Helsinki University of Technology Laboratory for Theoretical Computer Science

Research Reports 87

Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion tutkimusraportti 87

Espoo 2004 HUT-TCS-A87

SETS IN ABELIAN GROUPS WITH DISTINCT SUMS OF PAIRS

Harri Haanpää and Patric R.J. Östergård

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology Laboratory for Theoretical Computer Science
Research Reports 87
Teknillisen korkeakoulun tietojenkäsittelyteorian laboratorion tutkimusraportti 87
Espoo 2004 HUT-TCS-A87

SETS IN ABELIAN GROUPS WITH DISTINCT SUMS OF PAIRS

Harri Haanpää and Patric R.J. Östergård

Helsinki University of Technology
Department of Computer Science and Engineering
Laboratory for Theoretical Computer Science

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietojenkäsittelyteorian laboratorio

Distribution:
Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O.Box 5400
FIN-02015 HUT
Tel. +358-0-451 1
Fax. +358-0-451 3369
E-mail: lab@tcs.hut.fi

ISBN 951-22-6939-2
ISSN 1457-7615

Multiprint Oy
Helsinki 2004

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 $s(G) \geq k$. We develop bounds for $s(G)$, and we determine $v(k)$ for $k \leq 15$ by determining $s(G)$ for Abelian groups of order up to 183 using exhaustive backtrack search with isomorph rejection.

KEYWORDS: Additive base, backtrack search, difference set, packing

CONTENTS

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.

Let $s(G)$ denote the cardinality of the largest S_2-set in G. Two central functions in the study of S_t-sets are $v(k)$ and $v_\gamma(k)$, which give the order of the smallest Abelian and cyclic group G, respectively, for which $s(G) \geq k$. Since cyclic groups are a special case of Abelian groups, clearly $v(k) \leq v_\gamma(k)$, 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 $k \leq 15$ are determined. In this paper we develop bounds for $s(G)$, and we determine $v(k)$ for $k \leq 15$ by determining $s(G)$ 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, 3, 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 $A(k, 6, w) \geq \binom{k}{w}/v(k)$.

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 $k \leq 15$.

2 GROUP AUTOMORPHISM AND SUBSET EQUIVALENCE

By a result attributed to Gauss, every finite Abelian group may be expressed as a direct product of a finite number of cyclic groups of prime power order. This form is particularly convenient for investigating the automorphisms of finite Abelian groups, which were described by Shoda [9]. By arranging together the cyclic direct factors whose orders are powers of the same prime, any finite Abelian group G may be expressed as a direct product of Abelian p-groups, i.e., Abelian groups of prime power order, whose orders are powers of distinct primes. Then $A(G)$, the automorphism group of G, is 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.

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

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

with $\det(M_p) \neq 0 \mod p$, where h_{ij} are integers in the range $0 \leq h_{ij} < p^{e_\mu}$ with $\mu = \max(i,j)$.

The order of an element $g \in G$ is the least positive integer n such that

$$\underbrace{a + \cdots + a}_{n} = 0.$$

The maximum order of an element in an Abelian group is the least common divisor of the orders of the cyclic factors. It can be shown that the number of elements of maximum order in G is at least $\phi(|G|)$, where ϕ is the Euler totient function.

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 $S = \phi(S')$, where $\phi : G \mapsto G$ is a function of the form $\phi(g) = \alpha(g) + b$, where $\alpha \in A(G)$ is an automorphism of G, and $b \in G$ is a constant. The functions ϕ form a group which we denote with $E(G)$ under function composition. The functions ϕ preserve the distinct sums of pairs property, 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 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. In the following, a, b, c, and d are distinct columns of the parity check matrix of an $[n, n-r, 5]$ code, or, equivalently, distinct non-zero elements in an S_2-set that contains the zero element.

Any subset of the set of columns of the parity check matrix of an $[n, n-r, 5]$ code that has fewer than 5 elements is linearly independent, so $a+b+c+d \neq 0$ and $a+b+c \neq 0$ for all a, b, c, and d. In an S_2-set that contains the zero element, $a+b \neq c+d$ and $a+b \neq c+0$ for all a, b, c, and d. Clearly, in $\mathbb{Z}_2^r$ these conditions are equivalent. Therefore, the columns of the parity check matrix of an $[n, n-r, 5]$ code together with the all-zero vector form an S_2-set of size $n+1$, and one can obtain the columns of a parity check matrix of an

$[n, n-r, 5]$ code from an S_2-set of size $n+1$ that contains the all-zero vector by removing the all-zero vector.

It only remains to note that any S_2-set is equivalent to one that contains the zero element, as can easily be seen by choosing an arbitrary element of the S_2-set and applying the equivalence mapping that adds the additive inverse of the chosen element to each element of the set. □

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

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

where $n_2(G)$ is the index of the subgroup of G formed by involutions and the additive 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. $|D_d|$ may be larger than zero for the $v-1$ nonzero elements of G. Suppose that $|D_d| > 1$ for some d. Then any two pairs in D_d, say (s_1, s_2) and (s_3, s_4), must have at least one point in common, or $s_1 + s_4 = s_2 + s_3$ would lead to a contradiction. Without loss of generality, assume that $s_2 = s_3$. Now three cases must be considered separately.

1. If d is of order 2 in G, $D_d \subseteq \{(s_1, s_2), (s_2, s_1)\}$. We denote the number of d of order 2 with $|D_d| > 1$ by v_2.
2. If d is of order 3 in G, $D_d \subseteq \{(s_1, s_2), (s_2, s_4), (s_4, s_1)\}$. We denote the number of d of order 3 with $|D_d| > 1$ by v_3.
3. If d is of order larger than 3 in G, $D_d \subseteq \{(s_1, s_2), (s_2, s_4)\}$ with $s_1 \neq s_4$. We denote the number of d of order larger than 3 with $|D_d| > 1$ by v_n.

It is not difficult to verify that in each of the three cases the sets D_d are maximal.

By counting, we obtain that

$$v - 1 + v_2 + 2v_3 + v_n \geq k(k-1). \qquad (2)$$

For $d \neq 0$ of order other than 2, we call s a middle element with difference d, if $\{s-d, s, s+d\} \subseteq S$. Obviously, if s is a middle element with difference d, then s is also a middle element with difference $-d$. If some s were a middle element with two distinct differences d and d' with $d \neq -d'$, then $(s-d') + (s+d') = (s-d) + (s+d)$ would be a contradiction; thus, each $s \in S$ can be a middle element with at most two distinct differences. Note that 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. It follows that $3v_3 + v_n \leq 2k$. Substituting this into (2) we get

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

Obviously, v_2 is bounded by the number of elements of order 2 in G. Recall that we denote with n_2 the index of the subgroup formed by the involutions and the additive identity. By dropping the $-v_3$ from (3) and substituting $v_2 = v/n_2 - 1$, the theorem follows. □

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

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

Proof. For all cyclic groups, $v_2 \leq 1$ and from (3) we get

$$v \geq v - 1 + v_2 \geq v - 1 + v_2 - v_3 \geq k(k-3).$$

□

It is known that $\binom{k}{2} \leq v(k) < k^2 + O(k^{36/23})$ [2, 4]. It would be interesting to find an infinite sequence of groups G for which $|G| < \alpha s(G)^2$ for some $\alpha < 1$. The theorem following the next lemma shows that it suffices to restrict the attention to families of the form $G' \times \mathbb{Z}_2^m$ for some fixed Abelian group G'.

Lemma 4. *For a given n_0, there are only finitely many Abelian groups G for which $n_2(G) \leq n_0$ and which have no direct $\mathbb{Z}_2$-factor.*

Proof. Note that $n_2(G_1 \times G_2) = n_2(G_1)n_2(G_2)$ for any G_1 and G_2. Since $n_2(\mathbb{Z}_n)$ equals $n/2$ for even $n \geq 2$, and n for odd $n > 2$, we may observe that $n_2(\mathbb{Z}_n) \geq n^{1/2}$ for $n > 2$, and therefore for a group G with no direct $\mathbb{Z}_2$-factors we have that $n_2(G) \geq |G|^{1/2}$. Thus, all groups G of order greater than n_0^2 that have no direct $\mathbb{Z}_2$-factors have $n_2(G) > n_0$, and since there are only a finite number of Abelian groups of order at most n_0^2, the lemma follows. □

Theorem 5. *If for some $\alpha < 1$ there are infinitely many Abelian groups G for which $|G| < \alpha s(G)^2$, 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. Let n_0 be the largest integer for which $1 - \frac{1}{n_0+1} \leq \alpha$.

By assumption and Theorem 2, for the groups in question we must have $(1 - \frac{1}{n_2(G)+1})(s(G)^2 - 3s(G) + 2) < \alpha s(G)^2$. For $n_2(G) > n_0$, since $(1 - \frac{1}{n_2(G)+1}) > \alpha$, there is some s_0 such that the inequality holds for no $s(G) \geq s_0$.

Thus for every G that satisfies the property in the theorem, either $s(G) < s_0$ or $n_2(G_k) \leq n_0$. Since there are only finitely many G with $|G| < \alpha s_0^2$, there must be infinitely many groups for which $n_2(G) \leq n_0$.

Split the infinitely many groups with $n_2(G) \leq n_0$ and $|G| < \alpha s(G)^2$ into equivalence classes such that two groups G_1 and G_2 are in the same class, iff $G_1 = G_2 \times \mathbb{Z}_2^m$ for some m. As $n_2(G_1) = n_2(G_2 \times \mathbb{Z}_2^m) = n_2(G_2)n_2(\mathbb{Z}_2^m)$ and $n_2(\mathbb{Z}_2^m) = 1$, we have that $n_2(G_1) = n_2(G_2)$, and every equivalence class will contain a group with no direct $\mathbb{Z}_2$-factors. However, by the previous lemma there are only a finite number of such groups with $n_2(G) \leq n_0$, so at least one of the classes must contain an infinite number of groups. □

By Theorem 5, to look for an infinite family of groups with $|G| < \alpha s(G)^2$ it is sufficient to examine families of the form $G' \times \mathbb{Z}_2^m$. Theorem 2 would seem to indicate that G' with a small $n_2(G)$ would be most promising. The following theorem lets us exclude certain groups from the search.

Theorem 6. *For all $m \geq 0$,*

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

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

We will show that $\hat{\phi}^{-1}$ maps all S_2-sets in G to S_2-sets in $\mathbb{Z}_2^{m+k}$. By contraposition, we need to show that $\hat{\phi}$ 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 $S = \{a, b, c, d\} \subseteq \mathbb{Z}_2^{m+k}$. We define $\overline{S} = \{\overline{a}, \overline{b}, \overline{c}, \overline{d}\}$ and $\overline{\overline{S}} = \{\overline{\overline{a}}, \overline{\overline{b}}, \overline{\overline{c}}, \overline{\overline{d}}\}$. Note that in $\overline{S} \subseteq \mathbb{Z}_2^m$ and $\overline{\overline{S}} \subseteq \mathbb{Z}_2^k$ repetition of elements is possible.

Since S is not an S_2-set, we must have $\overline{a}+\overline{b}+\overline{c}+\overline{d} = 0$ and $\overline{\overline{a}}+\overline{\overline{b}}+\overline{\overline{c}}+\overline{\overline{d}} = 0$. From the structure of $\hat{\phi}$, also $\overline{\hat{\phi}(a)} + \overline{\hat{\phi}(b)} + \overline{\hat{\phi}(c)} + \overline{\hat{\phi}(d)} = 0$. It remains to show that one of $\phi(\overline{\overline{a}}) + \phi(\overline{\overline{b}}) = \phi(\overline{\overline{c}}) + \phi(\overline{\overline{d}})$, $\phi(\overline{\overline{a}}) + \phi(\overline{\overline{c}}) = \phi(\overline{\overline{b}}) + \phi(\overline{\overline{d}})$, and $\phi(\overline{\overline{a}}) + \phi(\overline{\overline{d}}) = \phi(\overline{\overline{b}}) + \phi(\overline{\overline{c}})$ holds for all $\overline{\overline{a}}, \overline{\overline{b}}, \overline{\overline{c}}, \overline{\overline{d}} \in \mathbb{Z}_2^k$. This can be verified by exhaustive enumeration.

The second and third case can be proven entirely analogously by letting $G' = \mathbb{Z}_8$, $k = 3$, and $\phi([x_1, x_2, x_3]) = [4x_1 + 2x_2 + x_3]$ for the second case, and $G' = \mathbb{Z}_4 \times \mathbb{Z}_4$, $k = 4$, and $\phi([x_1, x_2, x_3, x_4]) = [2x_1 + x_2, 2x_3 + x_4]$ for the third case.

□

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

Theorem 7. *Let G be an Abelian 2-group with $\mathbb{Z}_{16}$ as a subgroup. All bijections $\phi : \mathbb{Z}_2^m \mapsto G$, where $m = \log_2 |G|$ map at least one non-S_2-subset $S \subseteq \mathbb{Z}_2^m$ to an S_2-subset $\phi(S) \subseteq G$.*

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

We denote the elements of a subgroup of G that is isomorphic to $\mathbb{Z}_{16}$ with $0, \ldots, 15$. We will consider the elements of this subgroup, which we denote by $\mathbb{Z}_{16}$, and elements of $\mathbb{Z}_2^m$ that map onto this subgroup. In our proof we will repeatedly make use of steps of the following type: If a subset $S = \{a, b, c, d\} \subseteq \phi^{-1}(\mathbb{Z}_{16}) \subseteq \mathbb{Z}_2^m$ is not an S_2-set, then $\phi(S) \subseteq \mathbb{Z}_{16}$ must not be an S_2-set. Thus, $\phi(a)+\phi(b) = \phi(c)+\phi(d)$, $\phi(a)+\phi(c) = \phi(b)+\phi(d)$, or $\phi(a)+\phi(d) = \phi(b)+\phi(c)$. By solving for $\phi(d)$, it is straightforward to find that $\phi(d) \in \{\phi(a)+\phi(b)-\phi(c), \phi(a)+\phi(c)-\phi(b), \phi(b)+\phi(c)-\phi(a)\}$.

Choose b_0, b_1, and b_2 such that $\phi(b_0) = 0$, $\phi(b_1) = 1$, and $\phi(b_2) = 2$. Let $b_3 = b_0 + b_1 + b_2$. Thus, $\{b_0, b_1, b_2, b_3\}$. Since $\{b_0, b_1, b_2, b_3\}$ is not an S_2-set in $\mathbb{Z}_2^m$, $\{0, 1, 2, \phi(b_3)\}$ must not be an S_2-set in $\mathbb{Z}_{16} \leq B$, and we get $\phi(b_3) \in \{-1, 1, 3\}$. Since ϕ 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 $\phi(b_3) \neq 1$. Whether $\phi(b_3)$ equals -1 or 3, in each case, $\{b_0, b_1, b_2, b_3\}$ map to consecutive elements of the $\mathbb{Z}_{16}$; without loss of generality, let $\phi(b_3) = 3$.

Choose b_4 such that $\phi(b_4) = 4$ 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 $\phi(b_5) \in \{-3, 3, 5\}$. As $\{b_2, b_3, b_4, b_5\}$ is not an S_2-set, we get $\phi(b_5) \in \{1, 3, 5\}$, and as $b_3 \neq b_5$, it follows that $\phi(b_5) = 5$.

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

4 BACKTRACKING WITH ISOMORPH REJECTION

Our algorithm 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 distinct sums of pairs property to be violated, or if the subset after augmentation is equivalent to a subset that has been searched at another point in the search, 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 $\phi \in E(G)$ maps S to a set that precedes S in the lexicographical ordering:

$$\text{iscanon}(S)\colon\ \forall \phi \in E,\ \phi\,(S) \succeq S$$

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].

We do not carry out a complete equivalence test. Choose e to be an element of maximal order in G. For all ordered pairs of elements (s_1, s_2) that lie in the orbit of the pair $(0, e)$ under the action of E, we calculate an equivalence mapping that maps (s_1, s_2) to $(0, e)$. That is, we compute a right transversal $T_{0,e}$ of the subgroup $E_{0,e}$, the subgroup of $E(G)$ that fixes the additive identity and e pointwise. We only use elements of $T_{0,e}$ for isomorph rejection.

We may write $T_{0,e} = T_e T_0$, where T_0 is a right transversal of E_0, the subgroup of $E(G)$ that fixes the additive identity, and T_e is a right transversal of $E_{0,e}$ in E. For all G, $|T_0| = |G|$, and $|T_e|$ equals the length of the orbit of e under $E_0 = A$. All elements of G that are of maximum order lie in the same orbit under the action of A, and their number is bound by $|T_e| \geq \phi(|G|)$, where ϕ is the Euler totient function, and equality holds for those G, each of whose primary Abelian components has exactly one cyclic factor of maximum order. In particular, equality holds for cyclic groups. Thus, for any Abelian group G, $T_{0,e}$ is at least as large as for the cyclic group of the same order. Therefore we expect our isomorph rejection to be at least as effective for Abelian groups as it is for cyclic groups.

The subgroup $E_{0,e}$ may be large for Abelian groups with primary factors that are a direct product of several cyclic groups. In such cases our isomorph rejection procedure misses opportunities for pruning the search. However, we have not expanded our equivalence testing to consider elements in $E_{0,e}$, since for cyclic groups $E = T_{0,e}$, and $E_{0,e}$ consists of the identity mapping only—our search for values of $v(k)$ is limited by the cyclic groups, which we in any case must consider.

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 $T_{0,e}$ for isomorph rejection. For the elements of G we use lexicographical ordering with the exception that the element e precedes all other elements except the identity element. We only consider the elements of $T_{0,e}$ that map an ordered pair of elements (s_1, s_2) in the current subset S to $(0, e)$. In the search branch where both elements are included in the current set this is sufficient, as clearly the canonical subset must also contain those two elements. In the other branches this results in missed opportunities for pruning the search tree. We expect the advantage of faster equivalence checking to compensate for this disadvantage, but have not carried out explicit tests.

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 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.

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 subset is summarized in Table 1 and Table 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 would be advantageous, the experimental results appear not to show any such pattern.

ACKNOWLEDGEMENTS

The work of the first author was supported in part by the Helsinki Graduate School of Computer Science and Engineering (HeCSE) and by the Nokia Foundation, and the work of the second author was supported in part by the Academy of Finland under project no. 100500.

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

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

$\lvert G\rvert$	$s(G) : G$	$s(G) : G$
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	$13 : \mathbb{Z}_2^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5,$ $\mathbb{Z}_2^2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$14 : \mathbb{Z}_{180}, \mathbb{Z}_4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$

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

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	$\mathbb{Z}_{183}$	$\{0, 1, 2, 14, 18, 21, 27, 52, 81, 86, 91, 128, 139, 161, 169\}$

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

REFERENCES

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

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

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

[4] R. L. Graham and 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, 2nd ed. (Springer, New York, 1994).

[6] H. Haanpää, A. Huima, and P. R. J. Östergård, Sets in $\mathbb{Z}_n$ with distinct sums of pairs, Discrete Appl. Math., to appear.

[7] R. E. Jamison, The Helly bound for singular sums, Discr. 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.

HELSINKI UNIVERSITY OF TECHNOLOGY LABORATORY FOR THEORETICAL COMPUTER SCIENCE RESEARCH REPORTS

HUT-TCS-A74	Sam Sandqvist Aspects of Modelling and Simulation of Genetic Algorithms: A Formal Approach. September 2002.
HUT-TCS-A75	Tommi Junttila New Canonical Representative Marking Algorithms for Place/Transition-Nets. October 2002.
HUT-TCS-A76	Timo Latvala On Model Checking Safety Properties. December 2002.
HUT-TCS-A77	Satu Virtanen Properties of Nonuniform Random Graph Models. May 2003.
HUT-TCS-A78	Petteri Kaski A Census of Steiner Triple Systems and Some Related Combinatorial Objects. June 2003.
HUT-TCS-A79	Heikki Tauriainen Nested Emptiness Search for Generalized Büchi Automata. July 2003.
HUT-TCS-A80	Tommi Junttila On the Symmetry Reduction Method for Petri Nets and Similar Formalisms. September 2003.
HUT-TCS-A81	Marko Mäkelä Efficient Computer-Aided Verification of Parallel and Distributed Software Systems. November 2003.
HUT-TCS-A82	Tomi Janhunen Translatability and Intranslatability Results for Certain Classes of Logic Programs. November 2003.
HUT-TCS-A83	Heikki Tauriainen On Translating Linear Temporal Logic into Alternating and Nondeterministic Automata. December 2003.
HUT-TCS-A84	Johan Wallén On the Differential and Linear Properties of Addition. December 2003.
HUT-TCS-A85	Emilia Oikarinen Testing the Equivalence of Disjunctive Logic Programs. December 2003.
HUT-TCS-A86	Tommi Syrjänen Logic Programming with Cardinality Constraints. December 2003.
HUT-TCS-A87	Harri Haanpää, Patric R. J. Östergård Sets in Abelian Groups with Distinct Sums of Pairs. February 2004.

ISBN 951-22-6939-2
ISSN 1457-7615