A Kneser-type theorem for restricted sumsets*

Mario Huicochea [†1]

[1]CONACYT/UAZ, Zacatecas, Mexico

Abstract

Let $G = (G, +, 0_G)$ be a commutative group, A and B be nonempty finite subsets of G and $H = \{c \in G :\ c + A + B = A + B\}$. Kneser's Theorem is a fundamental result in Additive Number Theory and it establishes that $|A + B| \geq |A + H| + |B + H| - |H|$. For any subset S of $A \times B$, write $A \overset{S}{+} B = \{a+b :\ (a, b) \in S\}$. For any $c \in G$, set $r_{A,B}(c) = |\{(a, b) \in A \times B :\ a+b = c\}|$. An important problem in Additive Number Theory is to find a Kneser-type theorem for the restricted sumsets $A \overset{S}{+} B$. In particular, more than 20 years ago V. Lev proved that if $\{c \in A+B :\ r_{A,B}(c) \geq k\} \subseteq A \overset{S}{+} B$, for all $a \in A$ (resp $b \in B$) there is at most one $b' \in B$ (resp. $a' \in A$) such that $(a, b') \notin S$ (resp. $(a', b) \notin S$), and $A \overset{S}{+} B \neq A + B$, then

$$\left| A \overset{S}{+} B \right| > \left(1 - \frac{|A||B|}{(|A| + |B|)^2}\right)(|A| + |B|) - k - 1.$$

In the same paper, Lev proposed as a problem to improve $1 - \frac{|A||B|}{(|A|+|B|)^2}$ to something of the form $1 - w$ with $w \to 0$ whenever $\frac{|(A\times B)\setminus S|}{|A||B|} \to 0$. Lev's problem has been solved for some particular groups and some specific subsets S of $A \times B$. However, it remains open for arbitrary groups and arbitrary large subsets S of $A \times B$. Here, as a consequence of the main result of this paper, it is shown that if we take $-2k - s + 2$ instead of $-k - 1$ in the lower bound of $\left| A \overset{S}{+} B \right|$, then indeed we can take as the coefficient of $|A| + |B|$ something of the form $1 - w$ with $w \to 0$ whenever $\frac{|(A\times B)\setminus S|}{|A||B|} \to 0$.

1 Introduction

In this paper $\mathbb{R}, \mathbb{Z}, \mathbb{Z}^+, \mathbb{Z}_0^+$ denote the set of real numbers, integers, positive integers and nonnegative integers, respectively. Let $G = (G, +, 0_G)$ be a commutative group, H be a subgroup of G, A and B be subsets of G, $c \in G$ and $k \in \mathbb{Z}^+$. Write

$$\begin{aligned}
A + B &:= \{a + b :\ a \in A,\ b \in B\} \\
A + c &:= A + \{c\} \\
-A &:= \{-a :\ a \in A\} \\
r_{A,B}(c) &:= |\{(a, b) \in A \times B :\ a + b = c\}| \\
A \overset{k}{+} B &:= \{d \in G :\ r_{A,B}(d) \geq k\} \\
\mathrm{Stab}(A) &:= \{b \in G :\ A + b = A\}.
\end{aligned}$$

We will denote by $\pi_H : G \to G/H$ the canonical projection. To avoid confusion, $\pi_H(c)$ (resp. $\pi_H(A)$) will be an element (resp. subset) in the quotient group G/H, while $c + H$ (resp. $A + H$) will denote a subset of G.

*The full version of this work can be found in [6].

†Email: dym@cimat.mx Research of CONAHCYT/UAZ

One of the most important problems in Additive Number Theory is to find a sharp lower bound for a sumset in terms of the size of the sets and the technical properties demanded for these sets. A fundamental result in this direction is Kneser's Theorem which can be stated as follows.

Theorem 1. *Let G be a commutative group and A and B be nonempty finite subsets of G. Write $H = \mathrm{Stab}(A+B)$. Then*

$$|A+B| \geq |A+H| + |B+H| - |H|.$$

Proof. See [17, Thm.5.5]. □

An easy consequence of Kneser's Theorem is the next result.

Corollary 2. *Let G be a commutative group and A and B be nonempty finite subsets of G such that $|A+B| < |A| + |B| - 1$. Write $H = \mathrm{Stab}(A+B)$. Then*

$$|\pi_H(A+B)| = |\pi_H(A)| + |\pi_H(B)| - 1.$$

Proof. See [2, Ch.6]. □

There are a number of proofs, generalizations and applications of Kneser's Theorem; see [2, 12, 17].

Let G be a commutative group, A and B be nonempty subsets of G and S be a subset of $A \times B$. The restricted sumset of A and B by S is

$$A \overset{S}{+} B := \{a+b : (a,b) \in S\}.$$

Let $s \geq 0$ and $k \in \mathbb{Z}^+$. We say that $A \overset{S}{+} B$ is *s-regular* if for all $a \in A$ and $b \in B$, we have that $|\{b' \in B : (a,b') \notin S\}|, |\{a' \in A : (a',b) \notin S\}| \leq s$. We say that $A \overset{S}{+} B$ is *(k,s)-regular* if $A \overset{S}{+} B$ is s-regular and $A \overset{k}{+} B \subseteq A \overset{S}{+} B$. There are several problems where instead of considering the sum of each pair of elements in $A \times B$, we want to take just some of them. In particular, the cases where $S = \{(a,b) \in A \times B : a \neq b\}$ or $S = \{(a,b) \in A \times B : r_{A,B}(a+b) \geq n\}$ for a given $n \in \mathbb{Z}^+$ have been widely studied; see for example [1, 7, 8, 10, 13, 14, 17, 18]. Also for arbitrary large subsets S of $A \times B$, a number of results can be found nowadays; see [9, 11, 15, 16, 17]. An important problem in this area is to try to generalize Kneser's Theorem for restricted sumsets. If $A \overset{S}{+} B = A + B$, then Kneser's Theorem can be used to find a lower bound for $\left|A \overset{S}{+} B\right|$ in terms of $|A|, |B|$ and $|\mathrm{Stab}(A+B)|$. Thus it remains to study how can we bound $\left|A \overset{S}{+} B\right|$ below when $A \overset{S}{+} B \neq A + B$. An important step in this direction was given by V. Lev with the next theorem (which is stated in [8] with slightly different notation).

Theorem 3. *Let $k \in \mathbb{Z}^+$, G be a commutative group, A and B be nonempty finite subsets of G and S be a subset of $A \times B$ such that $A \overset{S}{+} B$ is $(k,1)$-regular. Write $w = \frac{|A||B|}{(|A|+|B|)^2}$. If $A \overset{S}{+} B \neq A + B$, then*

$$\left|A \overset{S}{+} B\right| > (1-w)\left(|A| + |B|\right) - k - 1.$$

Proof. See [8, Thm.4]. □

With the notation as in Theorem 3, notice that $w \leq \frac{1}{4}$ and the equality is achieved when $|A| = |B|$. Thus the coefficient $1 - w$ can be as small as $\frac{3}{4}$. In [8, Sec.4], Lev proposed as a problem to improve $1 - w$ in Theorem 3. There are already partial results.

- In the case $G = \mathbb{Z}/p\mathbb{Z}$, S. Guo and Z. W. Sun gave in [4] a lower bound for $\left|A\overset{S}{+}B\right|$ when $S = \{(a,b) \in A \times B : \ a - b \notin C\}$ for a subset C of $\mathbb{Z}/p\mathbb{Z}$.
- When $G = \mathbb{Z}$, Lev gave in [9] a lower bound for $\left|A\overset{S}{+}A\right|$. Later P. Mazur in [11] and X. Shao and W. Xu in [16] found nontrivial lower bounds for $\left|A\overset{S}{+}B\right|$ and inverse results in this direction.
- In the case G is torsion free or elementary abelian, H. Pan and Sun provided a nontrivial lower bound $\left|A\overset{S}{+}B\right|$ when $S = \{(a,b) \in A \times B : \ a - b \notin C\}$ for a subset C of G.
- For arbitrary finite commutative groups G, Lev in [7] and Guo in [3] gave lower bounds for $\left|A\overset{S}{+}B\right|$ when $S = \{(a,b) \in A \times B : \ a \neq b\}$. Later this was generalized by Y. O. Hamidoune, S. C. López and A. Plagne in [5].

More information about this topic can be found in Lev's nice survey [10]. Lev's problem remains open for arbitrary groups and large subsets S of $A \times B$, and this problem is the main motivation of this paper. Instead of considering just $(k,1)$-regular restricted sumsets, we will work with (k,s)-regular restricted sumsets.

2 Main results

To state the main result of this paper, we need two definitions. Let G be a commutative group, A and B be nonempty finite subsets of G and $m \in \{1, 2, \ldots, \min\{|A|, |B|\}\}$.

⋆ We say that (A, B, m) is a *Pollard triple* if

$$\sum_{k=1}^{m} \left|A\overset{k}{+}B\right| \geq m\,|A| + m\,|B| - 2m^2 + 3m - 2.$$

⋆ We say that (A, B, m) is a *Kneser triple* if there is a subset A' of A and a subset B' of B satisfying

$$\left|A \setminus A'\right| + \left|B \setminus B'\right| \leq m - 1$$

and

$$A'\overset{m}{+}B' = A' + B' = A\overset{m}{+}B.$$

For $m \in \{1, 2, \ldots, \min\{|A|, |B|\}\}$, a result of D. Grynkiewicz establishes that (A, B, m) is either Pollard or Kneser.

Theorem 4. *Let $s \geq 1$, $u \in [0, 1)$, G be a commutative group, A and B be nonempty finite subsets of G, $k \in \{2, 3, \ldots, \min\{|A|, |B|\}\}$ and S be a subset of $A \times B$ such that $|S| \geq (1-u)|A||B|$ and $A\overset{S}{+}B$ is (k,s)-regular. Assume that $A\overset{S}{+}B \neq A + B$.*

i) If $k \leq \sqrt{\frac{u|A||B|}{2}}$ and $\left(A, B, \left\lceil\sqrt{\frac{u|A||B|}{2}}\right\rceil\right)$ is a Pollard triple, then

$$\left|A\overset{S}{+}B\right| \geq |A| + |B| - \sqrt{8u|A||B|} - 2.$$

ii) If $k \le \sqrt{\frac{u|A||B|}{2}}$ *and* $\left(A, B, \left\lceil \sqrt{\frac{u|A||B|}{2}} \right\rceil\right)$ *is a Kneser triple, then*

$$\left|A \overset{S}{+} B\right| \ge |A| + |B| - \sqrt{\frac{u|A||B|}{2}} - s.$$

iii) If $k > \sqrt{\frac{u|A||B|}{2}}$ *and* (A, B, k) *is a Pollard triple, then*

$$\left|A \overset{S}{+} B\right| \ge |A| + |B| - \frac{u|A||B|}{k} - 2k.$$

iv) If $k > \sqrt{\frac{u|A||B|}{2}}$ *and* (A, B, k) *is a Kneser triple, then*

$$\left|A \overset{S}{+} B\right| \ge |A| + |B| - k - s + 1.$$

If $k \le \sqrt{\frac{u|A||B|}{2}}$, then i) and ii) in Theorem 4 lead to

$$\left|A \overset{S}{+} B\right| \ge |A| + |B| - \sqrt{8u|A||B|} - s - 2. \tag{1}$$

If $k > \sqrt{\frac{u|A||B|}{2}}$, then iii) and iv) in Theorem 4 imply

$$\left|A \overset{S}{+} B\right| \ge |A| + |B| - \frac{u|A||B|}{k} - 2k - s + 3 \ge |A| + |B| - \sqrt{2u|A||B|} - 2k - s + 3. \tag{2}$$

Using that $|A| + |B| \ge 2\sqrt{|A||B|}$, we get from (1) and (2) the next corollary.

Corollary 5. *Let* $s \ge 1$, $u \in [0, 1)$, G *be a commutative group,* A *and* B *be nonempty finite subsets of* G, $k \in \{2, 3, \dots, \min\{|A|, |B|\}\}$ *and* S *be a subset of* $A \times B$ *such that* $|S| \ge (1 - u)|A||B|$ *and* $A \overset{S}{+} B$ *is* (k, s)*-regular. Assume that* $A \overset{S}{+} B \ne A + B$*. Then*

$$\left|A \overset{S}{+} B\right| \ge \left(1 - \sqrt{2u}\right)(|A| + |B|) - 2k - s + 2.$$

Corollary 5 is a nontrivial step in the solution of Lev's problem, i.e. to solve the problem, it would be enough to have $-k - 1$ instead of $-2k - s + 2$ in the lower bound of $\left|A \overset{S}{+} B\right|$.

We sketch the proof of Theorem 4.

i) For $m \in \{1, 2, \dots, \min\{|A|, |B|\}\}$, a result of D. Grynkiewicz, see [2, Thm.12.1], establishes that either the triple (A, B, m) is a Pollard triple or it is a Kneser triple.

ii) Assume that (A, B, m) is a Pollard triple. It is proven that

$$u|A||B| + m\left|A \overset{S}{+} B\right| \ge m\,|A| + m\,|B| - 2m^2,$$

which implies the claim of the theorem in this case. This crucial lemma is proven using some auxiliary subsets, partitions and elementary combinatorial arguments.

iii) Assume that (A, B, m) is a Kneser triple. Then there is a subset A' of A and a subset B' of B satisfying that

$$\left|A \setminus A'\right| + \left|B \setminus B'\right| \leq m - 1$$

and

$$A' \overset{m}{+} B' = A' + B' = A \overset{m}{+} B.$$

It is shown that

$$\left|A \overset{S}{+} B\right| \geq |A| + |B| - m - 1 - s.$$

This lemma is proven using partitions, projections and Kneser's Theorem.

References

[1] B. Bajnok, On the minimum size of restricted sumsets in cyclic groups, *Acta Math. Hungar.* **148** (2016), 228-256.

[2] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30 Springer, 2013.

[3] S. Guo, Restricted sumsets in a finite Abelian group, *Discrete Math.* **309** (2009), 6530-6534.

[4] S. Guo, Z. W. Sun, A variant of Tao's method with application to restricted sumsets, *J. Number Theory* **129** (2009), 434-438.

[5] Y. O. Hamidoune, S. C. López, A. Plagne, Large restricted sumsets in general Abelian groups, *European J. Combin.* **34** (2013), 1348-1364.

[6] M. Huicochea, A Kneser-type theorem for restricted sumsets, *SIAM J. Discrete Math.* **37** (2023), 83-93.

[7] V. Lev, Restricted set addition in groups, I. The classical setting, *J. London Math. Soc.* **62** (2000), 27-40.

[8] V. Lev, Restricted set addition in groups, II. A generalization of the Erdös-Heilbronn conjecture, *Electron. J. Combin.* **7** (2000) Paper 4, 1-10.

[9] V. Lev, Restricted set addition in groups, III. Integer sumsets with generic restrictions, *Periodica Math. Hungarica* **42** (2001), 89-98.

[10] V. Lev, Restricted set addition in abelian groups: results and conjectures, *J. Théor. Nombres Bordeaux* **17** (2005), 181-193.

[11] P. Mazur, A structure theorem for sets of small popular doubling, *Acta Arith.* **171** (2015), 221-239.

[12] M.B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math., vol. 165, Springer-Verlag, New York, 1996.

[13] H. Pan and Z. Wei, Restricted sumsets and a conjecture of Lev, *Israel J. Math.* **154** (2006), 21-28.

[14] F. Petrov, Restricted product sets under unique representability, *Mosc. J. Comb. Number Theory* **7** (2017), 73-78.

[15] X. Shao, On an almost all version of the Balog-Szemerédi-Gowers theorem, *Discrete Anal.* (2019) Paper 12, 1-18.

[16] X. Shao and W. Xu, A robust version of Freiman's 3k-4 theorem and applications, *Math. Proc. of the Cambridge Philos. Soc.* **166** (2019), 567-581.

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

[18] V. Vu and P. Wood, The inverse Erdös-Heilbronn problem, *Electron. J. Combin.* **16** (2009) Paper 100, 1-8.