

## A quadratic lower bound for subset sums

by

MATT DEVOS, LUIS GODDYN, BOJAN MOHAR  
and ROBERT ŠÁMAL (Burnaby)

**1. Introduction.** All groups considered in this paper are abelian, and we shall use additive notation. Let  $G$  be such a group. If  $A, B \subseteq G$ , then we let  $A + B = \{a + b : a \in A, b \in B\}$ . If  $g \in G$ , we let  $g + A = A + g = \{g\} + A$ , and we call any such set a *shift* of  $A$ . The *stabilizer* of  $A$  is  $\text{stab}(A) = \{g \in G : g + A = A\}$ ; note that this is a subgroup of  $G$ . We define  $\Sigma(A) = \{\sum_{a \in A'} a : A' \subseteq A\}$ , so  $\Sigma(A)$  is the set of group elements which can be represented as sums of subsets of  $A$ . For any positive integer  $n$ , we let  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ .

In a lovely paper [2] which contains many of the ideas needed in our proof, Erdős and Heilbronn proved that  $\Sigma(A) = G$  whenever  $G \cong \mathbb{Z}_p$  for a prime  $p$  and  $A \subseteq G \setminus \{0\}$  satisfies  $|A| \geq 3\sqrt{6p}$ . They conjectured that assuming  $|A| \geq 2\sqrt{p}$  is sufficient; this was confirmed by Olson [4] and further sharpened by Dias da Silva and Hamidoune [1].

**THEOREM 1.1.** *Let  $p$  be a prime and let  $A \subseteq \mathbb{Z}_p \setminus \{0\}$ . If  $|A| > \lfloor \sqrt{4p-7} \rfloor$ , then  $\Sigma(A) = \mathbb{Z}_p$ .*

To see that this theorem is essentially best possible, let  $A \subseteq \mathbb{Z}_p$  be the set  $\{-\lfloor \sqrt{p} \rfloor, \dots, -1, 1, \dots, \lfloor \sqrt{p} \rfloor\}$  and note that  $\lfloor p/2 \rfloor \notin \Sigma(A)$ . Such a strong conclusion does not hold in general abelian groups, due to the existence of proper nontrivial subgroups. For instance, if  $H < G$  has  $[G : H] = 3$  and we take  $A = H$ , then  $\Sigma(A) = H$  even though  $A$  contains one third of the

2000 *Mathematics Subject Classification*: Primary 11B75.

*Key words and phrases*: subset sums, additive bases, abelian groups.

Research of L. Goddyn supported by a Canada NSERC Discovery Grant.

Research of B. Mohar (on leave from IMFM & FMF, Department of Mathematics, University of Ljubljana, Ljubljana, Slovenia) supported in part by the Slovenian ARRS Research Grant P1-0297 and in part by an NSERC Discovery Grant and CRC program.

Research of R. Šámal (on leave from Institute for Theoretical Computer Science (ITI), Charles University, Prague, Czech Republic) supported by PIMS postdoctoral fellowship.

elements in  $G$ . In cyclic groups, Vu found a suitable assumption on  $A$  which permits a similar conclusion.

**THEOREM 1.2** (Vu [6]). *There exists a constant  $c$  so that  $\Sigma(A) = \mathbb{Z}_n$  whenever  $A \subseteq \mathbb{Z}_n$  has size at least  $c\sqrt{n}$  and has the added property that every number in  $A$  is relatively prime to  $n$ .*

The constant in this theorem is quite large. It is derived from a very deep theorem of Szemerédi and Vu [5] on arithmetic progressions in sumsets. Our main theorem, which is quite elementary by comparison, can be used to obtain Theorem 1.2 with a constant of  $c = 8$ .

Our main result gives a lower bound on  $|\Sigma(A)|$ , but before introducing it, we shall pause to introduce Kneser’s addition theorem, an essential tool in our proof. Moreover, a simple corollary of it gives a natural lower bound on  $|\Sigma(A)|$  which is of interest.

**THEOREM 1.3** (Kneser [3]). *Let  $A_1, \dots, A_m$  be finite nonempty subsets of  $G$ . If  $H = \text{stab}(\sum_{i=1}^m A_i)$ , then*

$$\left| \sum_{i=1}^m A_i \right| \geq |H|(1 - m) + \sum_{i=1}^m |A_i + H|.$$

**COROLLARY 1.4.** *Let  $A \subseteq G$  and set  $H = \text{stab}(\Sigma(A))$ . Then*

$$|\Sigma(A)| \geq |H| + |H| \cdot |A \setminus H|.$$

*Proof.* Let  $A = \{a_1, \dots, a_m\}$ . Then  $\Sigma(A) = \sum_{i=1}^m \{0, a_i\}$ , and we obtain the desired bound by applying Kneser’s theorem to the right hand side of this equation. ■

Our main theorem gives an alternative bound on  $|\Sigma(A)|$  which improves upon that from the previous corollary in the case when  $|H|$  is small.

**THEOREM 1.5.** *Let  $A \subseteq G$  and set  $H = \text{stab}(\Sigma(A))$ . Then*

$$|\Sigma(A)| \geq |H| + \frac{1}{64}|A \setminus H|^2.$$

As mentioned earlier, direct application of this result yields Theorem 1.1 with a weaker constant and Theorem 1.2 with the stronger constant  $c = 8$ . To see this latter implication, let  $A \subseteq \mathbb{Z}_n$  have size  $\geq 8\sqrt{n}$ , assume it has the property that every element in  $A$  is relatively prime to  $n$ . Suppose (for a contradiction) that  $\Sigma(A) \neq \mathbb{Z}_n$ . Then  $H = \text{stab}(\Sigma(A))$  is a proper subgroup of  $\mathbb{Z}_n$ , so  $A \cap H = \emptyset$  since every element in  $A$  generates the entire group. But then our bound yields  $|\Sigma(A)| \geq |H| + \frac{1}{64}|A \setminus H|^2 > n$ —a contradiction.

With some extra work we can improve our constant  $1/64$  somewhat. Indeed, it follows from our arguments that the same result holds with a constant of “almost”  $1/48$ . We suspect that Theorem 1.5 may almost hold with  $1/4$  in place of  $1/64$ : it seems likely that  $|\Sigma(A)| \geq \frac{1}{4}|A \setminus H|^2 - O(|A|)$ . The extreme example we know of is essentially the same as that mentioned

earlier in connection with Olson’s theorem. Namely, if  $A = \{-n, -(n - 1), \dots, n - 1, n\} \subseteq \mathbb{Z}$ , then  $|A| = 2n + 1$ ,  $H = \text{stab}(\Sigma(A)) = \{0\}$ , and  $\Sigma(A) = \{-n(n - 1)/2, \dots, n(n - 1)/2\}$  has size  $n(n - 1) + 1$ .

Theorem 1.5 may be bootstrapped to give a bound on subsequence sums. If  $\mathbf{a}$  is a sequence of elements in  $G$ , we let  $\Sigma(\mathbf{a})$  denote the set of all sums of subsequences of  $\mathbf{a}$ . Note that if  $\mathbf{a} = (a_1, \dots, a_n)$  and all the  $a_i$ ’s are distinct then  $\Sigma(\mathbf{a}) = \Sigma(\{a_1, \dots, a_n\})$ ; so subsequence sums generalize the notion of subset sums.

If  $H \leq G$ , we call any element of  $G/H \setminus \{H\}$  a *nontrivial  $H$ -coset* of  $G$ . We let  $q_H^j(\mathbf{a})$  (for each  $j \in \mathbb{N}$ ) denote the number of nontrivial  $H$ -cosets of  $G$  which contain at least  $j$  terms of  $\mathbf{a}$ .

**THEOREM 1.6.** *Let  $\mathbf{a} = (a_1, \dots, a_n)$  be a sequence of elements in  $G$ , and let  $H = \text{stab}(\Sigma(\mathbf{a}))$ . Then*

$$|\Sigma(\mathbf{a})| \geq |H| + \frac{1}{64}|H| \cdot \sum_{j \in \mathbb{N}} (q_H^j(\mathbf{a}))^2.$$

**2. Proofs.** The goal of this section is to prove our main results, Theorems 1.5 and 1.6. In fact, these theorems are easily seen to be equivalent, and our approach will be to first prove Theorem 1.5 in the special case when  $H = \{0\}$ , and then use this to prove the two main results in general.

Before we immerse ourselves in the details of the proof, let us sketch our strategy. As in [2], the key goal is to show that in every set  $A \subseteq G$  with  $|A| = 2(u + 1)$  we can find a subset  $B$  of size  $u + 1$  such that  $\Sigma(B)$  is large, provided  $\Sigma(A)$  has trivial stabilizer (Lemma 2.7). To establish this, we first use an inductive hypothesis to find a set  $B$  of size  $u$ . Then we will try to find an element  $c \in C = A \setminus B$  such that by appending  $c$  to  $B$ , the size of  $S = \Sigma(B)$  grows significantly (thus maintaining our quadratic bound). In other words, we want  $\Delta_S(c) := |(S + c) \setminus S|$  to be large. Special cases of this task are dealt with in Lemma 2.4 (if “ $S$  is small”) and in Lemma 2.5 (if “ $S$  is big”). In the work-horse of our proof, Lemma 2.6, we use these two to handle all possible cases.

We also need to introduce a couple of definitions. If  $G$  is a group and  $B \subseteq G$  then a (*directed*) *Cayley graph*  $\text{Cayley}(G, B)$  is a graph with vertex-set  $G$  and with an arc  $(g, g + b)$  for every  $g \in G$  and  $b \in B$ . If  $B \subseteq G$  then we use  $\langle B \rangle$  to denote the subgroup of  $G$  generated by  $B$ .

During the course of our proof we will often use Kneser’s theorem (Theorem 1.3) and the following easy observations.

**OBSERVATION 2.1.** *We have  $\text{stab}(S) \leq \text{stab}(S + T)$  whenever  $S, T \subseteq G$ . In particular, if  $B \subseteq A$ , then  $\text{stab}(\Sigma(B)) \leq \text{stab}(\Sigma(A))$ .*

**OBSERVATION 2.2.** *If  $A, B \subseteq G$  and  $|A| + |B| > |G|$ , then  $A + B = G$ .*

For every  $S \subseteq G$  and every  $x \in G$ , we define  $\Gamma_S(x) = |(S+x) \cap S|$  and  $\Delta_S(x) = |(S+x) \setminus S|$ . Note that  $\Gamma_S(x) + \Delta_S(x) = |S|$  and that  $\Delta_S(x) = \Delta_{G \setminus S}(x)$ . More interestingly, the following observation shows that  $\Delta_S$  is subadditive.

**OBSERVATION 2.3** (Erdős and Heilbronn [2]). *If  $x, y \in G$  then  $\Delta_S(x+y) \leq \Delta_S(x) + \Delta_S(y)$ .*

*Proof.* This is an immediate consequence of the following computation:

$$\begin{aligned} \Delta_S(x+y) &= |(S+x+y) \setminus S| \\ &\leq |(S+x+y) \setminus (S+y)| + |(S+y) \setminus S| \\ &= |(S+x) \setminus S| + |(S+y) \setminus S| = \Delta_S(x) + \Delta_S(y). \blacksquare \end{aligned}$$

If  $Q, S \subseteq G$ , we define the *deficiency of  $Q$  with respect to  $S$*  to be  $\text{def}_S(Q) = \min\{|Q \cap S|, |Q \setminus S|\}$ .

**LEMMA 2.4.** *Let  $C, S$  be finite subsets of a group  $H$  such that  $\text{def}_S(H) \leq \frac{1}{2}|C|$ . Then  $|C|^{-1} \sum_{c \in C} \Delta_S(c) \geq \frac{1}{2} \text{def}_S(H)$ . In particular, there exists  $c \in C$  with  $\Delta_S(c) \geq \frac{1}{2} \text{def}_S(H)$ .*

*Proof.* Recall that  $\Delta_S(c) = \Delta_{H \setminus S}(c)$  for every  $c$ . Hence, after possibly replacing  $S$  with  $H \setminus S$ , we may assume that  $\text{def}_S(H) = |S|$ . Our lemma now follows from the inequalities below.

$$\begin{aligned} \sum_{c \in C} \Delta_S(c) &= |C| \cdot |S| - \sum_{c \in C} \Gamma_S(c) \\ &\geq |C| \cdot |S| - \sum_{h \in H} \Gamma_S(h) = |C| \cdot |S| - |S|^2 \\ &\geq \frac{1}{2}|C| \cdot |S| = \frac{1}{2}|C| \cdot \text{def}_S(H). \blacksquare \end{aligned}$$

**LEMMA 2.5.** *Let  $C, S$  be finite subsets of a group  $H$  such that  $\text{def}_S(H) \geq \frac{1}{2}|C|$  and  $\langle C \rangle = H$ . Then there exists  $c \in C$  with  $\Delta_S(c) \geq \frac{1}{8}|C|$ .*

*Proof.* By possibly replacing  $S$  with  $H \setminus S$  we may assume that  $\text{def}_S(H) = |S|$  and therefore  $\frac{1}{2}|C| \leq |S| \leq \frac{1}{2}|H|$ . Now set  $r = \lfloor 4|S|/|C| \rfloor$ , let  $C^* = C \cup \{0\}$ , and let  $D = \sum_{i=1}^r C^*$ . Put  $K = \text{stab}(D)$  and let  $t = |C^* + K|/|K|$ , i.e.,  $t$  is the number of  $K$ -cosets in  $H$  intersecting  $C^*$ . If  $t \geq 2$ , then by Kneser’s addition theorem, we have

$$\begin{aligned} |D| &\geq r|C^* + K| - (r-1)|K| = r \left(1 - \frac{1}{t}\right) |C^* + K| + |K| \\ &\geq \frac{4|S| - |C|}{|C|} \left(1 - \frac{1}{t}\right) |C| + \frac{1}{t} |C| \\ &= 2|S| + \frac{t-2}{t} (2|S| - |C|) \geq 2|S|. \end{aligned}$$

If  $t = 1$ , then  $C \subseteq K$  and  $C$  generates  $H$ , so we must have  $H = K = D$  and again  $|D| \geq 2|S|$ . This brings us to the following easy inequality:

$$\sum_{d \in D} \Gamma_S(d) \leq \sum_{h \in H} \Gamma_S(h) = |S|^2 \leq \frac{1}{2}|D| \cdot |S|.$$

It follows that there exists  $d \in D$  with  $\Gamma_S(d) \leq \frac{1}{2}|S|$  and thus  $\Delta_S(d) \geq \frac{1}{2}|S|$ . By construction, we may choose  $c_1, \dots, c_n \in C$  with  $n \leq r$  so that  $d = \sum_{i=1}^n c_i$ . Now, by the subadditivity of  $\Delta_S$  we have  $\frac{1}{2}|S| \leq \Delta_S(d) \leq \sum_{i=1}^n \Delta_S(c_i)$  and it follows that there exists  $c \in C$  for which  $\Delta_S(c) \geq \frac{1}{2r}|S| \geq \frac{1}{8}|C|$  as desired. ■

LEMMA 2.6. *Let  $A \subseteq G$  satisfy  $|A| = 2u + 2$  and  $\text{stab}(\Sigma(A)) = \{0\}$ . Let  $\{B, C\}$  be a partition of  $A$  with  $|B| = u$ , and put  $S = \Sigma(B)$  and  $H = \langle C \rangle$ . If  $u \geq 16$  and  $|H| \geq \frac{5}{256}u^2 + \frac{1}{4}u$ , then one of the following holds:*

- (1)  $|S| \geq \frac{1}{16}(u + 1)^2$ .
- (2) There exists  $c \in C$  so that  $\Delta_S(c) \geq \frac{1}{8}(u + 1)$ .

*Proof.* Define an  $H$ -coset  $Q$  to be *sparse* if  $0 < |Q \cap S| < \frac{1}{4}(u + 1)$  and *dense* if  $|Q \setminus S| < \frac{1}{4}(u + 1)$ . If there is an  $H$ -coset  $Q$  with  $Q \cap S \neq \emptyset$  which is neither sparse nor dense, then  $\text{def}_S(Q) \geq \frac{1}{4}(u + 1)$ , so conclusion (2) follows by applying either Lemma 2.4 or Lemma 2.5 to  $C$  and an appropriate shift of  $Q \cap S$ . Thus, we may assume that every  $H$ -coset which contains a point of  $S$  is either sparse or dense.

If the sum of the deficiencies of the  $H$ -cosets (with respect to  $S$ ) is at least  $\frac{1}{4}(u + 1)$ , then by the averaging argument in Lemma 2.4, we find a  $c \in C$  for which  $\Delta_S(c) \geq \frac{1}{8}(u + 1)$ , and conclusion (2) is satisfied. Thus, we may assume that the sum of the deficiencies of the  $H$ -cosets is at most  $\frac{1}{4}(u + 1)$ . Since  $|S| \geq u$  this implies that there is at least one dense  $H$ -coset.

If  $R$  is a dense  $H$ -coset, then it follows from Observation 2.2 (and  $|\Sigma(C)| \geq |C| \geq \frac{1}{4}(u + 1)$ ) that  $\Sigma(C) + (R \cap S) = R$ . Consequently, if there are no sparse  $H$ -cosets, then  $H \leq \text{stab}(\Sigma(C) + S) = \Sigma(A)$ , which contradicts our assumptions. Thus, we may assume that there is at least one sparse  $H$ -coset. In particular,  $S$  has nonempty intersection with at least two  $H$ -cosets, so  $S \not\subseteq H$ .

If there exist four distinct dense  $H$ -cosets  $Q_1, \dots, Q_4$ , then

$$\begin{aligned} |S| &\geq \sum_{i=1}^4 |S \cap Q_i| = 4|H| - \sum_{i=1}^4 \text{def}_S(Q_i) \\ &\geq \frac{5}{64}u^2 + u - \frac{1}{4}(u + 1) \geq \frac{1}{16}(u + 1)^2. \end{aligned}$$

Thus, we may assume that there are at most three dense  $H$ -cosets. Now, for every  $b \in B$ , define  $S_b^+ = b + \Sigma(B \setminus \{b\})$  and  $S_b^- = \Sigma(B \setminus \{b\})$ . Note that  $S = S_b^+ \cup S_b^-$ .

CLAIM. *If  $R$  is a dense  $H$ -coset and  $b \in B$ , then either  $R + b$  or  $R - b$  is dense.*

*Proof.* If  $b \in H$ , then the claim holds trivially, so we may assume  $b \notin H$ . Let  $d = \text{def}_S(R)$  and suppose (for a contradiction) that neither  $R + b$  nor  $R - b$  is dense. Observe that  $S \cap (R + b)$  contains  $(S_b^- \cap R) + b$  and  $S \cap (R - b)$  contains  $(S_b^+ \cap R) - b$ . Suppose (without loss) that  $|S_b^- \cap R| \geq |S_b^+ \cap R|$ . Then we have

$$\begin{aligned} \frac{1}{4}(u + 1) &> \text{def}_S(R) + \text{def}_S(R + b) \geq d + |S_b^- \cap R| \\ &\geq d + \frac{1}{2}(|H| - d) \geq \frac{5}{512}u^2 + \frac{1}{8}u. \end{aligned}$$

This contradicts  $u \geq 16$ , thus establishing the claim. ■

Let  $W \subseteq G/H$  be the set of all dense  $H$ -cosets and set  $w = |W|$ . We have  $1 \leq w \leq 3$  by our earlier arguments, but it now follows from the claim (and  $S \not\subseteq H$ ) that  $w \geq 2$ , so  $w \in \{2, 3\}$ . For every  $b \in G$ , let  $\Gamma_b$  be the subgraph of  $\text{Cayley}(G/H, b + H)$  induced by  $W$ . It follows from the claim that  $\Gamma_b$  has no isolated vertices whenever  $b \in B \setminus H$ . Thus, every such  $\Gamma_b$  is either a directed path or a directed cycle. If the graphs  $\Gamma_b$  and  $\Gamma_{b'}$  both have an edge with the same ends, then either  $b' + H = b + H$  or  $b' + H = -b + H$ . It follows that either every  $\Gamma_b$  is a directed cycle, or every  $\Gamma_b$  is a directed path; in the latter case every pair of such paths have the same (unordered) ends. If  $\Gamma_b$  is a directed cycle for some  $b \in B \setminus H$ , then  $B \subseteq \langle H \cup \{b\} \rangle$  and we find that there are no sparse  $H$ -cosets, contradicting our previous conclusions.

Thus, we may assume that every  $\Gamma_b$  with  $b \in B \setminus H$  is a directed path. List the dense  $H$ -cosets  $W_1, \dots, W_w$  so that every  $\Gamma_b$  is a directed path with ends  $W_1$  and  $W_w$ . Setting  $Q = W_2 - W_1$  we find that  $W_1, \dots, W_w$  is an arithmetic progression in  $G/H$  with difference  $Q$ . Let  $W_0 = W_1 - Q$  and  $W_{w+1} = W_w + Q$ ; note that  $\{W_0, W_{w+1}\} \cap \{W_1, \dots, W_w\} = \emptyset$ .

Suppose first that  $|B \setminus H| \geq w$ . Choose  $w$  distinct elements  $b_1, \dots, b_w \in B \setminus H$  and for each of them choose  $\varepsilon_i \in \{-, +\}$  so that  $\varepsilon_i b_i \in Q$ . Now, let  $Z = W_1 \cap \bigcap_{i=1}^w S_{b_i}^{-\varepsilon_i}$  (in the exponent we treat  $\{+, -\}$  as a multiplicative group with identity  $+$ ). It follows from our construction that  $Z + \sum_{i=1}^w \varepsilon_i b_i \subseteq S \cap W_{w+1}$ . For every  $1 \leq i \leq w$  we have  $(S_{b_i}^{\varepsilon_i} \cap W_1) - \varepsilon_i b_i \subseteq W_0 \cap S$ , so each  $W_1 \cap S_{b_i}^{-\varepsilon_i}$  contains all but at most  $|W_0 \cap S|$  points of  $W_1 \cap S$ . Thus, setting  $d = \text{def}_S(W_1)$  we have the following inequalities (we use  $|H| \geq |C| > u + 1$  and  $|W_0 \cap S| < \frac{1}{4}(u + 1)$ ):

$$\begin{aligned} \frac{1}{4}(u + 1) &> \text{def}_S(W_1) + \text{def}_S(W_{w+1}) \geq d + |Z| \\ &\geq d + |H| - d - w|W_0 \cap S| \geq u + 1 - \frac{w}{4}(u + 1). \end{aligned}$$

However, this contradicts  $w \in \{2, 3\}$ . Thus  $|B \setminus H| < w$ . But then we must have  $|B \setminus H| = w - 1$ , and we again find that there are no sparse  $H$ -cosets, which contradicts our previous conclusions. This completes the proof. ■

Following Erdős and Heilbronn [2], we define a function  $L : \mathbb{N} \rightarrow \mathbb{N}$  by the following rule:

$$L(u) = \min_{\substack{A \subseteq G \setminus \{0\} : |A|=2u \\ \text{stab}(\Sigma(A))=\{0\}}} \max_{B \subseteq A : |B|=u} |\Sigma(B)|.$$

We let  $L(u) = \infty$  if no such set  $A$  exists. For every set  $B$  we have  $\Sigma(B) \supseteq B \cup \{0\}$ , so trivially  $L(u) \geq u + 1$ . Next we prove our main lemma which gives a better lower bound on  $L(u)$ .

LEMMA 2.7.  $L(u) \geq \frac{1}{16}u^2$  for every  $u \in \mathbb{N}$ .

*Proof.* We proceed by induction on  $u$ . Assume that the lemma holds for all integers  $\leq u$  and let  $A \subseteq G$  satisfy  $|A| = 2(u + 1)$  and  $\text{stab}(\Sigma(A)) = \{0\}$ . (If there is no such set, then we have defined  $L(u + 1) = \infty$ .) We will show that there exists  $B' \subseteq A$  with  $|B'| = u + 1$  and  $|\Sigma(B')| \geq \frac{1}{16}(u + 1)^2$ . It follows from our trivial bound  $L(u) \geq u + 1$  that we may assume  $u \geq 16$ .

Apply the lemma inductively to obtain a set  $B \subseteq A$  with  $|B| = u$  and  $|\Sigma(B)| \geq \frac{1}{16}u^2$ . Put  $C = A \setminus B$ . To apply Lemma 2.6, which is our aim, we need a lower bound on the size of  $H = \langle C \rangle$ . We do this by estimating  $|\Sigma(C)|$ . To this end, we apply the lemma inductively twice more: choose a set  $C_1 \subseteq C$  of size  $\lceil u/2 \rceil$  with  $|\Sigma(C_1)| \geq \frac{1}{64}u^2$  and (since  $2\lceil u/4 \rceil + \lceil u/2 \rceil \leq 2(u + 3)/4 + (u + 1)/2 = u + 2$ ) a set  $C_2 \subseteq C \setminus C_1$  of size  $\lceil u/4 \rceil$  with  $|\Sigma(C_2)| \geq \frac{1}{256}u^2$ . Put  $C_3 = C \setminus (C_1 \cup C_2)$ . Now  $\Sigma(C) = \Sigma(C_1) + \Sigma(C_2) + \Sigma(C_3)$ . Since  $\Sigma(C)$  has trivial stabilizer (Observation 2.1), Kneser’s theorem gives the following inequality (in the last inequality we use the trivial bound  $|\Sigma(X)| \geq |X| + 1$  if  $0 \notin X$ ):

$$\begin{aligned} |\Sigma(C)| &= |\Sigma(C_1) + \Sigma(C_2) + \Sigma(C_3)| \\ &\geq |\Sigma(C_1)| + |\Sigma(C_2)| + |\Sigma(C_3)| - 2 \\ &\geq \frac{5}{256}u^2 + \frac{1}{4}u - 1. \end{aligned}$$

Let  $S = \Sigma(B)$  and recall that  $H = \langle C \rangle$ . Since  $\Sigma(C)$  has trivial stabilizer,  $\Sigma(C) \subset H$ , so  $|H| \geq \frac{5}{256}u^2 + \frac{1}{4}u$ . Since  $u \geq 16$  by assumption, we may apply Lemma 2.6 to deduce that either  $|S| \geq \frac{1}{16}(u + 1)^2$ , in which case we are finished, or there exists  $c \in C$  so that  $\Delta_S(c) \geq \frac{1}{8}(u + 1)$ . In the latter case we have

$$\begin{aligned} |\Sigma(B \cup \{c\})| &= |S + \{0, c\}| = |S| + \Delta_S(c) \\ &\geq \frac{1}{16}u^2 + \frac{1}{8}(u + 1) > \frac{1}{16}(u + 1)^2. \end{aligned}$$

This completes the proof. ■

LEMMA 2.8. *If  $A \subseteq G$  satisfies  $\text{stab}(\Sigma(A)) = \{0\}$ , then*

$$|\Sigma(A)| \geq 1 + \frac{1}{64}|A \setminus \{0\}|^2.$$

*Proof.* We may assume that  $0 \notin A$  since this has no effect on our bound. Set  $|A| = u$ . The lemma holds trivially if  $u \leq 8$ , so we may assume  $u > 8$ . By the previous lemma we may choose a subset  $B \subseteq A$  of size  $\lfloor u/2 \rfloor$  such that  $|\Sigma(B)| \geq L(\lfloor u/2 \rfloor) \geq (u - 1)^2/64$ . Let  $C = A \setminus B$ . Then by Kneser’s theorem we have

$$\begin{aligned} |\Sigma(A)| &= |\Sigma(B) + \Sigma(C)| \geq |\Sigma(B)| + |C| - 1 \\ &\geq \frac{1}{64}u^2 - \frac{1}{32}u + \frac{1}{2}u - 1 \geq 1 + \frac{1}{64}u^2. \blacksquare \end{aligned}$$

Note that by recursively applying Lemma 2.7 we can improve the constant  $1/64$  to “almost”  $1/48$ : In the above proof, we have used the fact that  $|\Sigma(B)| \geq L(|B|)$  (together with Lemma 2.7) to bound  $|\Sigma(B)|$ . On the other hand, for  $|\Sigma(C)|$  we have used a straightforward bound  $|\Sigma(C)| \geq |C| + 1$ . We could instead use the same procedure recursively with  $C$  in place of  $A$ . This yields

$$|\Sigma(A)| \geq \frac{1}{16} \left( \left\lfloor \frac{u}{2} \right\rfloor^2 + \left\lfloor \frac{u}{4} \right\rfloor^2 + \left\lfloor \frac{u}{8} \right\rfloor^2 + \dots \right) = \frac{1}{48} u^2 - O(u).$$

Next we prove our main theorem for sequences.

*Proof of Theorem 1.6.* For  $Q \in G/H$  we let  $c(Q) = |\{1 \leq j \leq n : a_j \in Q\}|$ . Let further  $s$  be the maximum of  $c(Q)$  for nontrivial cosets  $Q$  (i.e.,  $Q \in G/H \setminus \{H\}$ ). Finally, put  $A_j = \{Q : c(Q) \geq j\}$  and note that  $|A_j| = \varrho_H^j(\mathbf{a})$ . By applying Kneser’s theorem and Lemma 2.8 in the quotient group  $G/H$ , we have

$$\begin{aligned} |\Sigma(\mathbf{a})| &= |H| \cdot \left| \sum_{j=1}^s \Sigma(A_j) \right| \geq |H| \cdot \left( \sum_{j=1}^s |\Sigma(A_j)| - s + 1 \right) \\ &\geq |H| + \frac{1}{64}|H| \cdot \sum_{j \in \mathbb{N}} (\varrho_H^j(\mathbf{a}))^2, \end{aligned}$$

which completes the proof.  $\blacksquare$

Finally, we prove our main theorem for sets.

*Proof of Theorem 1.5.* Let  $A = \{a_1, \dots, a_n\}$  and put  $\mathbf{a} = (a_1, \dots, a_n)$ . By applying Theorem 1.6 we have

$$|\Sigma(A)| = |\Sigma(\mathbf{a})| \geq |H| + \frac{1}{64}|H| \cdot \sum_{j \in \mathbb{N}} (\varrho_H^j(\mathbf{a}))^2.$$

Since  $A$  is a set,  $\varrho_H^j(\mathbf{a}) = 0$  for every  $j > |H|$ . Further  $\sum_{j=1}^{|H|} \varrho_H^j(\mathbf{a}) = |A \setminus H|$ . It follows from this (and the Cauchy–Schwarz inequality) that  $|H| \cdot \sum_{j \in \mathbb{N}} (\varrho_H^j(\mathbf{a}))^2 \geq |A \setminus H|^2$ . Combining this with the above inequality yields the desired bound.  $\blacksquare$

## References

- [1] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. 26 (1994), 140–146.
- [2] P. Erdős and H. Heilbronn, *On the addition of residue classes mod  $p$* , Acta Arith. 9 (1964), 149–159.
- [3] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.
- [4] J. E. Olson, *An addition theorem modulo  $p$* , J. Combin. Theory 5 (1968), 45–52.
- [5] E. Szemerédi and V. H. Vu, *Finite and infinite arithmetic progressions in sumsets*, Ann. of Math. (2) 163 (2006), 1–35.
- [6] V. H. Vu, *Olson’s theorem for cyclic groups*, arXiv:math.NT/0506483.

Department of Mathematics  
Simon Fraser University  
Burnaby, B.C. V5A 1S6, Canada  
E-mail: mdevos@sfu.ca  
goddyn@sfu.ca  
mohar@sfu.ca  
rsamal@sfu.ca

*Received on 2.12.2006  
and in revised form on 16.6.2007*

(5337)