TRANSLATION INVARIANCE IN GROUPS OF PRIME ORDER

VSEVOLOD F. LEV

Abstract. We prove that there is an absolute constant $c > 0$ with the following property: if $\mathbb{Z}/p\mathbb{Z}$ denotes the group of prime order p, and a subset $A \subset \mathbb{Z}/p\mathbb{Z}$ satisfies $1 < |A| < p/2$, then for any positive integer $m < \min\{c|A|/\ln|A|, \sqrt{p/8}\}$ there are at most $2m$ non-zero elements $b \in \mathbb{Z}/p\mathbb{Z}$ with $|(A+b) \setminus A| \le m$. This (partially) extends onto prime-order groups the result, established earlier by S. Konyagin and the present author for the group of integers.

We notice that if $A \subset \mathbb{Z}/p\mathbb{Z}$ is an arithmetic progression and $m < |A| < p/2$, then there are exactly $2m$ non-zero elements $b \in \mathbb{Z}/p\mathbb{Z}$ with $|(A+b) \setminus A| \le m$. Furthermore, the bound $c|A|/\ln|A|$ is best possible up to the value of the constant c. On the other hand, it is likely that the assumption $m < \sqrt{p/8}$ can be dropped or substantially relaxed.

1. Background and motivation

For a finite subset A and an element b of an additively written abelian group, let

$$\Delta_A(b) := |(A+b) \setminus A|.$$

If A does not contain cosets of the subgroup, generated by b, then the quantity $\Delta_A(b)$ can be interpreted as the smallest number of arithmetic progressions with difference b into which A can be partitioned. We also note that $|A| - \Delta_A(b)$ is the number of representations of b as a difference of two elements of A; thus, $\Delta_A(b)$ measures the "popularity" of b as such a difference (with 0 corresponding to the largest possible popularity).

The function Δ_A has been considered by a number of authors, the two earliest appearances in the literature we are aware of being [EH64] and [O68]. Evidently, we have $\Delta_A(0) = 0$; other well-known properties of this function are as follows:

P1. $\Delta_A(-b) = \Delta_A(b)$ for any group element b.

P2. If the underlying group is finite and $\bar{A}$ is the complement of A, then $\Delta_{\bar{A}}(b) = \Delta_A(b)$ for any group element b.

P3. $\Delta_A(b_1 + \dots + b_k) \le \Delta_A(b_1) + \dots + \Delta_A(b_k)$ for any integer $k \ge 1$ and group elements $b_1, \dots, b_k$.

2010 *Mathematics Subject Classification.* Primary: 11B75; Secondary: 11B25, 11P70.
Key words and phrases. Popular differences, set addition, additive combinatorics.

P4. Any finite, non-empty subset B of the group contains an element b with $\Delta_A(b) \ge \left(1 - \frac{|A|}{|B|}\right)|A|$.

The interested reader can find the proofs in [EH64, O68, HLS08] or work them out as an easy exercise. We confine ourselves to the remark that the last property follows by averaging over all elements of B.

The basic problem arising in connection with the function Δ_A is to show that it does not attain "too many" small values; that is, every set B contains an element b with $\Delta_A(b)$ large, with the precise meaning of "large" determined by the size of B. Accordingly, we let

$$\mu_A(B) := \max_{b\in B} \Delta_A(b).$$

Property P4 readily yields the simple lower-bound estimate

$$\mu_A(B) \ge \left(1 - \frac{|A|}{|B|}\right)|A|; \tag{1}$$

however, this estimate is far from sharp, and insufficient for most applications.

Notice, that if d is a group element of sufficiently large order, A is an arithmetic progression with difference d, and $B = \{d, 2d, \dots, md\}$ with $m = |B| \le |A|$, then $\mu_A(B) = |B|$. Thus,

$$\mu_A(B) \ge |B| \tag{2}$$

is the best lower-bound estimate one can hope to prove under the assumption $B \cap (-B) = \varnothing$ (cf. Property P1). In view of the trivial inequality $\mu_A(B) \le |A|$, a necessary condition for (2) to hold is $|B| \le |A|$, but this may not be enough to require: say, an example presented in [KL] shows that (2) fails in general for the group of integers, unless $|B| < c|A|/\ln|A|$ with a sufficiently small absolute constant c. As shown in [KL], this last assumption already suffices.

Theorem 1 ([KL, Theorem 1]). *There is an absolute constant $c > 0$ such that if A is a finite set of integers with $|A| > 1$, and B is a finite set of positive integers satisfying $|B| < c|A|/\ln|A|$, then $\mu_A(B) \ge |B|$.*

2. The main result

It is natural to expect that an analogue of Theorem 1 remains valid for groups of prime order, particularly since the arithmetic progression case is "worst in average" for these groups: namely, it is easy to derive from [L98, Theorem 1] that for all sets A and B of given fixed size in such a group, satisfying $B \cap (-B) = \varnothing$, the sum $\sum_{b\in B} \Delta_A(b)$ is minimized when A is an arithmetic progression, and $B = \{d, 2d, \dots, md\}$, where m is a positive integer and d is the difference of the progression. The goal of this note is to establish the corresponding supremum-norm result.

Throughout, we denote by $\mathbb{Z}$ the group of integers, and by $\mathbb{Z}/p\mathbb{Z}$ with p prime the group of order p.

Theorem 2. *There exists an absolute constant $c > 0$ with the following property: if p is a prime and the sets $A, B \subset \mathbb{Z}/p\mathbb{Z}$ satisfy $1 < |A| < p/2$, $B \cap (-B) = \varnothing$, and $|B| < \min\{c|A|/\ln|A|, \sqrt{p/8}\}$, then $\mu_A(B) \ge |B|$.*

As Property P2 shows, the assumption $|A| < p/2$ of Theorem 2 does not restrict its generality. In contrast, the assumption $|B| < \sqrt{p/8}$ seems to be an artifact of the method and it is quite possible that the assertion of Theorem 2 remains valid if this assumption is substantially relaxed or dropped altogether.

We notice that Theorem 2 is formally stronger than Theorem 1. However, the proof of the former theorem (presented in Section 4) relies on the latter one, used "as a black box". The proof also employs a rectification result of Freiman, and elements of the argument used in [KL] to prove Theorem 1, in a somewhat modified form.

The rest of this paper is divided into three parts: having prepared the ground in the next section, we prove Theorem 2 in Section 4, and present an application to the problem of estimating the size of a restricted sumset in the last section.

3. The toolbox

In this section we collect some auxiliary results, needed in the course of the proof of Theorem 2.

Given a subset B of an abelian group and an integer $h \ge 1$, by hB we denote the *h-fold sumset of B*:

$$hB := \{b_1 + \dots + b_h \colon b_1, \dots, b_h \in B\}.$$

Our first lemma is an immediate consequence of Property P3.

Lemma 1. *For any integer $h \ge 1$ and finite subsets A and B of an abelian group we have*

$$\mu_A(hB) \le h\mu_A(B).$$

The following lemma of Hamidoune, Lladó, and Serra gives an estimate which, looking deceptively similar to (1), for B small is actually rather sharp. We quote below a slightly simplified version, which is marginally weaker than the original result.

Lemma 2 ([HLS08, Lemma 3.1])**.** *Suppose that A and B are non-empty subsets of a finite cyclic group such that $B \cap (-B) = \varnothing$ and the size of A is at most half the size of the group. If every element of B generates the group, then*

$$\mu_A(B) > \left(1 - \frac{|B|}{|A|}\right)|B|.$$

Yet another ingredient of our argument is a rectification theorem due to Freiman.

Theorem 3 ([N96, Theorem 2.11])**.** *Let p be a prime and suppose that $B \subset \mathbb{Z}/p\mathbb{Z}$ is a subset with $|B| < p/35$. If $|2B| \le 2.4|B| - 3$, then B is contained in an arithmetic progression with at most $|2B| - |B| + 1$ terms.*

Finally, we need a lemma showing that if B is a dense set of integers, then the difference set

$$B - B := \{b' - b'' \colon b', b'' \in B\}$$

contains a long block of consecutive integers.

Lemma 3 ([L06, Lemma 3])**.** *Let B be a finite, non-empty set of integers. If $\max B - \min B < \frac{2k-1}{k}|B| - 1$ with an integer $k \ge 2$, then $B - B$ contains all integers from the interval $(-|B|/(k-1), |B|/(k-1))$.*

4. Proof of Theorem 2

For real $u < v$ and prime p, by φ_p we denote the canonical homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}/p\mathbb{Z}$, and by $[u, v]_p$ the image of the set $[u, v] \cap \mathbb{Z}$ under φ_p. In a similar way we define $[u, v)_p$ and $(u, v)_p$.

We begin with the important particular case where B is a block of consecutive group elements, starting from 1. Thus, we assume that p is a prime, $A \subset \mathbb{Z}/p\mathbb{Z}$ satisfies $1 < |A| < p/2$, and $m < \min\{c|A|/\ln|A|, \sqrt{p/8}\}$ is a positive integer (where c is the constant of Theorem 1), and show that, letting then $B := [1, m]_p$, we have $\mu_A(B) \ge m$.

Suppose, for a contradiction, that $\mu_A(B) < m$. Since A is a union of $\Delta_A(1)$ blocks of consecutive elements of $\mathbb{Z}/p\mathbb{Z}$, so is its complement $\bar{A} := (\mathbb{Z}/p\mathbb{Z}) \setminus A$, and we choose integers $u < v$ such that $[u, v)_p \subseteq \bar{A}$ and

$$v - u \ge \frac{|\bar{A}|}{\Delta_A(1)} > \frac{p}{2m} > m. \tag{3}$$

Rectifying the circle, we identify A with a set of integers $\mathcal{A} \subseteq [v, u+p)$, and B with the set $\mathcal{B} := [1, m] \cap \mathbb{Z}$. Inequality (3) shows that an arithmetic progression in $\mathbb{Z}/p\mathbb{Z}$ with difference $d \in [1, m]_p$ cannot "jump over" the block $[u, v)_p$; hence, $\mu_A(B) = \mu_{\mathcal{A}}(\mathcal{B})$. On the other hand, we have $\mu_{\mathcal{A}}(\mathcal{B}) \ge |\mathcal{B}| = m$ by Theorem 1. It follows that $\mu_A(B) \ge m$, the contradicting sought.

We notice that so far instead of $m < \sqrt{p/8}$ we have only used the weaker inequality

$$m < \sqrt{p/2}; \tag{4}$$

this observation is used below in the proof.

Having finished with the case where B consists of consecutive elements of $\mathbb{Z}/p\mathbb{Z}$, we now address the general situation. Suppose, therefore, that $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ satisfy the assumptions of the theorem and, again, assume that $\mu_A(B) < |B|$.

For a subset S of an abelian group we write $S^{\pm} := S \cup \{0\} \cup (-S)$; thus, by Property P1, we have $\mu_A(S^{\pm}) = \mu_A(S)$ for any finite subset A of the group, and if $S \cap (-S) = \varnothing$, then $|S^{\pm}| = 2|S| + 1$.

If $|2B^{\pm}| \geq \frac{1}{3}|A| + 1$, then by the well-known Cauchy-Davenport inequality (see, for instance, [N96, Theorem 2.2]), we have $|12B^{\pm}| > 2|A|$. Thus, using Lemma 1 and estimate (1), and assuming that c is sufficiently small, we conclude that

$$\mu_A(B) = \mu_A(B^{\pm}) \geq \frac{1}{12}\mu_A(12B^{\pm}) > \frac{1}{24}|A| \geq |B|,$$

a contradiction; accordingly, we assume

$$|2B^{\pm}| < \frac{1}{3}|A| + 1.$$

Let $C := (2B^{\pm}) \cap [1, p/2)_p$. Observing that $|C| = (|2B^{\pm}| - 1)/2 < \frac{1}{6}|A|$, by Lemmas 2 and 1 and the assumption $\mu_A(B) < |B|$ we get

$$\frac{5}{6}|C| < \mu_A(C) = \mu_A(2B^{\pm}) \leq 2\mu_A(B^{\pm}) = 2\mu_A(B) \leq 2(|B| - 1) = |B^{\pm}| - 3;$$

hence,

$$|2B^{\pm}| = 2|C| + 1 < \frac{12}{5}|B^{\pm}| - \frac{31}{5} < 2.4|B^{\pm}| - 3. \tag{5}$$

We now apply Theorem 3 to derive that the set $B^{\pm}$ is contained in an arithmetic progression with at most $|2B^{\pm}| - |B^{\pm}| + 1 < \frac{1}{3}|A| < p/2 + 1$ terms. Taking into account that $0 \in B^{\pm}$ and dilating A and B suitably, we assume without loss of generality that $B^{\pm} \subseteq (-p/4, p/4)_p$ and $B^{\pm}$ is actually contained in a block of at most $|2B^{\pm}| - |B^{\pm}| + 1$ consecutive elements of $\mathbb{Z}/p\mathbb{Z}$.

Let $\mathcal{B} \subseteq [1, p/4)$ be the set of integers such that $B^{\pm} = \varphi_p(\mathcal{B}^{\pm})$, and write $l := \max(\mathcal{B}^{\pm}) - \min(\mathcal{B}^{\pm})$. From (5) we conclude that

$$l \leq |2B^{\pm}| - |B^{\pm}| < \frac{3}{2}|B^{\pm}| - 1 = \frac{3}{2}|\mathcal{B}^{\pm}| - 1.$$

Therefore, by Lemma 3 (applied with $k = 2$) we have

$$[1, |\mathcal{B}^{\pm}| - 1] \subseteq \mathcal{B}^{\pm} - \mathcal{B}^{\pm} = 2\mathcal{B}^{\pm},$$

whence

$$[1, |B^{\pm}| - 1]_p \subseteq 2B^{\pm}.$$

Recalling that the result is already established for the consecutive residues case, and observing that $|B^{\pm}| - 1 = 2|B| < \sqrt{p/2}$ (to be compared with (4)), we obtain

$$\mu_A(2B^{\pm}) \geq \mu_A([1, |B^{\pm}| - 1]_p) \geq |B^{\pm}| - 1 = 2|B|.$$

Using now Lemma 1 we get

$$2\mu_A(B) = 2\mu_A(B^{\pm}) \geq \mu_A(2B^{\pm}) \geq 2|B|,$$

a contradiction completing the proof of Theorem 2.

5. An application: restricted sumsets in abelian groups

Given two subsets A and B of an abelian group and a mapping $\tau\colon B \to A$, let

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

Restricted sumsets of this form, generalizing in a natural way the "classical" restricted sumset $\{a+b\colon a \in A,\, b \in B,\, a \neq b\}$, were studied, for instance, in [L00]. Since

$$|(A+b_1) \cup (A+b_2)| = |A| + |(A+b_1-b_2) \setminus A|$$

for any $b_1, b_2 \in B$, we have

$$|A+B| \geq |A| + \mu_A(B-B)$$

and, furthermore,

$$|A \overset{\tau}{+} B| \geq |A| + \mu_A(B-B) - 2;$$

hence, lower-bound estimates for $\mu_A(B-B)$ translate immediately into estimates for the cardinalities of the sumset $A+B$ and the restricted sumset $A \overset{\tau}{+} B$. Here we confine ourselves to stating three corollaries of estimate (1), Lemma 2, and Theorem 2, respectively.

Theorem 4. *Suppose that A and B are finite subsets of an abelian group. If for some real $\varepsilon > 0$ we have $|B| \leq (1-\varepsilon)|A|$ and $|B-B| \geq \varepsilon^{-1}|A|$, then*

$$|A+B| \geq |A| + |B|$$

and

$$|A \overset{\tau}{+} B| \geq |A| + |B| - 2$$

for any mapping $\tau\colon B \to A$.

Theorem 5. *Suppose that p is a prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ are non-empty. If $|A| < p/2$ and $|B| < \sqrt{|A|} + 1$, then for any mapping $\tau\colon B \to A$ we have*

$$|A \overset{\tau}{+} B| \geq |A| + |B| - 3.$$

For the proof just notice that if $2 \le |B| \le (p+1)/2$, then by the Cauchy-Davenport inequality there exists a subset $C \subseteq B - B$ with $C \cap (-C) = \varnothing$ and $|C| = |B| - 1$, whence, in view of Lemma 2,

$$\mu_A(B-B) \ge \mu_A(C) \ge \left(1 - \frac{|C|}{|A|}\right)|C| = |B| - 1 - \frac{(|B|-1)^2}{|A|} > |B| - 2.$$

Theorem 6. *Suppose that p is a prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$. If $1 < |A| < p/2$ and $0 < |B| < \min\{\sqrt{p/8},\, c|A|/\ln|A|\}$, where c is a positive absolute constant, then for any mapping $\tau\colon B \to A$ we have*

$$|A \overset{\tau}{+} B| \ge |A| + |B| - 3.$$

In connection with the last two theorems we notice that a construction presented in [L00] shows that for (non-empty) subsets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ and a mapping $\tau\colon B \to A$, the estimate $|A \overset{\tau}{+} B| \ge |A| + |B| - 3$ may fail in general, even if the right-hand side is substantially smaller than p. A question raised in [L00] and ramaining open till now is whether this estimate holds true under the additional assumption that τ is injective and $|A| + |B| \le p$.

References

[EH64] P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149–159.

[HLS08] Y.O. Hamidoune, A.S. Lladó, and O. Serra, On complete subsets of the cyclic group, *J. Comb. Theory, Series A* **115** (7) (2008), 1279–1285.

[KL] S.V. Konyagin and V.F. Lev, On the number of popular differences, *Israel J. Math.*, to appear.

[L06] V.F. Lev, Large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$, *Israel J. Math.* **154** (2006), 221–233.

[L98] ———, Linear equations over $\mathbb{F}_p$ and moments of exponential sums, *Duke Math. J.* **107** (2) (2001), 239–263.

[L00] ———, Restricted set addition in groups. II. A generalization of the Erdős-Heilbronn conjecture, *Electron. J. Combin.* **7** (2000), Research Paper 4, 10 pp. (electronic).

[N96] M.B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics **165**, Springer-Verlag, New York, 1996.

[O68] J.E. Olson, An addition theorem modulo p, *J. Comb. Theory* **5** (1968), 45–52.

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel
E-mail address: seva@math.haifa.ac.il