ACTA ARITHMETICA
138.1 (2009)

Asymptotically tight bounds on subset sums

by

Simon Griffiths (Cambridge)

1. Introduction. For a subset A of a finite abelian group G we define

$$\Sigma(A) = \Big\{ \sum_{a\in B} a : B \subset A \Big\},$$

the set of all elements which may be expressed as a sum of elements of A (with repetition not allowed). For a subset $S \subset G$ the *stabiliser* $\mathrm{Stab}(S)$ of S is the set of elements $g \in G$ such that $S+g=S$; the stabiliser is a subgroup of G. We say that S has *trivial stabiliser* if $\mathrm{Stab}(S)=\{0\}$. A recent result of DeVos, Goddyn, Mohar and Šámal [1] shows that if $\Sigma(A)$ has trivial stabiliser then its size is at least quadratic in the size of A.

Theorem 1.1 ([1]). *Let $A \subset G \setminus \{0\}$, and suppose that $\Sigma(A)$ has trivial stabiliser. Then $|\Sigma(A)| \ge |A|^2/64$.*

It is noted in [1] that the above theorem can be proved with $1/64$ replaced by $1/48 - o(1)$, where $o(1)$ denotes a function which converges to 0 as $|A| \to \infty$. Our aim is to improve this further by showing the result holds with the constant replaced by $1/4 - o(1)$. This result is asymptotically best possible as seen by considering $A=\{-n,-(n-1),\ldots,n-1,n\}\subset \mathbb{Z}_N$, with N large.

Theorem 1.2. *Let $A \subset G\setminus\{0\}$, and suppose $\Sigma(A)$ has trivial stabiliser. Then $|\Sigma(A)| \ge (1/4 - o(1))|A|^2$.*

We follow [1] in deducing related results for the case when A has non-trivial stabiliser.

Theorem 1.3. *Let $A \subset G$, and let H be the stabiliser of $\Sigma(A)$. Then*

$$|\Sigma(A)| \ge (1/4 - o(1))|A\setminus H|^2,$$

where $o(1)$ denotes a function which converges to 0 as $|A\setminus H|/|H| \to \infty$.

Remark. As the $o(1)$ term of the above statement converges to zero as $|A\setminus H|/|H| \to \infty$, rather than as $|A \setminus H| \to \infty$, our result is only an

2000 *Mathematics Subject Classification*: 11B75, 11P99.
Key words and phrases: subset sums, complete subsets, abelian groups.

DOI: 10.4064/aa138-1-3

improvement on the result of [1] in the case where $|A \setminus H|$ is large relative to $|H|$.

Erdős and Heilbronn [3] proved that if $A \subset \mathbb{Z}_p$ with p prime, and $|A| \geq 3\sqrt{6p}$, then $\Sigma(A) = \mathbb{Z}_p$—the connection of this result to the current discussion is that this result is proved by giving a quadratic lower bound on $|\Sigma(A)|$ for $A \subset \mathbb{Z}_p$. They conjectured that the constant $3\sqrt{6}$ of their theorem could be replaced by 2; this was proved by Olson [6] and further sharpened by Dias da Silva and Hamidoune [2]. To prove a similar result in $\mathbb{Z}_n$ for n composite, one must put extra conditions on the set A. The following theorem of Vu [7] shows that one way in which this can be done is to demand that A is contained in $\mathbb{Z}_n^*$, the elements coprime to n.

Theorem 1.4 (Vu [7]). *There is a constant c such that every subset $A \subset \mathbb{Z}_n^* \subset \mathbb{Z}_n$ with $|A| \geq c\sqrt{n}$ satisfies $\Sigma(A) = \mathbb{Z}_n$.*

The constant obtained in the original proof of the theorem is quite large. As a corollary of their main theorem DeVos, Goddyn, Mohar and Šámal [1] improved the constant to $c = 8$. We improve this further, by replacing the constant by $2 + o(1)$.

Theorem 1.5. *Let $A \subset \mathbb{Z}_n^* \subset \mathbb{Z}_n$ be such that $\Sigma(A) \neq \mathbb{Z}_n$. Then $|A| \leq (2 + o(1))\sqrt{n}$.*

Remark. This result is asymptotically best possible: consider for example the case $n = p^2$, where p is a large prime, and $A = \{-(p-1), \dots, -1, 1, \dots \dots, p-1\}$. All elements of A are coprime to n, and the element $p(p-1)/2+1$ is not in $\Sigma(A)$ so that $\Sigma(A) \neq \mathbb{Z}_n$, while $|A| = 2p - 2 = (2 - o(1))\sqrt{n}$.

Theorems 1.2 and 1.3 will be deduced from Theorem 1.6 which we state below. The latter says that if $A \subset G \setminus \{0\}$ is such that $\Sigma(A)$ has trivial stabiliser, and has the extra property that $A \cap (-A) = \emptyset$, then $\Sigma(A) \geq (1/2 - o(1))|A|^2$. We now state this result formally.

Let $n_9 = 1$, and for $k \geq 10$ let $n_k = 2^{k^2}$. We also define a sequence of real numbers α_k as follows: $\alpha_9 = 1/64$ and

$$\alpha_k = \min\left\{\frac{6}{5}\,\alpha_{k-1}, \frac{1}{2} - \frac{1}{2^{k-1}}\right\} \quad \text{for } k \geq 10.$$

It is clear that the sequence α_k is increasing and converges to $1/2$ as $k \to \infty$.

Theorem 1.6. *Let $A \subset G\setminus\{0\}$ and let $k \geq 9$. Suppose that $A \cap (-A) = \emptyset$, that $\Sigma(A)$ has trivial stabiliser and that $|A| \geq n_k$. Then $|\Sigma(A)| \geq \alpha_k |A|^2$.*

The layout of the article is as follows. We shall conclude the introduction by introducing definitions and observations that will be used throughout the article. In Section 2 we assume Theorem 1.6 and deduce Theorems 1.2 and 1.3. In Section 3 we establish preliminary lemmas required for the proof of

Theorem 1.6. We prove Theorem 1.6 in Section 4. We then turn to Theorem 1.5, which is proved in Section 5.

Given a set $S \subset G$ and an element $c \in G$ we write $S + c$ for the set $\{s + c : s \in S\}$. We define $\lambda_S(c)$, or simply $\lambda(c)$, to be the number of elements in $S + c$ which are not in S, i.e. $\lambda(c) = |(S + c) \setminus S|$. The following properties of λ are elementary:

(i) $\lambda(0) = 0$,
(ii) $\lambda(-c) = \lambda(c)$ for all $c \in G$,
(iii) $\lambda(b + c) \leq \lambda(b) + \lambda(c)$ for all $b, c \in G$ (subadditivity of λ).

For sets $A_1, \ldots, A_r \subset G$, we define their *sumset* by

$$\sum_{i=1}^{r} A_i = \{a_1 + \cdots + a_r : a_i \in A_i \text{ for } i = 1, \ldots, r\}.$$

We shall also use the notation rA for $\sum_{i=1}^{r} A = \{a_1 + \cdots + a_r : a_i \in A\}$. The key sumset inequality we shall use is *Kneser's addition theorem.*

THEOREM 1.7 (Kneser [5]). *Let $A_1, \ldots, A_r \subset G$ and let H be the stabiliser of $\sum_{i=1}^{r} A_i$. Then*

$$\Big|\sum_{i=1}^{r} A_i\Big| \geq \sum_{i=1}^{r} |A_i| - (r-1)|H|.$$

Let $B \subset A \subset G$. We may express $\Sigma(A)$ as $\Sigma(A) = \Sigma(B) + \Sigma(A \setminus B)$. It is then easily observed that

$$\mathrm{Stab}(\Sigma(B)) \subset \mathrm{Stab}(\Sigma(A)).$$

In particular, if $\Sigma(A)$ has trivial stabiliser then so does $\Sigma(B)$. These observations shall be used throughout.

2. Proofs of Theorems 1.2 and 1.3. In this section we assume Theorem 1.6 and prove Theorems 1.2 and 1.3. Let $(n_k)_{k\geq 9}$ and $(\alpha_k)_{k\geq 9}$ be the sequences defined above, and for a natural number n let $k(n)$ be the largest integer k such that $n \geq 2n_k$. We define

$$f(n) = \alpha_{k(n)}/2 - 1/n^2.$$

It is clear that $f(n) \to 1/4$ as $n \to \infty$, i.e. f is of the form $1/4 - o(1)$.

Proof of Theorem 1.2. Let $A \subset G \setminus \{0\}$ be such that $\Sigma(A)$ has trivial stabiliser, and let $n = |A|$. We prove Theorem 1.2 by showing $|\Sigma(A)| \geq f(n)n^2$. Let $m = \lfloor n/2 \rfloor$. It is possible to partition A into two subsets A_1, A_2 with cardinalities m and $n-m$ respectively, with the property $A_i \cap (-A_i) = \emptyset$ for $i = 1, 2$. Let $k = k(n)$. By the definition of $k(n)$ we have $m \geq n_k$, and so applying Theorem 1.6 to A_1, A_2 individually we obtain $|\Sigma(A_1)| \geq \alpha_k m^2$ and $|\Sigma(A_2)| \geq \alpha_k (n-m)^2$. We have $\Sigma(A) = \Sigma(A_1) + \Sigma(A_2)$, and so applying

Kneser's theorem (and using the fact that $\Sigma(A)$ has trivial stabiliser) we obtain

$$|\Sigma(A)| \geq |\Sigma(A_1)| + |\Sigma(A_2)| - 1 \geq \alpha_k m^2 + \alpha_k (n-m)^2 - 1.$$

We note $m^2 + (n-m)^2 \geq n^2/2$, and so

$$|\Sigma(A)| \geq \alpha_k n^2/2 - 1 = f(n)n^2. \ \blacksquare$$

Let $A \subset G \setminus \{0\}$, and suppose $\Sigma(A)$ has trivial stabiliser, Theorem 1.2 gives $|\Sigma(A)| \geq f(|A|)|A|^2$ for some function $f(n) \to 1/4$ as $n \to \infty$. Of course by setting $f'(n) = f(n) - 1/n^2$, we have

$$(1) \qquad |\Sigma(A)| \geq 1 + f'(|A|)|A|^2$$

for a function $f'(n) \to 1/4$ as $n \to \infty$. Let $m(n) = \lfloor \sqrt{n} \rfloor$ and define

$$f_2(n) = (1 - m(n)^{-1})^2 f'(m(n)).$$

It is clear that $f_2(n) \to 1/4$ as $n \to \infty$, i.e. $f_2(n)$ is of the form $1/4 - o(1)$.

Proof of Theorem 1.3. Let $m(n)$ and $f_2(n)$ be as defined above. Let $A \subset G$, let H be the stabiliser of $\Sigma(A)$, and let $n = |A \setminus H|/|H|$. We prove Theorem 1.3 by demonstrating that

$$|\Sigma(A)| \geq f_2(n)|A \setminus H|^2.$$

We work in G/H; an element Q of G/H is a coset of H. We let $h = |H|$ and define a sequence $A_1, \ldots, A_h$ of subsets of G/H by

$$A_i = \{Q \in G/H : |A \cap Q| \geq i\}.$$

Note that the coset Q appears in exactly $|A \cap Q|$ of the sets A_i; this implies

$$\sum_{i=1}^{h} |A_i| = |A|.$$

Writing A_i' for $A_i \setminus \{H\}$ we have

$$\sum_{i=1}^{h} |A_i'| = |A \setminus H|.$$

The key observation is that $\Sigma(A)$ consists exactly of those elements which lie in cosets in $\Sigma(A_1') + \cdots + \Sigma(A_h')$, so that

$$|\Sigma(A)| = h|\Sigma(A_1') + \cdots + \Sigma(A_h')|.$$

We now put a lower bound on $|\Sigma(A_1') + \cdots + \Sigma(A_h')|$. The sets $A_1', \ldots, A_h'$ are decreasing in size; let j be maximal such that $|A_j'| \geq m(n)$. Now $\sum_{i>j} |A_i'| < hm(n)$, so that

$$\sum_{i=1}^{j} |A_i'| \geq |A \setminus H| - hm(n) \geq h(n - m(n)) \geq hn(1 - m(n)^{-1}).$$

For all $i \le j$ we have $|A'_i| \ge m(n)$, so that from (1), and the fact that f' is increasing, we have

$$|\Sigma(A'_i)| \ge 1 + f'(|A'_i|)|A'_i|^2 \ge 1 + f'(m(n))|A'_i|^2.$$

Since H is the stabiliser of $\Sigma(A)$ it follows that $\Sigma(A'_1) + \cdots + \Sigma(A'_j)$ has trivial stabiliser in G/H, and so by Kneser's theorem, $|\Sigma(A'_1) + \cdots + \Sigma(A'_j)| \ge |\Sigma(A'_1)| + \cdots + |\Sigma(A'_j)| - (j-1)$. Hence

$$|\Sigma(A'_1) + \cdots + \Sigma(A'_j)| \ge \sum_{i=1}^{j} (1 + f'(m(n))|A'_i|^2) - (j-1) \ge f'(m(n)) \sum_{i=1}^{j} |A'_i|^2.$$

We now apply Cauchy–Schwarz to obtain

$$|\Sigma(A'_1) + \cdots + \Sigma(A'_j)| \ge \frac{f'(m(n))}{j} \Big(\sum_{i=1}^{j} |A'_i| \Big)^2 \ge \frac{f'(m(n))}{h} (hn(1 - m(n)^{-1}))^2,$$

and so

$$|\Sigma(A'_1) + \cdots + \Sigma(A'_j)| \ge (1 - m(n)^{-1})^2 f'(m(n)) hn^2.$$

We now simply note that $|\Sigma(A'_1) + \cdots + \Sigma(A'_h)| \ge |\Sigma(A'_1) + \cdots + \Sigma(A'_j)|$ and recall that $|\Sigma(A)| = h|\Sigma(A'_1) + \cdots + \Sigma(A'_h)|$ to obtain

$$|\Sigma(A)| \ge (1 - m(n)^{-1})^2 f'(m(n)) h^2 n^2 = f_2(n)|A \setminus H|^2. \ \blacksquare$$

3. Some preliminary lemmas. In this section we prove the key lemmas which are central to our proof of Theorem 1.6 in Section 4. That proof will work by building up a set $B \subset A$ with $|\Sigma(B)|$ large. During this process we shall inspect the current choice of B and let $S = \Sigma(B)$. We shall then attempt to find an element $c \in C = A \setminus B$ with $\lambda_S(c)$ relatively large, and then add c to B; this leads to a set with size one more than $|B|$, with a significantly larger set of sums. We shall recall results proved previously ([3, Lemma 3.1] and [1, Lemma 3.2]) which enable one to put a lower bound on $\max_{c \in C} \lambda(c)$. More importantly, we strengthen Lemma 3.2 to Lemma 3.4, a result which is best possible, up to an error term; furthermore, for our applications of the lemma the error term is small asymptotically.

For a subset $Q \subset G$, we define

$$\mathrm{def}_Q(S) = \min\{|S \cap Q|, |Q \setminus S|\}.$$

Let $\varrho(d)$ be the number of representations of d as a difference of two elements of S, i.e. $\varrho(d) = |\{(x,y) \in S^2 : x - y = d\}| = |S \cap (S + d)|$. The equality $|(S+d) \cap S| + |(S+d) \setminus S| = |S|$ implies that $\lambda(d) = |S| - \varrho(d)$. A key fact will be that

$$\sum_{d \in G} \varrho(d) = |S|^2;$$

this follows from the fact that each pair of elements (x,y) of S has a unique difference $x-y$, so is counted exactly once by the sum. In the following lemmas, H denotes a finite abelian group. The following two lemmas were originally proved in [3] and [1] respectively; we give proofs so that the reader may become familiar with ideas which we shall use in the more involved proof of Lemma 3.4.

LEMMA 3.1 ([3]). *Let $C,S \subset H$ be such that $\operatorname{def}_H(S) \le |C|/2$. Then*

$$\frac{1}{|C|}\sum_{c\in C}\lambda(c) \ge \frac{\operatorname{def}_H(S)}{2}.$$

In particular, $\lambda(c) \ge \operatorname{def}_H(S)/2$ for some $c \in C$.

Proof. Exchanging S for $H \setminus S$ if required we may assume $\operatorname{def}_H(S) = |S| \le |H|/2$; this is allowed as $\lambda_S(c) = \lambda_{H\setminus S}(c)$ for all $c \in C$. From the facts $\lambda(c) = |S| - \varrho(c)$ and $\sum_{d\in H}\varrho(d) = |S|^2$ we deduce that

$$\sum_{c\in C}\lambda(c) = |C|\,|S| - \sum_{c\in C}\varrho(c) \ge |C|\,|S| - |S|^2.$$

We also have $|C| \ge 2\operatorname{def}_H(S) = 2|S|$, so that $|C|-|S| \ge |C|/2$. It follows that

$$\sum_{c\in C}\lambda(c) \ge |S|(|C|-|S|) \ge \frac{|C|\,|S|}{2} = \frac{|C|\operatorname{def}_H(S)}{2}. \ \blacksquare$$

LEMMA 3.2 ([1]). *Let $C,S \subset H$ be such that $H = \langle C\rangle$ and $\operatorname{def}_H(S) \ge |C|/2$. Then there exists $c \in C$ with $\lambda(c) \ge |C|/8$.*

Sketch proof. Again we may assume $\operatorname{def}_H(S) = |S| \le |H|/2$. We cannot proceed as in the previous proof, because we obtain no information in the case $|C| \le |S|$. Instead we consider not only the elements of C but all elements which can be expressed as a sum of a small number of elements of C; we then obtain the required result from the subadditivity of λ. Suppose for contradiction that $\lambda(c) < |C|/8$ for all $c \in C$, and suppose d may be expressed as a sum of k elements of C. Then by the subadditivity of λ we have $\lambda(d) < k|C|/8$. Using the notation rA for the set $\{a_1+\cdots+a_r : a_i \in A\}$, we see that the set of elements that may be expressed as a sum of at most r elements of C is the set rC^* where $C^* = C \cup \{0\}$. We may assume for all $d \in rC^*$ that $\lambda(d) < r|C|/8$ and so $\varrho(d) > |S| - r|C|/8$. An application of Kneser's theorem (see [1] for details) now shows that for $r = \lfloor 4|S|/|C|\rfloor$ we have $|rC^*| \ge 2|S|$. For this value of r we have $\varrho(d) > |S| - r|C|/8 \ge |S| - |S|/2 = |S|/2$ for all $d \in rC^*$, so that

$$\sum_{d\in rC^*}\varrho(d) > |rC^*|\,\frac{|S|}{2} \ge |S|^2.$$

This contradicts the equality $\sum_{d\in H}\varrho(d) = |S|^2$, and the result is proved. $\blacksquare$

With greater care, and with extra conditions, the result of Lemma 3.2 can be greatly improved: one can find an element $c \in C$ with $\lambda(c)$ almost $|C|$. The extra conditions we need are that $C \cap (-C) = \emptyset$, that $|C|$ is large, and that $\operatorname{def}_H(S)/|C|$ is large. We will again use the subadditivity of λ. In our sketch proof of Lemma 3.2 we used the fact that if $\lambda(c) < \eta$ then for each r we have $\lambda(d) < r\eta$ for all $d \in rC^*$, and so $\varrho(d) > |S| - r\eta$ for all $d \in rC^*$. To obtain an improved result we must use this statement simultaneously for many values of r rather than once for a single value of r. Again it is important to have a lower bound on $|rC^*|$ (although below we take a different set C^*). We first prove Lemma 3.3 which gives an improved lower bound on $|rC^*|$; we will then prove Lemma 3.4 which gives a new bound on $\lambda(c)$. We define $C^* = C \cup (-C) \cup \{0\}$.

LEMMA 3.3. *Let $C \subset H$ be such that $H = \langle C \rangle$, $C \cap (-C) = \emptyset$, $\Sigma(C)$ has trivial stabiliser and $|C| \geq 2^{2k+11}$. Then for all positive integers r, either $rC^* = H$ or*

$$|rC^*| \geq 2\left(1 - \frac{1}{2^{k+2}}\right) r|C|.$$

Proof. Let K be the stabiliser of rC^*. If $C \subset K$ then $K = H$ and $rC^* = H$ and we are done. So we may assume C^* meets at least one non-trivial coset of K. Note that C^* also meets K as $0 \in C^* \cap K$. Let $Q_1, \ldots, Q_p$ be the non-trivial cosets of K meeting C^*. It follows that rC^* is the set of elements of the cosets in $r\{K, Q_1, \ldots, Q_p\}$. By the definition of K the set $r\{K, Q_1, \ldots, Q_p\}$ has trivial stabiliser in H/K so that an application of Kneser's theorem yields

$$|r\{K, Q_1, \ldots, Q_p\}| \geq r(p+1) - (r-1) \geq rp,$$

and so $|rC^*| \geq rp|K|$. So to complete the proof we must show that

$$|K| \geq 2\left(1 - \frac{1}{2^{k+2}}\right) \frac{|C|}{p}.$$

In the case where $|C \cap K| \geq |C|/2^{k+2}$ we use the fact that K contains $\Sigma(C \cap K)$ together with Theorem 1.1 (which we may apply to $C \cap K$, as $\Sigma(C \cap K)$ has trivial stabiliser) to deduce

$$|K| \geq |\Sigma(C \cap K)| \geq \frac{|C \cap K|^2}{64} \geq \frac{1}{64}\frac{|C|^2}{2^{2k+4}} \geq 2|C|$$

(the final inequality follows from $|C| \geq 2^{2k+11}$), and we are done. We may now assume that $|C \cap K| \leq |C|/2^{k+2}$. This implies $|C \setminus K| \geq (1 - 2^{-(k+2)})|C|$ and likewise $|C' \setminus K| \geq (1 - 2^{-(k+2)})|C'|$, where C' denotes $C \cup (-C)$. Alternatively $|C' \cap \bigcup_{i=1}^{p} Q_i| \geq (1 - 2^{-(k+2)})|C'|$, so by the pigeon hole principle some coset Q must have

$$|C' \cap Q| \ge \left(1 - \frac{1}{2^{k+2}}\right)\frac{|C'|}{p} = 2\left(1 - \frac{1}{2^{k+2}}\right)\frac{|C|}{p},$$

and so noting $|K| = |Q| \ge |C' \cap Q|$ we are done. ∎

We now deduce the required strengthening of Lemma 3.2:

LEMMA 3.4. *Let $C \subset H$ be such that $H = \langle C \rangle$, $C \cap (-C) = \emptyset$, $\Sigma(C)$ has trivial stabiliser and $|C| \ge 2^{2k+11}$, and let $S \subset H$ be such that $\mathrm{def}_H(S) \ge 2^{k+1}|C|$. Then there exists $c \in C$ with $\lambda(c) \ge (1 - 2^{1-k})|C|$.*

Proof. For all $d \in H$ we have $\lambda_S(d) = \lambda_{H \setminus S}(d)$, so that exchanging S with $H \setminus S$ if required, we may assume $\mathrm{def}_H(S) = |S| \le |H|/2$. As in previous proofs, we shall proceed by assuming the result fails and from this deduce that $\sum_d \varrho(d) > |S|^2$, a contradiction. On this occasion we must be much more precise in our lower bound on $\sum_d \varrho(d)$. It will be useful to use the fact that $\sum_d \varrho(d) = \int_0^{|S|} |D_t|\, dt$ where $D_t = \{d \in H : \varrho(d) \ge t\}$ (1).

Suppose that every element $c \in C$ has $\lambda(c) < (1 - 2^{1-k})|C|$. This implies $\lambda(c) < (1-2^{1-k})|C|$ for all $c \in C^*$, since $\lambda(0) = 0$ and $\lambda(-c) = \lambda(c)$. By the subadditivity of λ, for all r and all $d \in rC^*$ we have $\lambda(d) < r(1 - 2^{1-k})|C|$, and so $\varrho(d) > |S| - r(1 - 2^{1-k})|C|$. For each $r = 1, \ldots, \lfloor |S|/|C| \rfloor$, we define

$$I_r = (|S| - (r+1)(1 - 2^{1-k})|C|, |S| - r(1 - 2^{1-k})|C|].$$

For $t \in I_r$ we have $t \le |S| - r(1 - 2^{1-k})|C|$ and so $D_t \supset rC^*$, and applying Lemma 3.3 we deduce $|D_t| \ge 2(1 - 2^{-(k+2)})r|C|$.

Note also that for $t \le |S| - (\lfloor |S|/|C| \rfloor + 1)(1 - 2^{1-k})|C|$ we have $D_t \supset \lfloor |S|/|C| \rfloor C^*$, and so $|D_t| \ge 2(1 - 2^{-(k+2)})\lfloor |S|/|C| \rfloor |C|$. Using the fact that $\lfloor |S|/|C| \rfloor \ge (|S| - |C|)/|C| \ge (1 - 2^{-(k+1)})|S|/|C|$ we have

$$|D_t| \ge 2\left(1 - \frac{1}{2^{k+2}}\right)\left\lfloor \frac{|S|}{|C|} \right\rfloor |C| \ge 2\left(1 - \frac{1}{2^{k+2}}\right)\left(1 - \frac{1}{2^{k+1}}\right)|S|$$

for all $t \le |S| - (\lfloor |S|/|C| \rfloor + 1)(1 - 2^{1-k})|C|$. Note that $\lfloor |S|/|C| \rfloor + 1 \le |S|/|C| + 1 \le (1 + 2^{-(k+1)})|S|/|C|$ so that the above bound on $|D_t|$ holds for all $t \le |S| - (1 - 2^{1-k})(1 + 2^{-(k+1)})|S|$ and so certainly for all $t \le 3|S|/2^{k+1}$. We obtain

$$\sum_{d \in H} \varrho(d) = \int_0^{|S|} |D_t|\, dt \ge \sum_{r=1}^{\lfloor |S|/|C| \rfloor} \int_{t \in I_r} |D_t|\, dt + \int_0^{3|S|/2^{k+1}} |D_t|\, dt,$$

(1) We choose this representation, rather than the sum $\sum_{t=1}^{|S|} |D_t|$, as it means we do not have to concern ourselves with integer parts, etc.

and so

$$\sum_{d\in H}\varrho(d) \ge \sum_{r=1}^{\lfloor |S|/|C|\rfloor} 2\Big(1-\frac{1}{2^{k-1}}\Big)\Big(1-\frac{1}{2^{k+2}}\Big)r|C|^2 + \frac{3|S|}{2^{k+1}}\,2\Big(1-\frac{1}{2^{k+2}}\Big)\Big(1-\frac{1}{2^{k+1}}\Big)|S|.$$

Since $\lfloor |S|/|C|\rfloor \ge (1-2^{-(k+1)})|S|/|C|$ we have

$$\sum_{r=1}^{\lfloor |S|/|C|\rfloor} r = (\lfloor |S|/|C|\rfloor)(\lfloor |S|/|C|\rfloor+1)/2 \ge (1-2^{-(k+1)})|S|^2/2|C|^2,$$

and so

$$\sum_{d\in H}\varrho(d) \ge \Big(1-\frac{1}{2^{k+1}}\Big)\Big(1-\frac{1}{2^{k-1}}\Big)\Big(1-\frac{1}{2^{k+2}}\Big)|S|^2 + \frac{3}{2^k}\Big(1-\frac{1}{2^{k+2}}\Big)\Big(1-\frac{1}{2^{k+1}}\Big)|S|^2.$$

However, this quantity is larger than $|S|^2$, a contradiction. ■

4. Proof of Theorem 1.6. Let us recall the sequences $(n_k)_{k\ge 9}$ and $(\alpha_k)_{k\ge 9}$ which appear in the statement of Theorem 1.6. The sequence $(n_k)_{k\ge 9}$ is defined by $n_9 = 1$ and $n_k = 2^{k^2}$ for $k \ge 10$. The only information we shall use about this sequence is that for $k \ge 10$ it satisfies

$$n_k > 2^{5k+15} \quad\text{and}\quad n_k/2^k \ge n_{k-1}. \tag{2}$$

We recall the sequence $(\alpha_k)_{k\ge 9}$ defined by $\alpha_9 = 1/64$ and

$$\alpha_k = \min\Big\{\frac{6}{5}\alpha_{k-1}, \frac{1}{2}-\frac{1}{2^{k-1}}\Big\} \quad \text{for } k \ge 10.$$

Having proved all the necessary preliminary results we now proceed towards our proof of Theorem 1.6. The proof is by induction on k. The case $k = 9$ follows from Theorem 1.1, so we turn to the induction step. We let $k \ge 10$ and suppose the result holds for all smaller values of k. Let A be a set of size n satisfying the conditions of Theorem 1.6; we may assume $n \ge n_k$, else there is nothing to prove. As mentioned previously, we shall build up a set $B \subset A$ with $\Sigma(B)$ large. We define a function $g(t)$ for $t \in \{\lfloor n/2^k\rfloor, \ldots, \lceil n-n/2^k\rceil\}$ by $g(\lfloor n/2^k\rfloor) = 0$ and then inductively by

$$g(t+1) = g(t) + \Big(1-\frac{1}{2^{k-1}}\Big)(n-t).$$

We shall deduce Theorem 1.6 from the following lemma.

LEMMA 4.1. *Let A be as above. Then for all $t \in \{\lfloor n/2^k \rfloor, \ldots, \lceil n - n/2^k \rceil\}$ there is a subset $B \subset A$ of cardinality t with either $|\Sigma(B)| \geq g(t)$ or $|\Sigma(B)| \geq \alpha_k n^2$.*

Theorem 1.6 now follows by taking B of cardinality $\lceil n - n/2^k \rceil$ with either $|\Sigma(B)| \geq g(\lceil n - n/2^k \rceil)$ or $|\Sigma(B)| \geq \alpha_k n^2$. In the latter case we are done immediately as $|\Sigma(A)| \geq |\Sigma(B)|$. In the former case we note that

$$g(\lceil n - n/2^k \rceil) \geq \left(1 - \frac{1}{2^{k-1}}\right) \sum_{t=n/2^k}^{n-n/2^k} n - t = \left(1 - \frac{1}{2^{k-1}}\right) \sum_{t=n/2^k}^{n-n/2^k} t,$$

and we may bound the sum by

$$\sum_{t=n/2^k}^{n-n/2^k} t \geq \left(1 - \frac{1}{2^k}\right)^2 \frac{n^2}{2} - \frac{n^2}{2^{2k+1}} \geq \left(\frac{1}{2} - \frac{1}{2^k}\right) n^2.$$

Hence

$$|\Sigma(A)| \geq \left(1 - \frac{1}{2^{k-1}}\right)\left(\frac{1}{2} - \frac{1}{2^k}\right) n^2 \geq \left(\frac{1}{2} - \frac{1}{2^{k-1}}\right) n^2 \geq \alpha_k n^2,$$

and Theorem 1.6 is proved.

We must now prove Lemma 4.1. We do this by induction on t. The result is trivial for $t = \lfloor n/2^k \rfloor$. If we ever find a set B with $|\Sigma(B)| \geq \alpha_k n^2$ then the induction is trivial from that point on. So for the induction step we let B be a set of size t with $|\Sigma(B)| \geq g(t)$, and set $S = \Sigma(B)$ and $C = A \setminus B$. We will then show either that $|S| \geq \alpha_k n^2$ or that

$$\lambda(c) \geq \left(1 - \frac{1}{2^{k-1}}\right)|C| = \left(1 - \frac{1}{2^{k-1}}\right)(n - t) \quad \text{for some } c \in C. \tag{3}$$

The induction step is then completed by considering $B \cup \{c\}$, as $B \cup \{c\}$ is then a set of size $t + 1$ with $\Sigma(B \cup \{c\}) = S \cup (S + c)$, and so

$$|\Sigma(B \cup \{c\})| \geq |S| + \lambda(c) \geq g(t) + (1 - 2^{1-k})(n - t) = g(t + 1).$$

Let us first note a lower bound on $|S|$ which we shall use during the proof: since $|B| = t \geq \lfloor n/2^k \rfloor \geq n/2^{k+1}$, it is immediate from Theorem 1.1 that

$$|S| \geq \frac{|B|^2}{64} \geq \frac{n^2}{2^{2k+8}} \geq 2^{3k+7} n. \tag{4}$$

Let $H = \langle C \rangle$. As in [1], we must analyse the intersection of S with the cosets of H. We begin with some lower bounds on $|H|$ that we shall use during the proof. The set C is contained in A, so that $C \cap (-C) = \emptyset$ and $0 \notin C$; this also implies that $\Sigma(C)$ has trivial stabiliser; note moreover that

$|C| = n - t \geq n/2^k$. An application of Theorem 1.1 yields

$$|H| \geq |\Sigma(C)| \geq \frac{|C|^2}{64} \geq \frac{n^2}{2^{2k+6}} \geq 2^{3k+9}n,$$

while an application of the induction hypothesis of Theorem 1.6 yields

$$|H| \geq |\Sigma(C)| \geq \alpha_{k-1}|C|^2 \geq \frac{3}{4}\,\frac{\alpha_k n^2}{2^{2k}}.$$

We say that a coset Q of H is *sparse* if $|S \cap Q| \leq 2^{k+1}n$, *very sparse* if $|S \cap Q| \leq |C|/2$, and *dense* if $|Q \setminus S| \leq 2^{k+1}n$. We note that if Q is dense then $|S \cap Q|$ must be fairly large, in particular,

$$(5) \qquad |S \cap Q| \geq |H| - 2^{k+1}n \geq \frac{3}{4}\,\alpha_k n^2/2^{2k} - 2^{k+1}n \geq \alpha_k n^2/2^{2k+1},$$

as $\alpha_k n/2^{2k+2} \geq 2^{k+1}$.

Lemma 4.2. *If any of the following conditions* (i), (ii) *or* (iii) *holds then there is an element $c \in C$ with $\lambda(c) \geq (1 - 2^{1-k})|C|$.*

(i) *There is a coset Q which is neither sparse nor dense.*
(ii) *There are at least 2^{2k+5} cosets that are sparse but not very sparse.*
(iii) *No coset Q is dense.*

Proof. (i) Suppose Q is neither sparse nor dense. Then $\operatorname{def}_Q(S) \geq 2^{k+1}n \geq 2^{k+1}|C|$. An application of Lemma 3.4 to a shift of $S \cap Q$ then shows that there exists $c \in C$ with $\lambda_{S\cap Q}(c) \geq (1 - 2^{1-k})|C|$, and we are done, as $\lambda_S(c) \geq \lambda_{S\cap Q}(c)$.

(ii) Suppose that $Q_1, \ldots, Q_{2^{2k+5}}$ are sparse but not very sparse. For each $i = 1, \ldots, 2^{2k+5}$ let $S_i = S \cap Q_i$, and let $\overline{S} = \bigcup_{i=1}^{2^{2k+5}} S_i$. Then

$$\lambda(c) = \lambda_S(c) \geq \lambda_{\overline{S}}(c) = \sum_{i=1}^{2^{2k+5}} \lambda_{S_i}(c).$$

We write $\lambda_i(c)$ for $\lambda_{S_i}(c)$ and $\overline{\lambda}(c)$ for $\lambda_{\overline{S}}(c)$. We shall show that

$$\overline{\lambda}(c) = \sum_{i=1}^{2^{2k+5}} \lambda_i(c) \geq |C| \quad \text{for some } c \in C.$$

We first note that $|\overline{S}| \geq 2^{2k+5}|C|/2 \geq 2^{2k+4}|C|$. We work as in the proofs of results in Section 3. Suppose for contradiction that $\overline{\lambda}(c) < |C|$ for all $c \in C$. Then by the subadditivity of $\overline{\lambda}$ (which follows from the subadditivity of the λ_i), we have $\overline{\lambda}(d) < 2^{2k+3}|C|$ for all $d \in 2^{2k+3}(C \cup \{0\})$. For each i we let $\varrho_i(d) = |(S_i + d) \cap S_i|$, so that $\varrho_i(d) = |S_i| - \lambda_i(d)$ and $\sum_{d\in G} \varrho_i(d) = |S_i|^2$. We let $\overline{\varrho}(d) = \sum_i \varrho_i(d)$. It follows that $\overline{\varrho}(d) = |\overline{S}| - \overline{\lambda}(d)$, so that

$$\overline{\varrho}(d) > |\overline{S}| - 2^{2k+3}|C| \geq |\overline{S}|/2 \quad \text{for all } d \in 2^{2k+3}(C \cup \{0\});$$

the final inequality follows from the bound $|\overline{S}| \geq 2^{2k+4}|C|$ obtained earlier.

We shall put a lower bound on $|2^{2k+3}(C\cup\{0\})|$, and use it to deduce that $\sum_{d\in G}\varrho_i(d) > |S_i|^2$ for some i, a contradiction. Namely, we show that $|2^{2k+3}(C\cup\{0\})| \ge 2^{k+2}n$. Let K be the stabiliser of $2^{2k+3}(C\cup\{0\})$. If $C\subset K$ then $K=H$ and $|K|=|H|\ge 2^{k+2}n$. Hence we may assume $C\cup\{0\}$ meets a non-trivial coset of K. Let $R_1,\dots,R_p$ be the non-trivial cosets of K which have non-empty intersection with C. Then the elements of $2^{2k+3}(C\cup\{0\})$ are exactly the elements of the cosets in $2^{2k+3}\{K,R_1,\dots,R_p\}$. The definition of K implies that $2^{2k+3}\{K,R_1,\dots,R_p\}$ has trivial stabiliser in H/K, so that an application of Kneser's theorem yields

$$\begin{aligned}|2^{2k+3}(C\cup\{0\})| &= |K|\,|2^{2k+3}\{H,R_1,\dots,R_p\}|\\ &\ge |K|(2^{2k+3}(p+1)-(2^{2k+3}-1)) \ge 2^{2k+3}p|K|.\end{aligned}$$

An application of the pigeon hole principle shows that $|K|\ge |C|/(p+1)\ge |C|/2p$, and it is immediate that $|2^{2k+3}(C\cup\{0\})|\ge 2^{2k+2}|C|\ge 2^{k+2}n$. We now obtain the required contradiction, as

$$\sum_{d\in 2^{2k+3}(C\cup\{0\})}\overline{\varrho}(d) > 2^{k+2}n\,\frac{|\overline{S}|}{2} = 2^{k+1}n|\overline{S}|,$$

and so, since $\overline{\varrho}=\sum_i\varrho_i$ and $|\overline{S}|=\sum_i|S_i|$, we must have, for some i,

$$\sum_{d\in 2^{2k+3}(C\cup\{0\})}\varrho_i(d) > 2^{k+1}n|S_i| \ge |S_i|^2.$$

(iii) Suppose no coset is dense. If moreover some coset is not sparse we are done by (i), so we may assume all cosets are sparse. If there are 2^{2k+5} or more cosets which are sparse but not very sparse, then we are done by (ii). Hence we may assume there are at most 2^{2k+5} cosets which are sparse but not very sparse. Since $|S\cap Q|\le 2^{k+1}n$ for all sparse cosets we may assume at most 2^{3k+6} elements of S are in cosets that are sparse but not very sparse. By (4) we have $|S|\ge 2^{3k+7}n$, so at least $2^{3k+6}n\ge 2n$ elements of S belong to very sparse cosets. Applying Lemma 3.1 to each very sparse coset we deduce that

$$\sum_Q\sum_{c\in C}\lambda_{S\cap Q}(c) \ge \sum_Q\frac{|C|}{2}\operatorname{def}_Q(S) = \frac{|C|}{2}\sum_Q|S\cap Q| \ge |C|n$$

where the summation is taken over very sparse cosets Q. Changing the order of summation and averaging, we find $c\in C$ with $\sum_Q\lambda_{S\cap Q}(c)\ge n$, and we are done, as $\lambda(c)=\lambda_S(c)\ge\sum_Q\lambda_{S\cap Q}(c)\ge n$. ∎

A very simple addition theorem in finite abelian groups is that if $A,B\subset G$ satisfy $|A|+|B|>|G|$ then $A+B=G$. Let $\mathcal{D}$ denote the set of dense cosets,

$$\mathcal{D}=\{Q\in G/H : Q \text{ is dense}\}\subset G/H,$$

and $\overline{\mathcal{D}}$ the set of all elements of dense cosets,

$$\overline{\mathcal{D}} = \bigcup_{Q\in\mathcal{D}} Q \subset G.$$

Claim. *S is not contained in $\overline{\mathcal{D}}$.*

Proof. Theorem 1.1 implies that $|\Sigma(C)| \geq |C|^2/64 \geq n^2/2^{2k+6} > 2^{k+1}n$. Let Q be a dense coset. Then $|S\cap Q| \geq |H| - 2^{k+1}n$, and so $|\Sigma(C)| + |S\cap Q| > |H|$. By considering an appropriate shift of $S \cap Q$ we obtain (from the simple addition theorem stated above) that $Q \subset \Sigma(C) + (S \cap Q) \subset \Sigma(A)$. Suppose the Claim is false. Then every coset Q meeting S is dense. Then it follows that $\Sigma(A)$ is a union of cosets of H and so has non-trivial stabiliser, a contradiction. ∎

If either of the conditions (i) or (iii) of Lemma 4.2 holds then we are done. Using this together with the above Claim, we note that we may proceed with the following assumptions:

I. Every coset is either sparse or dense.
II. There is a dense coset.
III. S is not contained in $\overline{\mathcal{D}}$.

From this information we shall deduce that $|S| \geq \alpha_k n^2$, completing the proof. To prove this it suffices by (5) to show that there are at least 2^{2k+1} dense cosets, i.e. show $|\mathcal{D}| \geq 2^{2k+1}$. We begin by recalling a Claim from [1].

Claim ([1]). *If Q is dense and $b \in B$ then one of the cosets $Q + b$ or $Q - b$ is dense.*

Proof. If $b \in H$ then this is trivial, so suppose $b \notin H$. Let S_- be the set of elements in $S \cap Q$ which may be represented as a sum of elements of $B\setminus\{b\}$, and let S_+ be the set of elements in $S\cap Q$ which may be represented as b plus a sum of elements of $B \setminus \{b\}$. We note that $S \cap (Q + b) \supset S_- + b$ so that $|S\cap(Q+b)| \geq |S_-|$, and $S\cap(Q-b) \supset S_+ - b$ so that $|S\cap(Q-b)| \geq |S_+|$. As $|S_-| + |S_+| \geq |H| - 2^{k+1}n > 2^{k+1}n$ we deduce that one of these sets and hence one of the sets $S \cap (Q + b), S \cap (Q - b)$ has cardinality greater than $2^{k+1}n$. The claim is then proved, as we may assume all cosets are either sparse or dense. ∎

Fix $Q_0 \in \mathcal{D}$ and let K be a maximal subgroup of G/H for the property that $Q_0 + K \subset \mathcal{D}$. Let us also define a subgroup $\overline{K}$ of G by

$$\overline{K} = \bigcup_{Q\in K} Q.$$

Lemma 4.3. *If $|B \cap \overline{K}| \geq 9|B|/10$ then $|S| \geq \alpha_k n^2$.*

Proof. We know that B is not contained in $\overline{K}$, for if it were then we would have $S \subset \overline{K} \subset \overline{\mathcal{D}}$, contradicting III. Let $b \in B \setminus \overline{K}$. From the above

Claim we know that for each $Q \in Q_0 + K$ either $Q + b$ or $Q - b$ is dense. This implies that there must be at least $|K|/2$ dense cosets outside of $Q_0 + K$, so that the total number of dense cosets is at least $3|K|/2$.

Let us now estimate the size of $\overline{K}$. Since $C \subset \overline{K}$ and $|B \cap \overline{K}| \geq 9|B|/10$ we deduce that $|A \cap \overline{K}| \geq 9|A|/10$. Since $A' = A \cap \overline{K}$ is a subset of A, we infer that $\Sigma(A')$ has trivial stabiliser, so that by applying the induction hypothesis of Theorem 1.6 to A' we obtain $|\Sigma(A')| \geq 81\alpha_{k-1}n^2/100$, and since $\Sigma(A') \subset \overline{K}$ it follows that $|\overline{K}| \geq 81\alpha_{k-1}n^2/100$.

Since $|\overline{K}| = |K|\,|H|$, we deduce that $|H| \geq 81\alpha_{k-1}n^2/100|K|$. We may assume that $|K| \leq 2^{2k+1}$, since we are done if there are at least 2^{2k+1} dense cosets. Let Q be a dense coset. Then

$$|S \cap Q| \geq |H| - 2^{k+1}n \geq \frac{81\alpha_{k-1}n^2}{100|K|} - 2^{k+1}n \geq \frac{4\alpha_{k-1}n^2}{5|K|}$$

where the final inequality follows from $\alpha_{k-1}n/100|K| \geq n/2^{2k+15} \geq 2^{k+1}$. Since there are at least $3|K|/2$ dense cosets Q we have

$$|S| \geq \frac{3|K|}{2}\,\frac{4\alpha_{k-1}n^2}{5|K|} = \frac{6\alpha_{k-1}n^2}{5} \geq \alpha_k n^2. \ \blacksquare$$

Hence we may assume that

$$|B \setminus \overline{K}| \geq \frac{|B|}{10} \geq \frac{n}{2^{k+4}} \geq 2^{4k+3}. \tag{6}$$

Suppose that $B \setminus \overline{K}$ meets at least 2^{2k+2} distinct cosets of H. Then it is possible to find cosets $Q_1, \ldots, Q_{2^{2k+1}}$ not in $\overline{K}$ which meet B and have the property that $Q_i \neq -Q_j$ for each i, j. The Claim shows that for each $i = 1, \ldots, 2^{2k+1}$ one of the cosets $Q_0 + Q_i$ or $Q_0 - Q_i$ is dense. Since we find a different dense coset for each $i = 1, \ldots, 2^{2k+1}$, we find at least 2^{2k+1} dense cosets, and we are done.

Hence we may assume that B meets at most 2^{2k+2} cosets Q of H with Q not in $\overline{K}$. It follows from this, and (6), that for one such coset Q we have $|B \cap Q| \geq 2^{2k+1}$. We write $\mathrm{order}(Q)$ for the order of Q in G/H. The following lemma will allow us to deduce that $\mathrm{order}(Q) \geq 2^{2k+1}$.

Lemma 4.4. *Let Q be a coset with $|B \cap Q| \geq \mathrm{order}(Q)$ and $\mathrm{order}(Q) \leq 2^{2k+1}$, and let R be a dense coset. Then $R + Q$ is dense.*

Proof. Let $p = \mathrm{order}(Q) \leq 2^{2k+1}$ and let $b_1, \ldots, b_{p-1}$ be $p - 1$ elements of $B \cap Q$. Since R is dense we have $|S \cap R| \geq |H| - 2^{k+1}n$. We partition $S \cap R$ into

$$S^+ = ((b_1 + \cdots + b_{p-1}) + \Sigma(B \setminus \{b_1, \ldots, b_{p-1}\})) \cap R,$$

the elements which can be expressed as a sum of elements of B in such a way that all the elements $b_1, \ldots, b_{p-1}$ are included, and S^-, the elements of $S \cap R$ which can be expressed as a sum of elements of B in which not all of $b_1, \dots, b_{p-1}$ are used. We note that $-(b_1 + \dots + b_{p-1}) \in Q$, so we have $S \cap (R+Q) \supset S^+ - (b_1 + \dots + b_{p-1})$ and hence $|S \cap (R+Q)| \geq |S^+|$.

We will also be able to relate $|S \cap (R+Q)|$ to $|S^-|$. Consider the bipartite graph with vertex sets S^- and $S \cap (R+Q)$ in which a vertex $x \in S^-$ is joined to $y \in S \cap (R+Q)$ if $y - x = b_i$ for some $i = 1, \dots, p-1$. The vertices of S^- all have positive degree, while the degree of vertices in $S \cap (R+Q)$ is certainly at most $p-1$. It follows that $|S \cap (R+Q)| \geq |S^-|/(p-1)$.

We now have

$$2|S \cap (R+Q)| \geq |S^+| + |S^-|/p \geq (|S^+| + |S^-|)/p \geq |S \cap R|/p.$$

Recall that R is dense so that by (5) we have $|S \cap R| \geq \alpha_k n^2/2^{2k+1} \geq n^2/2^{2k+7}$. Using this together with the fact that $p \leq 2^{2k+1}$ we obtain

$$|S \cap (R+Q)| \geq \frac{|S \cap R|}{2p} \geq \frac{n^2}{2^{4k+9}} > 2^{k+1} n,$$

the final inequality following from the bound $n \geq n_k \geq 2^{5k+10}$. This shows us that $R+Q$ is not sparse; since we are assuming that all cosets are either sparse or dense it follows that $R+Q$ is dense. ∎

So if it were the case that $\operatorname{order}(Q) \leq 2^{2k+1}$ then the above lemma would show that Q is in the stabiliser of $\mathcal{D}$, but now the subgroup $\langle K \cup \{Q\} \rangle$ contradicts the maximality of K. Hence we may assume $\operatorname{order}(Q) \geq 2^{2k+1}$. Our proof of the theorem is completed with this final lemma.

LEMMA 4.5. *Suppose there is a coset Q with $|B \cap Q| \geq 2^{2k+1}$ and* $\operatorname{order}(Q) \geq 2^{2k+1}$. *Then there are at least 2^{2k+1} dense cosets.*

Proof. We know there is at least one dense coset R. Consider the cosets $R - iQ$ for positive integers i. If they are all dense then we have found $\operatorname{order}(Q) \geq 2^{2k+1}$ dense cosets and we are done. Hence we may assume there is some non-negative integer i such that $R - iQ$ is dense, but $R - (i+1)Q$ is not. Set $Q_0 = R - (i+1)Q$ and $Q_1 = R - iQ$, and for $j = 2, \dots, 2^{2k+1}$ let $Q_j = Q_1 + (j-1)Q$. We show that Q_j is dense for each $j = 2, \dots, 2^{2k+1}$. Let $b_1, \dots, b_{2^{2k+1}}$ be 2^{2k+1} elements of $B \cap Q$. We partition $S \cap Q_1$ into $S^- = \Sigma(B \setminus \{b_1, \dots, b_{2^{2k+1}}\})$, the set of elements which may be expressed as a sum of elements of B without using any of the elements $b_1, \dots, b_{2^{2k+1}}$, and S^+, the elements of $S \cap Q_1$ which can be expressed as a sum of elements of B in which at least one of $b_1, \dots, b_{2^{2k+1}}$ is used.

We can relate the size of S^+ to the size of $S \cap Q_0$; this will allow us to bound the size of S^+. Consider the bipartite graph with vertex sets S^+ and $S \cap Q_0$ in which a vertex $x \in S^+$ is joined to $y \in S \cap Q_0$ if $x - y = b_i$ for some $i = 1, \dots, 2^{2k+1}$. The vertices of S^+ all have positive degree, while the degree of vertices in $S \cap Q_0$ is certainly at most 2^{2k+1}. It follows that $|S^+| \leq 2^{2k+1}|S \cap Q_0|$. However, Q_0 is not dense. Since we are assuming all cosets are either sparse or dense we may assume Q_0 is sparse, so that $|S\cap Q_0|\le 2^{k+1}n$. It follows that $|S^+|\le 2^{3k+2}n$. As Q_1 is dense we have a lower bound on $|S\cap Q_1|$ from (5). Noting that $S\cap Q_1=S^+\cup S^-$ we obtain

$$|S^-|\ge|S\cap Q_1|-|S^+|\ge\frac{\alpha_k n^2}{2^{2k+1}}-2^{3k+2}n\ge\frac{n^2}{2^{2k+7}}-2^{3k+2}n>2^{k+1}n,$$

the final inequality following from the fact $n\ge n_k>2^{5k+10}$. Now for each $i=2,\dots,2^{2k+1}$ we have $S\cap Q_i\supset S^-+b_1+\dots+b_{i-1}$, and so $|S\cap Q_i|>2^{k+1}n$. This implies that these cosets are not sparse, so they are dense. ∎

5. Proof of Theorem 1.5. In this section we prove Theorem 1.5. The first half of the section is devoted to proving Lemma 5.2, which is the appropriate variant of Lemma 3.4 for the new setting of $A\subset\mathbb{Z}_n^*\subset\mathbb{Z}_n$. We then turn in the second half of the section to applying this, and previous lemmas, to prove the required result. As in Section 3, it is important to find lower bounds on the cardinalities of the sets rC^*, where $C^*=C\cup(-C)\cup\{0\}$.

LEMMA 5.1. *Let $C\subset H$ be such that $H=\langle\{c\}\rangle$ for each $c\in C$ and $C\cap(-C)=\emptyset$. Then for all positive integers r we have either $rC^*=H$ or*

$$|rC^*|\ge 2r|C|.$$

Proof. Let K be the stabiliser of rC^*. If there is an element c in $C\cap K$ then $K=H$ and $rC^*=H$, and we are done. So we may assume $C^*\cap K=\{0\}$. Let $Q_1,\dots,Q_p$ be the non-trivial cosets of K meeting C^*. It follows that rC^* is the set of all elements of the cosets in $r\{K,Q_1,\dots,Q_p\}$. By the definition of K the set $r\{K,Q_1,\dots,Q_p\}$ has trivial stabiliser in H/K so that an application of Kneser's theorem yields

$$|r\{K,Q_1,\dots,Q_p\}|\ge r(p+1)-(r-1)\ge rp,$$

and so $|rC^*|\ge rp|K|$. So to complete the proof we must show that

$$|K|\ge 2|C|/p.$$

However, the set $C'=C\cup(-C)$ has size $2|C|$ and is contained in $\bigcup_{i=1}^p Q_i$, so that we may deduce from the pigeon hole principle that for some coset Q we have

$$|C'\cap Q|\ge|C'|/p=2|C|/p,$$

and so noting $|K|=|Q|\ge|C'\cap Q|$ we are done. ∎

We now deduce the key result we need for finding elements $c\in C$ with large $\lambda(c)$.

LEMMA 5.2. *Let $C\subset H$ be such that $H=\langle\{c\}\rangle$ for each $c\in C$ and $C\cap(-C)=\emptyset$. Let $\gamma>4$ and let $S\subset H$ be such that $\operatorname{def}_H(S)\ge\gamma|C|$. Then there exists $c\in C$ with $\lambda(c)\ge(1-4\gamma^{-1})|C|$.*

Proof. For all $d \in H$ we have $\lambda_S(d) = \lambda_{H\setminus S}(d)$, so that exchanging S with $H \setminus S$ if required, we may assume $\operatorname{def}_H(S) = |S| \le |H|/2$. As in the proofs of Section 3, we shall proceed by assuming the result fails and from this deduce that $\sum_d \varrho(d) > |S|^2$, a contradiction. It will be useful to use the fact that $\sum_d \varrho(d) = \int_0^{|S|} |D_t|\,dt$ where $D_t = \{d \in H : \varrho(d) \ge t\}$.

Suppose that every element $c \in C$ has $\lambda(c) < (1-4\gamma^{-1})|C|$. This implies $\lambda(c) < (1-4\gamma^{-1})|C|$ for all $c \in C^*$, since $\lambda(0) = 0$ and $\lambda(-c) = \lambda(c)$. Hence by the subadditivity of λ, for all r and $d \in rC^*$ we have $\lambda(d) < r(1-4\gamma^{-1})|C|$, and so $\varrho(d) > |S| - r(1-4\gamma^{-1})|C|$.

For each $r = 1, \ldots, \lfloor |S|/|C| \rfloor$, we define

$$I_r = (|S| - (r+1)(1-4\gamma^{-1})|C|, |S| - r(1-4\gamma^{-1})|C|].$$

For $t \in I_r$ we have $t \le |S| - r(1-4\gamma^{-1})|C|$, and so $D_t \supset rC^*$. Applying Lemma 5.1 we deduce $|D_t| \ge 2r|C|$.

Note also that for $t \le |S| - (\lfloor |S|/|C| \rfloor + 1)(1-4\gamma^{-1})|C|$ we have $D_t \supset \lfloor |S|/|C| \rfloor C^*$ and so $|D_t| \ge 2\lfloor |S|/|C| \rfloor |C|$. Therefore using the fact that $\lfloor |S|/|C| \rfloor \ge (|S| - |C|)/|C| \ge (1-\gamma^{-1})|S|/|C|$ we have

$$|D_t| \ge 2\left\lfloor \frac{|S|}{|C|} \right\rfloor |C| \ge 2(1-\gamma^{-1})|S|$$

for all $t \le |S| - (\lfloor |S|/|C| \rfloor + 1)(1-4\gamma^{-1})|C|$. Note that $\lfloor |S|/|C| \rfloor + 1 \le |S|/|C| + 1 \le (1+\gamma^{-1})|S|/|C|$, so that the above bound on $|D_t|$ holds for all t satisfying $t \le |S| - (1-4\gamma^{-1})(1+\gamma^{-1})|S|$, and so certainly for all $t \le 3\gamma^{-1}|S|$. We obtain

$$\sum_{d\in H} \varrho(d) = \int_0^{|S|} |D_t|\,dt \ge \sum_{r=1}^{\lfloor |S|/|C| \rfloor} \int_{t\in I_r} |D_t|\,dt + \int_0^{3\gamma^{-1}|S|} |D_t|\,dt,$$

and so

$$\sum_{d\in H} \varrho(d) \ge \sum_{r=1}^{\lfloor |S|/|C| \rfloor} 2(1-4\gamma^{-1})r|C|^2 + 6\gamma^{-1}(1-\gamma^{-1})|S|^2.$$

Since $\lfloor |S|/|C| \rfloor \ge (1-\gamma^{-1})|S|/|C|$ we have

$$\sum_{r=1}^{\lfloor |S|/|C| \rfloor} r = (\lfloor |S|/|C| \rfloor)(\lfloor |S|/|C| \rfloor + 1)/2 \ge (1-\gamma^{-1})|S|^2/2|C|^2,$$

and so

$$\sum_{d\in H} \varrho(d) \ge (1-\gamma^{-1})(1-4\gamma^{-1})|S|^2 + 6\gamma^{-1}(1-\gamma^{-1})|S|^2.$$

However, this quantity is larger than $|S|^2$, a contradiction. ∎

Proof of Theorem 1.5. Since the required result is asymptotic it suffices to prove it for $n \geq n_0$, for some n_0. Let n_0 be chosen such that $\sqrt{n} \geq 160n^{1/4}$ and $\log_{3/2}(n) \leq n^{1/4}$ for all $n \geq n_0$. For $n \geq n_0$ we define $f_4(n) = 1+15n^{-1/4}$ and $f_3(n) = 2(f_4(n) + n^{-1/2}) = 2 + 30n^{-1/4} + 2n^{-1/2}$. It is clear that $f_3(n)$ is of the form $2 + o(1)$. To prove Theorem 1.5 we show that a set $A \subset \mathbb{Z}_n^* \subset \mathbb{Z}_n$ with $|A| \geq f_3(n)\sqrt{n}$ must have $\Sigma(A) = \mathbb{Z}_n$. Let us note that if $|A| \geq f_3(n)\sqrt{n} = 2f_4(n)\sqrt{n} + 2$ then it is possible to partition A into subsets A_1 and A_2, each with cardinality at least $f_4(n)\sqrt{n}$ and satisfying $A_i \cap (-A_i) = \emptyset$ for $i = 1, 2$. Our proof will work by showing that

$$|\Sigma(A_i)| > n/2 \quad \text{for } i = 1, 2.$$

We are then done, as $\Sigma(A) \supset \Sigma(A_1) + \Sigma(A_2)$, and $S + T \supset \mathbb{Z}_n$ whenever $S, T \subset \mathbb{Z}_n$ are such that $|S| + |T| > n$.

During the proof we will rely essentially on the results we have proved which give us an element $c \in C$ with large value of $\lambda(c)$. We now recall the three bounds we shall need (we write $\lambda(S, C)$ for the maximum value of $\lambda_S(c)$ over elements $c \in C$):

$$\begin{aligned} \lambda(S,C) &\geq |S|/2 \quad &&\text{for } \operatorname{def}_{\mathbb{Z}_n}(S) \leq |C|/2, \\ \lambda(S,C) &\geq |C|/8 \quad &&\text{for } \operatorname{def}_{\mathbb{Z}_n}(S) \geq |C|/2, \\ \lambda(S,C) &\geq (1 - 4n^{-1/4})|C| \quad &&\text{for } \operatorname{def}_{\mathbb{Z}_n}(S) \geq n^{1/4}|C|. \end{aligned}$$

These bounds are taken from Lemmas 3.1, 3.2 and 5.2 respectively. It is valid to apply these lemmas for sets $C \subset A_i$, $i = 1, 2$, because this certainly implies that $C \cap (-C) = \emptyset$ and $C \subset \mathbb{Z}_n^*$, and so $\mathbb{Z}_n$ is generated by each element $c \in C$.

Fix $i \in \{1, 2\}$. We show that $|\Sigma(A_i)| > n/2$. We do this by building up a set $B \subset A_i$ with $\Sigma(B)$ large. We define

$$g(t) = \max_{B \subset A_i,\, |B|=t} |\Sigma(B)|.$$

Given $B \subset A_i$ of cardinality t and such that $|\Sigma(B)| = g(t)$, we let $S = \Sigma(B)$, $C = A_i \setminus B$, and $\lambda(S, C) = \max_{c \in C} \lambda_S(c)$. By considering $B \cup \{c\}$, a set of cardinality $t + 1$, we deduce that

$$g(t + 1) \geq g(t) + \lambda(S, C).$$

Note that we may assume at all times that $|S| \leq n/2$, so that $\operatorname{def}_{\mathbb{Z}_n}(S) = |S|$, for we are immediately done if $|S| > n/2$; so we use the three inequalities above concerning $\lambda(S, C)$, with $|S|$ in place of $\operatorname{def}_{\mathbb{Z}_n}(S)$.

LEMMA 5.3. *Let $n \geq n_0$. Let $A \subset \mathbb{Z}_n^* \subset \mathbb{Z}_n$ with $A \cap (-A) = \emptyset$ and $|A| \geq \sqrt{n} + 15n^{1/4}$. Then $|\Sigma(A)| > n/2$.*

Proof. It suffices to prove this when the size of A is the integer above $\sqrt{n} + 15n^{1/4}$, so we may assume $|A| \leq 9\sqrt{n}/8$. We put lower bounds on $g(t)$

using the bounds on $\lambda(S,C)$ given above. We work in three main stages, corresponding to the three different lower bounds we have on $\lambda(S,C)$.

STAGE 1. Let t_1 be the least t such that $g(t) \geq (|A|-t)/2$. We note that $g(1)=2$. Let $2 \leq t < t_1$, let B be a set of size t with $S=\Sigma(B)$ satisfying $|S|=g(t)$, and let $C=A\setminus B$. We have $|S| \leq (|A|-t)/2 = |C|/2$. From our bounds on λ we have $\lambda(S,C) \geq |S|/2$, and so $g(t+1) \geq 3g(t)/2$, so that $g(t) \geq 2(3/2)^{t-1} \geq (3/2)^t$. It follows that $t_1 \leq \log_{3/2}(|A|) \leq \log_{3/2}(n) \leq n^{1/4}$.

STAGE 2. Let t_2 be the least t such that $g(t) \geq 9n^{3/4}/8$. Let $t_1 \leq t \leq \min\{t_1+9n^{1/4}, t_2\}$, let B be a set of size t with $S=\Sigma(B)$ satisfying $|S|=g(t)$, and let $C=A\setminus B$. We have $|S| \geq |C|/2$ and $|C|=|A|-t \geq \sqrt{n}$, so that $\lambda(S,C) \geq |C|/8 \geq \sqrt{n}/8$, and so $g(t+1) \geq g(t)+\sqrt{n}/8$. Hence $g(t) \geq g(t_1)+(t-t_1)\sqrt{n}/8$, and so certainly $t_2 \leq t_1+9n^{1/4} \leq 10n^{1/4}$.

STAGE 3. Let t_3 be the least t such that $g(t) > n/2$. Let $t_2 \leq t < t_3$, let B be a set of size t with $S=\Sigma(B)$ satisfying $|S|=g(t)$, and let $C=A\setminus B$. We have $|S|=g(t) \geq g(t_2) \geq 9n^{3/4}/8 \geq n^{1/4}|C|$ (certainly $|C| \leq |A| \leq 9\sqrt{n}/8$), so that

$$\lambda(S,C) \geq (1-4n^{-1/4})|C| = (1-4n^{1/4})(|A|-t),$$

which gives $g(t+1) \geq g(t)+(1-4n^{-1/4})(|A|-t)$ for $t_2 \leq t < t_3$. We now use these to calculate $g(t)$ in this range,

$$g(t) \geq g(t_2)+(1-4n^{-1/4})\sum_{t'=t_2}^{t}(|A|-t') = g(t_2)+(1-4n^{-1/4})\sum_{t'=|A|-t}^{|A|-t_2} t'.$$

Using the bounds $\sum_{t'=r}^{s} t' \geq (s^2-r^2)/2 = (s+r)(s-r)/2 \geq s(s-r)/2$ and $|A|-t_2 \geq \sqrt{n}+5n^{1/4}$ we obtain

$$\begin{aligned} g(t) &\geq (1-4n^{-1/4})\frac{(|A|-t_2)(t-t_2)}{2} \geq (1-4n^{-1/4})\frac{(\sqrt{n}+5n^{1/4})(t-t_2)}{2} \\ &> \frac{\sqrt{n}}{2}(t-t_2). \end{aligned}$$

It is then immediate that $t_3-t_2 \leq \sqrt{n}$, whence $t_3 \leq \sqrt{n}+10n^{1/4}$. Of course we now have $|\Sigma(A)| \geq g(t_3) > n/2$. ∎

A more delicate version of the above proof, in which there are $\log n$ stages (an initial stage as Stage 1 above, followed by $\log n$ stages in which $g(t)$ doubles) allows one to deduce Lemma 5.3 with the condition on $|A|$ weakened to $|A| \geq \sqrt{n}+10\log_2 n$. This then implies that any subset $A \subset \mathbb{Z}_n^* \subset \mathbb{Z}_n$ with $|A| \geq 2\sqrt{n}+20\log_2 n+2$ must have $\Sigma(A)=\mathbb{Z}_n$.

NOTE. Theorem 1.5 has been proved independently by Hamidoune, Lladó and Serra [4]; furthermore, their error term is smaller, being simply an additive constant.

References

[1] M. DeVos, L. Goddyn, B. Mohar and R. Šámal, *A quadratic lower bound for subset sums*, Acta Arith. 129 (2007), 187–195.

[2] 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.

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

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

[5] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.

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

[7] V. H. Vu, *Some new results on subset sums*, J. Number Theory 124 (2007), 229–233.

Churchill College
Cambridge
CB3 0DS, UK
E-mail: sg332@cam.ac.uk

Received on 31.5.2008 (5727)