ADDITION THEOREMS IN ACYCLIC SEMIGROUPS

JAVIER CILLERUELO, YAHYA O. HAMIDOUNE, AND ORIOL SERRA

Dedicated to Mel Nathanson

Abstract. We give a necessary and sufficient condition on a given family $\mathcal{A}$ of finite subsets of integers for the Cauchy-Davenport inequality

$$|\mathcal{A}+\mathcal{B}| \geq |\mathcal{A}|+|\mathcal{B}|-1,$$

to hold for any family $\mathcal{B}$ of finite subsets of integers. We also describe the extremal families for this inequality. We prove this result in the general context of acyclic semigroups, which contain also the semigroup of sequences of elements in an ordered group.

1. Introduction

Recently some additive results have been considered in the setting of the semigroup of subsets of integers, see e.g. [1] where Sidon sets are generalized to this context. Following this direction introduced by two of the authors, in this paper we consider some extensions of Cauchy–Davenport Theorem to the semigroup of subsets of integers, but we shall do the proof in the more general context of acyclic semigroups.

We denote a semigroup $(M,\cdot)$, where '$\cdot$' is a binary associative operation on the set M with a neutral element, simply by M. The semigroup M is *acyclic* if

M1. $x\cdot y = x$ implies $y=1$, for every $x\in M$.
M2. $x\cdot y = 1$ implies $x=y=1$, for every $x,y\in M$.

Our basic examples are the following ones. Let G be an ordered group and let $P=G_+=\{x:\ x\geq 1\}$. The set M of finite subsets of P with the product

$$a\cdot b=\{\alpha\beta:\ \alpha\in a,\beta\in b\}$$

is an acyclic semigroup with neutral element$\{1\}$, where 1 is the neutral element of G. We call M the *sumset* semigroup of G.

2000 *Mathematics Subject Classification.* 11B60, 11B34, 20D60.

For our second example, let P^I denote the set of functions from a set I to P with the induced product

$$(f \cdot g)(y) = f(y) \cdot g(y)$$

is an acyclic semigroup with neutral element the constant function 1. In particular, if $|I| = 1$ then P^I is isomorphic to P (as semigroups). For $|I| \geq 2$, P^I is the semigroup of sequences of elements in P indexed by I. In particular, if $P = \mathbb{N}$ then $\mathbb{N}^I$ is the free abelian monoid generated by I, an important object in factorization theory, see for instance [2].

Acyclic semigroups have the following important property.

Lemma 1. *For any finite nonempty subset S of an acyclic semigroup M and for every $x \neq 1$, we have $xS \neq S$.*

Proof. Suppose that $xS = S$. Take $a \in S$. Then $x^j a \in S$ for all j by induction. Since S is finite we have $x^j a = x^{k+j} a$ for some j and $k > 0$. By axiom M2 we have $x^k = 1$ and then $x = 1$. □

2. Cayley graphs on semigroups

Let M be a semigroup. Let S be a finite subset of M. The Cayley graph $\mathrm{Cay}(M, S)$ of S in M has the elements of M as vertices and there is an arc (x, y) colored $s \in S$ whenever $y = xs$. Note that the resulting graph is oriented, edge–colored, and it may have parallel arcs. If $1 \in S$ then it has a loop at every vertex.

If M is an acyclic semigroup and $1 \in S$ then the only finite directed cycles in the Cayley graph $\mathrm{Cay}(M, S)$ are the loops. This fact motivates the terminology. In what follows we assume that M is an acyclic semigroup.

We shall write $\delta(S) = \min\{|xS| : x \in M\}$, the minimum out-degree of a vertex in $\mathrm{Cay}(M, S)$. A subset S will be called *regular* if $\delta(S) = |S|$. We say that S is *biregular* if in addition $|Sx| = |S|$ for every $x \in M$.

We are interested in obtaining lower bounds for the cardinality of the product of two sets in M. To this end we use the isoperimetric method, see e.g. [3, 4].

For a positive integer k and a finite set $S \subset M$ with $1 \in S$, denote by

$$\kappa_k(S) = \min\{|XS| - |X| : |X| \geq k\}$$

the k-th isoperimetric connectivity of S.

It follows from the definition that, for every pair X and S of finite sets in M with $|X| \geq k$ we have

$$|XS| \geq |X| + \kappa_k(S).$$

Note also that $\kappa_i(S) \le \kappa_{i+1}(S)$ for each $i \ge 1$. A subset $F \subset M$ with $|F| \ge k$ is said to be a *k–fragment* of S if

$$|FS| - |S| = \kappa_k(S).$$

A k–fragment of S with minimal cardinality will be called a *k–atom* of S.

Lemma 2. *Let F and S be finite nonempty subsets of an acyclic semigroup M with $1 \in S$. There is an element $a \in F$ such that $|(F \setminus a)S| \le |FS| - 1$.*

In particular, every k–fragment of S in M contains a k–atom of S with cardinality k.

Proof. Consider the subgraph of $\mathrm{Cay}(M, S)$ induced on F. Since the graph has no directed cycles, (except for the loops) there is an element $a \in F$ with indegree $\delta^-(a) = 1$ (just the loop). It follows that $a \in (FS) \setminus (F \setminus a)S$.

Now suppose that F is a k–fragment, so that $|FS| = |F| + \kappa_k(S)$. Let A be the smallest k–fragment contained in F. Suppose that $|A| > k$. By the first part of the Lemma there is $a \in A$ such that $|(A \setminus a)S| \le |AS| - 1 = |A| - 1 + \kappa_k(S)$, contradicting the minimality of $|A|$. Hence $|A| = k$ and A is a k–atom. □

Theorem 3 (Cauchy-Davenport for acyclic semigroups)**.** *Let S be a finite subset of acyclic semigroup M with $1 \in S$. For every nonempty finite subset X of M, we have*

$$|XS| \ge |X| + \delta(S) - 1,$$

and the inequality is best possible. In particular, we have

$$|XS| \ge |X| + |S| - 1$$

for each finite subset $X \subset M$ if and only if S is regular.

Proof. By Lemma 2 there is a 1–fragment with cardinality one, say $X = \{a\}$. Then, by the definition, $|XS| - |X| \ge \kappa_1(S) = |aS| - 1 \ge \delta(S) - 1$.

By taking $x \in M$ such that $|xS| = \delta(S)$ and $X = \{x\}$ we see that the equality holds. □

Note that, without the assumption $1 \in S$ the best one can say in general is just $|XS| \ge 1$ in contrast with the trivial bound $|XS| \ge \max\{|X|, |S|\}$ in a group. The following example illustrates this remark.

Example 4. *Consider the sumset semigroup of the integers. For a subset $A = \{a_1 < a_2 < \cdots < a_n\}$ we denote by $d(A) = \max_{1 \le i < n}(a_{i+1} - a_i)$ the length of the largest gap in A.*

Let $\mathcal{A} = \{A_1, \cdots, A_k\}$ be a collection of subsets of integers with gaps of length at most k, namely $\max_i d(A_i) \le k$, and with $\min(A_i) = m$, $\max(A_i) = M$ for each i. Let $P = \{0, 1, \cdots, k\}\}$. We have $\mathcal{A} + P = \{m, m+1, , M+k\}$, and hence

$$|\mathcal{A} + P| = 1.$$

However $|\mathcal{A}|$ can be arbitrarily large.

Note that if $S = \{\{0\}, P\}$ then $\delta(S) = 2$ and $|\mathcal{A} + S| = |\mathcal{A}| + 1$.

Let M be the sumset semigroup of the integers. One can characterize the sets for which the classical Cauchy–Davenport inequality holds in M. Define a partial order in M by

$$x \preceq y \Leftrightarrow \begin{cases} x = y, & \text{or} \\ \min(x) < \min(y), & \text{or} \\ \min(x) = \min(y) \text{ and } \max(x) < \max(y). \end{cases}$$

Proposition 5. *Let M be the sumset semigroup of the integers. Then S is regular if and only if S is a chain.*

Proof. For any $z \in M$ we observe that $(\min(zx), \max(zx)) = (\min(z) + \min(x), \max(z) + \max(x))$. If all the pairs $(\min(x), \max(x))$, $x \in S$, are all distinct then the pairs $(\min(zx), \max(zx))$, $x \in S$, are all distinct. Thus all the elements $zx,\ x \in S$ are also distinct and $|zS| = |S|$.

On the other hand, if $(\min(x), \max(x)) = (\min(y), \max(y))$ for distinct elements $x, y \in S$ we have that $xz = yz = [\min(x), \max(x) + k]$ when $z = [0, k]$ and $k \geq \max(x) - \min(x)$. Thus $\delta(S) < |S|$. □

As a consequence of the above Proposition that the classical Cauchy–Davenport inequality holds for chains in the sumset semigroup of the integers.

Corollary 6. *Let S be a chain in the sumset semigroup of the integers with $1 \in S$. Then, for each finite nonempty subset $X \subset M$,*

$$|XS| \geq |X| + |S| - 1.$$

The following example shows that there are antichains in the sumset semigroup of the integers with $|\mathcal{A} + \mathcal{A}| = |\mathcal{A}| + 1$, the minimum possible value given by Theorem 3.

Example 7. *Let $\mathcal{A}_0$ be an arbitrary family of sets of integers in the interval $[m, M]$. Let $\mathcal{A}_1 = \{[2m - M, m] \cup A \cup [M, 2M - m],\ A \in \mathcal{A}_0\}$. Note that, for every pair $A, A' \in \mathcal{A}_1$ we have $A + A' = [4m - 2M, 4M - 2m]$. By setting $\mathcal{A} = \mathcal{A}_1 \cup \{0\}$ we have a family with $|\mathcal{A} + \mathcal{A}| = |\mathcal{A}| + 1$.*

We conjecture that Theorem 3 holds in the semigroup of finite sequences of elements from a torsion–free group:

Conjecture 1. *Let G be a torsion–free group and I a finite set. Then for every nonempty finite subsets $S, T \subset G^I$ with $1 \in S$ we have*

$$|ST| \geq |T| + \delta(S) - 1.$$

3. Vosper's Theorem

We next analyze the case of equality in the Cauchy-Davenport theorem for acyclic abelian semigroups.

A set $P \subset M$ of the form $P = a\{1, r, r^2, \dots r^{k-1}\}$ is called an r– progression.

Lemma 8. *Let S be a biregular finite nonempty subset of an acyclic semigroup M with $1 \in S$ and let $u \in M \setminus \{1\}$. If*

$$|\{1, u\}S| = |S| + 1,$$

then uS is an u–progression.

Proof. Since $\delta(S) = |S|$, we have $|uS| = |S|$, which implies

$$|S \cap uS| = 2|S| - |\{1, u\}S| = |S| - 1.$$

It follows that the subgraph $\Gamma(uS)$ of $\Gamma = Cay(M, \{1, u\})$ induced by uS contains $|S| - 1$ arcs. Since S is biregular we can not have $su = s'u$ for a pair of distinct elements $s, s' \in S$, so that the indegree of every element in $\Gamma(uS)$ is at most one. Since $\Gamma(uS)$ is acyclic it is a path of length $|S|$. This implies that uS is an u–progression. □

Theorem 9 (Vosper Theorem for acyclic semigroups)**.** *Let M be an abelian acyclic semigroup. Let S be a regular nonempty finite subset of M with $1 \in S$ and $|S| \geq 2$. Let X be a finite subset of M with $|X| \geq 2$. If*

$$|XS| = |X| + |S| - 1,$$

then one of the following conditions holds:

(i) *There are $u, v \in X$ such that $uS^* = vS^*$,*
(ii) *There is $u \in M$ such that uS is an r–progression for some $r \in M$. Moreover, if X is also regular, then there is $u' \in M$ such that $u'X$ is an r–progression as well.*

Proof. By the definition, we have $\kappa_2(S) \leq |S| - 1$. By Theorem 3, since S is regular we have $\kappa_2(S) = |S| - 1$. By Lemma 2, there is a 2–atom of S with cardinality two contained in X. Thus there are $u, v \in X$ with $|\{u, v\}S| = |S| + 1$. We consider two cases.

Case 1. $v \notin (uS)$ and $u \notin (vS)$. In this case (i) holds.

Case 2. $v \in uS$ or $u \in vS$. We may assume that $v = us$ for some $s \in S$. Then $|\{u, us\}S| = |\{1, s\}(uS)| = |S| + 1$. By Lemma 8, uS is an r–progression for some r, say $uS = a\{1, r, \cdots, r^{k-1}\}$.

Now if X is also regular then Xu is a regular set and $|(Xu)S| = |X| + |S| - 1$. We can write $(Xu)S = Xa\{1, r, \dots, r^{k-1}\} = Xa\{1, r\} \cdots \{1, r\}$. Since $|(Xu)S| = |X| + |S| - 1$ we have $|Xa\{1, r\}| = |aX\{1, r\}| = |X| + 1$ and we likewise conclude that aX is an r–progression. □

In the sumset semigroup of the integers, both conclusions in the above Theorem may hold as illustrated by the following example.

Example 10. *Let*

$$\mathcal{A} = \{\{0\}, \{0, 3, 6, 9\}, \{0, 2, 3, 6, 9, 10\}, \{0, 1, 4, 7, 9, 11\}\}.$$

Since $\mathcal{A}$ is a chain, it is biregular. Now let

$$\mathcal{B} = \{\{0, 1, 2, 3, 4, 5, 6\}, \{0, 1, 3, 4, 5, 6\}\}.$$

We have $|\mathcal{A} + \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| - 1$ and $\mathcal{A}$ is not a progression.

References

[1] J. Cilleruelo and O. Serra, Sidon families of k-sets, preprint (2008).

[2] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[3] Yahya Ould Hamidoune, Some additive applications of the isopermetric approach, *Annales de l'Inst. Fourier*, to appear; arXiv:0706.0635.

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

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

Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid.

E-mail address: franciscojavier.cilleruelo@uam.es

UER Combinatoire, Univ. Paris VI

E-mail address: hamidoune@math.jussieu.fr

Dept. Matemàtica Aplicada 4, Univ. Politècnica de Catalunya

E-mail address: oserra@ma4.upc.edu