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, $|\Gamma(A)| \geq \min(|V|, |A| + k)$.*