ELSEVIER
Discrete Mathematics 229 (2001) 89–99
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Spanning subset sums for finite Abelian groups

J.R. Griggs[1]

Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA

Abstract

We survey the state of research to determine the maximum size of a nonspanning subset of a finite abelian group G of order n. The smallest prime factor of n, denote it here by p, plays a crucial role. For prime order, $G=\mathbf{Z}_p$, this is essentially an old problem of Erdős and Heilbronn, which can be solved using a result of Dias da Silva and Hamidoune. We provide a simple new proof for the solution when n is even ($p=2$). For composite odd n, we deduce the solution, for $n\geqslant 2p^2$, from results obtained years ago by Diderrich and, recently, by Gao and Hamidoune. Only a small family of cases remains unsettled.

1. Overview

Let $G=(G,+)$ be a finite abelian group. We let $G^*:=G\setminus\{0\}$. $\mathbf{Z}_n$ denotes the group $\mathbf{Z}/n\mathbf{Z}$ of integers $\bmod n$ under addition. For $S=\{s_1,\ldots,s_k\}\subseteq G$, we say that S *spans* G if every $g\in G$ is a sum of distinct elements of S, i.e., $g=\sum_{i=1}^{k}\varepsilon_i s_i$, where each ε_i is 0 or 1. We say that S spans G *nontrivially* if each $g\in G$ is a sum of one or more elements of S, so that, in particular, there is such a sum equalling zero with not all ε_i equal to zero. Note that we consider only sums with distinct elements.

We consider here the maximum size of nonspanning subsets S of G. For instance, $S=\{0,2,4,6\}$ fails to span $G=\mathbf{Z}_8$, while inserting any additional element from G to S now gives a set that spans G (nontrivially). However, it is perhaps surprising that there is a nonspanning set of size 5 that fails to span the element 4 in $\mathbf{Z}_8$: $\{-2,-1,0,1,2\}$ is one; another is $\{-3,-2,0,2,3\}$. Any six elements span $\mathbf{Z}_8$ nontrivially. Indeed, any five nonzero elements do it.

There are slightly different flavors of this problem, depending on whether we permit $0\in S$ and whether we require S to span G nontrivially. We shall concentrate on two versions. We define $w(G)$ to be the maximum size of a nonspanning subset S of G, while $e(G)$ denotes the maximum size of a subset $S\subseteq G^*$ that fails to span G nontrivially.

E-mail address: griggs@math.sc.edu (J.R. Griggs).
[1] Research supported in part by Grants NSA/MSP MDA904-95H1024 and NSF DMS-9701211.

PII: S0012-365X(00)00203-X

We now give the values of w and e for nontrivial abelian groups of order $n \leqslant 10$. We include a set S achieving $w(G)$. We also present a set T achieving $e(G)$, unless (as is usually the case) it is enough to just take S with its zero element removed.

n	G	w	S	e	T
2	$\mathbf{Z}_2$	1	$\{0\}$	1	$\{1\}$
3	$\mathbf{Z}_3$	2	$\{0,1\}$	1	
4	$\mathbf{Z}_4$	3	$\{0,1,3\}$	2	
	$\mathbf{Z}_2 \oplus \mathbf{Z}_2$	2	$\{(0,0),(0,1)\}$	2	$\{(0,1),(1,0)\}$
5	$\mathbf{Z}_5$	3	$\{0,1,2\}$	2	
6	$\mathbf{Z}_6$	4	$\{0,1,2,5\}$	3	
7	$\mathbf{Z}_7$	4	$\{0,1,2,6\}$	3	
8	$\mathbf{Z}_8$	5	$\{0,1,2,6,7\}$	4	
	$\mathbf{Z}_4 \oplus \mathbf{Z}_2$	5	$\{(0,0),(1,0),(1,1),(3,0),(3,1)\}$	4	
	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$	4	$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}$	3	
9	$\mathbf{Z}_9$	5	$\{0,1,2,7,8\}$	4	
	$\mathbf{Z}_3 \oplus \mathbf{Z}_3$	5	$\{(0,0),(0,1),(1,0),(1,1),(1,2)\}$	4	
10	$\mathbf{Z}_{10}$	5	$\{0,2,4,6,8\}$	4	

This problem of spanning subsets was brought to our attention by colleagues at the time, Jared Wunsch and Barbara Flinn, who were investigating sums of elements in the cyclic 2-groups $G = \mathbf{Z}_{2^k}$; in our notation, they asked for $w(G)$. Trivially, $w(G) \geqslant 2^{k-1}$, but no good general upper bound was apparent. Examples showing that $w(G) > 2^{k-1}$ for $k = 2,3$ suggested that the problem could be difficult. We managed to solve this problem and extend the result to determine $w(G)$ for arbitrary abelian 2-groups (i.e., of order 2^k). Related work was brought to our attention, especially a famous closely related problem of Erdős and Heilbronn [5] (cf. [7]), which asks, in our notation, for $e(\mathbf{Z}_p)$ when p is a prime. It was then natural to formulate the problems of determining $w(G)$ and $e(G)$ for general finite abelian groups G.

In Section 2, we provide some general bounds on our parameters. We show that $w(G)$ and $e(G)$ agree to within one. An additivity result is derived that implies an upper bound of $(n/2) + 1$ (resp., $n/2$) on $w(G)$ (resp., $e(G)$) for G of order n. For even n, this is just one above the easy lower bounds obtained by taking S to be a subgroup of G of index 2. Groups of prime order behave rather differently for this problem than groups of composite order. If n is a prime p, so that $G = \mathbf{Z}_p$, the possible values of the parameters w and e were narrowed down years ago to a range of just three values, each around $2p^{1/2}$.

In contrast, we present in Theorem 3 of Section 2 the following general lower bound for all G of composite order n: If p denotes the smallest prime factor of composite n, then a lower bound of $(n/p) + p - 2$ (resp., $(n/p) + p - 3$) is obtained on $w(G)$ (resp., $e(G)$). In Theorem 4 we present a family of groups G for which this lower bound in NOT sharp.

In Section 3 we present the complete solution of our problems for groups of even order. We show that the lower bounds of Section 2 are sharp for all sufficiently large even n.

Groups of odd order are discussed in Section 4. From rather recent work of Dias da Silva and Hamidoune [2] we derive in Section 4 the complete solution to the Erdős–Heilbronn problem above for $G=\mathbf{Z}_p$. The rest of the paper concerns the remaining values of n, which are the odd composites. Consider composite n with smallest prime divisor $p>2$. Our earlier drafts included the conjecture that the lower bounds of Theorem 3 above must be sharp for all $n>n_0(p)$. We then received a paper independently addressing this problem by Gao and Hamidoune [6]. It cites fundamental work in this same area performed years ago.

Diderrich and Mann [4] formulated another version of our problem in the early 1970s, when they asked, for any finite group $(G,+)$ (not necessarily abelian), for the *critical number* $c(G)$, which they define to be the minimum $c\in\mathbf{Z}^+$ such that for every $S\subseteq G^*$ of size at least c, every element of G can be expressed as a nontrivial sum over some subset of S. Thus, for abelian groups G of order $n\geqslant 3$, we have the general relation

$$e(G)=c(G)-1.$$

We continue to use the w,e notation we introduced here, however: Besides making sense even when $n\leqslant 2$, our notation has the advantage that it is natural to ask for a characterization of the extremal sets S, which achieve $e(G)$ yet do not span G nontrivially (and similarly for $w(G)$). While it appears that $w(G)=e(G)+1$ for all G of order $n\geqslant 5$ (i.e., $w(G)=c(G)$), it is not obviously true, and it remains open in one family of cases. So we shall work with both w and e throughout the paper.

Diderrich and Mann determined $e(G)$ when $n=|G|$ is even, so they essentially obtained our Even Groups Theorem 5. However, we still include our proof here, since it is shorter, simpler, and (unlike the earlier proof) self-contained. Their theorem is more general though, as it is not restricted to *abelian* groups; It concerns $e(G)$ for groups G of even order n that contain a maximal subgroup of order $n/2$.

In Diderrich's [3] paper of the same period, what is essentially our general lower bound above for composite n, Theorem 3, is obtained. We include our proof here, which is very similar, only for completeness. Diderrich's main work in [3] is to consider abelian G of order $n=pq$, where primes $p<q$, so that $G=\mathbf{Z}_{pq}$. He proves that the general lower bound $n/p+p-3$ on $e(G)$ is sharp for $q>2p$. It follows that the bounds of Theorem 3 are sharp for $n=pq$, $q>2p$.

For arbitrary even $n\geqslant 10$, the bounds of Theorem 3 are sharp by the Even Groups Theorem. Diderrich conjectured that his lower bound on $e(G)$ would also be sharp for any abelian group G of order n, with smallest prime divisor $p>2$, provided that n/p is composite. Gao and Hamidoune's new work [6] establishes this result, and our conjecture above for $n>n_0(p)$ now follows (Theorem 8).

A 1986 paper of Mann and Wou [8] takes care of the case that $G=\mathbf{Z}_p\oplus\mathbf{Z}_p$, p odd, where again the general lower bound on $e(G)$ is sharp. The proofs of [3,8,6] are difficult and dependent on various earlier results in the theory.

In Section 5 we discuss what is left to determine. It remains to deal with the cyclic groups $G=\mathbf{Z}_{pq}$ where p,q are odd primes with $p\leqslant q<2p$. Here, we can narrow the gap somewhat using Theorem 4 and an upper bound of Diderrich (Theorem 12). The open cases for determining $w(G)$ and $e(G)$ are where $p+\lfloor 2\sqrt{p-2}\rfloor+1<q<2p$. We suspect that the lower bounds of Theorem 4 are sharp for these cases.

2. General bounds

We begin by noting the close relationship between our two parameters, $e(G)$ and $w(G)$.

Theorem 1. *Let G be a finite abelian group. Then $e(G)\leqslant w(G)\leqslant e(G)+1$.*

Proof. If a set $S\subseteq G$ fails to span G, then removing 0 from S (if it is there) gives a nonspanning, nonzero subset. Thus, $e(G)\geqslant w(G)-1$.

If $w(G)=|G|-1$, then $e(G)\leqslant|G^*|=|G|-1=w(G)$. Else, if $w(G)<|G|-1$, consider any $S\subseteq G^*$ with $|S|=w(G)+1$. Let $x\in S$. By definition of w, $S\backslash\{x\}\cup\{0\}$ spans G. In particular, it spans $-x$. Thus, S spans $x+(-x)=0$ nontrivially. Consequently S spans all of G nontrivially, so $e(G)<w(G)+1$, or $e(G)\leqslant w(G)$. □

We now give upper bounds on $w(G)$ and $e(G)$ based on expressing elements of G as sums of at most three elements of a spanning set. For even G, these bounds are never off of the actual values by more than one, in view of the general lower bound for groups of composite order that we provide.

Theorem 2. *Let G be a finite abelian group of order n. If n is even* (*resp*., *odd*) *then for every subset $S\subseteq G^*$ of size $>n/2$, every $g\in G$ can be written as a nontrivial sum of at most three* (*resp*., *two*) *distinct elements of S. Hence*,

$$w(G)\leqslant 1+\frac{n}{2}\quad\text{and}\quad e(G)\leqslant\frac{n}{2}.$$

Proof. We first establish that whenever R is a subset of G of size greater than $n/2$, then each $g\in G$ may be written as the sum of two elements of R. To see this, note that the sets R and $g-R$ cannot be disjoint, since the sum of their sizes is greater than n. Thus, there are elements $x_1,x_2\in R$ such that $g=x_1+x_2$. If $g\notin 2G=\{h+h\colon h\in G\}$, these two elements are distinct.

Now fix $S\subseteq G^*$ of size $>n/2$, and fix $g\in G$. If n is even, then $2G\neq G$, so $2G$ has at most $n/2$ elements. Consequently, the set $S':=g-2G$ also has at most $n/2$ elements, so there exists an element $s\in S\backslash S'$. Set $R=(S\backslash\{s\})\cup\{0\}$, so that $|R|=|S|>n/2$. By the argument in the last paragraph, there exist $x_1,x_2\in R$ such that $g-s=x_1+x_2$. Since $g-s\notin 2G$, we have $x_1\neq x_2$. Thus, $g=s+x_1+x_2$ is the sum of three distinct elements. If either of the x_i is 0, then we delete it from the expression, and we have that g is the sum of two or three distinct elements of S.

On the other hand, if n is odd, set $R = S \cup \{0\}$. Then $2|R| > n + 2$, so R and $g - R$ intersect in at least two elements, i.e., we may write $g = x_1 + x_2$, with $x_1, x_2 \in R$, in at least two different ways. But g can be written $x + x$ in only one way (the map $x \mapsto 2x$ is a bijection since n is odd), so we can write $g = x_1 + x_2$ with distinct $x_1, x_2 \in R$. Thus, g is the sum of one or two distinct elements of S, depending on whether one of the x_i is 0. □

Here are the general lower bounds, which are essentially the same as the one for $e(G)$ found by Diderrich [3].

Theorem 3. *Let G be an abelian group of order n, a composite number. Let p be the smallest prime divisor of n. Then*

$$w(G) \geqslant \frac{n}{p} + p - 2 \quad \text{and} \quad e(G) \geqslant \frac{n}{p} + p - 3.$$

Proof. By Theorem 1, it suffices to show the first inequality. It suffices to exhibit a nonspanning $S \subseteq G$ with $|S| = (n/p) + p - 2$. We may write $G = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_r}$ with $p \mid n_1$. Then G has the subgroup H of index p, $H = \mathbf{Z}_{n_1/p} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_r}$. The map $\phi(x) := H + x$ projects G onto its quotient $G/H = \mathbf{Z}_p$. Let S contain $H = \phi^{-1}(0)$ and any $p - 2$ elements of $\phi^{-1}(1)$. Then S fails to span any elements of $\phi^{-1}(p-1)$. □

The lower bounds in Theorem 3 are not sharp in general, by a variation of the Erdős–Heilbronn example (cf. Section 4).

Theorem 4. *Let p, q be primes such that $2 < p \leqslant q \leqslant p + \lfloor 2\sqrt{p-2} \rfloor + 1$, and let $n = pq$ and $G = \mathbf{Z}_n$. Then*

$$w(G) \geqslant |S| = \frac{n}{p} + p - 1 \quad \text{and} \quad e(G) \geqslant \frac{n}{p} + p - 2.$$

Proof. For $a = (p+q)/2 - 1$, take $S = \{-a, -a+1, \ldots, a\}$. Then S does not span the element $(pq-1)/2$. To show this, we need to check that

$$1 + 2 + \cdots + a = \frac{a^2 + a}{2} < \frac{pq - 1}{2},$$

which reduces after some manipulation to

$$(q-p)^2 - 2(q-p) + (4 - 4p) < 0.$$

Since each term is divisible by 4, this becomes

$$(q-p)^2 - 2(q-p) + (8 - 4p) \leqslant 0.$$

By the quadratic formula, this holds if and only if

$$q - p \leqslant \lfloor \sqrt{4p - 7} \rfloor + 1,$$

or, equivalently (see the proof of Theorem 7),

$$q - p \leqslant \lfloor 2\sqrt{p-2} \rfloor + 1. \qquad \square$$

Note that such q exist for infinitely many p.

3. Even groups theorem

Theorems 2 and 3 in the previous section determine $e(G)$ and $w(G)$ to within 1 for groups G of even order n. Values for $n \leqslant 10$ were listed in Section 1. That the lower bounds are the actual values for all larger n is a principal result of the paper. As noted in the Introduction, this theorem can also be deduced from earlier work of Diderrich and Mann [4].

Theorem 5 (Even Groups Theorem). *If G is an abelian group of even order $n \geqslant 10$, then*

$$w(G) = \frac{n}{2} \quad \text{and} \quad e(G) = \frac{n}{2} - 1.$$

Proof. The groups of even order n, $10 \leqslant n \leqslant 18$, were checked by computer, as well as directly by hand. We omit the lengthy, but routine, details.

Now assume $n > 18$ is even, and G is an abelian group of order n. In view of Theorems 1 and 3, it suffices to prove that $e(G) \leqslant (n/2) - 1$. Let S be a subset of G^* of size $n/2$. Let $T = S \cup \{0\}$.

Now fix a subgroup H of index 2. Then, for any $g \in G$, $H + 2g = H$, so that $2g \in H$. Also, the sets T and $g - T$ cannot be disjoint, because of their sizes, so g has a representation as $t_1 + t_2$ with $t_i \in T$. If $g \notin H$, since $2g \in H$, it means that $t_1 \neq t_2$ in its representation $g = t_1 + t_2$. Tossing away 0, if it is one of the t_i's, we have expressed g as a subset sum in S.

So from now on, we assume $g \in H$, and split the proof into three cases according to $k := |T \cap H|$.

Case 1. $k \geqslant (n/4) + 3$. By Theorem 2, $S \cap H$ spans H, so in particular, g is a subset sum.

Case 2. $3 \leqslant k < (n/4) + 3$. Consider the collection of sums $h + j$ with $h \in T \cap H$ and $j \in T \cap (G \backslash H)$. These $k(|T| - k)$ sums belong to $G \backslash H$, so some element v occurs in this collection with multiplicity at least

$$\left\lceil \frac{k(|T| - k)}{|G \backslash H|} \right\rceil = \left\lceil \frac{k((n/2) + 1 - k)}{n/2} \right\rceil \geqslant \left\lceil \frac{3((n/2) - 2)}{n/2} \right\rceil = 3.$$

In other words, we can write $v = h_i + j_i$, for $i = 1, 2, 3$, such that the h_i (resp., j_i) are distinct elements of $T \cap H$ (resp., $T \cap (G \backslash H)$). Since $g - v \notin H$, and since as above T and $(g - v) - T$ are not disjoint, we can write $g - v = h + j$ with $h \in T \cap H$ and $j \in T \cap (G \backslash H)$. Pick i so that $h_i \neq h$ and $j_i \neq j$ (which is possible since there are three choices for i). Then we have $g = h + j + h_i + j_i$, which is a sum of distinct elements of T. Omitting 0 as one of the terms, if present, gives a subset sum from S.

Case 3. $k \leqslant 2$. Now T contains $G \backslash H$, with the possible exception of a single element r. Fix $v \in T \cap (G \backslash H)$. The $(n/2)^3$ sums $x_1 + x_2 + x_3$ with each $x_i \in G \backslash H$ assume each value in $G \backslash H$ with equal multiplicity. In particular, $g - v$ can be represented $(n/2)^2$ ways as such a sum. Exactly $n/2$ of these sums have $x_1 = x_2$, since for any $x \in G \backslash H$ we get a unique such representation using $x = x_1 = x_2$ by choosing $x_3 = g - v - x - x$. Similarly, $n/2$ of these sums have $x_1 = x_3$, and $n/2$ have $x_2 = x_3$. Also, $n/2$ of these sums have $x_1 = v$, since for any $x_2 \in G \backslash H$ we have a unique choice for x_3. Similarly, $n/2$ sums have $x_2 = v$, and $n/2$ have $x_3 = v$. The same holds with v replaced by r. Thus, there remain at least

$$(n/2)^2 - 9(n/2) = n(n - 18)/4 > 0$$

sums $x_1 + x_2 + x_3$ equalling $g - v$ with distinct $x_i \in G \backslash H$ not equal to either v or r. So there exists a subset sum representation $g = x_1 + x_2 + x_3 + v$. $\square$

4. Groups of odd order

The case of prime order p, $G = \mathbf{Z}_p$, is exceptional for our spanning set problem. Erdős and Heilbronn [5] observed that the residues

$$a_1 = 1, \quad a_2 = -1, \ldots, a_k = (-1)^{k-1} \lfloor (k+1)/2 \rfloor$$

fail to span the element $(p-1)/2$ if $k < 2(p^{1/2} - 1)$. On the other hand, they proved that any set of $\geqslant 3(6p)^{1/2}$ nonzero residues span $\mathbf{Z}_p$.

Olson [9] gave an upper bound that left a range of at most three possible values each for $e(\mathbf{Z}_p)$ and $w(\mathbf{Z}_p)$. About 25 years later, Dias da Silva and Hamidoune [2] applied very different methods to obtain the following remarkable result:

Theorem 6 (Dias da Silva and Hamidoune [2]). *Let $S \subseteq \mathbf{Z}_p$ with cardinality $c_p + 1$, where $c_p = \lfloor (4p - 7)^{1/2} \rfloor$. Then every element of $\mathbf{Z}_p$ can be written as a sum of $\lfloor (c_p + 1)/2 \rfloor$ elements of S.*

Dias da Silva and Hamidoune observed that for infinitely many primes p, the bound implied by their theorem for the Erdős–Heilbronn problem ($e(\mathbf{Z}_p)$) is sharp. They used the Erdős–Heilbronn construction above (for even k). But, in fact, Theorem 6 leads to a complete solution of the Erdős–Heilbronn problem. This was pointed out by Barbara Flinn. We also provide a slightly nicer formula for c_p.

Theorem 7. *For primes $p \geqslant 3$,*

$$w(\mathbf{Z}_p) = c_p \quad \text{and} \quad e(\mathbf{Z}_p) = c_p - 1 \quad \text{where} \quad c_p = \lfloor 2\sqrt{p-2} \rfloor.$$

Proof. Careful application of Theorem 6 yields that the stated formulas are upper bounds on $w(\mathbf{Z}_p)$ and $e(\mathbf{Z}_p)$. Now to achieve these bounds, let i be the maximum integer such that the set

$$A=\{-i,-i+1,\ldots,i-1,i\}$$

fails to span all of $\mathbf{Z}_p$. Let $S=A$, unless the larger set $A\cup\{i+1\}$ also fails to span $\mathbf{Z}_p$, in which case we take the larger set for S. (For instance, we take $S=\{-2,-1,0,1,2,3\}$ when $p=11$. Although it does span $(p-1)/2=5$, it fails to span 7.) One can check this construction gives $|S|=c_p$, so that S achieves $w(\mathbf{Z}_p)$. Deleting 0 gives a set that achieves $e(\mathbf{Z}_p)$.

Regarding c_p, since

$$2(p-2)^{1/2}=(4p-8)^{1/2}\leqslant(4p-7)^{1/2},$$

we have

$$\lfloor 2(p-2)^{1/2}\rfloor\leqslant\lfloor(4p-7)^{1/2}\rfloor=c_p.$$

Further, equality holds here, unless $2(p-2)^{1/2}<c_p$, which means that

$$4p-8<c_p^2\leqslant 4p-7,$$

which is impossible, since modulo 8, $4p-7\equiv 5$ is not a quadratic residue. □

The proof of Dias da Silva and Hamidoune of Theorem 6 employed exterior algebra (Grassmann derivatives) and the representation theory of the symmetric group. We found a simpler proof that avoids representation theory, but we do not include it here, since a paper of Alon et al. [1] already appeared that includes a proof avoiding representation theory.

Then what can we say about groups of composite odd order? The previous version of the paper contained the conjecture that equality holds in Theorem 3 for $n>n_0(p)$. This we now confirm in light of the evidence recently brought to our attention by Gao and Hamidoune:

Theorem 8. *Let p be a prime. If $n>2p^2$ has smallest prime divisor p, then for any abelian group G of order n,*

$$w(G)=\frac{n}{p}+p-2\quad\textit{and}\quad e(G)=w(G)-1.$$

Further, these bounds are exceeded by at most one for smaller values of n.

Proof. We now go through the earlier results on the critical number and apply them to $w(G)$ and $e(G)$ to derive Theorem 8.

Besides obtaining the general lower bound that corresponds to our Theorem 3, Diderrich determined $e(G)$ to within one for groups of order a product of two primes:

Theorem 9 (Diderrich [3]). *Let G be an abelian group of order pq, where p, q are primes with $p \leqslant q$. Then*

$$p + q - 3 \leqslant e(G) \leqslant p + q - 2.$$

Moreover, if $q \geqslant 2p$, then $e(G) = p + q - 3$.

For $n = pq$ and $q > p$, the only possibility for G here is $\mathbf{Z}_{pq}$. For $q \geqslant 2p$, we see that $e(G)$ achieves its lower bound; The lower bound on $w(G)$ in Theorem 3 is one higher, so by Theorem 1, $w(G)$ also achieves its lower bound for these values. For $n = pq$ and $p \leqslant q < 2p$, Theorems 1, 3, and 9 imply that e and w are within one of their lower bounds.

For $p = q$, besides the cyclic group $\mathbf{Z}_{p^2}$, there is the group $G = \mathbf{Z}_p \oplus \mathbf{Z}_p$, which Mann and Wou considered for $p > 2$:

Theorem 10 (Mann and Wou [8]). *Let p be an odd prime. Then*

$$e(\mathbf{Z}_p \oplus \mathbf{Z}_p) = 2p - 3.$$

Applying this result, we find that for $\mathbf{Z}_p \oplus \mathbf{Z}_p$, it again holds that w and e equal their lower bounds.

Gao and Hamidoune made a major breakthrough on this problem in 1998 by resolving the case (conjectured by Diderrich) that n has three or more prime factors > 2:

Theorem 11 (Gao and Heilbronn [6]). *Let G be an abelian group of odd order n. Let p be the smallest prime divisor of n. Suppose n/p is composite. Then*

$$e(G) = (n/p) + p - 3.$$

Once again, the lower bounds on w and e are sharp for these groups. Theorem 8 now follows.

5. Further research

To complete the determination of $w(G)$ and $e(G)$, it remains to consider the case $G = \mathbf{Z}_{pq}$, where primes p, q satisfy $p \leqslant q < 2p$. The Even Groups Theorem 5 takes care of $p = 2$. Our lower bounds in Theorem 4, which exceed the bounds of Theorem 3 by one, are sharp, in view of Diderrich's upper bound in Theorem 9.

Theorem 12. *Let p, q be primes such that $2 < p \leqslant q \leqslant p + \lfloor 2\sqrt{p-2} \rfloor + 1$, and let $G = \mathbf{Z}_{pq}$. Then*

$$w(G) = p + q - 1 \quad \textit{and} \quad e(G) = p + q - 2.$$

For q above the threshold in Theorem 12, we still cannot pin down the exact values of w and e:

Theorem 13. *Let p, q be odd primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$, and let $G = \mathbf{Z}_{pq}$. Then*

$$p + q - 2 \leqslant w(G) \leqslant p + q - 1 \quad \textit{and} \quad p + q - 3 \leqslant e(G) \leqslant p + q - 2.$$

Only for the groups described in Theorem 13 do we not yet know the precise values of $w(G)$ and $e(G)$. In view of the relationship between $w(G)$ and $e(G)$ in Theorem 2, there are three possibilities left for each n in Theorem 13: Both parameters equal their lower bounds, both equal their upper bounds, or both equal $p + q - 2$. We suspect that the lower bounds are again sharp here, since the simple construction for small q that forces both to reach their upper bounds no longer works in the range described in Theorem 13.

Besides closing this gap, work is needed to determine the nonspanning sets $S \subseteq G$ which achieve $w(G)$ or $e(G)$.

Acknowledgements

Many people contributed to this long-running little project and several deserve to be co-authors. The author is particularly grateful to Barbara Flinn and Bjorn Poonen for a variety of essential ideas. Barb pointed out that Theorem 6 completely solves the Erdős–Heilbronn problem. Bjorn extended our solution for two-groups to the Even Groups Theorem 5. He noticed the general lower bound, Theorem 3, and he showed that it is not tight if $n = pq$ when p and q are twin primes. Bing Zhou pushed the argument further, which led us to formulate Theorem 4. Others who made suggestions or brought related work to our attention include Chih-Chang Ho, Christopher Malon, Vic Miller, Oren Patashnik, Herb Taylor, and Jared Wunsch. Finally, we thank George Diderrich, whose generous spirit encouraged us to persevere with the project.

References

[1] N. Alon, M.B. Nathanson, I. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56 (1996) 404–417.

[2] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (1994) 140–146.

[3] G.T. Diderrich, An addition theorem for abelian groups of order pq, J. Number Theory 7 (1975) 33–48.

[4] G.T. Diderrich, H.B. Mann, Combinatorial problems in finite abelian groups, in: J.N. Srivastava (Ed.), A Survey of Combinatorial Theory, North-Holland, Amsterdam, 1973, pp. 95–100.

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

[6] W. Gao, Y.O. Hamidoune, On additive bases, Acta Arith. 88 (1999) 233–237.

[7] R.K. Guy, Unsolved Problems in Number Theory, 2nd Edition, Springer, New York, 1994, pp. 129–130.

[8] H.B. Mann, Y.F. Wou, An addition theorem for the elementary Abelian group of type (p, p), Monatsh. Math. 102 (1986) 273–308.
[9] J.E. Olson, An addition theorem modulo p, J. Combin. Theory 5 (1968) 45–52.