[8] M. Pinsker, On the complexity of a concentrator. *7th International Teletraffic Conference, Stockholm*, 1973, 316/1–318/4
[9] N. Pippenger, Superconcentrators, *SIAM Journal of Computing*, **6** (1977), 298–304
[10] P. Sarnak, Personal communication, 1988
[11] A. Schrijver, A short proof of Minc's conjecture, *J. Combin. Theory*, **A25** (1978), 80–1
[12] K. Zarankiewicz, *Colloq. Maths.*, **2** (1951), Problem 101 on page 301

Sum-free subsets

N. Alon* and D. J. Kleitman*

Abstract

A subset A in an Abelian group is called *sum-free* if $(A+A)\cap A = \emptyset$. We prove that for every finite Abelian group G, every set B of n non-zero elements of G contains a sum-free subset A of cardinality $|A| > \frac{2}{7}n$. The constant $\frac{2}{7}$ is best possible.

1 Introduction

A subset A of an Abelian group is called *sum-free* if $(A+A)\cap A = \emptyset$, i.e., if there are no (not necessarily distinct) $a,b,c \in A$ such that $a+b = c$. There is a considerable amount of results concerning sum-free subsets of Abelian groups. Many of these appear in the survey article [14] and some of its references. Our research here was motivated by a question we heard from Y. Caro, who asked if there is a positive constant c, such that any set B of n positive integers contains a sum-free subset A of cardinality

$$A > cn.$$

We have found a very simple proof of the following statement, which answers this question. Not surprisingly we learned later that almost the same result, without the strict inequality and with a rather similar proof, had been proved by Erdős more than twenty years ago (see [7]).

Proposition 1.1 *Any set B of n non-zero integers contains a sum-free subset A of cardinality*

* Work supported in part by a grant from the United States–Israel Binational Science Foundation and by a Bergman Memorial grant.

$$|A| > \tfrac{1}{3}n.$$

We can show that the constant $\frac{1}{3}$ cannot be replaced by $\frac{12}{29}$ (or any bigger constant), improving the result in [7], which asserts that the constant $\frac{1}{3}$ cannot be replaced by $\frac{3}{7}$. Although this is a very modest improvement, we believe it is worth mentioning, as it suggests that $\frac{1}{3}$ may actually be the best possible constant.

For a subset B of an Abelian group, let $s(B)$ denote the maximum cardinality of a sum-free subset of B. Similarly, for a sequence $A = (a_1, a_2, \ldots, a_n)$ of (not necessarily distinct) elements of an Abelian group, let $s(A)$ denote the maximum number of elements in a sum-free subsequence $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ of A, i.e., the maximum k such that there are $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$, where the set $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ is a sum-free set. In these notations, Proposition 1.1 is simply the statement that for every set B of non-zero integers, $s(B) > \frac{1}{3}|B|$. Its proof applies to sequences as well, and establishes the following result (which is clearly stronger than Proposition 1.1).

Proposition 1.2 *For any sequence B of non-zero integers, $s(B) > \frac{1}{3}|B|$.*

On he other hand, we construct sequences B with $s(B) < \frac{11}{28}|B|$. Moreover, we show that, for every sequence A, there is a sequence B such that

$$\frac{s(B)}{|B|} \leqslant \frac{s(A)}{|A|} - \frac{1}{(|A| - s(A) + 1)!\,\mathrm{e}|A|}.$$

Therefore, the infimum of the ratio $s(B)/|B|$, as B ranges over all sequences of integers, is not attained.

Babai and Sós [4] raised the problem of estimating the maximum size of the sum-free subsets of n elements of general groups. Our main result in this paper is the following theorem, which settles this problem for finite Abelian groups.

Theorem 1.3 *For any finite Abelian group G, every set B of non-zero elements of G satisfies $s(B) > \frac{2}{7}|B|$. The constant $\frac{2}{7}$ is best possible. Similarly, every sequence A of non-zero elements of G satisfies $s(A) > \frac{2}{7}|A|$, and the constant $\frac{2}{7}$ is optimal.*

Our paper is organized as follows. In Section 2 we present simple proofs of Propositions 1.1 and 1.2 which slightly improve Erdős' result. We construct sets B and sequences A of non-zero integers with relatively small values of $s(B)/|B|$ and $s(A)/|A|$.

In Section 3 we consider general finite Abelian groups and prove Theorem 1.3. Finally, Section 4 includes several extensions and consequences of the above results and a few open problems.

2 Sum-free subsets of integers

We first prove Proposition 1.2 (which implies Proposition 1.1). Let $B = (b_1, b_2, \ldots, b_n)$ be a sequence of n non-zero integers. Let $p = 3k+2$ be a prime, which satisfies

$$p > 2 \max_{1 \leqslant i \leqslant n} |b_i|,$$

and put $C = \{k+1, k+2, \ldots, 2k+1\}$. Observe that C is a sum-free subset of the cyclic group Z_p and that

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \tfrac{1}{3}.$$

Let us choose at random an integer x $(1 \leqslant x < p)$ according to a uniform distribution on $\{1, 2, \ldots, p-1\}$, and define $d_1, \ldots, d_n$ by $d_i \equiv xb_i \pmod{p}$ $(0 \leqslant d_i < p)$. Trivially, for every fixed i $(1 \leqslant i \leqslant n)$ as x ranges over all the numbers $1, 2, \ldots, p-1$, d_i ranges over all non-zero elements of Z_p and hence

$$\Pr(d_i \in C) = \frac{|C|}{p-1} > \tfrac{1}{3}.$$

Therefore the expected number of elements b_i such that $d_i \in C$ is more than $\frac{1}{3}n$. Consequently, there is an x $(1 \leqslant x < p)$ and a subsequence A of B of cardinality $|A| > \frac{1}{3}|B|$, such that $xa \pmod{p} \in C$ for all $a \in A$. This A is clearly sum-free, since if $a_1 + a_2 = a_3$ for some $a_1, a_2, a_3 \in A$ then $xa_1 + xa_2 \equiv xa_3 \pmod{p}$, contradicting the fact that C is a sum-free subset of Z_p. This completes the proof. □

Next we show that the constant $\frac{1}{3}$ in Proposition 1.1 cannot be replaced by $\frac{12}{29}$. Put $B = \{1, 2, 3, 4, 5, 6, 10\}$. If $A \subseteq B$ is sum-free, then $|A \cap \{1, 2\}| \leqslant 1$, $|A \cap \{3, 6\}| \leqslant 1$ and $|A \cap \{5, 10\}| \leqslant 1$, Consequently, if A has more than 3 elements, then A has precisely one element from each of the 3 pairs $\{1, 2\}$, $\{3, 6\}$ and $\{5, 10\}$. However, in this case, since $4 \in A$, $2 \notin A$ and hence $1 \in A$. As A is sum-free, $3 \notin A$ and $5 \notin A$ and hence $6 \in A$ and $10 \in A$. This is a contradiction, since $4 + 6 = 10$. Therefore, for the above set B, $s(B) \leqslant 3 = \frac{3}{7}|B|$. In fact, $s(B) = 3$ since, e.g., $\{1, 3, 10\}$ is sum-free. A similar simple case analysis shows that, if $A \subseteq B$, $|A| = 3$ and $A \cup \{8\}$ is sum-free, then $\{1, 10\} \subseteq A$.

Indeed, $4 \notin A$ and hence A contains precisely one element from each of the pairs $\{1,2\}$, $\{3,6\}$ and $\{5,10\}$. If $2 \in A$ then $6 \notin A$ and $10 \notin A$ and hence $\{2,3,5\} = A$, contradicting the fact that it is sum-free. Thus $2 \notin A$ and $1 \in A$. If $5 \in A$ then $3 \notin A$ (as $5+3 = 8$) and $6 \notin A$, which is impossible. Hence $10 \in A$ and $\{1,10\} \subsetneq A$, as claimed. We next apply these properties of the set B to construct a set C with $s(C) \leqslant \frac{12}{29}|C|$ $(< \frac{3}{7}|C|)$. Put $C = B \cup 7B \cup 8B \cup 9B \cup \{64\}$. Clearly $|C| = 29$ and $s(C) \leqslant 4s(B)+1 = 13$. We claim that in fact $s(C) \leqslant 12$. Indeed, suppose this is false, and let $A \subseteq C$ be a sum-free subset of C of cardinality 13. Then clearly

$$|A \cap B| = |A \cap 7B| = |A \cap 8B| = |A \cap 9B| = 3$$

and $64 \in A$. For each $i \in \{1,7,8,9\}$ define $A_i = A \cap iB$ and $A_i' = \{a/i : a \in A_i\}$. Clearly each A_i' is a sum-free subset of B of cardinality 3. Since $64 = 8 \cdot 8$, $A_8' \cup \{8\}$ is sum-free and hence $\{1,10\} \in A_8'$. Therefore $8, 80 \in A$. Hence $A_1 \cup \{8\}$ is sum-free and thus $1, 10 \in A$. It follows that $6 \cdot 9 = 64-10$, $1 \cdot 9 = 8+1$, $2 \cdot 9 = 10+8$ and $10 \cdot 9 = 80+10$ are not in A. Thus $A_9' = \{3,4,5\}$ and hence $27, 36, 45 \in A$. Consequently $7 \cdot 1 = 8-1 \notin A$, $7 \cdot 5 = 45-10 \notin A$, $7 \cdot 4 = 27+1 \notin A$ and $7 \cdot 10 = 80-10 \notin A$. Thus $A_7' = \{2,3,6\}$ and $21, 42 \in A$, contradicting the fact that A is sum-free. Therefore $s(C) \leqslant \frac{12}{29}|C|$ as claimed and the constant $\frac{1}{3}$ cannot be replaced by $\frac{12}{29}$. Notice that the same estimate holds for each of the sets

$$C_m = C \cup 1000C \cup 1000^2 C \cup \ldots \cup 1000^{m-1} C.$$

Hence, for every positive integer m there is a set of $n = 29m$ positive integers such that $s(C_m) \leqslant \frac{12}{29}|C_m|$.

In the case of sequences, we can obtain better upper bounds than the above one. Here we need the following well-known theorem of Schur [13].

Theorem 2.1 (Schur [13], see also, e.g., [14] or [10]) *For every $k \geqslant 2$ there exists a finite smallest possible integer $f(k) \leqslant k!\,\mathrm{e}$, such that there is no partition of the integers $\{1,2,\ldots,f(k)\}$ into k sum-free sets. In particular, $f(2) = 5$ and $f(3) = 14$.*

The next lemma provides a way of constructing sequences B with a relatively small value of $s(B)/|B|$.

Lemma 2.2 *Let $A = (a_1, a_2, \ldots, a_n)$ be a sequence of n non-zero integers and put $s = s(A)$. Suppose there exists a set $C = \{c_1, \ldots, c_k\}$ of k integers such that every sum-free sequence of A of cardinality s contains at least one term that is equal to a member of C. Let $f = f(k)$ be the number given in Theorem 2.1, and let B be the sequence $(b_{ij} = ja_i : 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant f)$. Then $s(B) \leqslant fs-1$. Hence*

$$\frac{s(B)}{|B|} \leqslant \frac{s(A)}{|A|} - \frac{1}{nf}. \tag{2.1}$$

Proof The sequence B is a union of the f sequences $B_j = (ja_1, ja_2, \ldots, ja_n)$ for $1 \leqslant j \leqslant f$. Since each such sequence is simply a product of the members of A by the constant j, we have that $s(B_j) = s(A) = s$. Consequently,

$$s(B) \leqslant \sum_{j=1}^{f} s(B_j) = sf.$$

To complete the proof we must show that the last inequality is strict. Assume it is not and let D be a sum-free subsequence of B of cardinality sf. Clearly D must contain precisely s elements from each B_j. We now define a partition of $\{1,2,\ldots,f\}$ into $|C| = k$ subsets as follows. For each j $(1 \leqslant j \leqslant f)$ D contains a sum-free sequence of s elements of B_j. Let $(d_1, \ldots, d_s)$ be this subsequence. Clearly $(d_1/j, d_2/j, \ldots, d_s/j)$ is a sum-free subsequence of A of cardinality s. By the definition of $C = \{c_1, \ldots, c_k\}$, there are i and l $(1 \leqslant i \leqslant s,\ 1 \leqslant l \leqslant k)$ such that $d_i/j = c_l$. Choose, arbitrarily, such i and l and assign j to the lth class of the partition. Since $f = f(k)$ was chosen according to Theorem 2.1, there is an l $(1 \leqslant l \leqslant k)$ and there are (not necessarily distinct) j_1, j_2 and j_3 such that $j_1 + j_2 = j_3$ and j_1, j_2 and j_3 all belong to the lth class in the partition defined above. Consequently, there are $d_1, d_2, d_3 \in D$ such that $d_i = c_l j_i$ for $1 \leqslant i \leqslant 3$. However, in this case,

$$d_1 + d_2 = c_l(j_1 + j_2) = c_l j_3 = d_3,$$

contradicting the fact that D is sum-free. Hence, our assumption that $s(B) = sf$ is false and $s(B) \leqslant sf-1$. This completes the proof. □

Corollary 2.3 *For every sequence A of non-zero integers there is a sequence B such that*

$$\frac{s(B)}{|B|} \leqslant \frac{s(A)}{|A|} - \frac{1}{(|A|-s(A)+1)!\,\mathrm{e}|A|}.$$

Proof Suppose $A = (a_1, a_2, \ldots, a_n)$ and $s = s(A)$. Let C be the set of all values of the first $n-s+1$ members of A. Clearly the set C has $k \leqslant n-s+1$ members. By Theorem 2.1, $f(k) \leqslant k!\,\mathrm{e}$. Thus, the assertion of the corollary follows from Lemma 2.2. □

Corollary 2.4 *Let S be the following sequence of 140 elements: $S = (ijl : 1 \leqslant i \leqslant 2,\ 1 \leqslant j \leqslant 5,\ 1 \leqslant l \leqslant 14)$. Then $s(S) \leqslant 55$. Hence $s(S)/|S| \leqslant \frac{11}{28}$.*

Proof Let A be the sequence $A = (1,2)$. Clearly $s = s(A) = 1$ and s, A, $k = 2$ and $C = \{1,2\}$ satisfy the hypotheses in Lemma 2.2. Since, by Theorem 2.1, $f(2) = 5$, Lemma 2.2 implies that, for the sequence $B = (ij : 1 \leqslant i \leqslant 2,\ 1 \leqslant j \leqslant 5)$, $s(B) \leqslant 5-1 = 4$. In fact, since, e.g., $(1,3,8,10)$ is sum-free, $s(B) = 4$. Put $k = 3$ and $C = \{1,2,4\}$. One can easily check that C, k, $s = 4$ and $A = (ij : 1 \leqslant i \leqslant 2,\ 1 \leqslant j \leqslant 5)$ satisfy the hypotheses of Lemma 2.2. Since, by Theorem 2.1, $f(3) = 14$, the lemma implies that, for the sequence S defined by the corollary, $s(S) \leqslant 4 \cdot 14 - 1 = 55$, as needed. □

Remark 2.5 Lemma 2.2 (or Corollary 2.3) clearly enables us to construct from S sequences B with $s(B)/|B| < \frac{11}{28}$. Since it does not seem that this method suffices to close the gap between the lower bound in Proposition 1.2 and the upper bound in the last corollary, we omit the detailed computation of $s(B)$ for the resulting sequences B,

3 Sum-free subsets in finite Abelian groups

In this section we prove Theorem 1.3. We first show that, for any finite Abelian group G and every sequence A of non-zero elements of G, $s(A) > \frac{2}{7}|A|$. This clearly implies a similar inequality for subsets of G. The basic method in the proof is similar to that used in the proof of Proposition 1.2, but requires several additional ideas. We start with the following simple observations concerning the cyclic group Z_n. Define

$$I_1 = \{x \in Z_n : \tfrac{1}{3}n < x \leqslant \tfrac{2}{3}n\},$$

$$I_2 = \{x \in Z_n : \tfrac{1}{6}n < x \leqslant \tfrac{1}{3}n \text{ or } \tfrac{2}{3}n < x \leqslant \tfrac{5}{3}n\}.$$

One can easily check that both I_1 and I_2 are sum-free subsets of Z_n.

For any divisor d of n, let dZ_n denote the subgroup of all multiples of d in Z_n, i.e., $dZ_n = \{0, d, 2d, \ldots, n-d\}$. Clearly dZ_n has n/d elements. In our proof we need the values of the fractions $|dZ_n \cap I_j|/|dZ_n|$ for all divisors d of n and $j = 1,2$. Clearly these can be computed by a straightforward case analysis, which is summarized in the following statement, the easy detailed proof of which is omitted.

Lemma 3.1 *The table contains the quantities $|dZ_n \cap I_j|/|dZ_n|$ for all possible $n \geqslant 2$ and $d|n$ $(1 \leqslant d < n)$ depending on the value of $|dZ_n| = n/d$ modulo 6.*

$\frac{n}{d}$	$\frac{\lvert dZ_n \cap I_1\rvert}{\lvert dZ_n\rvert}$	$\frac{\lvert dZ_n \cap I_2\rvert}{\lvert dZ_n\rvert}$
$6k$	$\frac{2k}{6k} = \frac{1}{3}$	$\frac{2k}{6k} = \frac{1}{3}$
$6k+1$	$\frac{2k}{6k+1} \geqslant \frac{2}{7}$	$\frac{2k}{6k+1} \geqslant \frac{2}{7}$
$6k+2$	$\frac{2k+1}{6k+2}$	$\frac{2k}{6k+2}$
$6k+3$	$\frac{2k+1}{6k+3} = \frac{1}{3}$	$\frac{2k+1}{6k+3} = \frac{1}{3}$
$6k+4$	$\frac{2k+1}{6k+4} \geqslant \frac{1}{4}$	$\frac{2k+2}{6k+4} > \frac{1}{3}$
$6k+5$	$\frac{2k+2}{6k+5} > \frac{1}{3}$	$\frac{2k+2}{6k+5} > \frac{1}{3}$

In particular, for all admissible values of n and d,

$$\frac{4}{7}\frac{|dZ_n \cap I_1|}{|dZ_n|} + \frac{3}{7}\frac{|dZ_n \cap I_2|}{|dZ_n|} \geqslant \frac{2}{7}. \tag{3.1}$$

We can now prove the lower bounds in Theorem 1.3. Let G be an arbitrary finite Abelian group and let $B = (b_1, b_2, \ldots, b_m)$ be a sequence of m non-zero elements of G. As is well known, G is a direct sum of cyclic groups and therefore there are n and s such that G is a subgroup of the direct sum H of s copies of Z_n. Thus we can think of the elements of B as members of H. Each such element b_i is, in fact, a vector $b_i = (b_{i1}, b_{i2}, \ldots, b_{is})$, where, for each i, $0 \leqslant b_{i1}, \ldots, b_{is} < n$ and not all the b_{ij} are zero. Let us choose a random element $(x_1, x_2, \ldots, x_s)$ of $H = Z_n^s$ according to a uniform distribution and define m elements $f_1, f_2, \ldots, f_m$ of the cyclic group Z_n by

$$f_i = \sum_{j=1}^{s} x_j b_{ij} \pmod{n}.$$

Notice that, for every fixed i $(1 \leqslant i \leqslant m)$, the mapping

$$(x_1, x_2, \ldots, x_s) \mapsto \sum_{j=1}^{s} x_j b_{ij} \pmod{n}$$

is a homomorphism from H to Z_n. Moreover, if d_i is the greatest common divisor of $b_{i1}, b_{i1}, \ldots, b_{is}$ and n then $d_i < n$, $d_i | n$ and the image of

this homomorphism is just d_iZ_n. Consequently, as $x = (x_1,\dots,x_s)$ ranges over all elements of H, f_i ranges over all elements of d_iZ_n and attains each value of d_iZ_n the same number of times. It follows that, for each $j = 1,2$,

$$\Pr(f_i \in I_j) = \frac{|d_iZ_n \cap I_j|}{|d_iZ_n|}.$$

For each divisor d of n $(1 \leq d < n)$, let m_d denote the number of elements b_i in B such that $\gcd(b_{i1}, b_{i2},\dots,b_{is},n) = d$. Clearly $\sum_{d|n,d<n} m_d = m$ and, for $j = 1,2$, the expected number of elements b_i such that $f_i \in I_j$ is

$$M_j = \sum_{\substack{d|n\\ d<n}} m_d \frac{|dZ_n \cap I_j|}{|dZ_n|}.$$

Moreover, since $x = (0,0,\dots,0) \in H$ maps every b_i into $f_i = 0 \notin I_1$, it follows that there is an $x = (x_1,\dots,x_s) \in H$ and a subsequence A of strictly more than M_1 elements of B such that each $a = (a_1,\dots,a_s) \in A$ is mapped by x into $\sum_{i=1}^s x_ia_i \pmod n \in I_1$. Clearly this A is a sum-free subsequence of B (since I_1 is sum-free) and thus

$$s(B) > M_1 = \sum_{\substack{d|n\\ d<n}} m_d \frac{|dZ_n \cap I_1|}{|dZ_n|}. \tag{3.2}$$

Similarly, since I_2 is sum-free,

$$s(B) > M_2 = \sum_{\substack{d|n\\ d<n}} m_d \frac{|dZ_n \cap I_2|}{|dZ_n|}. \tag{3.3}$$

Combining (3.1), (3.2) and (3.3), we obtain

$$\begin{aligned} s(B) = \tfrac{4}{7}s(B) + \tfrac{3}{7}s(B) &> \tfrac{4}{7}M_1 + \tfrac{3}{7}M_2 \\ &\geq \sum_{\substack{d|n\\ d<n}} m_d\left(\frac{4}{7}\frac{|dZ_n \cap I_1|}{|dZ_n|} + \frac{3}{7}\frac{|dZ_n \cap I_2|}{|dZ_n|}\right) \\ &\geq \sum_{\substack{d|n\\ d<n}} m_d \times \tfrac{2}{7} = \tfrac{2}{7}m. \end{aligned}$$

Therefore B contains a sum-free subsequence of more than $\frac{2}{7}|B|$ members, completing the proof of the lower bounds (for sequences and sets) in Theorem 1.3.

The fact that $\frac{2}{7}$ is optimal (for both sets and sequences) follows from the following result of Rhemtulla and Street [12].

Theorem 3.2 (Rhemtulla and Street [12]) *Let $p = 3k+1$ be a prime and let G be the elementary Abelian group Z_p^s. Then $|G| = p^s$ and the maximum cardinality of a sum-free subset of G is kp^{s-1}.*

In view of this theorem, if we choose $G = Z_7^s$ and $B = G\backslash\{0\}$, then $|B| = 7^s - 1$ and $s(B) = 2\cdot 7^{s-1}$. Since s can be arbitrarily large, this shows that the constant $\frac{2}{7}$ in Theorem 1.3 is optimal (for sets, and hence for sequences too). □

4 Extensions, concluding remarks and open problems

1. One can easily generalize Proposition 1.2 (and 1.1) to the case of real numbers. This was done by Erdős in [7], where he proves the next statement for sets B.

Proposition 4.1 *For any sequence B of non-zero reals, $s(B) \geq \frac{1}{3}|B|$.*

The proof is similar to that of Proposition 1.2. If $B = (b_1, b_2,\dots,b_n)$ is a sequence of non-zero reals and $\epsilon = \min_{1\leq i\leq n}|b_i|$, we choose, randomly, a real number x according to a uniform distribution on $[1/\epsilon, 10n/\epsilon]$ and compute the numbers $d_i = b_ix \pmod 1$. One can easily show that the expected number of $d_i - s$ that belong to $[\frac{1}{3},\frac{2}{3})$ is more than $\frac{1}{3}(n-1)$ and hence there is an x and a subsequence A of at least $\frac{1}{3}n$ members of B such that $xa \pmod 1 \in [\frac{1}{3},\frac{2}{3})$ for each $a \in A$. This subsequence is sum-free, since $[\frac{1}{3},\frac{2}{3})$ is sum-free with respect to addition modulo 1.

In fact here also we can improve on Erdős's result and prove that strict inequality holds.

Proposition 4.1′ *For any sequence B of non-zero reals, $s(B) > \frac{1}{3}|B|$.*

To prove this fact, we apply Proposition 1.2. Given any arbitrary sequence $B = (b_1,\dots,b_n)$ of reals, we claim that there is a sequence $C = (c_1,\dots,c_n)$ of integers such that, for any $\epsilon_1,\dots,\epsilon_n \in \{\pm1, 0\}$, the sign of $\sum_{i=1}^n \epsilon_ib_i$ (which is 0, +1 or −1) is equal to that of $\sum_{i=1}^n \epsilon_ic_i$. To prove this we argue as follows. For each of the 3^n possible vectors $\epsilon = (\epsilon_1,\dots,\epsilon_n)$, let $E(\epsilon)$ be an equation or an inequality with the n variables $x_1,\dots,x_n$ defined as follows: if $\sum_{i=1}^n \epsilon_ib_i = 0$ then $E(\epsilon)$ is the equation $\sum_{i=1}^n \epsilon_ix_i = 0$. If $\sum_{i=1}^n \epsilon_ib_i > 0$, let q be a positive rational so that $\sum_{i=1}^n \epsilon_ib_i \geq q$

and let $E(\epsilon)$ be the inequality $\sum_{i=1}^{n} \epsilon_i x_i \geqslant q$. Similarly, if $\sum_{i=1}^{n} \epsilon_i b_i < 0$, then $E(\epsilon)$ is the inequality $\sum_{i=1}^{n} \epsilon_i x_i \leqslant q$, where q is an arbitrary negative rational satisfying $\sum_{i=1}^{n} \epsilon_i b_i \leqslant q$. Consider the linear program in the n variables $x_1, \ldots, x_n$ consisting of the 3^n constraints $E(\epsilon)$. This program has a feasible real solution $(b_1, \ldots, b_n)$. Since all the constraints have rational coefficients it also has a rational solution $(d_1, \ldots, d_n)$. By multiplying all these numbers d_i by a suitable integer we obtain a sequence of integers $(c_1, \ldots, c_n)$ such that, for any $\epsilon_1, \ldots, \epsilon_n \in \{\pm 1, 0\}$,

$$\operatorname{sign}\left(\sum_{i=1}^{n} \epsilon_i b_i\right) = \operatorname{sign}\left(\sum_{i=1}^{n} \epsilon_i c_i\right).$$

Returning to Proposition 4.1′, let $B = (b_1, \ldots, b_n)$ be a sequence of non-zero reals. By the above discussion there is a sequence $C = (c_1, \ldots, c_n)$ of integers satisfying

$$\operatorname{sign}\left(\sum_{i=1}^{n} \epsilon_i b_i\right) = \operatorname{sign}\left(\sum_{i=1}^{n} \epsilon_i c_i\right)$$

for all $\epsilon_i \in \{\pm 1, 0\}$. In particular, no c_i is zero and $s(B) = s(C)$. By Proposition 1.2 $s(C) > \frac{1}{3}n$ and hence $s(B) > \frac{1}{3}n$, completing the proof of Proposition 4.1′. □

2. Motivated by Schur's theorem (stated in Section 2) and by the problem of estimating Ramsey numbers (see, e.g. [14] or [10]), various authors considered the problem of partitioning all the non-zero elements of a group into the minimum possible number of sum-free subsets. As noted by Abbott and Hanson [1], the original argument of Schur easily implies that the non-zero elements of no finite Abelian group of order n can be partitioned into less than $c_1 \log n / \log\log n$ sum-free subsets, where c_1 is an absolute constant. On the other hand, as is also observed in [1], the non-zero elements of any finite Abelian group of order n can be partitioned into $O(\log n)$ sum-free subsets. By repeatedly applying Theorem 1.3 (and Proposition 4.1), we clearly obtain the following more general result.

Proposition 4.2 *Any set of n non-zero elements in an arbitrary finite Abelian group can be partitioned into $O(\log n)$ sum-free subsets. Similar statements hold for any set of non-zero reals.*

3. A close inspection of the proof of Theorem 1.3 shows that the constant $\frac{2}{7}$, although the best possible for the general case, can be improved for many groups G. Thus for example the proof of Proposition 1.2 shows that, for any sequence B of non-zero elements of a cyclic group of prime order $p = 3k+2$,

$$s(B) \geqslant \frac{k+1}{3k+1}|B|$$

(and this is best possible for each such p, as can be easily shown using the well-known Cauchy–Davenport theorem [5], [6]). Similarly, for any sequence B of non-zero elements of Z_p, where $p \equiv 1 \pmod 3$ is a prime, $s(B) \geqslant \frac{1}{3}|B|$ and this is best possible for each such p. The proof of Theorem 1.3 easily gives that, for any sequence B of non-zero elements of Z_2^s

$$s(B) \geqslant \frac{2^{s-1}}{2^s - 1}|B|.$$

This again is best possible for each s. By modifying the proof of Theorem 1.3, we can also improve the constants for various cyclic groups. in particular, we can show that if n is not divisible by any prime congruent to 2 modulo 3 then, for any sequence B of non-zero elements in Z_n, $s(B) \geqslant \frac{1}{3}|B|$. The proof is similar to that of Proposition 1.2; we multiply all the elements of B by a random member of Z_n^* (i.e., by a random number which is relatively prime to n) and compute the expected value of the numbers that are mapped to a certain sum-free subset of Z_n. The situation is more complicated when n is divisible by primes congruent to 2 modulo 3. A fruitful approach here is to multiply, for each divisor d of n, the elements of B by a random element of dZ_n^* and obtain a lower bound for $s(B)$ by computing the expected number of elements of B mapped to a certain sum-free subset of Z_n, (e.g., the subset $\{x \in Z_n : \frac{1}{3}n \leqslant x < \frac{2}{3}n\}$. This lower bound can be expressed as a linear combination of the quantities $m_d = \{b_i \in B : \gcd(b_i, n) = d\}$. All these lower bounds and the constraints $m_d \geqslant 0$ and $\sum m_d = |B|$ define a linear program from which a lower bound to $s(B)$ can be extracted. Using this method we can prove, for example, the following.

Proposition 4.3 *For any prime $p \equiv 2 \pmod 3$ and any $s \geqslant 1$, every sequence B of non-zero elements of the cyclic group Z_{p^s} satisfies $s(B) > \frac{1}{3}|B|$.*

We omit the somewhat tedious (though not too complicated) details of the proof. □

4. The proof of Proposition 1.2 (or 4.1) can be easily modified to show that, for any $r \geqslant 2$, any sequence B of n non-zero reals contains a subsequence A of size $\Omega(n/r)$ such that there are no $a_1, a_2, \ldots, a_r, a_{r+1} \in A$ such that $\sum_{i=1}^{r} a_i = a_{r+1}$. A similar statement for general Abelian groups is false. In fact, in Z_2^n the set of all non-zero elements B has cardinality $N = 2^n - 1$. Trivially, any subset A of B of cardinality $|A| = x$ with $\binom{x}{2} > 2^n - 1$ has $a_1, a_2, a_3, a_4 \in A$ such that, in Z_2^n, $a_1 + a_2 = a_3 + a_4$ and hence $a_1 + a_2 + a_3 = a_4$. Some related results have recently been obtained by Zs. Tuza.

5. Let us call a subset A of an Abelian group G weakly sum-free if there are no three *distinct* elements $a_1, a_2, a_3 \in A$ such that $a_1 + a_2 = a_3$. For a set $B \subseteq G$, let $\mathrm{ws}(B)$ denote the maximum cardinality of a weakly sum-free subset of B. Since each sum-free set is weakly sum-free, Theorem 1.3 implies that, for every Abelian group G and for every set B of non-zero elements of G, $\mathrm{ws}(B) > \frac{2}{7}|B|$. Using some of the methods of [2] we can show that the constant $\frac{2}{7}$ is optimal here too. Indeed, take $G = Z_7^s$ and $B = G \backslash (0)$. Then $|B| = 7^s - 1$. Let $A \subseteq B$ be a weakly sum-free subset of B. To prove the optimality of the constant $\frac{2}{7}$ we show that, for every fixed $\epsilon > 0$, $|A| < 2 \cdot 7^{s-1} + \epsilon \cdot 7^s$, provided s is sufficiently large. Call an element a of A *good* if there are two distinct elements $b, c \in A$ such that $2a = b + c$. Otherwise it is *bad*. We claim that the number of bad elements is smaller than $\epsilon \cdot 7^s$, for $s > s_0(\epsilon)$. This is because otherwise, by the main result of [3] (see also [8] for a short proof and [9] for a much stronger result), there are three distinct bad elements a, b and c such that $2a = b + c$, contradicting the fact that a is bad. Therefore, if $|A| \geqslant 2 \cdot 7^{s-1} + \epsilon \cdot 7^s$ and $s > s_0(\epsilon)$, then A contains more than $2 \cdot 7^{s-1}$ good elements. It follows from the result of [12] (stated in Theorem 3.2 in Section 3) that there are three not necessarily distinct good elements d, e and f of A such that $d + e = f$. Clearly $d \neq f$ and $e \neq f$ (since $0 \notin A$). If $d \neq e$ then A is not weakly sum-free, contradicting its definition and completing the proof. Otherwise $2d = f$ and, since d is good, there are two distinct elements a and b of A such that $a + b = 2d = f$. Hence, in this case too, A is not weakly sum-free, completing the proof. □

6. An analogue of Proposition 1.2 can be established for measurable sets in the torus. Recall that the (one-dimensional) torus T is the group of real numbers x $(0 \leqslant x < 1)$ with addition modulo 1. Let μ be the usual Lebesque measure on T with $\mu(T) = 1$. We can prove the following.

   Proposition 4.4 *For any measurable $B \subseteq T$ and for any $\epsilon > 0$, there is a (measurable) sum-free set $A \subseteq B$ such that $\mu(A) > (\frac{1}{3} - \epsilon)\mu(B)$. The constant $\frac{1}{3}$ is best possible.*

   To prove this proposition, we use the fact that $f\colon T \to T$ defined by $f(x) = 2x \pmod 1$ is ergodic. For $i \geqslant 1$, put

   $$B_i = \{x \in B : \tfrac{1}{3} \leqslant f^{(i)}(x) = 2^i x \pmod 1 < \tfrac{2}{3}\}.$$

   Clearly B_i is sum-free. Since f is ergodic,

   $$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \mu(B_i) = \tfrac{1}{3}\mu(B),$$

   implying that $\mu(B) > (\frac{1}{3} - \epsilon)\mu(B)$ for some i. The fact that the constant $\frac{1}{3}$ is best possible is proved by showing that, for each sum-free $A \subseteq T$, $\mu(A) \leqslant \frac{1}{3}$. Indeed, suppose $A \subseteq T$ is measurable with $\mu(A) \geqslant \frac{1}{3} + \epsilon$, where $\epsilon > 0$. Let p be a large prime, and call an element $i \in Z_p$ *A-full* if

   $$\mu\left(A \cap \left[\frac{i}{p}, \frac{i+1}{p}\right]\right) > 0.9\frac{1}{p}.$$

   For sufficiently large p, the cardinality of the set $B \subseteq Z_p$ of all A-full elements of Z_p is clearly bigger than $\frac{1}{3}p + 1$. Consequently, by the Cauchy–Davenport theorem ([5], [6]), $|B + B| \geqslant 2|B| - 1 > \frac{2}{3}p$. Hence $(B + B) \cap B \neq \varnothing$ and there are $b_1, b_2, b_3 \in B$ such that $b_1 + b_2 \equiv b_3 \pmod p$. One can easily check that this implies that A is not sum-free, as needed. □

   By replacing the Cauchy–Devonport theorem by Kneser's theorem [11], we can show that the maximum-possible measure of a sum-free measurable subset of the n-dimensional torus is also $\frac{1}{3}$ for all $n \geqslant 1$.

7. Our proofs of Proposition 1.2 and 1.3 are probabilistic. In particular, they clearly supply an efficient randomized algorithm which, given a set of n non-zero integers B, finds, in expected polynomial time (in the length of the input), a sum-free subset of it of cardinality $\Omega(n)$. It would be interesting to find an efficient

deterministic algorithm for this problem. It would also be interesting to determine the best-possible constants in Propositions 1.1 and 1.2.

Acknowledgement

We would like to thank Y. Caro and I. Krasikov for helpful comments.

References

[1] H. L. Abbott & D. Hanson, A problem of Schur and its generalizations, *Acta Arithmetica*, **20** (1972), 175–87.
[2] N. Alon, Subset sums, *J. Number Theory*, **27** (1987), 196–205
[3] T. C. Brown & J. P. Buhler, A density version of a geometric Ramsey theorem, *J. Combinatorial Theory, Ser. A*, **32** (1982), 20–34
[4] L. Babai & V. T. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, *European J. Combin.*, **6** (1985), 101–14
[5] A. L. Cauchy, Recherches sur les nombres, *J. Ecole polytechn.*, **9** (1813), 99–116
[6] H. Davenport, On addition of residue classes, *J. London Math. Soc.*, **10** (1935), 30–2
[7] P. Erdős, External problems in number theory, *Proc. Symp. Pure Maths.*, Vol. VIII, AMS (1965), 181–9
[8] P. Frankl, R. L. Graham & V. Rödl, On subsets of Abelian groups with no 3-term arithmetic progressions, *J. Combinatorial Theory, Ser. A*, **45** (1987), 157–61
[9] H. Furstenberg & Y. Katznelson, An ergodic Szemerédi theorem for IP-systems and combinatorial theory, *J. d'Analyse Math.*, **45** (1985), 117–68
[10] R. L. Graham, B. L. Rothschild & J. H. Spencer, *Ramsey Theory*, Wiley, New York, 1980
[11] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Zeit.*, **58** (1953), 459–84
[12] A. H. Rhemtulla & Ann Penfold Street, Maximum sum-free sets in elementary Abelian p-groups, *Canad. Math. Bull.*, **14** (1971), 73–80.
[13] I. Schur, Uber die Kongruenz $x^m+y^m = z^m \pmod p$, *Jahresbericht der Deutschen Mathematiker Vereinigung*, **25** (1916), 114–17
[14] W. D. Wallis, Ann Penfold Street & Jennifer Seberry Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*. Lecture Notes in Mathematics, **292**, Springer, Berlin–Heidelberg–New York, 1972, Part 3, 123–277

Is there a different proof of the Erdős–Rado theorem?

James E. Baumgartner*

Abstract

We define the notion of an Erdős–Rado function which, if it exists, would make possible an essentially different approach to the Erdős–Rado theorem. Several combinatorial propositions, including $\omega_2 \to (\omega_1+2)^2_\omega$ and assertions about graphs on ω_2 due to Hajnal, imply the existence of Erdős–Rado functions. It is shown relatively consistent with $\mathrm{CH}+2^{\omega_1} = \omega_3$ that no Erdős–Rado functions exist. A list of open problems is included.

1 Introduction

The Erdős–Rado theorem [2], one of the cornerstones of combinatorial set theory has received several rather different-looking proofs over the years, including in particular the model-theoretic argument due to Simpson, yet, at bottom, all the proofs seem to make use of the fundamental ramification argument of Erdős and Rado. The purpose of this paper is to investigate the question whether a truly different proof is possible.

That question can be made precise as follows. Under CH, the first non-trivial version of the Erdős–Rado theorem (beyond Ramsey's theorem) says that $\omega_2 \to (\omega_1+1)^2_\omega$. In fact, the ramification argument yields rather more. For example, if $f\colon [\omega_2]^2 \to \omega$ and $g\colon [\omega_2]^2 \to \omega_1$ are given, it is possible to find a set X of order type ω_1+1 such that X is not only homogeneous for f but also end-homogeneous for g, i.e., whenever $\alpha,\beta,\gamma \in X$ and $\alpha < \beta < \gamma$ then $g\{\alpha,\beta\} = g\{\alpha,\gamma\}$. This is an example of a so-called canonical partition relation (see [1] for a

* The preparation of this paper was partially supported by National Science Foundation grant number DMS-870456.