ACTA ARITHMETICA
165.4 (2014)

Sum-dominant sets and restricted-sum-dominant sets in finite abelian groups

by

David B. Penman and Matthew D. Wells (Colchester)

1. Introduction. For a subset A of an abelian group G we define the *sumset*, *difference set* and *restricted sumset* of A with itself as

$$A + A = \{a_i + a_j : a_i, a_j \in A\},$$
$$A - A = \{a_i - a_j : a_i, a_j \in A\},$$
$$A \hat{+} A = \{a_i + a_j : a_i, a_j \in A \text{ and } a_i \neq a_j\}$$

respectively. Here we refer to sets A with $|A+A| > |A-A|$ as sum-dominant (some authors use the term MSTD, for *more sums than differences* sets). Though the fact that addition is commutative but subtraction usually is not might naively suggest that sum-dominant sets are rare if they exist at all, examples do exist and it is now known by Theorem 1 of [3], and the sharpened version of it which is Theorem 1.2 of [9], that a positive proportion of subsets of $\{0, 1, \ldots, n-1\}$ are sum-dominant.

Much of the study of sum-dominant sets has concerned subsets of the integers; however, the phenomenon in finite abelian groups has received some attention, notably from Hegarty [2], Nathanson [5] and Zhao [8]. The systematic study of restricted-sum-dominant sets in the integers was recently initiated in [6]; we are not aware of previous literature on restricted-sum-dominant sets in finite abelian groups.

Throughout this paper, G denotes a finite abelian group of order n. Following the practice of Nathanson and Zhao we write $\mathrm{MSTD}(G)$ for the collection of sum-dominant subsets of G; similarly $\mathrm{MRSTD}(G)$ denotes the corresponding collection of restricted-sum-dominant sets.

The paper is organised as follows. In Section 2 we detail the groups G which do not contain a sum-dominant set, and address the same issue for restricted-sum-dominant sets in Section 3. In Section 4 we list the groups G

2010 *Mathematics Subject Classification*: Primary 11B75.
Key words and phrases: sum-dominant set, restricted-sum-dominant set, finite abelian group.

DOI: 10.4064/aa165-4-6

for which $\mathrm{MSTD}(G) \neq \emptyset$, but $\mathrm{MRSTD}(G) = \emptyset$. We then show that all the remaining groups G contain restricted-sum-dominant sets: this process begins in Section 5 with a generalisation to restricted-sum-dominant sets of a result of Nathanson, which is then used in Section 6 to limit the cyclic groups of the form $\mathbb{Z}_m \times \mathbb{Z}_2$ with m odd which do not contain restricted-sum-dominant sets. Then powers of $\mathbb{Z}_{p^r}$ are considered in Section 7. The proof is finished off in Section 8.

In Section 9 we consider how much greater the sumset can be than the difference set in the context of a finite abelian group. The key functions here, for a subset A of the ambient group we are interested in, are

$$f(A) = \frac{\ln(|A+A|)}{\ln(|A-A|)} \quad \text{and} \quad g(A) = \frac{\ln(|A+A|/|A|)}{\ln(|A-A|/|A|)}.$$

It is known, by results of Freiman–Pigarev and Ruzsa (see e.g. [7, Chapter 6]) that for each finite subset A of an abelian group $3/4 \leq f(A) \leq 4/3$ and $1/2 \leq g(A) \leq 2$. In [6] we gave new record high values attained by both $f(A)$ and $g(A)$ in the integers; here we will show we can do slightly better in a finite cyclic group.

In Section 10 we give asymptotics for the number of restricted-sum-dominant sets in finite abelian groups, generalising results for sum-dominant sets due to Zhao [8]. Our arguments develop his and again follow slightly different lines for odd order and even order groups. We also extend his results on sum-dominant sets by weakening somewhat a condition. Finally, Section 11 contains a few remarks on future work.

Our main results are:

THEOREM 1.1. *The finite abelian groups which do not contain a sum-dominant set consist of all such groups of order less than* 12, $\mathbb{Z}_2^r$ *for all positive integers* r, $\mathbb{Z}_6 \times \mathbb{Z}_2$ *and* $\mathbb{Z}_{13}$. *All other finite abelian groups contain sum-dominant sets.*

THEOREM 1.2. *A finite abelian group* G *of odd order* n *contains restricted-sum-dominant sets if and only if* $n \geq 23$. *For even* n, *apart from* $\mathbb{Z}_2^r$ *for all positive integers* r, $\mathrm{MRSTD}(G) \neq \emptyset$ *for all* $n \geq 18$ *and* $\mathrm{MRSTD}(G) = \emptyset$ *for all* $n \leq 16$, *except for* $\mathbb{Z}_8 \times \mathbb{Z}_2$ *which does contain a restricted-sum-dominant set.*

Morever, a result on asymptotics of the number of restricted-sum-dominant sets is stated later. The proofs of Theorems 1.1 and 1.2 involve some computation, which we did with GAP; we thank Christopher Harden for advice on using GAP.

We will, unsurprisingly, make frequent use of the classification of finite abelian groups, which we quote below (see e.g. [1] for a proof).

THEOREM 1.3 (Fundamental theorem on finitely generated abelian groups). *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form*

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_t^{r_t}} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct. The direct product is unique except for possible rearrangement of the factors; that is, the number of factors is unique and the prime powers $p_i^{r_i}$ are unique.

We are concerned with finite abelian groups and so will be considering a direct product of cyclic groups of prime power order. Note also the obvious principle that if a subgroup of an abelian group contains a sum-dominant (respectively restricted-sum-dominant) set, then so does the larger group.

We often demonstrate that a particular group contains a sum-dominant set, or restricted-sum-dominant set, by giving an explicit example; we found most of these by hand, some from the explicit examples of sum-dominant sets in e.g. [2].

2. Finite abelian groups which do not contain sum-dominant sets. There are arbitrarily large finite abelian groups with no sum-dominant set.

LEMMA 2.1. *$\mathbb{Z}_2^r$ has no sum-dominant set.*

Proof. $A + A = A - A$ for each subset A of $\mathbb{Z}_2^r$. ∎

In [10] Zhao gives a table detailing $|\mathrm{MSTD}(\mathbb{Z}_n)|$ for all $n \le 25$. We have added corresponding figures for the number of restricted-sum-dominant sets, and checked all Zhao's calculations. (Note a typo in Zhao's table for $n = 20$: he gives 5400 sum-dominant sets but the correct figure is 5440).

Table 1. Small order cyclic groups

n	≤ 11	12	13	14	15	16	17	18
$\lvert\mathrm{MSTD}(\mathbb{Z}_n)\rvert$	0	24	0	28	60	384	272	792
$\lvert\mathrm{MRSTD}(\mathbb{Z}_n)\rvert$	0	0	0	0	0	0	0	108
n	19	20	21	22	23	24	25	
$\lvert\mathrm{MSTD}(\mathbb{Z}_n)\rvert$	1026	5440	4746	15224	15686	70632	56000	
$\lvert\mathrm{MRSTD}(\mathbb{Z}_n)\rvert$	0	520	0	3080	506	11712	3000	

It remains to confirm that $\mathrm{MSTD}(G) = \emptyset$ for all abelian G with $|G| \le 11$ by considering $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_3^2$. Computations show that $\mathrm{MSTD}(\mathbb{Z}_4 \times \mathbb{Z}_2) = \emptyset$.

Clearly a sum-dominant set A has $A - A \ne G$, i.e. $d \notin A - A$ for some $d \in G$, equivalently $A \cap (A+d) = \emptyset$, thus $|A| \le \lfloor n/2 \rfloor$ (see [7, Exercise 2.1.6]). For powers of $\mathbb{Z}_3$ we can do a little better by the following lemma.

LEMMA 2.2. *Every sum-dominant set $A \subset \mathbb{Z}_3^s$ has $|A| \leq 3^{s-1}$.*

Proof. If $A \subset \mathbb{Z}_3^s$ is a sum-dominant set, then $A - A \neq \mathbb{Z}_3^s$ so there is a subset $\{d, -d\} \subseteq \mathbb{Z}_3^s$ such that $\{d, -d\} \cap (A - A) = \emptyset$. Thus for each $a \in A$ we have $a + d \notin A - A$ and $a + 2d \notin A$. Suppose $a' \neq a$. Then $\{a, a+d, a+2d\} \cap \{a', a'+d, a'+2d\} = \emptyset$. Indeed, clearly $a + id \neq a' + id$ for $0 \leq i \leq 2$, and if $a + id = a' + jd$, where $0 \leq i \neq j \leq 2$, then $a' + (j-1)d = a$ with $(j-1)d = \pm d$, contradicting $\pm d \notin A - A$. Thus $\mathbb{Z}_3^s$ is partitioned into three-element sets and only one element of each such set can be in a sum-dominant set. ∎

COROLLARY 2.3. *The group $\mathbb{Z}_3^2$ contains no sum-dominant set.*

Proof. By Lemma 2.2 every sum-dominant set $A \subset \mathbb{Z}_3^2$ has $|A| \leq 3$. Since the property of being a sum-dominant set is invariant under translations, we can assume that $e = (0, 0) \in A$. The case $|A| = 1$ is trivial: if $A = \{e, a\}$ then $A + A = \{e, a, 2a\} = \{e, a, -a\} = A - A$. Finally, if $A = \{e, a, b\}$, then if $-a = b$ then $A + A = A - A$ so A is not sum-dominant. Otherwise $\{e, a, b, -a, -b\}$ are all distinct and $A + A = \{e, a, b, -a, -b, a + b\}$ attains its maximum possible order 6, i.e. A is a Sidon set. This is well-known to imply that all non-zero pairwise differences of A are also distinct so that $|A - A| = |A|^2 - |A| + 1 = 7 > 6$. ∎

An exhaustive computer search finds no sum-dominant sets in $\mathbb{Z}_6 \times \mathbb{Z}_2$. From Table 1, $\mathrm{MSTD}(\mathbb{Z}_{13}) = \emptyset$. We summarise the results of this section as

LEMMA 2.4. *$\mathbb{Z}_2^r$ for $r \geq 0$, $\mathbb{Z}_n$ for $n \leq 11$, $\mathbb{Z}_{13}$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_6 \times \mathbb{Z}_2$ and $\mathbb{Z}_3^2$ do not have any sum-dominant sets.*

3. Finite abelian groups with no restricted-sum-dominant subset

LEMMA 3.1.

(i) *For a finite abelian group G of odd order n, $\mathrm{MRSTD}(G) = \emptyset$ if $n < 23$.*
(ii) *For a finite abelian group G of even order, $\mathrm{MRSTD}(G) = \emptyset$ if $|G| \leq 16$, unless $G = \mathbb{Z}_8 \times \mathbb{Z}_2$.*

Proof. (i) We need, by Lemma 2.4, together with the obvious fact that $\mathrm{MRSTD}(G) \subseteq \mathrm{MSTD}(G)$, to prove that the abelian groups of order $n \in \{15, 17, 19, 21\}$ (which are all cyclic) have no restricted-sum-dominant set. This is again done by GAP computations, filtering out the diagonal to get restricted sumsets.

(ii) Again, using Lemma 2.4, this reduces to checking with GAP that $\mathbb{Z}_{12}$, $\mathbb{Z}_{14}$, $\mathbb{Z}_{16}$, $\mathbb{Z}_4^2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2^2$ have no restricted-sum-dominant set. ∎

We shall show in the next section that the lists in Lemmas 2.4 and 3.1 are exhaustive.

4. Groups which contain a sum-dominant set but no restricted-sum-dominant set

LEMMA 4.1. *Let* $G \in \{\mathbb{Z}_n\ (n \in \{12, 14, 15, 16, 17, 18, 19, 21\}),\ \mathbb{Z}_4^2,\ \mathbb{Z}_4 \times \mathbb{Z}_2^2\}$. *Then* $\mathrm{MSTD}(G) \neq \emptyset$ *but* $\mathrm{MRSTD}(G) = \emptyset$.

Proof. $\mathbb{Z}_{12}$ has the sum-dominant set $\{0, 1, 2, 4, 5, 9\}$, which has sumset $\mathbb{Z}_{12}$ but difference set missing 6. $\mathbb{Z}_{14}$ has a subset $\{0, 1, 4, 9, 10, 12, 13\}$, whose sumset is $\mathbb{Z}_{14}$ but whose difference set omits 7. $\mathbb{Z}_{15}$ has $\{0, 1, 2, 4, 5, 12\}$, which has sumset $\mathbb{Z}_{15} \setminus \{11\}$ but difference set omitting 6 and 9. $\mathbb{Z}_{16}$ has $\{0, 2, 3, 4, 7, 9, 13, 14\}$ with sumset $\mathbb{Z}_{16}$ but the difference set omitting 8. The set $\{0, 2, 4, 8, 9, 10, 15\} \subset \mathbb{Z}_{17}$ has sumset $\mathbb{Z}_{17} \setminus \{5\}$ but difference set $\mathbb{Z}_{17} \setminus \{3, 14\}$. Next $\{0, 1, 3, 4, 5, 6, 7, 10\} \subset \mathbb{Z}_{19}$ has sumset $\mathbb{Z}_{19} \setminus \{18\}$ but difference set $\mathbb{Z}_{19} \setminus \{8, 11\}$.

Furthermore $\{(0,0), (0,1), (1,2), (1,3), (2,0), (2,1), (3,0), (3,3)\} \subset \mathbb{Z}_4^2$ has sumset $\mathbb{Z}_4^2$ but difference set $\mathbb{Z}_4^2 \setminus (0,2)$. Also $\{(0,0,0), (1,0,1), (2,0,1), (3,0,0), (2,1,1), (1,1,0), (2,1,0), (3,1,1)\} \subset \mathbb{Z}_4 \times \mathbb{Z}_2^2$ has sumset $\mathbb{Z}_4 \times \mathbb{Z}_2^2$, but its difference set is $\mathbb{Z}_4 \times \mathbb{Z}_2^2 \setminus (2,0,0)$.

The second part of the claim was proved in Lemma 3.1. ∎

5. Restricted-sum-dominant sets in $\mathbb{Z}_m \times \mathbb{Z}_2$. In [5] Nathanson shows that $\mathbb{Z}_m \times \mathbb{Z}_2$ has sum-dominant sets for all odd $n \geq 7$ and all even $n \geq 10$. We modify his argument to obtain an analogous result for restricted-sum-dominant subsets of $\mathbb{Z}_m \times \mathbb{Z}_2$, which may be of independent interest. This result will be used in the next section to restrict the possible finite cyclic groups with no restricted-sum-dominant set.

THEOREM 5.1. *Let Ω be the set of subsets $A \subseteq \mathbb{Z}_m \times \mathbb{Z}_2$ with the property that, for each $a \in \mathbb{Z}_m$, at most one of $(a,0)$ and $(a,1)$ can be in A. Let $\hat{\Psi}(\mathbb{Z}_m \times \mathbb{Z}_2)$ denote the number of sets $A \in \Omega$ such that $A \hat{+} A = \mathbb{Z}_m \times \mathbb{Z}_2$. Then, writing $G = \mathbb{Z}_m \times \mathbb{Z}_2$, we have*

$$\hat{\Psi}(G) \geq \begin{cases} 2^m(1 - 2\sqrt{2}\, m/2^{m/2}) & \text{if } m \text{ is odd,} \\ 2^m(1 - 3m/2^{m/2}) & \text{if } m \text{ is even.} \end{cases}$$

Proof. Let $g = (b, \delta) \in G$ and $\hat{\phi}(g) = |\{A \in \Omega : g \notin A \hat{+} A\}|$. Then

$$|\Omega| - \hat{\Psi}(G) \leq \sum_{g \in G} \hat{\phi}(g). \tag{1}$$

If m is odd, then for $\delta = 1$ we can only obtain g as a sum of distinct elements of G and so we use the same argument as Nathanson (see [5, pp. 22–23]): Since $\gcd(m, 2) = 1$ there is a unique solution $a_0 \in \mathbb{Z}_m$ to the congruence

$2a_0 \equiv b \pmod m$, however $g = (b,1) \neq (a_0,\epsilon_0) + (a_0,\epsilon_0)$ as $\epsilon_0 + \epsilon_0 = 0$. The elements of $\mathbb{Z}_m \setminus a_0$ can be partitioned into $(m-1)/2$ disjoint pairs $\{a_j, b-a_j\}$ with $a_j \neq b - a_j$ which sum to b. Now, let $A \in \Omega$ be defined by

$$A = \{(a_j,\epsilon_j)\}_{j=0}^{(m-1)/2} \cup \{(b-a_j,\epsilon'_j)\}_{j=1}^{(m-1)/2} \tag{2}$$

where $\{\epsilon_j\}_{j=0}^{(m-1)/2}$ is an arbitrary sequence of 0's and 1's. Fixing $\epsilon'_j = \epsilon_j$ for all $j \in [1,(m-1)/2]$ we have $g \notin A + A$, and since $\delta = 1$ here this is equivalent to $g \notin A \hat{+} A$.

To count such sets A, note A comprises the singleton (a_0,ϵ_0) together with $(m-1)/2$ pairs of elements with their second coordinates dependent on each other and $\{\epsilon_j\}_{j=0}^{(m+1)/2}$ ranging over all possible sequences of 0's and 1's. Thus there are $2^{(m+1)/2}$ such sets A and so $\hat{\phi}(g) = 2^{(m+1)/2}$.

The next case (still with m odd) is $\delta = 0$. Here again the unique $a_0 \in \mathbb{Z}_m$ satisfying $2a_0 \equiv b \pmod m$ will give $g = (b,0) = (a_0,\epsilon_0) + (a_0,\epsilon_0) \in A + A$; of course this is not a restricted sum. Further consider the set A defined by (2) with $\epsilon'_j = \epsilon_j + 1 \pmod 2$ for all $j \in [1,(m-1)/2]$. In this case we see that $g \notin A \hat{+} A$. Again A consists of $(m-1)/2$ pairs of elements with second coordinates dependent on each other together with a singleton (a_0,ϵ_0) and therefore $\hat{\phi}(g) = 2^{(m-1)/2}$.

There are m elements $g \in G$ with $\delta = 1$ and m with $\delta = 0$, thus

$$\sum_{g \in G} \hat{\phi}(g) = 2m2^{(m+1)/2}.$$

Hence applying (1) we have

$$\hat{\Psi}(G) \geq 2^m - 2m2^{(m+1)/2} = 2^m\left(1 - \frac{2\sqrt{2}\,m}{2^{m/2}}\right)$$

when m is odd.

We now deal with m even, splitting into the cases of b odd and b even. If b is odd then the congruence $2a_0 \equiv b \pmod m$ has no solution and we can only obtain g from a sum of distinct elements of A. Thus $\mathbb{Z}_m$ partitions into $m/2$ pairs which sum to b. There are exactly m elements in G with odd b, so

$$\sum_{\substack{g \in G \\ b\,\text{odd}}} \hat{\phi}(g) = m2^{m/2}.$$

On the other hand if b is even then the congruence $2a_0 \equiv b \pmod m$ has two solutions, a_0 and $a_0 + m/2$, in $\mathbb{Z}_m$. When $\delta = 1$, again $\mathbb{Z}_m \setminus \{a_0, a_0 + m/2\}$ can be partitioned into $(m-2)/2$ pairs of elements which sum to b. Defining the set A to have the form

$$A = \{(a_j,\epsilon_j)\}_{j=0}^{(m-2)/2} \cup \{(b-a_j,\epsilon'_j)\}_{j=0}^{(m-2)/2} \tag{3}$$

and setting $\epsilon'_j = \epsilon_j$ for all $j \in [1,(m-2)/2]$ we have $g \notin A \hat{+} A$. With two singletons and $(m-2)/2$ pairs of elements with their second coordinates dependent on each other we get $\hat{\phi}(g) = 2^{(m+2)/2}$.

For $\delta = 0$ neither the element of G with first co-ordinate a_0 nor the one with first co-ordinate $a_0 + m/2$ gives (b,δ) as a restricted sum. Setting $\epsilon'_j = \epsilon_j + 1 \pmod m$ for all $j \in [1,(m-2)/2]$ in the set A given by (3) we have $g \notin A \hat{+} A$ and thus $\hat{\phi}(g) = 2^{(m+2)/2}$ here as well. Since G contains m elements with b even, we have

$$\sum_{\substack{g\in G\\ b\,\text{even}}} \hat{\phi}(g) = m2^{(m+2)/2} = 2m2^{m/2}.$$

Overall,

$$\sum_{g\in G} \hat{\phi}(g) = 3m2^{m/2}$$

and hence when m is even,

$$\hat{\Psi}(G) \ge |\Omega| - \sum_{g\in G} \hat{\phi}(g) = 2^m\biggl(1 - \frac{3m}{2^{m/2}}\biggr).$$

This completes the proof of Theorem 5.1. ∎

When m is odd, the bound in Theorem 5.1 yields a positive lower bound on $\hat{\Psi}(G)$ when $m \ge 11$ (compare Nathanson's lower bound on sum-dominant sets being positive for odd $m \ge 7$): for even m it works for $m \ge 10$ (which is also when Nathanson's sum-dominant set bound becomes positive for even m). The bound here is more explicit than the precise asymptotics we shall prove in Section 10 for large n.

COROLLARY 5.2. MRSTD$(\mathbb{Z}_m \times \mathbb{Z}_2) \ne \emptyset$ *if and only if* $m \ge 8$.

Proof. By Theorem 5.1, MRSTD$(\mathbb{Z}_m \times \mathbb{Z}_2) \ne \emptyset$ for $m \ge 10$. If $m = 8$, then $\{(0,0),(1,0),(1,1),(2,0),(2,1),(4,0),(7,0),(7,1)\}$ has restricted sumset $\mathbb{Z}_8 \times \mathbb{Z}_2$ whilst the difference set is missing $(4,1)$. We have already noted $\mathbb{Z}_9 \times \mathbb{Z}_2 \cong \mathbb{Z}_{18}$ contains a restricted-sum-dominant set (see Table 1). On the other hand we confirmed MSTD$(\mathbb{Z}_m \times \mathbb{Z}_2) = \emptyset$ for $m \le 6$ in Section 2 and none of the sum-dominant sets in $\mathbb{Z}_{14}$ is a restricted-sum-dominant set. ∎

6. Restricted-sum-dominant subsets of cyclic groups. To start proving that all the remaining finite abelian groups do contain a restricted-sum-dominant set, we show that MRSTD$(\mathbb{Z}_n) \ne \emptyset$ for all even $n \ge 18$ and for all odd $n \ge 23$. In Table 2 below, which exhibits some examples,

$$M = \{0,1,2,4,7,8,12,14,15\}, \qquad M_1 = \{0,1,2,4,7,8,12,14,15,18,19,20\}.$$

The restricted-sum-dominant subset of $\mathbb{Z}$ with the least diameter we know of is $M_2 = \{0,1,2,4,7,8,12,15,18,19,23,25,26,29,30,31\}$, which has

Table 2. Restricted-sum-dominant sets in $\mathbb{Z}_n$

n	Example set	$A \hat{+} A$	$A - A$
18	M	$\mathbb{Z}_{18}$	$\mathbb{Z}_{18} \setminus \{9\}$
20	$\{0,1,2,4,7,8,13,16,19\}$	$\mathbb{Z}_{20}$	$\mathbb{Z}_{20} \setminus \{10\}$
23	$\{0,2,3,4,7,9,13,14,16,20\}$	$\mathbb{Z}_{23} \setminus \{8\}$	$\mathbb{Z}_{23} \setminus \{8,15\}$
24	$\{0,1,2,4,7,8,11,15,17,18,21\}$	$\mathbb{Z}_{24}$	$\mathbb{Z}_{24} \setminus \{12\}$
25	$\{0,1,2,4,7,8,12,14,15,22\}$	$\mathbb{Z}_{25} \setminus \{0\}$	$\mathbb{Z}_{25} \setminus \{9,16\}$
27	$\{0,1,2,4,5,9,12,13,14,16,17,24\}$	$\mathbb{Z}_{27} \setminus \{8\}$	$\mathbb{Z}_{27} \setminus \{6,21\}$
28	$\{0,1,2,4,7,8,12,14,15,18,22\}$	$\mathbb{Z}_{28} \setminus \{0\}$	$\mathbb{Z}_{28} \setminus \{9,19\}$
29	$M_2 \setminus \{29,30,31\}$	$\mathbb{Z}_{29}$	$\mathbb{Z}_{29} \setminus \{9,20\}$
31	M_1	$\mathbb{Z}_{31}$	$\mathbb{Z}_{31} \setminus \{9,22\}$
32	$\{0,1,2,4,7,8,12,14,15,19,22,26,29\}$	$\mathbb{Z}_{32} \setminus \{0,25\}$	$\mathbb{Z}_{32} \setminus \{9,16,23\}$
33	$M_1 \cup \{22\}$	$\mathbb{Z}_{33}$	$\mathbb{Z}_{33} \setminus \{9,24\}$
35	$M_1 \cup \{22\}$	$\mathbb{Z}_{35}$	$\mathbb{Z}_{35} \setminus \{9,26\}$
36	$M \cup \{18,19,20,25,26,30,32,33\}$	$\mathbb{Z}_{36}$	$\mathbb{Z}_{36} \setminus \{9,27\}$
37	$M_1 \cup \{22\}$	$\mathbb{Z}_{37}$	$\mathbb{Z}_{37} \setminus \{9,28\}$
39	$M_1 \cup \{22\}$	$\mathbb{Z}_{39}$	$\mathbb{Z}_{39} \setminus \{9,30\}$

$M_2 \hat{+} M_2 = [1,61] \setminus \{58\}$ and $M_2 - M_2 = [-31,31] \setminus \{\pm 9, \pm 20\}$. For all $n \geq 63$, M_2 is clearly a restricted-sum-dominant subset of $\mathbb{Z}_n$. In fact M_2 is a restricted-sum-dominant subset of $\mathbb{Z}_n$ for all $n \geq 40$. This is because clearly $M_2 \hat{+} M_2 = \mathbb{Z}_n$ for all $n \in [40,57]$; modulo 58, $M_2 \hat{+} M_2 = \mathbb{Z}_{58} \setminus \{0\}$; for $n \in [59,61]$, $M_2 \hat{+} M_2 = \mathbb{Z}_n \setminus \{58\}$; and modulo 62, $M_2 \hat{+} M_2 = \mathbb{Z}_{62} \setminus \{0,58\}$. On the other hand, modulo 40, $M_2 - M_2$ omits 20; for $n \in [41,51]$, $M_2 - M_2 \cap \{\pm 9\} = \emptyset$; and for $n \in [52,62]$, $M_2 - M_2 \cap \{\pm 9 \pm 20\} = \emptyset$.

The remaining cases are covered by Table 2. However, by Lemma 4.1, $\mathrm{MRSTD}(\mathbb{Z}_{19}) = \emptyset$ and $\mathrm{MRSTD}(\mathbb{Z}_{21}) = \emptyset$ whilst $\mathrm{MRSTD}(\mathbb{Z}_n) \neq \emptyset$ for $n \in \{22,26,30,34,38\}$ by Corollary 5.2. Thus

Corollary 6.1. *The cyclic groups of prime power order which can appear as direct factors of a finite abelian group G for which $\mathrm{MRSTD}(G) = \emptyset$ are restricted to the groups $\mathbb{Z}_n$ with $n \in \{2,3,4,5,7,8,9,11,13,16,17,19\}$.*

7. Restricted-sum-dominant sets in $\mathbb{Z}_{p^r}^2$. We now consider how many times each of the factors in Corollary 6.1 can be repeated. Here we have the following examples: For $\mathbb{Z}_5^2$ the set

$$\{(0,0),(1,1),(4,2),(1,3),(3,4),(2,0),(3,1),(1,2),(4,3),(1,4)\}$$

has restricted sumset $\mathbb{Z}_5^2$ but difference set $\mathbb{Z}_5^2 \setminus \{(1,0),(4,0)\}$. For $\mathbb{Z}_7^2$ the set

$$\{(0,0),(2,0),(4,0),(0,1),(2,1),(5,1),(1,2),(4,2),(6,2),$$
$$(1,3),(4,3),(0,4),(4,4),(4,5),(6,5),(0,6),(3,6),(5,6)\}$$

has restricted sumset $\mathbb{Z}_7^2$ but difference set $\mathbb{Z}_7^2 \setminus \{(1,0),(6,0)\}$. For $\mathbb{Z}_{11}$ let $A_{11} = \{0,2,4,7,9\}$. We then consider

$$A_{11} \times A_{11} \cup \{(0,3),(1,0),(3,4),(4,1),(7,8),(10,7)\},$$

which has restricted sumset $\mathbb{Z}_{11}^2 \setminus \{(1,1),(1,10)\}$ and difference set $\mathbb{Z}_{11}^2 \setminus \{(1,1),(1,10),(10,1),(10,10)\}$. Similarly let $A_{13} = \{0,2,4,6,8,11\}$. Then

$$A_{13} \times A_{13} \cup \{(5,11),(8,12),(11,3),(11,12),(12,6),(12,8)\}$$

has restricted sumset $\mathbb{Z}_{13}^2 \setminus \{(5,5),(5,7)\}$ whilst the difference set is $\mathbb{Z}_{13}^2 \setminus \{(1,1),(1,12),(12,1),(12,12)\}$.

For $A_8' = \{0,2,4,8,9,10,15\} \subset \mathbb{Z}_{17}$, $A_8' + A_8' = \mathbb{Z}_{17} \setminus \{5\}$, $A_8' \hat{+} A_8' = \mathbb{Z}_{17} \setminus \{3,5,16\}$ and $A_8' - A_8' = \mathbb{Z}_{17} \setminus \{3,14\}$. The sumset of $A_8' \times A_8'$ comprises all $\mathbb{Z}_{17}^2$ except the ordered pairs containing 5, whilst the difference set is missing the ordered pairs which contain 3 or 14. These sets have order 256 and 225 respectively. Apart from $\{(3,3),(3,16),(16,3),(16,16)\}$ the restricted sumset contains all elements of the sumset, therefore $A_8' \times A_8'$ is a restricted-sum-dominant set in $\mathbb{Z}_{17}^2$. Similarly for $A_{19} = \{0,1,4,5,6,7,8,12\} \subset \mathbb{Z}_{19}$, with $A_{19} + A_{19} = \mathbb{Z}_{19} \setminus \{3\}$, $A_{19} \hat{+} A_{19} = \mathbb{Z}_{19} \setminus \{2,3\}$ and $A_{19} - A_{19} = \mathbb{Z}_{19} \setminus \{9,10\}$, $A_{19} \times A_{19}$ is a restricted-sum-dominant set in $\mathbb{Z}_{19}^2$.

Neither $\mathbb{Z}_3^2$ nor $\mathbb{Z}_4^2$ contains restricted-sum-dominant sets. In $\mathbb{Z}_3^3$, $\{(0,0,0),(0,1,0),(0,2,0),(1,0,0),(1,1,1),(1,2,2),(2,0,2),(2,1,1),(2,2,0)\}$ has restricted sumset $\mathbb{Z}_3^3$ but the difference set is missing $(0,0,1)$ and $(0,0,2)$. The restricted sumset of $\{(0,0,0),(0,1,0),(0,2,0),(0,3,1),(1,0,0),(1,1,1),(1,3,0),(2,0,0),(2,1,0),(2,2,1),(3,3,1)\} \subset \mathbb{Z}_4^2 \times \mathbb{Z}_2$ is $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ whilst its difference set omits $(0,0,1)$. This of course also gives a restricted-sum-dominant set in $\mathbb{Z}_4^3$. We summarise this as

COROLLARY 7.1. *$\mathbb{Z}_p^2$ has a restricted-sum-dominant set if and only if $p \geq 5$. Also $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3^3$ have restricted-sum-dominant sets.*

8. Remaining cases. The problem is now reduced to considering a direct product of the form $G_1 \times \cdots \times G_s$ where the G_i are taken from

$$\{\mathbb{Z}_2^r, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_8, \mathbb{Z}_3^2, \mathbb{Z}_9, \mathbb{Z}_{11}, \mathbb{Z}_{13}, \mathbb{Z}_4^2, \mathbb{Z}_{16}, \mathbb{Z}_{17}, \mathbb{Z}_{19}\}. \tag{4}$$

The idea now is for each G_i to work through the possible products with other $G_j, G_k, \ldots$ in (4) forming the finite abelian groups and verifying they contain restricted-sum-dominant sets. (We only consider groups of even order $n \geq 18$ and odd order $n \geq 23$ and we go through the list from left to right.)

Firstly we determine the r for which $\mathrm{MRSTD}(\mathbb{Z}_2^r \times G_i) \neq \emptyset$. By Corollary 5.2, $\mathbb{Z}_m \times \mathbb{Z}_2$ contains a restricted-sum-dominant set if and only if $m \geq 8$. From Section 7, $\mathrm{MRSTD}(\mathbb{Z}_4^2 \times \mathbb{Z}_2) \neq \emptyset$. Also $\mathrm{MRSTD}(\mathbb{Z}_2 \times \mathbb{Z}_3^2) \neq \emptyset$: the set $\{(0,0,0),(1,0,1)(2,0,0)(0,1,0),(1,1,0),(2,1,1),(0,2,0),(1,2,1),(2,2,0)\}$ has restricted sumset equal to $\mathbb{Z}_3^2 \times \mathbb{Z}_2$, but the difference set omits $(0,0,1)$.

Next we consider the G_i for which we must go to a second power of $\mathbb{Z}_2$. Since $\mathbb{Z}_5 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_{10} \times \mathbb{Z}_2$ and $\mathbb{Z}_7 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_{14} \times \mathbb{Z}_2$ it follows by Theorem 5.1 that $\mathrm{MRSTD}(\mathbb{Z}_5 \times \mathbb{Z}_2^2) \neq \emptyset$ and $\mathrm{MRSTD}(\mathbb{Z}_7 \times \mathbb{Z}_2^2) \neq \emptyset$.

We get a restricted-sum-dominant set $\{(0,0,0), (1,0,0), (2,0,0), (0,0,1), (4,0,1), (2,0,1), (0,1,0), (4,1,0), (5,1,0), (3,1,1)\} \subset \mathbb{Z}_6 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2^3$: the restricted sumset is equal to the entire group whilst the difference set is missing $(3,0,0)$. An example of a restricted-sum-dominant set in $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ is $\{(0,0,0,0), (0,0,1,0), (0,1,0,0), (0,1,1,1), (1,0,0,1), (1,0,1,0), (1,1,0,1), (1,1,1,0), (2,0,0,0), (2,0,1,0), (2,1,0,1), (2,1,1,0), (3,0,0,0), (3,0,1,0)\}$ with restricted sumset $\mathbb{Z}_4 \times \mathbb{Z}_2^3$ whilst the difference set omits $(0,0,0,1)$.

This covers products with $\mathbb{Z}_2^r$; we now focus on the remaining products with $\mathbb{Z}_3$. In $\mathbb{Z}_9 \times \mathbb{Z}_3$, $\{(0,0), (1,0), (2,1), (3,2), (4,0), (5,2), (6,1), (7,0), (8,0)\}$ has restricted sumset $\mathbb{Z}_9 \times \mathbb{Z}_3$ but the difference set omits $(0,1)$ and $(0,2)$. We saw earlier that $\mathbb{Z}_r \times \mathbb{Z}_3$ has no restricted-sum-dominant set for $r = 5, 7$. For $r = 6$, $\mathbb{Z}_6 \times \mathbb{Z}_3$ has a restricted-sum-dominant set by the above. For even $r \geq 8$, $\mathbb{Z}_r \times \mathbb{Z}_3$ has a restricted-sum-dominant set by Corollary 6.1.

Since $\mathrm{MRSTD}(\mathbb{Z}_{12} \times \mathbb{Z}_2) \neq \emptyset$ and $\mathbb{Z}_3 \times \mathbb{Z}_4^2 \cong \mathbb{Z}_{12} \times \mathbb{Z}_4$ it follows that $\mathrm{MRSTD}(\mathbb{Z}_4^2 \times \mathbb{Z}_3) \neq \emptyset$. The remaining products of $\mathbb{Z}_3$ with other groups in (4) are isomorphic to cyclic groups which we have already dealt with or have smaller order than we are concerned with here.

For products with $\mathbb{Z}_4$, since $\mathbb{Z}_8 \times \mathbb{Z}_2$ has a restricted-sum-dominant set it follows that $\mathbb{Z}_8 \times \mathbb{Z}_4$ and $\mathbb{Z}_{16} \times \mathbb{Z}_4$ also contain restricted-sum-dominant sets. All remaining products with $\mathbb{Z}_4$ have a subgroup with a restricted-sum-dominant set or have smaller order than we are concerned with here.

For products with $\mathbb{Z}_5$, the only case not covered by earlier results is $\mathbb{Z}_{15} \times \mathbb{Z}_3$: the set $\{(0,0), (1,0), (2,1), (3,2), (4,1), (5,0), (6,2), (7,1), (8,0), (9,0), (10,0), (11,0), (14,0)\}$ has restricted sumset $\mathbb{Z}_{15} \times \mathbb{Z}_3 \setminus \{(10,2)\}$ but the difference set is missing $\{(0,1), (0,2)\}$.

For products with $\mathbb{Z}_7$, the only case still to consider is $\mathbb{Z}_7 \times \mathbb{Z}_3^2 \cong \mathbb{Z}_{21} \times \mathbb{Z}_3$. Here $\{(0,0), (1,0), (2,0), (3,1), (4,2), (5,2), (6,1), (7,0), (8,2), (9,0), (11,1), (13,1), (14,2), (15,2)(16,1), (18,2), (19,1), (20,1)\}$ has $\{(0,1), (0,2)\}$ missing from the difference set whilst the restricted sumset is equal to $\mathbb{Z}_{21} \times \mathbb{Z}_3$.

For products with $\mathbb{Z}_8$, we saw above that $\mathbb{Z}_8 \times \mathbb{Z}_5$ has a restricted-sum-dominant set. $\mathbb{Z}_8 \times \mathbb{Z}_9$ has a subgroup $\mathbb{Z}_8 \times \mathbb{Z}_3$, which has a restricted-sum-dominant set; all remaining products with $\mathbb{Z}_8$ are covered by earlier results.

For $\mathbb{Z}_3^2$, there is a restricted-sum-dominant set in $\mathbb{Z}_9 \times \mathbb{Z}_3$ and in $\mathbb{Z}_{11} \times \mathbb{Z}_3 \cong \mathbb{Z}_{33}$. Similarly $\mathbb{Z}_3 \times \mathbb{Z}_{13}$ has such a set, $\mathbb{Z}_4^2 \times \mathbb{Z}_3$ was considered under products with $\mathbb{Z}_3$ and the remaining three cases are covered by Table 2.

The products with $\mathbb{Z}_9$, or groups beyond it in the list, will all contain large cyclic groups which have restricted-sum-dominant sets by Table 2 or earlier observations. This completes the proof of Theorems 1.1 and 1.2.

9. How much larger can the sumset be? In [6] we addressed the issue of finding finite sets $A \subseteq \mathbb{Z}$ for which $f(A) = \ln(|A+A|)/\ln(|A-A|)$ is large, obtaining a new record high value of this function, and similarly for $g(A) = \ln(|A+A|/|A|)/\ln(|A-A|/|A|)$. (The approximate values of these records are $f(Q_{10}) = 1.030597781\ldots$ and $g(Q_j) = 1.1259444\ldots$ for large enough j, for a certain sequence (Q_j) of sets of integers.) It was not immediately obvious to us whether it would be easier or harder to find large values of the functions analogous to f and g when A is taken from a finite abelian group rather than the integers: we do, however, show that we can get a slightly higher value of f and g by considering the reduction of Q_j modulo a suitable integer.

THEOREM 9.1. *Let $n = 4(4(j+1)+3) = 16j+28$ and define $Q'_j \subset \mathbb{Z}_n$ by*

$$\begin{aligned} Q'_j = \{0,2,4,12\} &\cup \{1,5,\ldots,1+4(4(j+1)+2)\} \\ &\cup \{24,40,\ldots,8+16j\} \cup \{4(4(j+1)+1)\}. \end{aligned}$$

Then for $j \geq 3$, $Q'_j \hat{+} Q'_j = \mathbb{Z}_n \setminus \{0,8\}$, $Q'_j + Q'_j = \mathbb{Z}_n$ and $Q'_j - Q'_j = \mathbb{Z}_n \setminus D_j$ where D_j is the set

$$\{6\} \cup \{14,\ldots,14+16j\} \cup \{18,\ldots,2+16j\} \cup \{26,\ldots,10+16j\} \cup \{16j+22\}.$$

Proof. We begin with the restricted sumset which contains the right hand sides of

$$\begin{aligned} \{0\} \hat{+} \{1,5,\ldots,4(4(j+1)+2)+1\} &= \{1,5,\ldots,4(4(j+1)+2)+1\}, \\ \{1\} \hat{+} \{1,5,\ldots,4((4j+1)+2)+1\} &= \{6,10,\ldots,4(4(j+1)+2)+2\}, \\ \{2\} \hat{+} \{1,5,\ldots,4(4(j+1)+2)+1)\} &= \{3,7,\ldots,4(4(j+1)+2)+3\} \end{aligned}$$

and also $2 = 0+2$. All that remains is to show $Q'_j \hat{+} Q'_j$ contains the claimed multiples of four. Now

$$\begin{aligned} Q'_j \hat{+} Q'_j &\supset \{0,4,12\} + \{24,40,\ldots,8+16j\} \\ &= \{24,28,\ldots,4(4(j+1)+1)\} \setminus \{32,48,\ldots,16(j+1)\} \end{aligned}$$

and noting that $4(4(j+1)+1) \equiv -8 \pmod{4(4(j+1)+3)}$ we have

$$\{24,40,\ldots,8+16j\} - 8 = \{16,32,\ldots,16j\} \subset Q'_j \hat{+} Q'_j.$$

We also have $\{0\} \hat{+} \{4,12,4(4(j+1)+1)\} = \{4,12,4(4(j+1)+1)\} \in Q'_j \hat{+} Q'_j$. We now have all elements claimed for $Q'_j \hat{+} Q'_j$, except for 20 and $16(j+1)$. To deal with these, note that since $8+16j \equiv -20 \pmod{4(4(j+1)+3)}$, we have $40 + (8+16j) = 20$, and also $24 + (8+16(j-1)) = 16(j+1)$: these are both sums of distinct elements of Q'_j, provided $j \geq 3$.

It is easy to check that 0 and 8 are not elements of $Q'_j \hat{+} Q'_j$. This completes the argument for the restricted sumset. However $0 = 0+0$ and $8 = 4+4$ are in the sumset.

Finally, we consider the difference set. Recall that we claim $Q'_j - Q'_j = \mathbb{Z}_n \setminus D_j$. Write $Q'_j = Q_{\text{odd}} \cup Q_{\text{even}}$ where $Q_{\text{odd}} = \{1, 5, \ldots, 1+4(4(j+1)+2)\}$ and $Q_{\text{even}} = \{0, 2, 4, 12\} \cup \{24, 40, \ldots, 8 + 16j\} \cup \{4(4(j+1)+1)\}$. Firstly $Q_{\text{odd}} - Q_{\text{odd}} = \{0, 4, \ldots, 4(4(j+1)+2)\}$, confirming that $Q'_j - Q'_j$ contains all the multiples of 4 we claim. On the other hand,

$$\begin{aligned} Q_{\text{even}} - Q_{\text{even}} \supseteq\ & \{0, 16, \ldots, 16(j-1)\} \cup \{16(j+1)\} \cup \{2\} \\ & \cup \{4, 20, \ldots, 4 + 16(j+1)\} \cup \{22, 38, \ldots, 6 + 16j\} \\ & \cup \{8, 24, \ldots, 8 + 16(j+1)\} \cup \{10, 10 + 16(j+1)\} \\ & \cup \{12, 28, \ldots, 12 + 16(j-1)\}. \end{aligned}$$

It is easy to notice that 6 and the arithmetic progression $\{14, 30, \ldots$ $\ldots, 14 + 16j\}$ are not in $Q_{\text{even}} - Q_{\text{even}}$ using congruence considerations. Similarly no element of $\{18, 34, \ldots, 2 + 16j\}$ or $\{26, 42, \ldots, 10 + 16j\}$ is a difference, and $16j+22$ is not in $Q_j - Q_j$ either. Thus the containment above is actually an equality.

From the union of $Q_{\text{odd}} - Q_{\text{odd}}$ and $Q_{\text{even}} - Q_{\text{even}}$, $Q'_j - Q'_j$ contains precisely the even elements claimed. For the odd elements we have

$$\begin{aligned} &\{1, 5, \ldots, 4(4(j+1)+2)+1\} \cup \{3, 7, \ldots, 4(4(j+1)+2)+3\} \\ &\qquad = \{1, 5, \ldots, 1 + 4(4(j+1)+2)\} - \{0, 2\} \subset Q'_j - Q'_j. \ \blacksquare \end{aligned}$$

COROLLARY 9.2. *Q'_j as defined above has $|Q'_j| = 5j + 12$. Moreover*

$$|Q'_j \hat{+} Q'_j| = 16j + 26 \quad \textit{for } j \geq 3, \qquad |Q'_j + Q'_j| = 16j + 28 \quad \textit{for } j \geq 2,$$
$$|Q'_j - Q'_j| = 13j + 25 \quad \textit{for } j \geq 1.$$

For $j = 1$,

$$Q'_1 = \{0, 1, 2, 4, 5, 9, 12, 13, 17, 21, 24, 25, 29, 33, 36, 37, 41\}$$

of order 17 has $Q'_1 \hat{+} Q'_1 = \mathbb{Z}_{44} \setminus \{0.8.20, 32\}$, $Q'_1 + Q'_1 = \mathbb{Z}_{44} \setminus \{20, 32\}$ and $Q'_1 - Q'_1 = \mathbb{Z}_{44} \setminus \{6, 14, 18, 26, 30, 38\}$. For $j = 2$,

$$Q'_2 = \{0, 1, 2, 4, 5, 9, 12, 13, 17, 21, 24, 25, 29, 33, 37, 40, 41, 45, 49, 52, 53, 57\}$$

of order 22 has $Q'_2 \hat{+} Q'_2 = \mathbb{Z}_{60} \setminus \{0, 8, 20, 48\}$, $Q'_2 + Q'_2 = \mathbb{Z}_{60}$ and $Q'_2 - Q'_2 = \mathbb{Z}_{60} \setminus \{6, 14, 18, 26, 30, 34, 42, 46, 54\}$.

Proof. For $j \geq 3$ these claims are immediate consequences of Theorem 9.1. For $j = 1$ and 2 they are simple computational checks (note that the argument for the difference set works for all $j \geq 1$). ∎

REMARK 9.3. Here $f(Q'_j)$ peaks for $j = 2$ at $\ln 60/\ln 51 = 1.041334216\ldots$, and with $|Q'_j| = 5j + 12$, as $j \to \infty$ we have $g(Q'_j) \to \ln(16/5)/\ln(13/5) = 1.212307041\ldots$. The analogous quantity for the restricted sumset, $\hat{f}(A) = \ln|A \hat{+} A|/\ln|A - A|$, peaks for $j = 7$ when $\hat{f}(Q'_j) = 1.036533123\ldots$. This is also higher than the corresponding figure we obtained for $A \subset \mathbb{Z}$ in [6].

10. Asymptotics for $|\mathrm{MRSTD}(G)|$

10.1. Introduction. The main aim of this section is to give asymptotics for the number of restricted-sum-dominant sets in finite abelian groups under mild conditions on the number of elements of small order in the group. We also slightly extend a result on the number of sum-dominant sets in a finite abelian group of even order due to Zhao [8] by weakening a hypothesis in it. Many of our arguments are straightforward modifications of those of Zhao. The two main results are, with $f_n \sim g_n$ denoting that $f_n/g_n \to 1$ as $n \to \infty$:

THEOREM 10.1. *Let $\{G_n\}$ be a sequence of finite abelian groups with $|G_n| \to \infty$.*

(i) (Even case) *If $\limsup_{n\to\infty} k_n/|G_n| < 1/2$, where G_n has $k_n > 0$ elements of order 2, then*

$$|\mathrm{MRSTD}(G_n)| \sim k_n \cdot 3^{|G_n|/2}.$$

(ii) (Odd case) *If every $|G_n|$ is odd and the proportion of elements in G_n with order less than $\log_\psi |G_n|$ approaches 0 as $n \to \infty$, then*

$$|\mathrm{MRSTD}(G_n)| \sim \frac{1}{2}|G_n|\psi^{|G_n|},$$

where $\psi = (1+\sqrt{5})/2$ is the golden ratio.

THEOREM 10.2. *If $\limsup_{n\to\infty} k_n/|G_n| < 1$, where G_n has $k_n > 0$ elements of order 2, then*

$$|\mathrm{MSTD}(G_n)| \sim k_n \cdot 3^{|G_n|/2}.$$

Note that, comparing with Zhao's results for sum-dominant sets, these results imply that the number of restricted-sum-dominant sets is asymptotically equal to the number of sum-dominant sets under the hypotheses of our theorems.

In the rest of this subsection we set up some simple upper and lower bounds on $|\mathrm{MRSTD}(G)|$ and $|\mathrm{MSTD}(G)|$ similar to ones in Zhao [8]. The following two subsections deal with the cases where the group has even order and odd order respectively.

By necessity $A - A \neq G$ for every restricted-sum-dominant set A. If $A - A \neq G$ and $A \hat{+} A = G$, then A is a restricted-sum-dominant set. Thus

$$\{A \subset G : A - A \neq G,\ A \hat{+} A = G\} \subseteq \mathrm{MRSTD}(G) \subseteq \mathrm{MSTD}(G) \subset \{A \subset G : A - A \neq G\}. \tag{5}$$

We use 'union bounds' similar to those in Section 2 of [8] to estimate the sizes of these sets. Letting G' denote a subset of G which does not contain 0 (the identity element) such that for each non-identity element $d \in G$, G' contains

either d or $-d$, but not both, we have

$$|\mathrm{MRSTD}(G)| \le |\{A \subset G : A - A \ne G\}| \le \sum_{d \in G'} |\{A \subset G : d \notin A - A\}|. \tag{6}$$

For a lower bound let $\widehat{D}_d = \{A \subset G : d \notin A - A, A \hat{+} A = G\}$ for $d \in G$. Adapting an argument from page 2311 of [8], we have

$$\{A \subset G : A - A \ne G,\ A \hat{+} A = G\} = \bigcup_{d \in G'} \widehat{D}_d;$$

a lower bound on its order is

$$\Big| \bigcup_{d \in G'} \widehat{D}_d \Big| \ge \sum_{d \in G'} |\widehat{D}_d| - \sum_{\substack{d_1, d_2 \in G' \\ d_1 \ne d_2}} |\widehat{D}_{d_1} \cap \widehat{D}_{d_2}|.$$

Now

$$\begin{aligned} |\widehat{D}_d| &= |\{A \subset G : d \notin A - A,\ A \hat{+} A = G\}| \\ &\ge |\{A \subset G : d \notin A - A\}| - \sum_{s \in G} |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| \end{aligned} \tag{7}$$

and

$$\begin{aligned} |\widehat{D}_{d_1} \cap \widehat{D}_{d_2}| &= |\{A \subset G : d_1, d_2 \notin A - A,\ A \hat{+} A = G\}| \\ &\le |\{A \subset G : d_1, d_2 \notin A - A\}|. \end{aligned}$$

Combining the above we obtain an inequality analogous to (3) in [8]:

$$\begin{aligned} |\mathrm{MRSTD}(G)| &\ge |\{A \subset G : A - A \ne G,\ A \hat{+} A = G\}| \\ &= \Big| \bigcup_{d \in G'} \widehat{D}_d \Big| \ge \sum_{d \in G'} |\widehat{D}_d| - \sum_{\substack{d_1, d_2 \in G' \\ d_1 \ne d_2}} |\widehat{D}_{d_1} \cap \widehat{D}_{d_2}| \\ &\ge \sum_{d \in G'} |\{A \subset G : d \notin A - A\}| \\ &\quad - \sum_{d \in G'} \sum_{s \in G} |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| \\ &\quad - \sum_{\substack{d_1, d_2 \in G' \\ d_1 \ne d_2}} |\{A \subset G : d_1, d_2 \notin A - A\}|. \end{aligned} \tag{8}$$

Zhao already has results, which we can use, for $|\{A \subset G : d \notin A - A\}|$ and $|\{A \subset G : d_1, d_2 \notin A - A\}|$ (see Lemmas 10.7, 10.9 and 10.10 below). To obtain $|\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}|$ we adapt arguments from his Section 3 relating the size of sets as in (8) above to independent sets (i.e. sets of vertices no two of which are adjacent) in a certain graph.

DEFINITION 10.3. For a collection of sets

$$\widehat{\mathcal{A}} = \{A \subset G : d_1, \dots, d_p \notin A - A,\ s_1, \dots, s_q \notin A \hat{+} A\} \tag{9}$$

we call the $d_1, \dots, d_p$ *forbidden differences* and the $s_1, \dots, s_q$ *forbidden restricted sums*. The *forbiddance graph* $\mathcal{G}(\widehat{\mathcal{A}})$ is the graph with vertex set G and an edge between two vertices if and only if their difference or restricted sum is forbidden.

Note that $\mathcal{G}(\widehat{\mathcal{A}})$ is a loopless graph: $x + x = s$ is banned in the restricted sumset, and the case $d = 0$ would lead to $A = \emptyset$.

DEFINITION 10.4. The *Fibonacci index* of a graph G is denoted by $i(\mathsf{G})$ and equal to the number of independent sets G contains.

LEMMA 10.5. $|\widehat{\mathcal{A}}| = i(\mathcal{G}(\widehat{\mathcal{A}}))$.

Proof. Two vertices are adjacent in $\mathcal{G}(\widehat{\mathcal{A}})$ if and only if $\{d_1, \dots, d_p\}$ contains their difference or $\{s_1, \dots, s_q\}$ contains their restricted sum. Thus an independent set is one where no difference is in $\{d_1, \dots, d_p\}$ and no restricted sum is in $\{s_1, \dots, s_q\}$—i.e. is a set in $\widehat{\mathcal{A}}$. ∎

In the following, F_n denotes the nth Fibonacci number ($F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$) and L_n the nth Lucas number ($L_1 = 1$, $L_2 = 3$ and $L_{n+2} = L_{n+1} + L_n$). Put $\psi = (1 + \sqrt{5})/2$. The path on n vertices and the n-vertex cycle are denoted by P_n and C_n respectively. Denoting the Cartesian graph product by $\Box$, the ladder and prism graphs on $2n$ vertices are denoted by $P_n \Box P_2$ and $C_n \Box P_2$ respectively. More explicitly, the ladder graph $P_n \Box P_2$ has vertex set $\{a_1, \dots, a_n, b_1, \dots, b_n\}$ with $\{a_1, \dots, a_n\}$ inducing a path a_1—$\cdots$—a_n, similarly $\{b_1, \dots, b_n\}$ inducing a path b_1—$\cdots$—b_n, and the only other edges are a_i—b_i for all $1 \leq i \leq n$. The prism graph has vertex set $\{a_1, \dots, a_n, b_1, \dots, b_n\}$ with $\{a_1, \dots, a_n\}$ inducing a cycle a_1—$\cdots$—a_n—a_1, similarly $\{b_1, \dots, b_n\}$ inducing a cycle b_1—$\cdots$—b_n—b_1, and the only other edges are a_i—b_i for all $1 \leq i \leq n$. These graphs will arise naturally as certain connected components in the forbiddance graph $\mathcal{G}(\mathcal{A})$ and we will need to know about the number of independent sets in them.

Some key facts from [8] about Fibonacci indices of graphs we shall require are:

LEMMA 10.6. *We have*

- $i(P_n) = F_{n+2}$.
- $i(C_n) = L_n = \psi^n + (-\psi)^{-n}$.
- $i(P_n \Box P_2) = \frac{1}{2}((1 + \sqrt{2})^{n+1} + (1 - \sqrt{2})^{n+1})$.
- $i(C_n \Box P_2) = (1 + \sqrt{2})^n + (1 - \sqrt{2})^n + (-1)^n$.
- *The Fibonacci index of a graph equals the product of the Fibonacci indices of its connected components.*

Proof. See the Appendix of [8]. ∎

We shall require the following results (Lemmas 3.4, 3.5, 3.10 and 3.15 of [8], which also contains the proofs).

LEMMA 10.7. *If d is a non-zero element of a finite abelian group G then*

$$\sum_{d\in G'} |\{A \subset G : d \notin A - A\}| = \sum_{d\in G'} L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)}.$$

LEMMA 10.8. *The sequence $(L_{2n}^{1/(2n)})$ is decreasing and the sequence $(L_{2n-1}^{1/(2n-1)})$ is increasing. Both sequences approach the limit $\psi = (1+\sqrt{5})/2$. In particular $L_2^{1/2} > L_4^{1/4} > L_{2n}^{1/(2n)}$ for all $n > 2$.*

LEMMA 10.9. *For a finite abelian group G of even order and distinct non-zero elements $d_1, d_2 \in G$ we have*

$$|\{A \subset G : d_1, d_2 \notin A - A\}| \le 7^{|G|/4}.$$

LEMMA 10.10. *Let $d_1, d_2 \in G$ be two non-zero elements such that $2d_1 \neq 0$, $2d_2 \neq 0$, $d_1 \neq d_2$ and $d_1 \neq -d_2$. Then*

$$|\{A \subset G : d_1, d_2 \notin A - A\}| \le 31^{|G|/8}.$$

10.2. Even order finite abelian groups

LEMMA 10.11. *Let G be a finite abelian group containing k elements of order 2. Then there are $|G|/(k+1)$ elements $s \in G$ for which there are $k+1$ elements $x \in G$ such that $2x = s$. For the remaining elements $s' \in G$ there is no $x \in G$ with $2x = s'$.*

Proof. Let K denote the set of all elements of G with order 1 or 2. Suppose s is such that for some $x \in G$ we have $2x = s$. For all $\kappa \in K$, $2(x+\kappa) = s$ so we get exactly $k+1$ elements in G whose double equals s. Otherwise s has no such representations, so $|2G| = |G|/(k+1)$. ∎

LEMMA 10.12. *Let $d, s \in G$ where d has order 2, let k denote the number of elements of order 2 in G, and set $\widehat{\mathcal{A}} = \{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}$. Then the forbiddance graph is a disjoint union of 4-cycles and at most $k+1$ copies of P_2. If n_{P_2} denotes the number of P_2 components and n_{C_4} denotes the number of 4-cycles in $\mathcal{G}(\widehat{\mathcal{A}})$, then $n_{P_2} + 2n_{C_4} = |G|/2$.*

Proof. This resembles Lemma 3.7 of [8]. The connected component of $\mathcal{G}(\widehat{\mathcal{A}})$ containing x contains $x, x+d, s-x-d, s-x$ (possibly with repetitions). As d has order 2, there are no other elements in the component. When all four elements are distinct, the component is a 4-cycle. Otherwise there are equalities. As $x \neq x+d$ there are two scenarios: $x = s-x-d$ or $x = s-x$.

When $x = s-x-d$ then $x+d = s-x$ as well and the connected component is a P_2. Now $x+d = s-x \Leftrightarrow 2x = s-d$ and when $s-d$ can

be expressed as a double of an element x of G, by Lemma 10.11, there are exactly $k+1$ such x. This contributes $(k+1)/2$ copies of P_2 to $\mathcal{G}(\widehat{\mathcal{A}})$.

On the other hand, if $x = s - x$ then $s = x + x$ but $x + x$ is not a restricted sum and we are left with a P_2 component. Again by Lemma 10.11 there are exactly $k+1$ such $x \in G$. These contribute $(k+1)/2$ copies of P_2 to the forbiddance graph. Thus overall we have at most $k+1$ copies of P_2.

The last claim $n_{P_2} + 2n_{C_4} = |G|/2$ simply follows from writing the graph as the disjoint union of its components. ∎

From the formulae for the Fibonacci indices of the path and the cycle, together with the fact that the Fibonacci index of a graph is the product of the Fibonacci indices of its connected components, we deduce that

$$i(\mathcal{G}(\widehat{\mathcal{A}})) = |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| = 3^{n_{P_2}} \cdot 7^{n_{C_4}}. \tag{10}$$

Next we give an upper bound on the right-hand side of the above.

LEMMA 10.13. *Let s, k and $\widehat{\mathcal{A}}$ be as in Lemma* 10.12. *Then if d has order* 2, *we get*

$$|\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| \le \left(\frac{3}{\sqrt{7}}\right)^{k+1} \cdot 7^{|G|/4}.$$

(*If d has order greater than* 2, *then*

$$|\{A \subset G :\ d \notin A - A,\ s \notin A \hat{+} A\}| \le |\{A \subset G :\ d \notin A - A\}|$$

and the right-hand side here is at most $7^{|G|/4}$ by Lemma 3.6 *of* [8].)

Proof. By Lemma 10.12 the number n_{P_2} of copies of P_2 is at most $k+1$, and $n_{P_2} + 2n_{C_4} = |G|/2$, so $n_{C_4} = (|G| - 2n_{P_2})/4$. Substituting this into (10) we get

$$i(\mathcal{G}(\widehat{\mathcal{A}})) = 3^{n_{P_2}} \cdot 7^{(|G|-2n_{P_2})/4} = \left(\frac{3}{\sqrt{7}}\right)^{n_{P_2}} \cdot 7^{|G|/4} \le \left(\frac{3}{\sqrt{7}}\right)^{k+1} \cdot 7^{|G|/4}.$$

The claim for d of order greater than 2 is obvious. ∎

We are now ready to complete the proofs of the even case of Theorem 10.1 and Theorem 10.2. We use Zhao's upper bound, his equation (6), i.e.

$$|\mathrm{MRSTD}(G)| \le |\mathrm{MSTD}(G)| \le k \cdot 3^{|G|/2}\left(1 + \frac{|G|}{k}\left(\frac{7}{9}\right)^{|G|/4}\right). \tag{11}$$

For the lower bound, if $\mathrm{ord}(d) = 2$ then $|\{A \subset G : d \notin A - A\}| = 3^{|G|/2}$ by Lemma 3.3 of [8], and $\sum_{s \in G} |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| \le$

$(3/\sqrt{7})^{k+1} \cdot 7^{|G|/4}$ by Lemma 10.13 above. Thus (7) gives

$$
\begin{aligned}
(12)\quad & |\{A \subset G : d \notin A - A,\ A \hat{+} A = G\}| \\
&\geq |\{A \subset G : d \notin A - A\}| - \sum_{s \in G} |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| \\
&\geq 3^{|G|/2} - |G|\left(\frac{3}{\sqrt{7}}\right)^{k+1} \cdot 7^{|G|/4}.
\end{aligned}
$$

Let $G_{(2)}$ be the set of elements of order 2 of G, so that $|G_{(2)}| = k$. Using (8) with (12) and the fact that $|\{A \subset G : d_1, d_2 \notin A - A\}| \leq 7^{|G|/4}$ by Lemma 10.9, we have

$$
\begin{aligned}
(13)\quad |\mathrm{MRSTD}(G)| &\geq \sum_{d \in G} |\{A \subset G : d \notin A - A,\ A \hat{+} A = G\}| \\
&\quad - \sum_{\substack{d_1, d_2 \in G' \\ d_1 \neq d_2}} |A \subset G : d_1, d_2 \notin A - A,\ A \hat{+} A = G\}| \\
&\geq \sum_{d \in G_{(2)}} |\{A \subset G : d \notin A - A,\ A \hat{+} A = G\}| \\
&\quad - \sum_{\substack{d_1, d_2 \in G' \\ d_1 \neq d_2}} |\{A \subset G : d_1, d_2 \notin A - A,\ A \hat{+} A = G\}| \\
&\geq k\left(3^{|G|/2} - |G|\left(\frac{3}{\sqrt{7}}\right)^{k+1} \cdot 7^{|G|/4}\right) - |G|^2 \cdot 7^{|G|/4} \\
&= k \cdot 3^{|G|/2}\left(1 - \left(|G| \cdot \left(\frac{3}{\sqrt{7}}\right)^{k+1} + \frac{|G|^2}{k}\right)\left(\frac{7}{9}\right)^{|G|/4}\right).
\end{aligned}
$$

From (11) and (13) we deduce, now writing G_n to denote our abelian group of order n and k_n to denote the number of elements of order 2 in it, that

$$
\begin{aligned}
1 - \left(|G_n|\left(\frac{3}{\sqrt{7}}\right)^{k_n+1} + \frac{|G_n|^2}{k_n}\right)\left(\frac{7}{9}\right)^{|G_n|/4} &\leq \frac{|\mathrm{MRSTD}(G_n)|}{k_n \cdot 3^{|G_n|/2}} \\
&\leq 1 + \frac{|G_n|}{k_n}\left(\frac{7}{9}\right)^{|G_n|/4},
\end{aligned}
$$

and we must show the LHS and RHS tend to 1 as $|G_n| \to \infty$. This will follow if

$$
(14)\quad |G_n|\left(\frac{3}{\sqrt{7}}\right)^{k_n+1}\left(\frac{7}{9}\right)^{|G_n|/4} \to 0 \ \Leftrightarrow\ |G_n| \cdot \left(\frac{7}{9}\right)^{\frac{|G_n|}{4}\left(1 - \frac{2(k_n+1)}{|G_n|}\right)} \to 0.
$$

Now $1-2(k_n+1)/|G_n|$ is positive if and only if $(k_n+1)/|G_n| < 1/2$. Thus

$$\limsup_{n\to\infty} \frac{k_n+1}{|G_n|} < \frac{1}{2}$$

gives the result.

We now give our sharpening of Zhao's sumset result in the even case. From Lemma 3.7 of [8] we see in the sumset case that $n_{P_2} \le (k+1)/2$. Then, applying similar calculations to Lemma 10.13, we obtain

$$|\{A \subset G : d \notin A-A,\ s \notin A+A\}| \le \left(\frac{3}{\sqrt{7}}\right)^{(k+1)/2} \cdot 7^{|G|/4}.$$

The equivalent condition to (14) for the sumset case then becomes

$$|G_n| \cdot \left(\frac{7}{9}\right)^{\frac{|G_n|}{4}(1-\frac{k_n+1}{|G_n|})} \to 0 \quad \text{and} \quad 1-\frac{k_n+1}{|G_n|} > 0 \ \Leftrightarrow\ \frac{k_n+1}{|G_n|} < 1.$$

Thus the condition $\limsup_{n\to\infty}(k_n+1)/|G_n| < 1-\frac{1}{2}\log_3 7 = 0.114\ldots$ in Zhao [8] can be relaxed to $\limsup_{n\to\infty}(k_n+1)/|G_n| < 1$.

10.3. Odd order finite abelian groups

LEMMA 10.14. *Let $d \in G$ be of odd order $\ell > 1$, $s \in G$ and $\widehat{\mathcal{A}} = \{A \subset G : d \notin A-A,\ s \notin A \hat{+} A\}$. Then $\mathcal{G}(\widehat{\mathcal{A}})$ consists of $(|G|/\ell - 1)/2$ prisms $C_\ell \,\square\, P_2$ and one 'chorded cycle' H_ℓ, i.e. a graph which consists of a $P_{(\ell-1)/2} \,\square\, P_2$ ladder H together with one further vertex adjoined to two adjacent vertices of degree 2 in H. (It is the graph in Figure 3 of [8] with the loop removed.)*

Proof. The forbiddance graph for $\{A \subset G : d \notin A-A\}$ consists of $|G|/\ell$ disjoint ℓ-cycles $C_x = \{x, x+d, \ldots, x+(\ell-1)d\}$. To allow for the forbidden sum s we also have to add edges $(x, s-x)$ to obtain $\mathcal{G}(\widehat{\mathcal{A}})$. Similarly to Lemma 3.11 in [8], for a vertex $x \in G$ there are two possible scenarios:

CASE 1. If $s-x$ is not in C_x then $s-(x+jd)$ is not in C_x either and so clearly the connected component is a prism $C_\ell \,\square\, P_2$.

CASE 2. When $s-x \in C_x$, the connected component of x in $\mathcal{G}(\widehat{\mathcal{A}})$ is an ℓ-cycle with $(\ell-1)/2$ edges $(x+jd, s-x-jd)$ between pairs of distinct vertices and a single vertex $x+id$ for which $x+id = s-x-id$, equivalently $2(x+id) = s$; of course this vertex does not give s as a restricted sum. Thus we indeed get the ladder with a triangle on the end described in the lemma, with $x+id$ being the unique vertex which is in a triangle and has degree 2.

Since $|G|$ is odd for each $s \in G$ there is a unique $x \in G$ such that $2x = s$. Thus $\mathcal{G}(\widehat{\mathcal{A}})$ contains exactly one copy of H_ℓ. This leaves all other components being prisms formed from two ℓ-cycles. Letting n_P denote the number of prisms we have $n_P = (|G|/\ell - 1)/2$. ∎

LEMMA 10.15. *The graph H_ℓ has*

$$i(H_\ell) = i(P_{(\ell-1)/2} \,\square\, P_2) + i(P_{(\ell-3)/2} \,\square\, P_2).$$

Proof. H_ℓ is a copy of $P_{(\ell-1)/2} \,\square\, P_2$ with a triangle on one end formed by joining a single vertex w to two end vertices u and v. Apart from u and v every vertex of $P_{(\ell-1)/2} \,\square\, P_2$ can be in an independent set with w. Thus there are $i(P_{(\ell-3)/2} \,\square\, P_2)$ independent sets containing w in addition to the $i(P_{(\ell-1)/2} \,\square\, P_2)$ which do not contain w. ∎

COROLLARY 10.16. *Let d, ℓ, s and $\widehat{\mathcal{A}}$ be as in Lemma* 10.14. *Then*

$$i(\mathcal{G}(\widehat{\mathcal{A}})) = |\{A \subset G : d \notin A - A,\ s \notin A \hat{+} A\}| = i(H_\ell) \cdot i(C_\ell \,\square\, P_2)^{(|G|/\ell-1)/2}.$$

Proof. Denoting by n_H the number of H_ℓ components and by n_P the number of prism components, we have $n_H + 2n_P = |G|/\ell$, and by Lemma 10.6, $i(\mathcal{G}(\widehat{\mathcal{A}})) = i(H_\ell)^{n_H} \cdot i(C_\ell)^{n_P}$. As noted in Lemma 10.14, $n_H = 1$ and $n_P = (|G|/\ell - 1)/2$. Hence $i(\mathcal{G}(\widehat{\mathcal{A}})) = i(H_\ell) \cdot i(C_\ell \,\square\, P_2)^{(|G|/\ell-1)/2}$. ∎

LEMMA 10.17. *If $\ell > 1$ is an odd integer then $i(C_\ell \,\square\, P_2) < (1+\sqrt{2})^\ell$.*

Proof. By the formula in Lemma 10.6,

$$i(C_\ell \,\square\, P_2) = (1+\sqrt{2})^\ell + (1-\sqrt{2})^\ell + (-1)^\ell,$$

which is strictly less than $(1+\sqrt{2})^\ell$ for all odd integers $\ell > 1$. ∎

LEMMA 10.18. *For the graph H_ℓ defined above, if $\ell > 1$ is odd then*

$$i(H_\ell) \le 3\sqrt{1+\sqrt{2}}\,(3\sqrt{2}-4)(1+\sqrt{2})^{\ell/2} < 1.14 \cdot (1+\sqrt{2})^{\ell/2}.$$

Proof. By Lemma 10.6, the fact that $\ell \ge 3$ is odd and some algebraic manipulations we obtain

$$\begin{aligned} i(P_{(\ell-1)/2} \,\square\, P_2) &= \frac{1}{2}\big((1+\sqrt{2})^{(\ell+1)/2} + (1-\sqrt{2})^{(\ell+1)/2}\big) \\ &= \frac{(1+\sqrt{2})^{\ell/2}}{2}\left(\sqrt{1+\sqrt{2}} + \sqrt{1+\sqrt{2}}\left(\frac{1-\sqrt{2}}{1+\sqrt{2}}\right)^{(\ell+1)/2}\right) \\ &= \frac{(1+\sqrt{2})^{\ell/2}}{2}\big(\sqrt{1+\sqrt{2}}\,\big(1 + (2\sqrt{2}-3)^{(\ell+1)/2}\big)\big) \\ &\le \frac{(18-12\sqrt{2})\sqrt{1+\sqrt{2}}}{2}(1+\sqrt{2})^{\ell/2}. \end{aligned}$$

By Lemma 10.15, $i(H_\ell)$ equals

$$\frac{1}{2}\big((1+\sqrt{2})^{(\ell+1)/2} + (1-\sqrt{2})^{(\ell+1)/2} + (1+\sqrt{2})^{(\ell-1)/2} + (1-\sqrt{2})^{(\ell-1)/2}\big).$$

Applying the upper bound on $\frac{1}{2}((1+\sqrt{2})^{(\ell+1)/2}+(1-\sqrt{2})^{(\ell+1)/2})$ we have

$$\begin{aligned} i(H_\ell) &\le \frac{(18-12\sqrt{2})\sqrt{1+\sqrt{2}}}{2}((1+\sqrt{2})^{\ell/2}+(1+\sqrt{2})^{(\ell-2)/2}) \\ &= (9-6\sqrt{2})\sqrt{1+\sqrt{2}}\,(1+\sqrt{2})^{\ell/2}\left(1+\frac{1}{1+\sqrt{2}}\right) \\ &= (9-6\sqrt{2})(1+\sqrt{2})^{1/2}\sqrt{2}\,(1+\sqrt{2})^{\ell/2}. \end{aligned}$$

Finally, note that $(9-6\sqrt{2})\sqrt{2(1+\sqrt{2})} = 1.1310\ldots < 1.14$. ∎

COROLLARY 10.19. *Let $|G|$ be odd and $s, d \in G$ with $d \neq 0$. Then*

$$|\{A \subset G : d \notin A-A,\ s \notin A \hat{+} A\}| < 1.14 \cdot (1+\sqrt{2})^{|G|/2}.$$

Proof. Applying Corollary 10.16 and Lemmas 10.17 and 10.18 we get

$$\begin{aligned} |\{A \subset G : d \notin A-A,\ s \notin A \hat{+} A\}| &= i(H_\ell)\cdot i(C_\ell \Box P_2)^{(|G|/\ell-1)/2} \\ &< 1.14\cdot(1+\sqrt{2})^{\ell/2}((1+\sqrt{2})^{\ell})^{(|G|/\ell-1)/2} \\ &= 1.14\cdot(1+\sqrt{2})^{|G|/2}. \ \blacksquare \end{aligned}$$

We can now complete the proof of the lower bound on $|\mathrm{MRSTD}(G)|$ in this case. Recall that G' denotes a subset of G which contains exactly one of d and $-d$ for each non-identity element (as G has odd order, it has no elements of order 2). Thus $|G'| = (|G|-1)/2 < |G|/2$. We use the same upper bound as in the sumset case, equation (8) of [8], specifically

$$|\mathrm{MRSTD}(G)| \le \sum_{d\in G'} |\{A \subset G : d \notin A-A\}| = \sum_{d\in G'} L_{\mathrm{ord}(G)}^{|G|/\mathrm{ord}(d)}. \tag{15}$$

Applying (8), then Lemmas 10.7, 10.10 and Corollary 10.19, we see that the order of $\mathrm{MRSTD}(G)$ is at least

$$\begin{aligned} &\sum_{d\in G'} |\{A \subset G : d \notin A-A\}| - \sum_{d\in G'}\sum_{s\in G} |\{A \subset G : d \notin A-A,\ s \notin A\hat{+}A\}| \\ &\qquad - \sum_{\substack{d_1,d_2\in G' \\ d_1\neq d_2}} |\{A \subset G : d_1, d_2 \notin A-A\}| \tag{16} \\ &\ge \sum_{d\in G'} |\{A \subset G : d \notin A-A\}| - \frac{|G|}{2}\sum_{s\in G} |\{A \subset G : d \notin A-A,\ s \notin A \hat{+} A\}| \\ &\qquad - \sum_{\substack{d_1,d_2\in G' \\ d_1\neq d_2}} |\{A \subset G : d_1, d_2 \notin A-A\}| \\ &\ge \Big(\sum_{d\in G'} L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)}\Big) - \frac{|G|^2}{2} 1.14\cdot(1+\sqrt{2})^{|G|/2} - |G|^2\cdot 31^{|G|/8}. \end{aligned}$$

Since $\mathrm{ord}(d)$ is odd for all $d \in G$, by Lemma 10.8 the sequence $(L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)})$ is increasing and $L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)} \geq L_3^{|G|/3} = 4^{|G|/3}$. Since $4^{1/3} > \sqrt{1+\sqrt{2}} > 31^{1/8}$, formulae (15) and (16) imply that

$$|\mathrm{MRSTD}(G)| \sim \sum_{d \in G'} L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)} \sim \frac{1}{2} \sum_{d \in G} L_{\mathrm{ord}(d)}^{|G|/\mathrm{ord}(d)} = \frac{1}{2}\psi^{|G|} \sum_{d \in G} (1 - \psi^{-2\mathrm{ord}(d)})^{|G|/\mathrm{ord}(d)}. \tag{17}$$

From the calculations following Lemma 4.2 on p. 2318 of [8], the asymptotics of the RHS of (17) are

$$|\mathrm{MRSTD}(G)| \sim \frac{1}{2}\psi^{|G|} \sum_{d \in G} (1 - \psi^{-2\mathrm{ord}(d)})^{|G|/\mathrm{ord}(d)} \sim \frac{1}{2}\psi^{|G|}|G|,$$

and the claim for the odd case of Theorem 10.1 follows.

11. Further questions and future research. It is natural to ask if one could generalise these results to non-abelian groups. Some first steps in considering some analogous questions have recently been taken in [4], where it is proven that in any finite group the proportion of sets A whose sumset $\{a + b : a, b \in A\}$ (we continue to write groups additively, even if they are not abelian) is equal to the difference set $\{a - b : a, b \in A\}$ is equal to 1. (More precisely, it is shown that for most sets, both sumset and difference set are the whole of the group.) It seems plausible that results in the same spirit as those above could be obtained, although the proofs would be more involved, perhaps especially when dealing with groups of 2-power order.

References

[1] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley, Reading, MA, 1967.

[2] P. V. Hegarty, *Some explicit constructions of sets with more sums than differences*, Acta Arith. 130 (2007), 61–77.

[3] G. Martin and K. O'Bryant, *Many sets have more sums than differences*, in: Additive Combinatorics, CRM Proc. Lecture Notes 43, Amer. Math. Soc, Providence, RI, 2007, 287–305.

[4] S. J. Miller and K. Vissuet, *Most subsets are balanced in finite groups*, in: Combinatorial and Additive Number Theory (New York, 2011/2012), Springer, to appear; arXiv:1308.2344.

[5] M. B. Nathanson, *Sets with more sums than differences*, Integers 7 (2007), no. 1, #A5;

[6] D. Penman and M. Wells, *On sets with more restricted sums than differences*, Integers 13 (2013), # A57.

[7] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2010.
[8] Y. Zhao, *Counting MSTD sets in finite abelian groups*, J. Number Theory 130 (2010), 2308–2322.
[9] Y. Zhao, *Sets characterized by missing sums and differences*, J. Number Theory 131 (2011), 2107–2134.
[10] Y. Zhao, *Sets with more sums than differences*, slides of a talk, 2009, retrieved Oct. 14, 2013; http://yufeizhao.com/papers/mstd_slides.pdf.

David B. Penman, Matthew D. Wells
Department of Mathematical Sciences
University of Essex
Wivenhoe Park
Colchester CO4 3SQ, United Kingdom
E-mail: dbpenman@essex.ac.uk
mwells@essex.ac.uk

Received on 21.10.2013
and in revised form on 21.7.2014 (7622)