$ or $A \cap F = \varnothing$.*

Proof. — The inequality $\mu(\Gamma^-) \leq |\delta(F)|$ holds clearly if V is infinite and follows in the finite case by Lemmas 2.3 and 2.4. Therefore $|A| = \mu(\Gamma) \leq \mu(\Gamma^-) \leq |\delta(F)|$. The result follows now using Proposition 2.6. □

The above result was proved for finite symmetric relations by Mader [23, sätz 1] and generalised to arbitrary finite relations in [9, proposition 1]. A basic property of atoms is the following.

Corollary 2.8. — *Let $\Gamma = (V, E)$ be a locally finite reflexive relation and let A be an atom of Γ.*

(i) Assume that $|A| \leq |\delta(A)|$. Then A is a block.
(ii) Assume that $|A| \geq |\delta(A)| + 1$. Then $\delta(A)$ is a block.

Proof. — Let f be an automorphism of Γ. Clearly $f(A)$ is an atom. We have also

$$f(\delta(A)) = f(V \setminus \Gamma(A)) = V \setminus \Gamma(f(A)) = \delta(f(A)).$$

The results follows now easily using Proposition 2.6. □

Let A and B be subsets of a group G. We write

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

Let $a \in G$, the *left translation* $\gamma_a : G \longrightarrow G$ is defined by the equality $\gamma_a(x) = ax$. As usual the image of a subgroup H by a left translation will be called a *left coset* of H.

Let S be a subset of G. The relation $x^{-1}y \ \in S$ is called a *Cayley relation.* It will be denoted by $\Lambda(G, S)$. Let $\Gamma = \Lambda(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = FS$.

The following result is easy to show and well known.

Lemma 2.9. — *Let G be a group and let S be a finite subset of G. Then $(\Lambda(G, S))^- = \Lambda(G, S^{-1})$.*

For every $a \in G$, $\gamma_a \in \mathrm{Aut}(\Lambda(G, S))$. In particular $\Lambda(G, S)$ is point transitive.

Cayley relations defined above form an important class of the relations with a transitive group of automorphisms.

We use the following result which is implicit in [12].

Lemma 2.10. — *Let G be a group containing a subset S and let B be a finite non-empty block of $\Lambda(G, S)$. Then B is a left coset of some subgroup of G.*

Proof. — Choose $b \in B^{-1}$ and set $H = bB$. Let $x \in H$. By Lemma 2.9, H is a block. Clearly $1 \in H$. Therefore $x \in H \cap \gamma_x(H)$, and hence $H = xH$. Therefore $HH = H$. Since H is finite, H is a subgroup. □

Theorem 2.11. — *Let G be a group and let S be a finite subset of G such that $1 \in S$. Let A be an atom of $\Lambda(G, S)$ containing an element a and let $b \in \delta(A)$.*

(i) If $|A| \leq |\delta(A)|$ then $a^{-1}A$ is a subgroup.
(ii) If $|A| \geq |\delta(A)| + 1$ then $b^{-1}\delta(A)$ is a subgroup.

Proof. — The result follows from Corollary 2.8 and Lemma 2.10. □

***Corollary 2.12* ([12, proposition 1]).** — *Let G be a group and let S be a finite subset of G such that $1 \in S$ and let A be an atom of $\Lambda(G,S)$ containing 1. Suppose that $\mu(\Lambda(G,S)) \leq \mu(\Lambda(G,S^{-1}))$. Then A is a subgroup. Moreover for every finite fragment F of $\Lambda(G,S)$, $FA = F$.*

Proof. — As shown in the proof of Corollary 2.7, we have $|A| = \mu(\Gamma) \leq \mu(\Gamma^-) \leq |\delta(F)|$. By Theorem 2.11, A is a subgroup. Since $1 \in A$, we have $F \subset FA$. Let $x \in F$. By Lemma 2.10, xA is an atom. By Corollary 2.7, $xA \subset F$. Hence $FA \subset F$. □

We shall now describe a method allowing to apply connectivity bounds for connected relations in the non connected case. This happens in Cayley relations when B generates a proper finite subgroup. In this case, one could decompose A as union of cosets modulo $\langle B \rangle$. We shall generalise this decomposition in the case of relations with a transitive group of automorphisms. Let us begin with an easy lemma

Lemma 2.13. — *Let $\Gamma = (V,E)$ be a point transitive relation and let C be a block. Let f be an automorphism of Γ. Then $\Gamma[C]$ and $\Gamma[f(C)]$ are isomorphic point transitive relations.*

Proof. — Clearly $f/C : C \longrightarrow f(C)$ defines an isomorphism from $\Gamma[C]$ onto $\Gamma[f(C)]$.

Let $x, y \in C$. Since Γ is point transitive, there is $g \in \mathrm{Aut}(\Gamma)$ such that $g(x) = g(y)$. By the definition of a block $g(C) = C$.

Now $g/C : C \longrightarrow C$ defines an automorphism of $\Gamma[C]$. □

Let $\Gamma = (V,E)$ be a reflexive relation. A subset C of V will be called a *component* of Γ if $\Gamma[C]$ is connected and if C is maximal with respect to this property. It follows easily from Zorn Lemma that every connected subset is contained in a component. It is easy also to check that two distinct components are disjoint. In particular the connected components form a partition. In follows also that a component is a block. The following remark follows easily from the definitions.

Remark 2.d. — Let $\Gamma = (V,E)$ be a reflexive relation and let $\{C_i; i \in I\}$ be a family of components of Γ and let $A \subset \bigcup_{i\in I} C_i$, be such that $\Gamma(A) \cap (\bigcup_{i\in I} C_i) = A$. There is $J \subset I$ such that $A = \bigcup_{j\in J} C_j$.

Remark 2.e. — Let $\Gamma = (V,E)$ be a reflexive relation. Then Γ has at most one infinite component.

By Remark 2.d, the union of two infinite components is connected. Hence any two infinite components must coincide.

We mention that the path connectedness, considered in section 8, leads to distinct notion of components in the infinite case. The following lemma contains all we need on components.

Lemma 2.14. — *Let $\Gamma = (V,E)$ be a reflexive point transitive relation and let C and D be components of Γ. Then the following conditions hold.*

(i) $\Gamma[C]$ and $\Gamma[D]$ are isomorphic point transitive relations.

(ii) $C = V$ or C is finite.

(iii) $\Gamma(A \cap C) = (\Gamma(A)) \cap C$ *and* $d(\Gamma[C]) = d(\Gamma)$.

Proof. — The validity of (i) follows easily from Lemma 2.14. The validity of (ii) follows from (i) and Remark 2.e.

Assume that (iii) does not hold. There are distinct connected components C_1 and C_2 such that $\Gamma(C_1) \cap C_2 \neq \varnothing$. Using the transitivity of $\mathrm{Aut}(\Gamma)$, we may construct a sequence of connected components $\{C_i; i \geq 1\}$ such that, $C_i \neq C_{i+1}$ and $\Gamma(C_i) \cap C_{i+1} \neq \varnothing$, for all $i \geq 1$.

For all $i, j \geq 1$, we have

$$C_i \neq C_{j+i}. \tag{1}$$

Assume the contrary and choose j minimal with respect to this property. By the definition $\bigcup_{0 \leq k \leq j} C_{i+k}$ is non-connected.

Hence there exists $A \subset \bigcup_{0 \leq k \leq j} C_{i+k}$ such that $\Gamma(A) \cap (\bigcup_{0 \leq k \leq j} C_{i+k}) = A$ and $A \neq \varnothing$. By Remark 2.d, there is $J \subset [i, i+j]$ such that $A = \bigcup_{i \in J} C_i$. By the construction of C_i, one should have $J = [i, j]$. In particular $\bigcup_{i \geq 1} C_i$ is connected, a contradiction.

Let A be a finite non-empty subset of $\bigcup_{i \geq 1} C_i$ By (1), there exists clearly j such that $A \cap C_j \neq \varnothing$ and $A \cap C_{j+1} = \varnothing$. In particular $\Gamma(A) \not\subset \bigcup_{i \geq 1} C_i$. It follows that $\bigcup_{i \geq 1} C_i$ is connected, contradicting the maximality of C_1. □

Lemma 2.15. — *Let* $\Gamma = (V, E)$ *be a locally finite reflexive point symmetric relation and let* C *be a component of* Γ.

Then for every non-empty finite subset A, *either* $\Gamma(\Gamma(A)) = \Gamma(A)$ *or* $|\Gamma(A)| \geq |A| + \kappa(\Gamma[C])$.

Proof. — Assume first C infinite. By Lemma 2.14, $V = C$ and the result holds trivially by Lemma 2.2.

Therefore we may assume C finite. By Lemma 2.14, all the connected components generate isomorphic relations. In particular $\kappa(\Gamma[C]) = \kappa(\Gamma[D])$.

Suppose $\Gamma(\Gamma(A)) \neq \Gamma(A)$. By Lemma 2.14.iii, there is a connected component D such that $\Gamma(\Gamma(A \cap D)) \neq \Gamma(A \cap D)$. In particular we have using Lemma 2.14.iii, $\Gamma(A \cap D) \neq D$.

By Lemma 2.2,

$$|\Gamma(A) \cap D| \geq |A \cap D| + \kappa(\Gamma[D]).$$

By Lemma 2.14.iii,

$$|\Gamma(A)| = |\Gamma(A \cap D)| + |\Gamma(A \setminus D)| \geq |A \cap D| + \kappa(\Gamma[C]) + |A \setminus D| = |A| + \kappa(\Gamma[C]).$$

□

3. Some basic additive inequalities generalised to relations

We begin by a generalisation of Mann Theorem to non-abelian groups and to relations with a transitive group of automorphisms.

A reflexive locally finite relation $\Gamma = (V, E)$ will be called a *Cauchy relation* if

$$\kappa(\Gamma) = \rho(\Gamma) - 1.$$

Lemma 3.1. — *Let $\Gamma = (V, E)$ be a reflexive locally finite relation. Then Γ is a Cauchy relation if and only if for every finite non-empty subset A of V,*

$$|\Gamma(A)| \geq \min(|V|, |A| + \rho(\Gamma) - 1).$$

If Γ is finite and regular, then Γ is a Cauchy relation if and only if Γ^- is a Cauchy relation.

Proof. — The first part follows easily from Lemma 2.1 and Lemma 2.2. The second part follows from Remark 2.a and Lemma 2.3. □

Lemma 3.2. — *Let B be a finite subset of a group G such that $1 \in B$. Then B is a Cauchy subset if and only if for every finite non-empty subset A of G,*

$$|AB| \geq \min(|G|, |A| + |B| - 1).$$

Proof. — Set $\Gamma = \Lambda(G, B)$. For every subset $F \subset G$, $\Gamma(F) = FB$. The result follows now easily by Lemma 3.1. □

According to Lemma 3.2, the Cauchy-Davenport inequality is satisfied for every non-empty subset A of G if B is a Cauchy subset. The Cayley graphs of such subsets are used in network models and said to be optimally connected.

Theorem 3.3. — *Let $\Gamma = (V, E)$ be a reflexive locally finite point transitive relation and let $v \in V$. Then Γ is a Cauchy relation if and only if one of the following conditions holds.*

(i) V is infinite and for every finite block B of Γ containing v,

$$|\Gamma(B)| \geq \min(|V|, |B| + d(\Gamma) - 1).$$

(ii) V is finite and for every block B of Γ containing v,

$$\min(|\Gamma(B)|, |\Gamma^-(B)|) \geq \min(|V|, |B| + d(\Gamma) - 1).$$

Proof. — By Lemma 3.1, the theorem is invariant by interchanging Γ and Γ^- in the finite case. We may assume without lost of generality V is infinite or $\mu(\Gamma) \leq \mu(\Gamma^-)$. The necessity follows by Lemma 3.1. Suppose that (ii) holds. We may assume that $\Gamma \neq V \times V$, since otherwise the result is obvious. By the transitivity of $\mathrm{Aut}(\Gamma)$, there exists an atom A of Γ such that $v \in A$.

By Corollary 2.8, A is a block.

It follows using the definition of an atom and (ii) that

$$\kappa(\Gamma) = |\Gamma(A)| - |A| \geq d(\Gamma) - 1.$$

By Lemma 2.2, we have $\kappa(\Gamma) = d(\Gamma) - 1$. Hence Γ is a Cauchy relation. □

Corollary 3.4. — *Let S be a finite subset of a group G such that $1 \in S$. Then S is a Cauchy subset if and only if one of the following conditions holds.*

(i) G is infinite and for every finite subgroup H of G,

$$|HS| \geq \min(|G|, |H| + |S| - 1).$$

(ii) G is finite and for every subgroup H of G,

$$\min(|SH|, |HS|) \geq \min(|G|, |H| + |S| - 1).$$

Proof. — Set $\Gamma = \Lambda(G,S)$. By Lemma 2.10 every finite block of Γ containing 1 is a subgroup. Observe that for every subgroup H, $|\Gamma^-(H)| = |HS^{-1}| = |SH|$. The result follows now using Theorem 3.3. □

The second part of Corollary 3.4 follows from [33, Theorem 1.2]. Zemor studied the same problem where B is not assumed to contain 1. A example contained in [33] shows that for a finite group G, the condition

$$\min(|SH|,|HS|) \geq \min(|G|,|H|+|S|-1)$$

can not be replaced by the weaker one

$$|HS| \geq \min(|G|,|H|+|S|-1).$$

***Corollary 3.5* ([24,25]).** — *Let B be a finite non-empty subset of an abelian group G. Then the following conditions are equivalent.*

(i) For every finite non-empty subset A of G,

$$|A+B| \geq \min(|G|,|A|+|B|-1).$$

(ii) For every finite subgroup H of G,

$$|H+B| \geq \min(|G|,|H|+|B|-1).$$

Proof. — Choose $b \in B$ and set $S = B - b$. Using Lemma 3.2, one see easily that (ii) holds if and only if S is a Cauchy subset. The result follows now using Corollary 3.4. □

The following result generalises a result proved in [10] for finite relations.

Theorem 3.6. — *Let Γ be a locally finite connected reflexive point transitive relation such that $d(\Gamma) \geq d(\Gamma^-)$. Then $\kappa(\Gamma) \geq d(\Gamma)/2$.*

Proof. — According to Lemma 2.3 and Remark 2.a, the statement is invariant if we replace Γ by Γ^- if V is finite. Hence we may assume without lost of generality $\mu(\Gamma) \leq \mu(\Gamma^-)$, in the finite case.

Let M be an atom of Γ. By Corollary 2.7, M is a block. It follows easily that $\Gamma[M]$ is point transitive and that any other atom T generates a relation isomorphic to $\Gamma[M]$. Since M is finite, we have by Remark 2.a, $d(\Gamma[M]) = d((\Gamma[M])^-)$. Set $t = d((\Gamma[M]))$. Set $d^+ = d(\Gamma)$ and $d^- = d(\Gamma^-)$. Let X be the graph obtained from Γ by deleting all the arcs interior to the atoms. As for every block, the atoms partition V. It follows that $d(X) = d^+ - t$ and $d(X^-) = d^- - t$. The number of edges of R originating in M is not greater than the number of edges terminating in $\partial(M)$. Therefore $\sum_{x\in M}(d^+ - t) \leq \sum_{x\in\partial(M)}(d^- - t)$.

Therefore $|M|(d^+ - t) \leq \kappa(\Gamma)(d^- - t)$. Hence $|M|(d^+ - t) \leq \kappa(\Gamma)(d^+ - t)$. Observe that $d^+ - t \neq 0$, since otherwise $\kappa(\Gamma) = 0$, contradicting the assumption that Γ is connected. It follows that $|M| \leq \kappa(\Gamma)$.

Let $x \in M$, we have

$$d(\Gamma) = |\Gamma(x)| = |\Gamma(x) \cap M| + |\Gamma(x) \cap \partial(M)|.$$

It follows that

$$d(\Gamma) \leq |M| + \kappa(\Gamma) \leq 2\kappa(\Gamma).$$

This proves the theorem. □

Corollary 3.7. — *Let $\Gamma = (V, E)$ be a locally finite reflexive point transitive relation such that $d(\Gamma) \geq d(\Gamma^-)$.*

Then for every non-empty finite subset A, either $\Gamma(\Gamma(A)) = \Gamma(A)$ or $|\Gamma(A)| \geq |A| + d(\Gamma)/2$.

Proof. — Let C be a component of Γ such that $A \cap C \neq \varnothing$. By Lemma 2.14, $d(\Gamma) = d(\Gamma(C))$. By Theorem 3.6, $\kappa(\Gamma[C]) \geq d(\Gamma)/2$. The result follows now from Lemma 2.15. □

Corollary 3.8. — *(Olson [27]) Let A and B be finite nonempty subsets of a group G such that $1 \in B$. Then $|AB| \geq \min(|A\langle B\rangle|, |A| + |B|/2)$.*

Proof. — Let $\Gamma = \Lambda(G, B)$. Clearly $d(\Gamma) = |B| = |B^{-1}| = d(\Gamma^-)$. By Corollary 3.7, either $ABB = AB$ or $|AB \geq |A| + |B|/2$.

The result is now obvious since the two conditions $ABB = AB$ and $A\langle B\rangle = AB$ are equivalent (observe that A and B are finite). The second one implies the first by multiplication with B. Assume the first one holds. Hence $AB^j = AB$, for all $j \geq 1$. Since A, B are finite, this last condition implies easily that $A\langle B\rangle = AB$. □

As we have seen, Theorem 3.6 generalises Corollary 3.8 (Olson [27]) to point transitive relations. In the finite case, this generalisation was proved in [10, Proposition 3.4] before the result of Olson.

A relation $\Gamma = (V, E)$ is said to be *arc-transitive* if for all x, y, v, $w \in V$, such that $(x, y) \in E$ and $(v, w) \in E$ and $x \neq y$ and $v \neq w$, there is $f \in \mathrm{Aut}(\Gamma)$ such that $v = f(x)$ and $w = f(y)$. Observe that a connected arc-transitive relation is point transitive also.

A basic example of arc transitive relation is the following one.

Let R be a division ring and U be a finite multiplicative subgroup of $R \setminus \{0\}$. Set $\Omega = \Lambda(R, U \cup \{0\})$. The relation Ω is clearly point transitive. Let us prove that it is arc transitive. Consider two arcs (a, b) and (c, d) such that $b \neq a$ and $d \neq c$. Therefore $b-a$, $d-c \in U$. Consider the application $f(x) = (d-c)(b-a)^{-1}(x-a)+c$. Clearly $f(a) = c$ and $f(b) = d$. It remains to show that $f \in \mathrm{Aut}(\Omega)$. Now f is the composition of a translation and an application of the form $g(x) = ux$, where $u \in U$. The translation is an automorphism by Lemma 2.9. It remains to show that $g \in \mathrm{Aut}(\Omega)$. This follows from the following obvious equivalence.

$$x - y \in U \quad \text{if and only if} \quad ux - uy \in U.$$

The following result is proved in [9] in the finite case.

Theorem 3.9. — *Let $\Gamma = (V, E)$ be a locally finite connected reflexive arc-transitive relation.*

Then Γ is a Cauchy relation. In particular $\kappa(\Gamma) = d(\Gamma) - 1$.

Proof. — According to Lemma 2.3 and Remark 2.a, the statement is invariant if we replace Γ by Γ^- if V is finite. Hence we may assume without lost of generality $\mu(\Gamma) \leq \mu(\Gamma^-)$, in the finite case.

Let M be an atom of Γ. We shall prove that $|M| = 1$. Suppose the contrary. By Lemma 2.2, $\Gamma[M]$ is connected. In particular, there are $x, y \in M$ with $x \neq y$ and $(x, y) \in E$. Since Γ is connected, $\kappa(\Gamma) \geq 1$. In particular there is $v \in M$ and $w \in M$, such that $(v, w) \in E$. By the transitivity of the group of automorphisms on the arcs, there is $f \in \mathrm{Aut}(\Gamma)$ such that $f(x) = v$ and $f(y) = w$. It follows that $f(M) \neq M$ and $f(M) \cap M \neq \varnothing$, contradicting Corollary 2.8.

It follows that $|M| = 1$. Hence $\kappa(\Gamma) = d(\Gamma) - 1$, by Lemma 2.2. □

Corollary 3.10. — *Let G be a group containing a finite subset B such that $1 \in B$. Assume that $\Lambda(\langle B\rangle, B)$ is arc-transitive.*

Then for every finite subset $A \subset G$, $|AB| \geq \min(|A\langle B\rangle|, |A| + |B| - 1)$.

Proof. — The proof is similar to the proof of Corollary 3.8. □

Corollary 3.11. — *Let R be a division ring and let P be a finite subset of R such that $0 \in P$ and $P \setminus \{0\}$ is multiplicative subgroup. Then P is a Cauchy subset of the additive subgroup generated by P.*

Proof. — The result follows easily by Corollary 3.10. □

Corollary 3.11 generalises an inequality proved by Davenport-Lewis in [6] in the case of finite fields. We shall improve this result in section 7.

The notion of a base can be generalised easily to relations as follows.

A subset A of a group G is said to be a base with order h if h is the smallest integer such that $G = A^h$.

Let $\Gamma = (V, E)$ be a point transitive reflexive relation. The *diameter* of Γ is the smallest integer k such that $\Gamma^k = V \times V$, where Γ^k is the composition of Γ with itself k times.

Clearly if $1 \in A$, then A is a base of order h if and only if $\Lambda(G, A)$ has diameter h.

Lemma 3.12. — *Let $X = (V, E)$ be a finite connected reflexive point transitive relation with diameter h. Then*

$$h \leq \max(2, 3 + \frac{|V| - 2d(\Gamma)}{\kappa(\Gamma)}).$$

Proof. — The result holds if $h \leq 2$. Assume the contrary. Choose $v \in V$ Let X be a nonempty subset of G. By the definition of κ, we have

$$|\Gamma(\Gamma)| \geq \min(|V|, |X| + \kappa(\Gamma)).$$

It follows that

$$|\Gamma^{h-2}(v)| \geq \min(|V|, d(\Gamma) + (h-3)\kappa(\Gamma)).$$

Since h is the exact diameter of X, there is $y \in V$ such that $\Gamma^-(y) \cap \Gamma^{h-2}(v) = \varnothing$. Hence

$$|V| \geq |d^-(y)| + d(v) + (h-3)\kappa(\Gamma) = 2d(\Gamma) + (h-3)\kappa(\Gamma).$$

□

Theorem 3.13 **([11])**. — *Let $\Gamma = (V, E)$ be a finite connected vertex transitive reflexive relation with diameter h. Then $h \leq \max\left(2, \frac{2|V|}{d(\Gamma)} - 1\right)$.*

Proof. — By Lemma 3.12,

$$h \leq \max(2, 3 + \frac{|V| - 2d(\Gamma)}{\kappa(\Gamma)}).$$

By Theorem 3.6,

$$h \leq \max(2, 3 + \frac{2(|V| - 2d(\Gamma))}{d(\Gamma)}).$$

Therefore

$$h \leq \max(2, \frac{2|V|}{|d(\Gamma)|} - 1).$$

□

There was an omission in the statement in [11]. We did add $\max(2, \dots)$, to correct the statement.

Theorem 3.13, applied to bases of finite groups, is proved independently by Rödseth [29]. This last result is used in [15] to generalise results of Cherly and Deshouillers [3], Jia and Nathanson [17] to arbitrary σ-finite groups.

4. The critical inequalities

We introduce in this section some new objects. The properties of these objects will be used later to solve the critical pair problem.

Let Γ be a relation on a set V. A fragment F of Γ is said to be a *strict fragment* if $\mu(\Gamma) + 1 \leq |F|$ and $\mu(\Gamma^-) + 1 \leq |\delta(F)|$.

The relation Γ is said to be *degenerate* if Γ has a finite strict fragment. Let G be a group containing a subset B such that $1 \in B$. We shall say that B is *degenerate* if $\Lambda(G, B)$ is degenerate.

Remark 4.a. — Let Γ be a relation on a finite set V and let $F \subset V$. The following conditions are equivalent.

(i) F is a strict fragment of Γ.
(ii) $\delta(F)$ is a strict fragment of Γ^-.

Proof. — Suppose that (i) holds. By Lemmas 2.3 and 2.4, $\delta(F)$ is a fragment of Γ^-. We have also $\delta^-(\delta(F)) = F$. Therefore (ii) holds. The other implication holds by duality using Lemmas 2.3 and 2.4. □

Lemma 4.1

(i) Let Γ be reflexive Cauchy relation on a set V. Then Γ is non-degenerate if and only if for all $A \subset V$ such that $2 \leq |A| < \infty$,

$$|\Gamma(A)| \geq \min(|V| - 1, |A| + \kappa(\Gamma) + 1).$$

(ii) Let B be a finite Cauchy subset of a group G such that $1 \in B$. Then B is non-degenerate if and only if for all $A \subset G$ such that $2 \leq |A| < \infty$,

$$|AB| \geq \min(|G| - 1, |A| + |B|).$$

Proof. — The result holds trivially if V is infinite. Observe that a fragment with cardinality $\neq 1$ is a strict fragment in this case. Assume the contrary. By Lemma 3.1, Γ^- is also a Cauchy relation.

Suppose that there is $A \subset V$ such that $2 \leq |A|$ and

$$|\Gamma(A)| < \min(|V| - 1, |A| + \kappa(\Gamma) + 1).$$

By Lemma 2.1, we have $|\Gamma(A)| = |A| + \kappa(\Gamma)$. Hence A is a fragment. We have $|\delta(A)| = |V| - |\Gamma(A)| \geq 2$. It follows that Γ is degenerate. Similarly one see easily that if Γ is degenerate then every strict fragment A verifies the inequality

$$|\Gamma(A)| < \min(|V| - 1, |A| + \kappa(\Gamma) + 1).$$

Clearly (ii) is a particular case of (1). □

Lemma 4.2. — *Let Γ be a reflexive regular Cauchy relation on a finite set V and let F be a fragment of Γ. The following conditions are equivalent.*

(i) $F = V \setminus \Gamma^-(x)$, for some $x \in V$.
(ii) $|F| = |V| - d(\Gamma)$.
(iii) $|\delta(F)| = 1$.

Proof. — Suppose that $F = V \setminus \Gamma^-(x)$, for some $x \in V$. We have

$$|F| = |V| - |\Gamma^-(x)| = |V| - d(\Gamma^-) = |V| - d(\Gamma).$$

Hence (ii) holds. Suppose now that (ii) holds. We have

$$|\delta(F)| = |V \setminus \Gamma(F)| = |V| - |F| - \kappa(\Gamma) = 1.$$

Hence (iii) holds. Suppose now that (iii) holds and take $\delta(F) = \{y\}$. By Lemmas 2.3 and 2.4,

$$F = \delta^-\delta(F) = V \setminus \Gamma^-(y).$$

□

The minimal cardinality of a strict fragment of a degenerate relation Γ will be denoted by $\omega(\Gamma)$. Clearly $\omega(\Gamma)$ is finite. A strict fragment of Γ with cardinality $\omega(\Gamma)$ will be called a *superatom* of Γ.

Lemma 4.3. — *Let Γ be a reflexive relation on a finite set V. Then Γ is degenerate if and only if it is Γ^- is degenerate.*

Proof. — Using Remark 4.a, a fragment F is strict with respect to Γ if and only if $\delta(F)$ is strict with respect to Γ^-. Using Lemma 2.4, we see easily that Γ is degenerate if and only if Γ^- is degenerate. □

Let Γ be a degenerate Cauchy relation and let K be a superatom of Γ. We shall say that Γ is *singular* if $|\delta(K)| \leq |K| - 1$.

Notice that Γ is singular if and only if $2\omega(\Gamma) + \kappa(\Gamma) - 1 \geq |V|$. In particular every singular relation is finite.

Proposition 4.4. — *Let Γ be a reflexive regular degenerate Cauchy relation. Assume that Γ is singular and let K and M be superatoms of Γ. Then either $\delta(K) = \delta(M)$ or $\delta(K) \cap \delta(M) = \varnothing$.*

Proof. — Suppose on the contrary that $\delta(K) \neq \delta(M)$ and $\delta(K) \cap \delta(M) \neq \varnothing$. By Lemma 2.4 $K \neq M$, $\delta^-(\delta(K)) = K$ and $\delta^-(\delta(M)) = M$. Using Lemma 2.5 applied to Γ^-, we have

$$|K \setminus M| = |M \setminus K| \leq |\delta(K) \setminus \delta(M)|.$$

Since $|K| > |\delta(K)|$ we have $K \cap M \neq \varnothing$. By Lemma 2.5, $K \cap M$ is a fragment of Γ. Since K is a superatom of Γ we have $|K \cap M| = 1$. Clearly

$$|K| = |M| = 1 + |M \setminus K| \leq |\delta(K)|,$$

a contradiction. □

Proposition 4.5. — *Let Γ be a reflexive degenerate Cauchy relation on a set V and let M be a superatom of Γ. Let F be a finite strict fragment of Γ such that $M \not\subset F$, $M \cap F \neq \varnothing$ and $|\delta(F)| \geq |M|$. Then*

(i) $|M \cap F| = 1$

(ii) $\Gamma(M \cap F) = \Gamma(M) \cap \Gamma(F)$.

Proof. — By Lemma 2.5, $|\delta(F) \setminus \delta(M)| < |M|$. Therefore $\delta(F) \cap \delta(M) \neq \varnothing$.

By Lemma 2.5, (ii) is satisfied and $M \cap F$ is a fragment of Γ. By the definition of a superatom and since $M \cap F \neq M$, we have $|M \cap F| = 1$. □

The above proposition generalises a result proved in the case of finite symmetric relations by Jung. Our finite symmetric relations are equivalent to undirected graphs considered by Jung, cf. [18, sätz 2]. The notion of a superatom coincides in this case with the notion of a 2-atom of Jung.

Corollary 4.6. — *Let Γ be a reflexive degenerate Cauchy relation. Assume that Γ is non-singular and let K and M be two distinct superatoms of Γ such that $K \cap M \neq \varnothing$. Then $|K \cap M| = 1$ and $\Gamma(K \cap M) = \Gamma(K) \cap \Gamma(M)$.*

Proof. — By the definition we have $|\delta(K)| \geq |K| = |M|$. By Proposition 4.5, we have $|K \cap M| = 1$ and $\Gamma(K \cap M) = \Gamma(K) \cap \Gamma(M)$. □

Corollary 4.7. — *Let Γ be a reflexive degenerate Cauchy relation such that $\omega(\Gamma) \leq \omega(\Gamma^-)$. Let M be a superatom of Γ and let F be a finite strict fragment of Γ. Then either $M \subset F$ or $|M \cap F| \leq 1$.*

Proof. — The inequality $\omega(\Gamma^-) \leq |\delta(F)|$ holds clearly if V is infinite and follows in the finite case by Remark 4.a. Therefore $|M| = \omega(\Gamma) \leq \omega(\Gamma^-) \leq |\delta(F)|$. The corollary follows now by Proposition 4.5. □

Proposition 4.8. — *Let Γ be a reflexive point transitive relation on a set V such that both Γ and Γ^- are non-singular degenerate Cauchy relations and $d(\Gamma) = d(\Gamma^-)$. Assume that*

$$3 \leq \min(\omega(\Gamma), \omega(\Gamma^-)).$$

Then one of the following conditions holds.

(i) Any three distinct superatoms of Γ *have an empty intersection.*
(ii) Any three distinct superatoms of Γ^- *have an empty intersection.*

Proof. — The statement is invariant by interchanging Γ and Γ^-. We may assume without lost of generality that $\omega(\Gamma) \leq \omega(\Gamma^-)$.

Suppose on the contrary that both (i) and (ii) are not satisfied. Choose two distinct superatoms A , B of Γ and an element x such that $x \in A \cap B$.

Since $A \cap B \neq \varnothing$, we have by Lemma 2.5

$$|\delta A \setminus \delta B| \leq |B \setminus A| < |B| = \omega(\Gamma). \tag{1}$$

As in the proof of Corollary 4.7, we have $\omega(\Gamma) \leq |\delta(A)|$. Therefore we have using (1), $\delta(A) \setminus \delta(B) \neq \varnothing$. Choose $y \in \delta(A) \setminus \delta(B)$.

Let K, L and M be distinct superatoms of Γ^- such that $y \in K \cap L \cap M$. Such superatoms exist by the transitivity of the group of automorphisms and by the hypothesis that (ii) is not satisfied. By Corollary 4.6,

$$K \cap L = K \cap M = L \cap M = \{y\}. \tag{2}$$

Suppose that there are F_1 and $F_2 \in \{K, L, M\}$ such that $F_1 \cup F_2 \subset \delta(A)$ and $F_1 \neq F_2$. By (2),

$$|F_1 \cap F_2| = 1. \tag{3}$$

Let $i \in \{1, 2\}$. By Lemma 2.4, $\delta(B)$ is a fragment of Γ^-. By Lemma 2.4, $A = \delta^-(\delta(A))$ and $A \subset \delta^-(F_1) \cap \delta^-(F_2)$. Hence $x \in \delta^-(F_1) \cap \delta^-(F_2)$. Now we have $y \in F_i \setminus \delta(B)$ and $x \in B \cap \delta^-(F_i) = \delta^-(\delta(B)) \cap \delta^-(F_i)$ (using Lemma 2.4). By Lemma 2.5, applied to Γ^- with $M = F_i$ and $F = \delta(B)$, we have $F_i \cap \delta(B) = \varnothing$ or $F_i \cap \delta(B)$ is a fragment of Γ^-. By the definition of a superatom we have $|F_i \cap \delta(B)| \leq 1$. Therefore

$$|(F_1 \cup F_2) \cap \delta(B)| \leq 2. \tag{4}$$

By (4) we have

$$|(F_1 \cup F_2) \cap (\delta(A) \setminus \delta(B))| \geq |F_1 \cup F_2| - 2. \tag{5}$$

By (3) and (5), we have

$$|\delta(A) \setminus \delta(B)| \geq |F_1| + |F_2| - 3 \geq \omega(\Gamma^-) \geq \omega(\Gamma).$$

This inequality contradicts (1). It follows that at most one superatom $F \in \{K, L, M\}$ is contained in $\delta(A)$. We may assume without loss of generality $K \not\subset \delta(A)$ and $L \not\subset \delta(A)$. By Lemma 2.4, $A \not\subset \delta^-(K)$ and $A \not\subset \delta^-(L)$.

By Corollary 4.7, $|A \cap (\delta^-(K) \cup \delta^-(L))| \leq 2$. Therefore

$$A \cap (\Gamma^-(K) \cap \Gamma^-(L)) = A \setminus (\delta^-(K) \cup \delta^-(L)) \neq \varnothing.$$

By (2) and Corollary 4.6,

$$\Gamma^-(y) = \Gamma^-(K \cap L) = \Gamma^-(L) \cap \Gamma^-(L).$$

Therefore $\Gamma^-(y) \cap A \neq \varnothing$, contradicting the assumption $y \in \delta(A)$. This contradiction proves the result. □

Proposition 4.8 generalises a result proved in [14].

5. The Vosper inequality

We apply in this section the results obtained in section 4 to the case of a finite group. Let G be a group and let $r \in G$. The subgroup of G generated by r will be denoted by $\langle r \rangle$. We recall the following elementary fact.

Remark 5.a. — Let S be a finite subset of G and let $r \in G$. The following conditions are equivalent.

(i) S is a union of right $\langle r \rangle$-cosets.
(ii) $\langle r \rangle S = S$.
(iii) $rS = S$.

In this section we study the inequality $|AB| \geq \min(|G| - 1, |A| + |B|)$, where A and B are subsets of a finite group G.

Theorem 5.1. — *Let B be a degenerate Cauchy subset of a finite group G such that $1 \in B$. Set $\Gamma = \Lambda(G, B)$. Let L be a superatom of Γ and let M be a superatom of Γ^- such that $1 \in L \cap M$.*

(i) If B is singular, then $x^{-1}\delta(L)$ is a subgroup for every $x \in \delta(L)$.

(ii) If B and B^{-1} are non-singular, then there are a subgroup H and $a \in G$ such that $L = H \cup Ha$ or $M = H \cup Ha$.

Proof. — Suppose first that Γ is singular. Choose $y \in \delta(K)$ and set $M = y^{-1}\delta(K)$. We have clearly $1 \in M$. Let $x \in M$. We have clearly $xM \cap M \neq \varnothing$. But

$$xM = x(G \setminus y^{-1}K) = \delta(xy^{-1}K).$$

By Proposition 4.4, $M = xM$. Hence $MM = M$ and therefore M is a subgroup. This proves (i).

Assume now that Γ and Γ^- are non-singular. By Lemma 4.4, Γ^- is degenerate. The result holds clearly if $\omega(\Gamma) = 2$ or $\omega(\Gamma^-) = 2$. Assume $\omega(\Gamma) \geq 3$ and $\omega(\Gamma^-) \geq 3$. By Lemma 3.1, B^{-1} is a Cauchy subset. By Proposition 4.8, there exists $\Psi \in \{\Gamma, \Gamma^-\}$ such that any three distinct superatoms of Ψ are disjoint.

Set $K = L$ if $\Gamma = \Psi$ and $K = M$ if $\Gamma^- = \Psi$. By Lemma 2.8, for any $x \in G$, xK is a superatom of Ψ. This observation will be used without reference.

Take $H = \{x \mid xK = K\}$. Clearly H is a subgroup contained in K. Let $Q = K \setminus H$. If $Q = \varnothing$, the result holds with $a = 1$. Assume $Q \neq \varnothing$ and let $a \in Q$.

Let $x \in Q$, we have $1 \in K \cap a^{-1}K \cap x^{-1}K$. By Proposition 4.8, two of these superatoms coincide. Since $a, x \in Q$, we have $a^{-1}K \neq K$ and $x^{-1}K \neq K$. Therefore $a^{-1}K = x^{-1}K$. Hence $x \in Ha$. Hence $Q \subset Ha$. Since $|K| \geq 3$ and $K = H \cup Q$, we have $|H| \geq 2$.

Let $x \in H$. We have $|xK \cap K| \geq |H| \geq 2$. By Corollary 4.6, $xK = K$. Therefore $HK = K$. Hence K is a union of right cosets of H. Hence $|Q| \geq |H|$ and therefore $|Q| = |H|$. It follows that $K = H \cup Ha$. □

Corollary 5.2. — *Let B be a degenerate Cauchy subset of a finite group G such that $1 \in B$. There are $S \in \{B, B^{-1}\}$, a subgroup H and $a \in G$ such that $H \cup Ha$ is a strict fragment of $\Lambda(G, S)$.*

Proof. — This result follows immediately from Theorem 5.1. □

Theorem 5.3. — *Let B be a subset of a finite group G such that $1 \in B$. Then the following conditions are equivalent.*

(i) For all $A \subset G$ such that $2 \leq |A|$,

$$|AB| \geq \min(|G| - 1, |A| + |B|).$$

(ii) For every subgroup H of G and for every $a \in G$ such that $|H \cup Ha| \geq 2$,

$$\min(|B(H \cup aH)|, |(H \cup Ha)B|) \geq \min(|G| - 1, |H \cup Ha| + |B|).$$

Proof. — Suppose that (i) holds. It follows that for every non-empty $A \subset G$,

$$|AB| \geq \min(|G|, |A| + |B| - 1).$$

By Lemma 3.2, B is a Cauchy subset.

By Lemma 4.1, B is non-degenerate. By Lemma 4.3, B^{-1} is non-degenerate. Hence for all $A \subset G$ such that $2 \leq |A|$,

$$|AB^{-1}| \geq \min(|G| - 1, |A| + |B|).$$

Therefore (ii) holds. Suppose that (i) is not satisfied. Hence there exists A such that $2 \leq |A|$ and

$$|AB| \leq \min(|G| - 2, |A| + |B| - 1).$$

Case 1. B is a Cauchy subset. — By Lemma 4.1, B is degenerate. By Corollary 5.2, there are $a \in G$ and a subgroup H such that $H \cup Ha$ is a fragment of $\Lambda(G, S)$ or a fragment of $\Lambda(G, S^{-1})$. In this case (ii) is not satisfied.

5.0.1. *Case 2. B is not a Cauchy subset.* — By Corollary 3.5, there exists a subgroup H of G such that $\min(|BH|, |HB|) \leq \min(|G| - 1, |H| + |B| - 2)$.

Clearly $|H| \geq 2$. Since $|H|$ divides $|G|$, $|BH|$ and $|HB|$, we have

$$\min(|BH|, |HB|) \leq \min(|G| - |H|, |H| + |B| - 1).$$

Therefore

$$\min(|BH|, |HB|) \leq \min(|G| - 2, |H| + |B| - 1).$$

It follows that (ii) is not satisfied (with $a = 1$). □

6. The critical pair theory

Let G be a group and let $r \in G \setminus \{1\}$. A subset $B \subset G$ will be called a *right progression with ratio r*, if there are $b \in G$ and a number k such that $1 \leq k < |\langle r \rangle|$ such that $B = \{b, rb, r^2b, \ldots, r^{k-1}b\}$.

A subset $B \subset G$ will be called a *right coprogression with ratio r*, if $G \setminus B$ is a right progression with ratio r.

A subset $B \subset G$ will be called a *left progression with ratio r*, if there are $b \in G$ and a number k such that $1 \leq k < |\langle r \rangle|$ such that $B = \{b, br, br^2, \ldots, br^{k-1}\}$.

A subset $B \subset G$ is a *left coprogression with ratio r*, if $G \setminus B$ is a left progression with ratio r.

We say that a subset $B \subset G$ is a *right semi-progression with ratio* r, if there are $b \in G$ and a number k such that $1 \leq k < |\langle r \rangle|$ satisfying the following properties.

(1) $B \supset \{b, rb, r^2b, \ldots, r^{k-1}b\}$

(2) $B \setminus \{b, rb, r^2b, \ldots, r^{k-1}b\}$ is a union (possibly void) of right $\langle r \rangle$-cosets.

A right semi-progression with $k = 1$ will be called a *right almost-periodic.*

A right semi-progression with $B \supset G \setminus \langle r \rangle b$ is a *right coprogression.* A subset B is said to be a *left semi-progression* if B^{-1} is a right semi-progression.

We introduce the following notion. Let $r \in G \setminus \{1\}$ and let $A \subset \langle r \rangle$. We say that $\{r^i, r^{i+1}, \ldots, r^j\}$ is an *r-string* of A if $\{r^i, r^{i+1}, \ldots, r^j\} \subset A$ and $\{r^{i-1}, r^{j+1}\} \cap A = \varnothing$.

Lemma 6.1. — *Let B be a finite subset of a group G and let $r \in G \setminus \{1\}$.*
If $|\{1, r\}B| = |B| + 1$, then B is a right semi-progression with ratio r.

Proof. — Take $B = B_1 \cup B_2 \cup \cdots \cup B_k$, where B_i is the intersection of B with an $\langle r \rangle$-right coset. We assume also $B_i \neq \varnothing$, for all $1 \leq i \leq k$.

We have

$$|\{1, r\}B| = |\{1, r\}B_1| + \cdots + |\{1, r\}B_k| = |B_1| + \cdots + |B_k| + 1.$$

It follows that there is j, $1 \leq j \leq k$, such that

(i) $|\{1, r\}B_j| = |B_j| + 1$.

(ii) $|\{1, r\}B_i| = |B_i|$, for all $i \neq j$.

By (ii), we have $rB_i = B_i$, for all $i \neq j$. It follows using Remark 5.a that B_i is an $\langle r \rangle$-right coset, for all $i \neq j$.

It remains to show that B_j is a right progression with ratio r. Take $x \in G$ such that $B_j \subset \langle r \rangle x^{-1}$ and let $C = B_j x$. It would be enough to show that C is an r-string.

We have clearly $|\{1, r\}C| = |C| + 1$ and $C \subset \langle r \rangle$. We decompose C into $\langle r \rangle$-strings. Clearly every string $\{r^i, r^{i+1}, \ldots, r^j\}$ of C determines uniquely an element r^{j+1} of $\{1, r\}C \setminus C$. Hence there is exactly one string. □

Lemma 6.2. — *Let G be a finite group and let B be a right semi-progression. If B is a Cauchy subset then one of the following conditions holds.*

(i) B is a right almost-periodic subset.

(ii) B is a right coprogression.

Proof. — We have $|\langle r \rangle B| = |B \setminus (\langle r \rangle b)| + |\langle r \rangle|$.

If $\langle r \rangle B = G$, then clearly B is right coprogression. Assume $\langle r \rangle B \neq G$.

By the definition of κ, we have

$$|B| - 1 = \kappa \leq |\partial\langle r \rangle| = |B \setminus (\langle r \rangle b)| = |B| - |B \cap b\langle r \rangle|.$$

It follows that $|B \cap (b\langle r \rangle)| = 1$. Thus B is right almost-periodic. □

Proposition 6.3. — *Let G be a finite group and B be a Cauchy subset of G such that $(|G|, |B| - 1) = 1$. Then B is degenerate if and only if B a right coprogression or a left coprogression.*

Proof. — Set $\Gamma = \Lambda(G,B)$. By Corollary 5.2, there are $S \in \{B, B^{-1}\}$, a finite subgroup H and $r \in G$ such that $K = H \cup Hr$ is a strict fragment $\Lambda(G,S)$. We have

$$|B| - 1 = |S| - 1 = \kappa(\Lambda(G,S)) = |(H \cup Ha)S| - |H \cup Ha|.$$

Hence $|H|$ divides $|B| - 1$. Therefore $|H| = 1$ and $r \neq 1$. Hence $K = \{1, r\}$. By Lemma 6.1, S is a right semi-progression with ratio r. The subset S can not be almost-periodic since otherwise $|\langle r \rangle|$ would divide $|S| - 1$.

By Lemma 6.2, S is a right coprogression. Clearly B is a right coprogression if $S = B$. It follows easily that B is a left coprogression if $S = B^{-1}$. □

We need the following lemma.

Lemma 6.4. — *Let A be a finite subset of a group G and let $r \in G \setminus \{1\}$. Let B be a finite right coprogression with ratio r such that $|B| \geq 2$ and $|AB| = |A| + |B| - 1 \leq |G| - 1$. Then A is a left progression with ratio r.*

Proof. — Take $B = G \setminus \langle r \rangle b \cup \{b, rb, r^2b, \ldots, r^{k-1}b\}$ and take $a \in A$. Let $C = a^{-1}A$ and let $D = Bb^{-1}$. Clearly $|CD| = |C| + |D| - 1 \leq |G| - 1$.

We shall prove first that $C \subset \langle r \rangle$. Assume there is $x \in C \setminus \langle r \rangle$. Since $D \supset G \setminus \langle r \rangle$, we have $x^{-1}\langle r \rangle \subset D$. It follows that $\langle r \rangle \subset CD$. Since $1 \in C$, we have $G \setminus \langle r \rangle \subset D \subset CD$. Therefore $CD = G$, a contradiction.

This shows that $C \subset \langle r \rangle$. The argument used in the last part of the proof of Lemma 6.1, shows that A is a left progression of $\langle r \rangle$. □

Lemma 6.5. — *Let A be a finite subset of a group G with cardinality m and let $r \in G \setminus \{1\}$. Let $B = (G \setminus b\langle r \rangle) \cup \{b, br, br^2, \ldots, br^{k-1}\}$ be a finite left coprogression with ratio r such that $|B| \geq 2$ and $|AB| = |A| + |B| - 1 \leq |G| - 1$. Then there are $a \in G$ such that $A = a\{1, r, \ldots, r^{m-1}\}b^{-1}$.*

Proof. — Take $a \in A$ and set $C = a^{-1}A$. We shall see that

$$b^{-1}Cb \subset \langle r \rangle \tag{1}$$

Assume there is $c \in C$ such that $b^{-1}cb \notin \langle r \rangle$. It follows that $c^{-1}b \notin b\langle r \rangle$. Since $B \supset G \setminus b\langle r \rangle$, we have $c^{-1}b\langle r \rangle \subset B$. It follows that $b\langle r \rangle \subset CB$. Since $1 \in C$, we have $G \setminus b\langle r \rangle \subset B \subset CB$. Therefore $CB = G$. It follows that $AB = G$, a contradiction.

Set now $B_1 = B \setminus b\langle r \rangle$ and $B_2 = B \cap (\langle r \rangle)$. Let us prove that

$$CB_1 \cap CB_2 = \varnothing. \tag{2}$$

We have clearly $|CB_1| \leq |CB| < |G|$. Since CB_1 is a union of left cosets we have $|CB_1| \leq |G| - |\langle r \rangle|$. On the other side $B_1 \subset CB_1$. Therefore $CB_1 = B_1$. Now (2) follows easily from (1).

It follows that

$$|C| + |B_1| + |B_2| - 1 = |CB| = |CB_1| + |CB_2| = |B_1| + |CB_2|.$$

Therefore

$$|CB_2| = |C| + |B_2| - 1. \tag{3}$$

Therefore $|(b^{-1}Cb)(b^{-1}B_2)| = |b^{-1}Cb| + |b^{-1}B_2| - 1$. Now $b^{-1}Cb$ and $b^{-1}B_2$ are subsets of $\langle r\rangle$. By Lemma 6.4, $b^{-1}Cb$ progression with ratio r. The result follows now easily. □

We prove now the main result of this section. It implies a generalisation of Vosper Theorem to any Cauchy subset of a finite group, where we replace the condition "$|G|$ is prime" in Vosper Theorem by the weaker one "$(|G|, |B| - 1) = 1$".

Theorem 6.6. — *Let G be a finite group and let B be a Cauchy subset of G such that $(|G|, |B| - 1) = 1$.*

Let $A \subset G$ such that $|AB| = |A| + |B| - 1 \leq |G| - 1$. Then one of the following conditions holds.

(i) $|A| = 1$ or $A = G \setminus aB^{-1}$, for some $a \in G$.

(ii) There are $a, b, r \in G$, $k, s \in \mathbf{N}$ such that

$$A = \{a, ar, ar^2, \ldots, ar^{k-1}\} \quad \text{and} \quad B = (G \setminus \langle r\rangle b) \cup \{b, rb, r^2b, \ldots, r^{s-1}b\}.$$

(iii) There are $a, b, r \in G$, $k, s \in \mathbf{N}$ such that

$$A = \{ab^{-1}, arb^{-1}, ar^2b^{-1}, \ldots, ar^{k-1}b^{-1}\} \quad \text{and} \quad B = (G\setminus b\langle r\rangle)\cup\{b, br, br^2, \ldots, br^{s-1}\}.$$

Proof. — Assume now that (i) does not hold. Then $|A| \geq 2$. By Lemma 4.2, $|\delta(A)| \geq 2$. It follows that A is a strict fragment and hence by Lemma 4.1, $\Lambda(G, B)$ is degenerate.

By Proposition 6.3, there exists $r \in G\setminus\{1\}$ such that B is a right coprogression or a left coprogression with ratio r. Consider first the case where B is a right coprogression. Choose $b \in G$ and $s \in \mathbf{N}$ such that $B = G \setminus \{b, rb, r^2b, \ldots, r^{s-1}b\}$

By Lemma 6.4, A is a left progression with ratio r. Choose $a \in G$ and $k \in \mathbf{N}$ such that $A = \{a, ar, ar^2, \ldots, ar^{k-1}\}$. Therefore (ii) holds. A similar argument using Lemma 6.5 shows that (iii) holds if B is a left coprogression. □

***Corollary 6.7* (Vosper Theorem).** — *Let p be a prime number, and let A and B be two non-empty subsets of Z_p such that*

$$|A + B| = |A| + |B| - 1 \leq p - 1.$$

Then one of the following conditions holds.

(i) $|A| = 1$ or $|B| = 1$

(ii) $A = Z_p \setminus (a - B)$, for some $a \in Z_p$.

(iii) A and B are arithmetic progressions with the same difference

Proof. — Vosper Theorem may be reduced without lost of generality to subsets B such that $0 \in B$ and $|B| \geq 2$. Using the Cauchy-Davenport Theorem, B is a Cauchy subset.

The result is now an obvious consequence of Theorem 6.6. □

***Corollary 6.8* ([14]).** — *Let B be a Cauchy subset of an abelian group G. Then B is degenerate if and only if one of the following conditions holds.*

and (i) B is a progression or B is a coprogression.

(ii) There exists a finite subgroup H such that

$$|H| \geq 2 \quad \textit{and} \quad |G| > |H+B| = |H| + |B| - 1.$$

The proof of this result follows along the lines of Theorem 5.3. One should use the fact that an abelian Cayley relation is isomorphic to its inverse to show that the inverse relation is also degenerate.

7. Diagonal forms over a division ring

The estimation of the range of a diagonal form is one of the classical applications of the critical pair theory, cf. [4, 29, 14]. Let us show that our methods imply the validity the estimation given in [4, 29, 14] for finite fields in the case of an arbitrary division ring.

Let us begin by a general lemma.

Lemma 7.1. — *Let G be a group and let B be a finite subset of G such that $1 \in B$. Assume that $\Lambda(\langle B\rangle, B)$ is a a nondegenerate Cauchy subset of G.*

Then for every finite subset A such that $|A| \geq 2$,

$$|AB| \geq \min(|A\langle B\rangle| - 1, |A| + |B|).$$

The proof is similar to the proof of Lemma 2.15.

Lemma 7.2. — *Let R be a division ring and let P be a finite subset of R such that $0 \in P$ and $P \setminus \{0\}$ is multiplicative subgroup. If $|R| > |P| \geq 4$, then P is neither an arithmetic progression nor a coprogression.*

Proof. — This result is proved in [25] in the case of primes fields. The argument given there is not easy to generalise to our case. But we shall deduce this result using the fact that $\Gamma = \Lambda(\langle P\rangle, P)$ is arc-transitive.

Consider the case of an arithmetic progression. The case of a coprogression works in the same way. Assume that P is an arithmetic progression. Set

$$P = \{a, a+r, a+2r, \ldots, a+(k-1)r\}.$$

We may assume without loss of generality that $r, 2r \in P$. Therefore one $P = \{b, b+1, b+2, \ldots, b+(k-1)\}$, where $b = ar^{-1}$. It follows that

$$|\Gamma(0) \cap \Gamma(1)| = k - 1 > |\Gamma(0) \cap \Gamma(2)|,$$

contradicting the arc-transitivity of Γ. □

Proposition 7.3. — *Let R be a division ring and let P be a finite subset of R such that $0 \in P$ and $P \setminus \{0\}$ is multiplicative subgroup. Let R_0 be the additive subgroup generated by P. Then P is a non-degenerate Cauchy subset of R_0.*

Proof. — By Corollary 3.11, P is a Cauchy subset of R_0. Suppose that P is degenerate. By Lemma 7.2, P can not be a progression or a coprogression. By Corollary 6.8, there is a finite non-trivial subgroup $H \subset R_0$ such that $|R_0| > |H+B| = |H|+|P|-1$. Let p be the characteristic of R. Clearly p divides the order of $|H|$. It follows that p

divides $|P|-1$. Since $P \setminus \{0\}$ is a subgroup, it follows that $u \in P \setminus \{0,1\}$ such that $u^p = 1$. Hence $(u-1)^p = 0$, a contradiction. □

Theorem 7.4. — *Let R be a division ring and let P be a finite subset of R such that $0 \in P$ and $P \setminus \{0\}$ is multiplicative subgroup. Let R_0 be the additive subgroup generated by P.*

Suppose that $|P| \geq 4$ and let $a_1, a_2, \ldots, a_n$ be non-zero elements of R. Then

$$|a_1P + a_2P + \cdots + a_nP| \geq \min(|R_0|, (2n-1)(|P|-1)+1).$$

Proof. — The proof is by induction. The statement is obvious for $n = 1$. Suppose it true for n. We may assume clearly $a_{n+1} = 1$. By Lemma 7.2, Proposition 7.3 and the induction hypothesis, we have

$$|b_1P + b_2P + \cdots + b_nP + P| \geq \min(|R_0| - 1, 2n(|P|-1)+2).$$

Set $U = P \setminus \{0\}$. Since

$$((a_1P + a_2P + \cdots + a_nP + P) \setminus \{0\})U = (a_1P + a_2P + \cdots + a_nP + P) \setminus \{0\}.$$

It follows that $|U|$ divides $|a_1P + a_2P + \cdots + a_nP + P| - 1$. It follows that

$$|a_1P + a_2P + \cdots + a_nP + P| \geq \min(|R_0| - 1, (2n+1)(|P|-1)+1).$$

It follows easily from this equality that

$$|a_1P + a_2P + \cdots + a_nP + P| \geq \min(|R_0|, (2n+1)(|P|-1)+1).$$

□

Theorem 7.4 was first proved in the case of $\mathbf{Z}_p$, by Chowla, Mann and Straus in [4]. Tietäväinen proved in [29] the above Theorem 7.4 in the case of finite fields with odd characteristics. We gave in [14] a proof for all finite fields based on the method of superatoms.

8. An application to networks

In this section, we identify a relation and its graph. We assume the loops coloured with white and the other edges coloured black.

A network will be modelled by a reflexive graph. The usual models are graphs without loops. Basically the two models are equivalent. The first one is more appropriate in our approach. In particular all the results and notions contained in this paper apply immediately. The second model requires some easy transformations. The reader could consider the black part as the network model and the white part as introduced for theoretical reasons. A point will be called a node or a vertex and an edge will be called a link (directed one).

Let $\Gamma = (V, E)$ be a reflexive graph. A *sink* of Γ is a proper finite subset of V such that $\Gamma(A) = A$. Clearly Γ is connected if and only if Γ has no sinks. We shall say that Γ is strongly connected if for all x,$y \in V$, there is a directed path from x to y. It is easy to show that a finite graph is connected if and only if it is strongly connected. This is not the case for infinite graphs. The Cayley graph $\Lambda(\mathbf{Z}, \{1\})$ is clearly connected and not strongly connected.

From now on, all the graphs considered will be assumed for simplicity finite.

Let $\Gamma = (V, E)$ be a finite reflexive regular graph. A set of vertices will be called a *cutset* if its deletion and its incident edges disconnects the graph. A cutset with smallest cardinality is called a *minimum cutset.* It is easy to see that the cardinality of a minimum cutset is $\kappa(\Gamma)$. Let us mention that a fragment is just a sink in the subgraph obtained by the deletion of a minimum cutset.

In a good network, the connectivity should be maximised. By Lemma 2.2, the maximal possible value of the connectivity is $d(\Gamma) - 1$. If In particular, if $\kappa(\Gamma) = d(\Gamma) - 1$, then after the failure of $d(\Gamma) - 2$ nodes, the remaining nodes remain connected. This property shows that Γ must be a Cauchy graph. The next property studied in network models is the superconnectdness. Let $x \in V$, clearly $\Gamma(x) \setminus \{x\}$ creates the sink $\{x\}$, it is thus a cutset with cardinality $d(\Gamma) - 1$. A similar remark holds for $\Gamma^-(x) \setminus \{x\}$. A graph is said to be superconnected if it has no other cutsets with cardinality $d(\Gamma) - 1$. It follows easily from the lemmas proved in section 3 that a graph is vosperian if and only if all its fragments are trivial, where a trivial fragment is either $\{x\}$ or $V \setminus \Gamma^-(x)$, for some $x \in V$.

Most of the models are Cayley graphs on cyclic groups, called usually *loop networks.* Several attempts were made to characterise superconnected loop networks, cf. [16] and the references mentioned there. A first solution to this problem, based on Kempermann critical pair theory, is contained in [16]. There is also a characterisation of vosperian abelian Cayley graphs in [16]. Easier characterisations, based on the properties of superatoms, are obtained later in [14].

Proposition 6.3 has the following implication.

Corollary 8.1. — *Let G be a finite group and let B be a Cauchy subset of G such that $(|G|, |B|) = 1$. Assume that B is neither a left coprogression nor a right coprogression. Then $\Lambda(G, B)$ is superconnected.* □

We conclude this section by explaining the characterisation of vosperian graphs in network reliability. This characterisation is contained in an unpublished manuscript of the present author.

Consider a reflexive regular graph Γ. Set $d(\Gamma) = d$. The following property will be denoted by $\mathbf{P}_k$:

$$\forall A, B \subset V,\ |A| = |B| = k,\ \exists\, k \text{ disjoint paths from } A \text{ into } B.$$

Clearly $\mathbf{P}_d$ can not hold, since every d paths starting from $\Gamma(x)$ contains two intersecting paths. Clearly the path starting in x must use an other vertex of $\Gamma(x)$. It is an easy consequence of Menger Lemma that Γ satisfies $\mathbf{P}_{d-1}$ if and only if Γ is a Cauchy graph. The Vosper property is in some sense the critical situation of this problem. In particular we have the following characterisation.

Γ is vosperian if and only if for all $A \notin \{\Gamma(x) : x \in V\}$, $B \notin \{\Gamma^-(x) : x \in V\}$, with $|A| = |B| = d$, there exist d disjoint paths from A into B.

References

[1] Brailowski L.V. and Freiman G. A., *On a product of finite subsets in a torsion free group*, J. Algebra, **130**, 1990, 462–476.

[2] Cauchy A., *Recherches sur les nombres*, J. Ecole Polytechnique, **9**, 1813, 99–116.

[3] Cherly J. and Deshouillers J-M., *Un théorème d'addition dans* $F_q[X]$, J. Number Theory, **34**, 128–131.

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

[5] Davenport H., *On the addition of residue classes*, J. London Math. Soc., **10**, 1935, 30–32.

[6] Davenport H. and Lewis D.J., *Notes on congruences (III)*, Quart. Math. Oxford, **(2) 17**, 1966, 339–344.

[7] Diderrich G.T., *On Kneser's addition theorem in groups*, Proc. Amer. Math. Soc., 1973, 443–451.

[8] Halberstam H. and Roth K.F., *sequences*, Springer-Verlag, 1982.

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

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

[11] Hamidoune Y.O., *An application of connectivity Theory in graphs to factorizations of elements in groups*, Europ. J. Combinatorics, **2**, 1981, 349–355.

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

[13] Hamidoune Y.O., *On a subgroup contained in words with a bounded length*, Discrete Math., **103**, 1992, 171–176.

[14] Hamidoune Y.O., *On subsets with a small sum in abelian groups*, Europ. J. of Combinatorics, **18**, 1997, 541–566.

[15] Hamidoune Y.O. and Rödseth Ö.J., *On bases for* σ*-finite groups*, Math. Scand., 1994, 246–254.

[16] Hamidoune Y.O., Llàdo A.S. and Serra O., *Vosperian and superconnected abelian Cayley digraphs*, Graphs and Combinatorics, **7**, 1991, 143–152.

[17] Jia X.B. and Nathanson M.B., *Additions theorems for* σ*-finite groups*, In Proc. Rademacher Centenary conference, contemporary mathematics, Amer math. Soc. 1194.

[18] Jung H.A., *Über den Zusammenhang von Graphen, mit Anwendungen auf symmetricher Graphen*, Math. Ann., **202**, 1973, 307–320.

[19] Kempermann J.H.B., *On complexes in a semigroup*, Indag. Math., **18**, 1956, 247–254.

[20] Kempermann J.H.B., *On small sumsets in abelian groups*, Acta Math., **103**, 1960, 66–88.

[21] Kneser M., *Anwendung eines satzes von Mann auf die Geometrie von Zahlen*, Proc. Int. Cong. Math. Amsterdam, **2**, 1954, 32.

[22] Kneser M., *Eine Satz über abelesche gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z., 1955, 429–434.

[23] Mader W., *Eine Eigenschaft der Atome endlicher Graphen*, Arch. Math., **22**, 1971, 333–336.

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

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

[26] Nathanson M.B., *Additive number theory: Inverse problems and the Geometry of sum-sets*, Springer-Verlag, 1994, to appear.

[27] Olson J.E., *On the sum of of two sets in a group*, J. Number Theory, **18**, 1984, 110–120.

[28] Olson J.E., *On the symmetric difference of two sets in a group*, Europ. J. Combinatorics, 1986, 43–54.

[29] Rödseth Ö.J., *Two remarks on linear forms in non-negative integers*, Math. Scand., **51**, 1982, 193–198.

[30] Tietäväinen A., *On diagonal forms over finite fields*, Ann. Univ. Turku Ser. A, 1968, 1–10.

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

[32] Vosper G., *Addendum to "The critical pairs of subsets of a group of prime order"*, J. London Math. Soc., **31**, 1956, 280–282.

[33] Zemor G., *A generalisation to noncommutative groups of a theorem of Mann*, Discrete Math., **126**, 1994, 365–372.

Y.O. HAMIDOUNE, Équipe de Combinatoire, Case 189, UFR 921, Université P. et M. Curie, Place Jussieu, 75230 Paris, France • *E-mail :* yha@ccr.jussieu.fr