Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 123 (2007) 144–153

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Sets in Abelian groups with distinct sums of pairs

Harri Haanpää [a,*,1], Patric R.J. Östergård [b,2]

[a] *Department of Computer Science and Engineering, Helsinki University of Technology, PO Box 5400, FI-02015 TKK, Finland*

[b] *Department of Electrical and Communications Engineering, Helsinki University of Technology, PO Box 3000, FI-02015 TKK, Finland*

Received 27 June 2002; revised 28 April 2006

Available online 17 August 2006

Communicated by David Goss

Abstract

A subset $S = \{s_1, \ldots, s_k\}$ of an Abelian group G is called an S_t-set of size k if all sums of t different elements in S are distinct. Let $s(G)$ denote the cardinality of the largest S_2-set in G. Let $v(k)$ denote the order of the smallest Abelian group for which $s(G) \geqslant k$. In this article, bounds for $s(G)$ are developed and $v(k)$ is determined for $k \leqslant 15$ by computing $s(G)$ for Abelian groups of order up to 183 using exhaustive backtrack search with isomorph rejection.

Keywords: Additive base; Backtrack search; Difference set; Packing

1. Introduction

This work considers a packing problem in finite Abelian groups. A subset S of an Abelian group, where $|S| = k$, is an S_t-set of size k if all sums of t different elements in S are distinct in the group. See [4,5] for open problems in additive number theory related to S_t-sets and similar configurations.

[*] Corresponding author.
E-mail address: harri.haanpaa@tkk.fi (H. Haanpää).

[1] The work was supported in part by the Helsinki Graduate School of Computer Science and Engineering (HeCSE) and by the Nokia Foundation.

[2] The work was supported in part by the Academy of Finland under Grants Nos. 100500, 107493, and 110196.

doi:10.1016/j.jnt.2006.06.007

Let $s(G)$ denote the cardinality of the largest S_2-set in G. Two central functions in the study of S_2-sets are $v(k)$ and $v_\gamma(k)$, which give the order of the smallest Abelian and cyclic group G, respectively, for which $s(G) \geqslant k$. Since cyclic groups are a special case of Abelian groups, clearly $v(k) \leqslant v_\gamma(k)$, and any upper bound on $v_\gamma(k)$ is also an upper bound on $v(k)$. In [6], the values of $v_\gamma(k)$ for $k \leqslant 15$ are determined. In this paper we develop bounds for $s(G)$, and we determine $v(k)$ for $k \leqslant 15$ by computing $s(G)$ for Abelian groups of small order.

One motivation for studying $v(k)$ and S_t-sets is that they have applications in coding theory [2–4]. A constant weight error-correcting code is a set of binary vectors of length k and weight w such that the Hamming distance between any two vectors is at least d. Given k, d, and w, the maximum number of vectors in such a code is denoted by $A(k,d,w)$. In [3, Theorem 16] it is shown that $A(k,6,w) \geqslant \binom{k}{w}/v(k)$.

In searching for an S_t-set of maximum size in a given group, symmetries of the search space should be utilized in developing efficient algorithms. This is the motivation behind considering the concepts of group automorphism and subset equivalence in Section 2. Several general bounds for the size of S_2-sets are proved in Section 3. The exhaustive computer search used is presented in Section 4, and the paper is concluded in Section 5 by presenting computational results for all Abelian groups of order at most 183. Thereby $v(k)$ is obtained for $k \leqslant 15$.

2. Group automorphism and subset equivalence

By a result attributed to Gauss, every finite Abelian group G can be expressed as a direct product of a finite number of cyclic groups of prime power order. We may arrange the cyclic direct factors so that factors whose orders are powers of the same prime appear consecutively; in effect, we are expressing the group as a direct product of Abelian p-groups, i.e., Abelian groups of prime power order, whose orders are powers of distinct primes. This form is particularly convenient for investigating the automorphisms of G: Shoda [9] showed that the automorphism group of G is then the direct product of the automorphism groups of the Abelian p-subgroups. Hence it suffices to consider the automorphism groups of Abelian p-groups only.

An Abelian p-group may be expressed as $G_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_k}}$, with p prime and e_i positive integers, and we may arrange the direct factors such that $e_1 \geqslant \cdots \geqslant e_k$. Shoda [9] found that when the elements of G_p are expressed as row vectors x, the automorphisms of G_p may be described as $\alpha(x) = xM_p$, where M_p is a matrix of the form

$$M_p = \begin{pmatrix} h_{11} & h_{12} & h_{13} & & h_{1k} \\ p^{e_1-e_2}h_{21} & h_{22} & h_{23} & \cdots & h_{2k} \\ p^{e_1-e_3}h_{31} & p^{e_2-e_3}h_{32} & h_{33} & & h_{3k} \\ & \vdots & & \ddots & \vdots \\ p^{e_1-e_k}h_{k1} & p^{e_2-e_k}h_{k2} & p^{e_3-e_k}h_{k3} & \cdots & h_{kk} \end{pmatrix} \tag{1}$$

with $\det M_p \not\equiv 0 \pmod{p}$, where h_{ij} are integers in the range $0 \leqslant h_{ij} < p^{e_\mu}$ with $\mu = \max(i,j)$.

In the backtrack search we will perform, the concept of equivalent subsets is essential in pruning the search. Two subsets S and S' of an Abelian group G are equivalent, if $S = \psi(S')$, where $\psi : G \mapsto G$ is a function of the form $\psi(x) = \alpha(x) + b$, where $\alpha \in A(G)$ is an automorphism of G, and $b \in G$ is a constant. The equivalence mappings ψ form a group which we denote by $E(G)$ under function composition. They also preserve the property that all sums of pairs are distinct, as α is an automorphism of G and adding the constant b to each element merely shifts each sum of two elements by $2b$.

3. Properties of S_2-sets

In this section, several bounds on S_2-sets are proved. We start by showing a one-to-one correspondence between binary linear codes and S_2-sets in elementary Abelian 2-groups of the form $\mathbb{Z}_2^m$, the direct product of m copies of $\mathbb{Z}_2$. The following theorem is implicitly used in [2]. A binary linear code with length n, dimension k, and minimum distance d is called an $[n, k, d]$ code.

Theorem 1. *There exists an $[n, n-r, 5]$ code iff there exists an S_2-set of size $n+1$ in $\mathbb{Z}_2^r$.*

Proof. Given a binary $r \times n$ matrix whose columns are distinct and nonzero, we may take the columns together with the zero vector to form a subset of $n+1$ elements in $\mathbb{Z}_2^r$. Conversely, given an $n+1$ element subset of $\mathbb{Z}_2^r$ that contains zero we may take the n nonzero elements as the columns of a binary $r \times n$ matrix M whose columns are distinct and nonzero.

If the matrix M is a parity check matrix of an $[n, n-r, 5]$ code, then any subset of fewer than five columns is linearly independent, that is, $a+b+c+d \neq 0$ and $a+b+c \neq 0$ for any distinct columns a, b, c, and d of the matrix. If the $(n+1)$-element subset S is an S_2-set, then $a+b \neq c+d$ and $a+b \neq c+0$ for any distinct and nonzero elements a, b, c, and d of the subset. These conditions are clearly equivalent in $\mathbb{Z}_2^r$.

It only remains to remark that given an S_2-set of size $n+1$ in $\mathbb{Z}_2^r$, we may obtain an S_2-set that contains the zero element by adding the inverse of an arbitrary element of the S_2-set to each of the elements. □

From Theorem 1 and [1], we know $s(\mathbb{Z}_2^r)$ for $r \leqslant 9$. The next theorem gives a bound for $s(G)$ for an arbitrary Abelian group G.

Theorem 2. *For a given finite Abelian group G, let $v = |G|$ and let S be a k-element S_2-set in G. Then*

$$v \geqslant \left(1 - \frac{1}{n_2(G)+1}\right)\left(k^2 - 3k + 2\right),$$

where $n_2(G)$ is the index of the subgroup of G formed by involutions and the identity.

Proof. Consider the $k(k-1)$ ordered pairs of distinct elements of S and partition them into sets $D_d = \{(s_1, s_2) \mid s_1, s_2 \in S,\ s_1 - s_2 = d\}$ according to their difference. Obviously $|D_0| = 0$. Suppose that $|D_d| > 1$ for some $d \in G$. Then for any two pairs in D_d, say (s_1, s_2) and (s_3, s_4), we have $s_1 + s_4 = s_2 + s_3$, which implies that $s_1 = s_4$ or $s_2 = s_3$. Without loss of generality, assume that $s_2 = s_3$. Now three cases must be considered separately. In each case below, it is straightforward to verify that the given set D_d is maximal; if D_d would contain another difference, S would not be an S_2-set.

(1) If d is of order 2 in G, then $D_d = \{(s_1, s_2), (s_2, s_1)\}$. We use v_2 to denote the number of d of order 2 with $|D_d| > 1$.
(2) If d is of order 3 in G, then $D_d = \{(s_1, s_2), (s_2, s_4), (s_4, s_1)\}$. We use v_3 to denote the number of d of order 3 with $|D_d| > 1$.
(3) If d is of order greater than 3 in G, then $D_d = \{(s_1, s_2), (s_2, s_4)\}$ with $s_1 \neq s_4$ and $s_4 - s_1 \neq d$. We use v_n to denote the number of d of order greater than 3 with $|D_d| > 1$.

There are $v-1$ possible nonzero differences that may occur at least once. Of these, v_2+v_n may occur twice, and v_3 may occur three times. By counting, we thus obtain the bound

$$v-1+v_2+2v_3+v_n \geqslant k(k-1). \tag{2}$$

Next we shall bound v_n from above. For $d \neq 0$ of order other than 2, we call s a middle element with difference d, if $\{s-d, s, s+d\} \subseteq S$. Additionally, if s is a middle element with difference d, where d is of order 3, then $s-d$ and $s+d$ are also middle elements with difference d. Thus, there are v_3 differences d for which there are three middle elements with difference d and v_n differences d for which there is one middle element with difference d. Now, observe that if s is a middle element with two differences d and d', then $(s-d')+(s+d')=(s-d)+(s+d)$, and we must have $d=\pm d'$; thus, each $s \in S$ can be a middle element with at most two distinct differences (d and $-d$). By calculating the total number of times an element of S occurs as a middle element in two ways, we obtain $3v_3+v_n \leqslant 2k$. Substituting this into (2) gives us

$$v-1+v_2-v_3 \geqslant k(k-3). \tag{3}$$

Now v_2 is bounded by the number of elements of order 2 in G, that is $v_2 \leqslant v/n_2(G)-1$, and $-v_3 \leqslant 0$. The theorem follows from substituting these into (3). □

The following result is given in [6]. Here it is an immediate corollary of the previous theorem.

Corollary 3. $v_\gamma(k) \geqslant k(k-3)$.

Proof. For finite cyclic groups, $v_2 \leqslant 1$, so from (3) we obtain

$$v \geqslant v-1+v_2 \geqslant v-1+v_2-v_3 \geqslant k(k-3). \qquad \square$$

From [2,4] we know that $\binom{k}{2} \leqslant v(k) < k^2+O(k^{36/23})$ and $k^2-O(k) < v_\gamma(k) < k^2+O(k^{36/23})$. For cyclic groups we thus know that the ratio $\alpha = v(k)/k^2$ tends to 1 as k tends to infinity, but in the general Abelian case the upper and lower bounds are separated by a factor of 2.

We examine the lower bound for $v(k)$. If there would be some $\alpha < 1$ such that $v(k) < \alpha k^2$ for infinitely many k, then we could establish that the lower bounds for $v(k)$ and $v_\gamma(k)$ are asymptotically different. After two lemmas, in Theorem 6 we find that the existence of infinitely many such k would imply that for some Abelian group G' there are infinitely many groups G of the form $G' \times \mathbb{Z}_2^m$ that satisfy $|G| < \alpha s(G)^2$.

Lemma 4. *For a given $\alpha < 1$, there are only finitely many Abelian groups G for which $n_2(G) > \alpha/(1-\alpha)$ and $|G| \leqslant \alpha s(G)^2$.*

Proof. By assumption and Theorem 2, for the groups in question we must have

$$\left(1-\frac{1}{n_2(G)+1}\right)\bigl(s(G)^2-3s(G)+2\bigr) < \alpha s(G)^2. \tag{4}$$

Since $1-1/(n_2(G)+1) > \alpha$, there is some s_0 such that (4) can only hold for $s(G) \leqslant s_0$; there is only a finite number of such Abelian groups. □

Lemma 5. *For a given $\alpha < 1$, there are only finitely many Abelian groups G with $n_2(G) \leqslant \alpha/(1-\alpha)$, no direct $\mathbb{Z}_2$-factor, and $|G| \leqslant \alpha s(G)^2$.*

Proof. Note that $n_2(G_1 \times G_2) = n_2(G_2)n_2(G_2)$ for any Abelian G_1 and G_2. Since $n_2(\mathbb{Z}_n)$ equals $n/2$ for even $n \geqslant 2$, and n for odd $n > 2$, we may observe that $n_2(\mathbb{Z}_n) \geqslant n^{1/2}$ for $n > 2$. By induction on the number of direct cyclic factors, we have $n_2(G) \geqslant |G|^{1/2}$ for an Abelian group G with no direct $\mathbb{Z}_2$-factors. Thus $\alpha/(1-\alpha) \geqslant n_2(G) \geqslant |G|^{1/2}$ from which we have $|G| \leqslant \alpha^2/(1-\alpha)^2$; there are only finitely many such Abelian groups. □

Theorem 6. *If for some $\alpha < 1$ there are infinitely many k for which $v(k) < \alpha k^2$, then for some Abelian group G' there are infinitely many Abelian groups G of the form $G' \times \mathbb{Z}_2^m$ for which $|G| < \alpha s(G)^2$.*

Proof. For each k with $v(k) < \alpha k^2$, choose a group G with $s(G) = k$ and $|G| \leqslant \alpha k^2$. By Lemma 4, only finitely many of these groups can have $n_2(G) > \alpha/(1-\alpha)$. Split the remaining infinitely many groups G with $n_2(G) \leqslant \alpha/(1-\alpha)$ into equivalence classes such that two groups G_1 and G_2 are in the same class, if $G_1 = G_2 \times \mathbb{Z}_2^m$ for some m; note that $n_2(G_1) = n_2(G_2)$. Thus each equivalence class is a subset of $\{G' \times \mathbb{Z}_2^m\colon m \geqslant 0\}$ for some Abelian group G' with no direct $\mathbb{Z}_2$-factors and $n_2(G') \leqslant \alpha/(1-\alpha)$, with a distinct G' for each equivalence class. By Lemma 5 there are only a finite number of such G', so there are only a finite number of equivalence classes, and at least one of the classes must contain an infinite number of groups. □

By Theorem 6, to search for infinitely many Abelian groups with $|G| < \alpha s(G)^2$ for any $\alpha < 1$ it suffices to search families of groups where each group in the family is of the form $G' \times \mathbb{Z}_2^m$ for some fixed Abelian group G'. Theorem 2 would seem to suggest that a G' with a small $n_2(G)$ would be the most promising. The following theorem shows that the groups $\mathbb{Z}_4$, $\mathbb{Z}_8$, and $\mathbb{Z}_4^2$ need not be separately considered as G', since using, respectively, $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, and $\mathbb{Z}_2^4$ instead allows packings that are never worse.

Theorem 7. *For all $m \geqslant 0$,*

(1) $s(\mathbb{Z}_2^m \times \mathbb{Z}_4) \leqslant s(\mathbb{Z}_2^{m+2})$,
(2) $s(\mathbb{Z}_2^m \times \mathbb{Z}_8) \leqslant s(\mathbb{Z}_2^{m+3})$, *and*
(3) $s(\mathbb{Z}_2^m \times \mathbb{Z}_4 \times \mathbb{Z}_4) \leqslant s(\mathbb{Z}_2^{m+4})$.

Proof. For the first case, let $G = \mathbb{Z}_2^m \times G'$, where $G' = \mathbb{Z}_4$, let $k = 2$, and define the bijection $f : \mathbb{Z}_2^k \mapsto G'$ as $f([x_1, x_2]) = [2x_1 + x_2]$. For notational convenience, we will represent an $x \in \mathbb{Z}_2^{m+k}$ as an ordered pair $(\bar{x}, \bar{\bar{x}})$ where $\bar{x} \in \mathbb{Z}_2^m$ and $\bar{\bar{x}} \in \mathbb{Z}_2^k$, and an $x \in G = \mathbb{Z}_2^m \times G'$ as an ordered pair $(\bar{x}, \bar{\bar{x}})$ where $\bar{x} \in \mathbb{Z}_2^m$ and $\bar{\bar{x}} \in G'$. We define the bijection $\hat{f} : \mathbb{Z}_2^{m+k} \mapsto G$ by letting $\hat{f}((\bar{x}, \bar{\bar{x}})) = (\bar{x}, f(\bar{\bar{x}}))$.

We will show that $\hat{f}^{-1}$ maps all S_2-sets in G to S_2-sets in $\mathbb{Z}_2^{m+k}$. By contraposition, we need to show that $\hat{f}$ maps all non-S_2-sets in $\mathbb{Z}_2^{m+k}$ to non-S_2-sets in G. It suffices to investigate 4-element subsets, since every set that is not an S_2-set has a 4-element subset that is not an S_2-set.

Let us choose any four-element non-S_2-set $S = \{(\bar{a}, \bar{\bar{a}}), (\bar{b}, \bar{\bar{b}}), (\bar{c}, \bar{\bar{c}}), (\bar{d}, \bar{\bar{d}})\} \subseteq \mathbb{Z}_2^{m+k}$, where $\{\bar{a}, \bar{b}, \bar{c}, \bar{d}\} \in \mathbb{Z}_2^m$ and $\{\bar{\bar{a}}, \bar{\bar{b}}, \bar{\bar{c}}, \bar{\bar{d}}\} \in \mathbb{Z}_2^k$ (repetition of elements is possible here).

Since S is not an S_2-set, we must have $\bar{a}+\bar{b}+\bar{c}+\bar{d}=0$ and $\bar{\bar{a}}+\bar{\bar{b}}+\bar{\bar{c}}+\bar{\bar{d}}=0$. From the structure of $\hat{f}$, it suffices to show that one of $f(\bar{\bar{a}})+f(\bar{\bar{b}})=f(\bar{\bar{c}})+f(\bar{\bar{d}})$, $f(\bar{\bar{a}})+f(\bar{\bar{c}})=f(\bar{\bar{b}})+f(\bar{\bar{d}})$, and $f(\bar{\bar{a}})+f(\bar{\bar{d}})=f(\bar{\bar{b}})+f(\bar{\bar{c}})$ holds for all $\bar{\bar{a}},\bar{\bar{b}},\bar{\bar{c}},\bar{\bar{d}}\in\mathbb{Z}_2^k$ satisfying $\bar{\bar{a}}+\bar{\bar{b}}+\bar{\bar{c}}+\bar{\bar{d}}=0$. This is easy to show: if two of $\bar{\bar{a}}$, $\bar{\bar{b}}$, $\bar{\bar{c}}$, and $\bar{\bar{d}}$ are equal, the remaining two must also be equal, and the condition clearly holds. If, on the other hand, $\{f(\bar{\bar{a}}), f(\bar{\bar{b}}), f(\bar{\bar{c}}), f(\bar{\bar{d}})\}=\{0,1,2,3\}\subseteq\mathbb{Z}_4$, then $0+3=1+2$.

The second and third case can be proven similarly by letting $G'=\mathbb{Z}_8$, $k=3$, and $f([x_1,x_2,x_3])=[4x_1+2x_2+x_3]$ for the second case, and $G'=\mathbb{Z}_4\times\mathbb{Z}_4$, $k=4$, and $f([x_1,x_2,x_3,x_4])=[2x_1+x_2,2x_3+x_4]$ for the third case. However, a somewhat more extensive case by case analysis is required in these cases. □

The next theorem shows that this proof idea cannot be extended to all Abelian 2-groups.

Theorem 8. *Let G be an Abelian 2-group with a subgroup isomorphic to $\mathbb{Z}_{16}$. All bijections $f:\mathbb{Z}_2^m\mapsto G$, where $m=\log_2|G|$ map at least one non-S_2-subset $S\subseteq\mathbb{Z}_2^m$ to an S_2-subset $f(S)\subseteq G$.*

Proof. Suppose the contrary, i.e., there is some f that maps all non-S_2-sets in $\mathbb{Z}_2^m$ to non-S_2-sets in G.

Let H denote a subgroup of G that is isomorphic to $\mathbb{Z}_{16}$. We denote the elements of H with $-8,\dots,7$ in the obvious way. In the following proof we consider the elements H and the elements of $\mathbb{Z}_2^m$ that f maps onto H. In our proof we will repeatedly make use of steps of the following type: if a subset $S=\{a,b,c,d\}\subseteq f^{-1}(H)\subseteq\mathbb{Z}_2^m$ is not an S_2-set, then $f(S)\subseteq H$ must not be an S_2-set. Thus, $f(a)+f(b)=f(c)+f(d)$, $f(a)+f(c)=f(b)+f(d)$, or $f(a)+f(d)=f(b)+f(c)$. By solving for $f(d)$, it is straightforward to find that $f(d)\in\{f(a)+f(b)-f(c), f(a)+f(c)-f(b), f(b)+f(c)-f(a)\}$.

Choose b_0, b_1, and b_2 such that $f(b_0)=0$, $f(b_1)=1$, and $f(b_2)=2$. Let $b_3=b_0+b_1+b_2$. Since $\{b_0,b_1,b_2,b_3\}$ is not an S_2-set in $\mathbb{Z}_2^m$, $\{0,1,2,f(b_3)\}$ must not be an S_2-set in H, and we get $f(b_3)\in\{-1,1,3\}$. Since f is a bijection and $b_1\neq b_3$ ($b_3=b_0+b_1+b_2$ and $b_0\neq b_2$), we get $f(b_3)\neq 1$. Whether $f(b_3)$ equals -1 or 3, in each case, $\{b_0,b_1,b_2,b_3\}$ map to consecutive elements of H; without loss of generality, let $f(b_3)=3$.

Choose b_4 such that $f(b_4)=4$ and let $b_5=b_0+b_1+b_4$ and $b_6=b_0+b_2+b_4$. Since $\{b_0,b_1,b_4,b_5\}$ is not an S_2-set, we must have $f(b_5)\in\{-3,3,5\}$. As $\{b_2,b_3,b_4,b_5\}$ is not an S_2-set, we get $f(b_5)\in\{1,3,5\}$, and as $b_3\neq b_5$, it follows that $f(b_5)=5$.

Since $\{b_0,b_2,b_4,b_6\}$ is not an S_2-set, we similarly obtain $f(b_6)\in\{-2,2,4\}$. By considering $\{b_1,b_3,b_4,b_6\}$ we similarly obtain $f(b_6)\in\{0,2,6\}$. Since $f^{-1}(2)=b_2\neq b_6$, there remains no possible value for $f(b_6)$, a contradiction. □

4. Backtracking with isomorph rejection

Our algorithm for computing a maximum S_2-set in an Abelian group is a backtrack search with isomorph rejection. First an ordering of the elements of the Abelian group G is defined. Starting from an empty set, at each level the algorithm tries adding, in turn, each element that succeeds all elements previously in the set. If the newly added element would cause the property that sums of pairs are distinct to be violated, or if the subset after augmentation is equivalent to a subset that has been searched at another point in the search, then that search branch need not be pursued further. A record of the largest S_2-set found so far is stored throughout the search, and the largest such subset is output at the end.

To describe the isomorph rejection process, we define the canonical representative of an equivalence class of subsets. Recall that $E(G)$ is the group of equivalence mappings in G. Then $E(G)$ partitions the subsets of G into orbits. Once an ordering on the elements of G is defined, the subsets in each orbit can be lexicographically ordered. The canonical representative of each orbit is the lexicographically first subset in that orbit; equivalently a subset S is canonical if no $\psi \in E(G)$ maps S to a set that precedes S in the lexicographical ordering:

$$\text{iscanon}(S): \quad \forall \psi \in E, \quad \psi(S) \succcurlyeq S.$$

It can be shown that if a nonempty subset S is a canonical representative of its equivalence class, then the subset $S \setminus \{\max(S)\}$ is also a canonical representative of its equivalence class. Therefore our algorithm constructs all canonical representatives via a path that consists of canonical representatives only, and throughout the search we may discard all augmentations of the current subset that are not canonical representatives of their equivalence class. Search algorithms with such structure are known as orderly algorithms [8].

Since the automorphism group of an Abelian group may be very large, we do not carry out a complete equivalence test. Our algorithm still constructs the canonical representatives, but it will also construct some subsets that are equivalent to subsets considered in other branches of the search.

We start by choosing an arbitrary element g of maximum order in G. We then compute a set T of automorphisms of G such that for each element $s \in G$ of maximum order, T will contain an automorphism that maps s to g. Throughout the search, we only consider equivalence mappings of the form $\psi(x) = \alpha(x) + b$, where $\alpha \in T$ and $b \in G$. It may be shown that $|T| \geqslant \phi(|G|)$, where ϕ is the Euler totient function, and equality holds for cyclic G; therefore we expect our isomorph rejection to exhibit at least comparable performance with non-cyclic Abelian groups as with cyclic groups.

As an additional simplification aiming to reduce computation time we choose a particular ordering of the elements of G and consider only an appropriate subset of the equivalence mappings for isomorph rejection. For ordering the group elements, we consider them as ordered tuples and order the elements in the lexicographical order of the tuples with the exception that the element g precedes all other elements except the identity element. In testing canonicity of a subset S, we only consider those equivalence mappings that map an ordered pair of elements (s_1, s_2) in the current subset S to $(0, g)$. Such an equivalence mapping exists whenever $s_2 - s_1$ is an element of maximum order in G, and whenever S contains such a pair, the canonical subset must contain the two elements 0 and g. When S contains no pair whose difference would be of maximum order in S, this results in further missed opportunities for pruning the search, but although we have not carried out explicit tests, we expect the faster equivalence testing to compensate for this.

It seems to be an open question whether every maximum S_2-set in a finite Abelian group G contains two elements whose difference is of maximum order in the group, or even whether in every finite Abelian group $|G|$ there is a maximum S_2-set with such two elements. If we restrict ourselves to S_2-sets where there are no such two elements, we can subtract the number of elements of maximum order in $|G|$ from the left-hand side of (2), considerably tightening the bound in Theorem 2. The number of elements of maximum order in a finite Abelian group G can be shown to be at least $\phi(|G|)$, and $\phi(|G|)$ is relatively large compared with $|G|$ when $|G|$ is the product of a small number of prime powers. Curiously, in the context of an analogous

Table 1
Orders that uniquely determine $s(G)$

$s(G)$	$\|G\|$
2	2
3	$3, \dots, 5$
4	$6, \dots, 10$
5	$11, \dots, 15, 17, \dots, 18$
6	$19, \dots, 23, 25, \dots, 27$
7	$28, \dots, 39, 41$
8	$42, \dots, 51, 53, \dots, 55$
9	$56, \dots, 71, 75$
10	$73, \dots, 74, 76, \dots, 79, 82, \dots, 95$
11	$97, 101, \dots, 107, 109, \dots, 113, 115, \dots, 116, 118, \dots, 119$
12	$114, 122, \dots, 124, 126, \dots, 146$
13	$147, \dots, 149, 151, \dots, 161, 163, \dots, 177, 179, 181$
14	$178, 182$
15	183

Table 2
Groups whose order does not uniquely determine $s(G)$

$\|G\|$	$s(G) : G$	$s(G) : G$
16	$5 : \mathbb{Z}_{16}, \mathbb{Z}_2 \times \mathbb{Z}_8$	$6 : \mathbb{Z}_2^4, \mathbb{Z}_2^2 \times \mathbb{Z}_4, \mathbb{Z}_4^2$
24	$6 : \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_{24}$	$7 : \mathbb{Z}_2^3 \times \mathbb{Z}_3$
40	$7 : \mathbb{Z}_2^3 \times \mathbb{Z}_5$	$8 : \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5, \mathbb{Z}_{40}$
52	$8 : \mathbb{Z}_{52}$	$9 : \mathbb{Z}_2^2 \times \mathbb{Z}_{13}$
72	$9 : \mathbb{Z}_2^3 \times \mathbb{Z}_3^2, \mathbb{Z}_8 \times \mathbb{Z}_3^2, \mathbb{Z}_2^3 \times \mathbb{Z}_9, \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3^2,$ $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$	$10 : \mathbb{Z}_{72}$
80	$9 : \mathbb{Z}_2^4 \times \mathbb{Z}_5$	$10 : \mathbb{Z}_{80}, \mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \mathbb{Z}_5, \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5, \mathbb{Z}_4^2 \times \mathbb{Z}_5$
81	$9 : \mathbb{Z}_3^4, \mathbb{Z}_3^2 \times \mathbb{Z}_9$	$10 : \mathbb{Z}_3 \times \mathbb{Z}_{27}, \mathbb{Z}_{81}, \mathbb{Z}_9^2$
96	$10 : \mathbb{Z}_2^5 \times \mathbb{Z}_3, \mathbb{Z}_2^3 \times \mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_3,$ $\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3$	$11 : \mathbb{Z}_2 \times \mathbb{Z}_{16} \times \mathbb{Z}_3, \mathbb{Z}_2^2 \times \mathbb{Z}_8 \times \mathbb{Z}_3, \mathbb{Z}_{96}$
98	$10 : \mathbb{Z}_2 \times \mathbb{Z}_7^2$	$11 : \mathbb{Z}_{98}$
99	$10 : \mathbb{Z}_3^2 \times \mathbb{Z}_{11}$	$11 : \mathbb{Z}_{99}$
100	$10 : \mathbb{Z}_2^2 \times \mathbb{Z}_5^2$	$11 : \mathbb{Z}_2^2 \times \mathbb{Z}_{25}, \mathbb{Z}_{100}, \mathbb{Z}_4 \times \mathbb{Z}_5^2$
108	$10 : \mathbb{Z}_2^2 \times \mathbb{Z}_3^3$	$11 : \mathbb{Z}_2^2 \times \mathbb{Z}_{27}, \mathbb{Z}_2^2 \times \mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{108}, \mathbb{Z}_4 \times \mathbb{Z}_3^3,$ $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9$
117	$11 : \mathbb{Z}_{117}$	$12 : \mathbb{Z}_3^2 \times \mathbb{Z}_{13}$
120	$11 : \mathbb{Z}_2^3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$12 : \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \mathbb{Z}_{120}$
121	$11 : \mathbb{Z}_{11}^2$	$12 : \mathbb{Z}_{121}$
125	$11 : \mathbb{Z}_5 \times \mathbb{Z}_{25}, \mathbb{Z}_5^3$	$12 : \mathbb{Z}_{125}$
150	$12 : \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5^2$	$13 : \mathbb{Z}_{150}$
162	$12 : \mathbb{Z}_2 \times \mathbb{Z}_3^4$	$13 : \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}, \mathbb{Z}_2 \times \mathbb{Z}_9^2\ \mathbb{Z}_2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_9,$ $\mathbb{Z}_{162},$
180	$13 : \mathbb{Z}_2^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5, \mathbb{Z}_2^2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$14 : \mathbb{Z}_{180}, \mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$

covering problem, every sum cover of $\mathbb{Z}_n$ for $n < 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$ is equivalent to one which contains 0 and 1; see [7] and its references.

Table 3
The values of $v(k)$ for $k \leqslant 15$

k	$v(k)$	G	Sample maximum packing
2	2	$\mathbb{Z}_2$	$\{0, 1\}$
3	3	$\mathbb{Z}_3$	$\{0, 1, 2\}$
4	6	$\mathbb{Z}_6$	$\{0, 1, 2, 4\}$
5	11	$\mathbb{Z}_{11}$	$\{0, 1, 2, 4, 7\}$
6	16	$\mathbb{Z}_2^4$	$\{(0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0), (0, 1, 0, 0), (1, 0, 0, 0), (1, 1, 1, 1)\}$
6	16	$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	$\{(0, 0, 0), (0, 0, 1), (0, 0, 2), (0, 1, 1), (1, 0, 1), (1, 1, 3)\}$
6	16	$\mathbb{Z}_4^2$	$\{(0, 0), (0, 1), (0, 2), (1, 0), (2, 3), (3, 0)\}$
7	24	$\mathbb{Z}_2^3 \times \mathbb{Z}_3$	$\{(0, 0, 0, 0), (0, 0, 1, 1), (0, 0, 0, 1), (0, 0, 0, 2), (0, 1, 0, 0), (1, 0, 0, 0), (1, 1, 1, 0)\}$
8	40	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$	$\{(0, 0, 0), (0, 1, 1), (0, 0, 2), (0, 2, 1), (0, 3, 3), (0, 3, 4), (1, 0, 0), (1, 2, 0)\}$
8	40	$\mathbb{Z}_{40}$	$\{0, 1, 5, 7, 9, 20, 23, 35\}$
9	52	$\mathbb{Z}_2^2 \times \mathbb{Z}_{13}$	$\{(0, 0, 0), (0, 1, 1), (0, 0, 1), (0, 0, 2), (0, 1, 4), (0, 1, 7), (1, 0, 0), (1, 0, 4), (1, 0, 9)\}$
10	72	$\mathbb{Z}_{72}$	$\{0, 1, 2, 4, 7, 13, 23, 31, 39, 59\}$
11	96	$\mathbb{Z}_2 \times \mathbb{Z}_{16} \times \mathbb{Z}_3$	$\{(0, 0, 0), (0, 1, 1), (0, 0, 1), (0, 0, 2), (0, 2, 0), (0, 4, 0), (0, 8, 0), (0, 11, 0), (1, 0, 0),$ $(1, 10, 1), (1, 13, 2)\}$
11	96	$\mathbb{Z}_2^2 \times \mathbb{Z}_8 \times \mathbb{Z}_3$	$\{(0, 0, 0, 0), (0, 0, 1, 1), (0, 0, 0, 1), (0, 0, 4, 0), (0, 0, 7, 2), (0, 1, 0, 0), (0, 1, 3, 0),$ $(0, 1, 6, 0), (1, 0, 0, 2), (1, 0, 2, 0), (1, 0, 5, 1)\}$
11	96	$\mathbb{Z}_{96}$	$\{0, 1, 2, 4, 10, 16, 30, 37, 50, 55, 74\}$
12	114	$\mathbb{Z}_{114}$	$\{0, 1, 4, 14, 22, 34, 39, 66, 68, 77, 92, 108\}$
13	147	$\mathbb{Z}_{147}$	$\{0, 1, 2, 4, 7, 29, 40, 54, 75, 88, 107, 131, 139\}$
13	147	$\mathbb{Z}_3 \times \mathbb{Z}_7^2$	$\{(0, 0, 0), (1, 0, 1), (0, 0, 1), (0, 0, 4), (0, 1, 0), (0, 2, 0), (0, 4, 2), (0, 5, 0), (1, 1, 2),$ $(1, 6, 4), (2, 0, 1), (2, 3, 2), (2, 4, 4)\}$
14	178	$\mathbb{Z}_{178}$	$\{0, 1, 2, 4, 16, 51, 80, 98, 105, 111, 137, 142, 159, 170\}$
15	183	$\mathbb{Z}_{183}$	$\{0, 1, 2, 14, 18, 21, 27, 52, 81, 86, 91, 128, 139, 161, 169\}$

5. Conclusions

We calculated the maximum S_2-set in each finite Abelian group up to order 183 using the backtrack procedure described. The results for the cyclic groups are taken from an earlier study reported in [6]. For each group, the size of the maximum such subsets is summarized in Tables 1 and 2. The orders for which $|G|$ determines $s(G)$ are listed in Table 1, and the groups for which $|G|$ alone does not determine $s(G)$ are listed in Table 2.

Of particular interest are the Abelian groups of least order that admit an S_2-set with a given number of elements. These, along with sample maximum packings, are given in Table 3. Even though Theorem 2 would appear to suggest that groups with many elements of order 2 could allow tight packings, the computational results give this hypothesis only weak support: while $v(k) < v_\gamma(k)$ for $k \in \{6, 7, 9\}$, for all other $2 \leqslant k \leqslant 15$ we have $v(k) = v_\gamma(k)$.

It remains an open problem whether it would be possible to find an infinite sequence of k for which $v(k) < \alpha k^2$ for some $\alpha < 1$. We have not been able to answer this question, but we have shown that if there is such a sequence, then there must be an infinite family of the form $F = \{G' \times \mathbb{Z}_2^m\colon m \in M \subseteq \mathbb{N}\}$, where G' is some Abelian group, such that $|G| < \alpha s(G)^2$ for each group G in F.

References

[1] A.E. Brouwer, Bounds on the size of linear codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 295–461.

[2] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, A new table of constant weight codes, IEEE Trans. Inform. Theory 36 (1990) 1334–1380.

[3] R.L. Graham, N.J.A. Sloane, Lower bounds for constant weight codes, IEEE Trans. Inform. Theory 26 (1980) 37–43.

[4] R.L. Graham, N.J.A. Sloane, On additive bases and harmonious graphs, SIAM J. Alg. Discrete Methods 1 (1980) 382–404.

[5] R.K. Guy, Unsolved Problems in Number Theory, second ed., Springer, New York, 1994.

[6] H. Haanpää, A. Huima, P.R.J. Östergård, Sets in $\mathbb{Z}_n$ with distinct sums of pairs, Discrete Appl. Math. 138 (2004) 99–106.

[7] R.E. Jamison, The Helly bound for singular sums, Discrete Math. 249 (2002) 117–133.

[8] R.C. Read, Every one a winner, or how to avoid isomorphism search when cataloguing combinatorial configurations, Ann. Discrete Math. 2 (1978) 107–120.

[9] K. Shoda, Über die Automorphismen einer endlichen abelschen Gruppe, Math. Ann. 100 (1928) 674–686.