CONSTRUCTION OF SELF-DUAL RADICAL 2-CODES OF GIVEN DISTANCE

CAROLIN HANNUSCH* and PIROSKA LAKATOS†‡

Institute of Mathematics, Debrecen University
4010 Debrecen, pf.12, Hungary
*carolinhannusch@web.de
†lakatos@science.unideb.hu

Received 10 January 2012
Accepted 4 July 2012
Published 21 September 2012

We prove that for arbitrary $n \in \mathbb{N}$ and $1 \leq d \leq \frac{n+1}{2}$ and for a field $K$ of characteristic 2 there exists an abelian group $G$ of order $2^n$ such that one of the powers of the radical of the group algebra $K[G]$ is a $(2^n, 2^{n-1}, 2^d)$-self-dual code. These codes are constructed for abelian groups $G$ with decomposition

$$G = C_{2^1}^{a_1} \times C_{2^2}^{s_1} \times C_{2^3}^{s_3}$$

i.e., $n = s_1a_1 + 2s_2 + s_3$,

where $a_1 \geq 3$ and $s_i \geq 0$ $(1 \leq i \leq 3)$.

Keywords: Group code; self-dual code; abelian code; radical code.

Mathematics Subject Classification: 94B05, 94B60

1. Introduction

A linear code $C$ is called a group code if $C$ is an ideal in a group algebra $K[G]$ where $K$ is a ring and $G$ is a finite group. Many classical linear error-correcting codes can be realized as ideals of group algebras.

Berman [1], in the case of characteristic 2, and Charpin [2], for characteristic $p \neq 2$, proved that all generalized Reed–Muller codes coincide with powers of the radical of the group algebra over an elementary abelian $p$-group. These codes form an important class containing many codes of practical value. Landrock and Manz [5] showed the relation between these results and the classical result of Jennings [4] related to the structure of the radical of group algebra $GF(p^m)[G]$, where $G$ is a finite $p$-group.

In this paper we solve Problem 2.6 of Drensky and Lakatos [3]. We prove that for arbitrary $n \in \mathbb{N}$ and $1 \leq d \leq \frac{n+1}{2}$ and for a field $K$ of characteristic 2 there

‡Research supported by Hungarian NFSR (OTKA) grant No. NK-81402.
exists an abelian group of order $2^n$ such that one of the powers of the Jacobson radical of group algebra $K[G]$ is a $(2^n, 2^{n-1}, 2^d)$ self-dual code.

The main tool is a theorem of Berman which describes, in term of the canonical decomposition of $G$ as a direct product of cyclic groups, the minimum distance of $R^j$, for $j$ half the nilpotency index of $R$, provided this nilpotency index is even.

1.1. Berman formula for the minimum distance for powers of the radical of abelian group algebra

Let $G$ be a finite abelian $p$-group and $K$ be a finite field of characteristic $p$, i.e., the group algebra $K[G]$ is monomial. If $p$ is an odd prime then the nilpotency index $T$ of the radical of the group algebra $K[G]$ is odd (see [4]). In this case $(R^l)^T = R^{2^T - l}$ for $0 \leq l \leq T$. Therefore for some $j$ ($1 \leq j \leq T$) $R^j$ is self-dual if and only if $j = T - j$ i.e., $T = 2j$. From this it follows that $T$ is even and $j = \frac{T}{2}$. This implies that self-dual abelian radical codes exist only if $p = 2$.

Next we recall Berman’s result [1] only for $p = 2$ (we slightly changed the notations and formulation for our purposes). Denote by $C_i$ the $i$th order cyclic group.

**Theorem [Berman].** Let $$G = C_{2^{a_1}} \times C_{2^{a_2}} \times \cdots \times C_{2^{a_m}},$$
be canonical decomposition of the abelian 2-group $G$ as a direct product of cyclic groups, where $a_1 > \cdots > a_m > 0$. Here $s_1, s_2, \ldots, s_m$ and $a_1, a_2, \ldots, a_m$ are positive integers.

Let $$l_{a_1}, l_{a_1-1}, \ldots, l_0 \quad \text{and} \quad m_{a_1}, m_{a_1-1}, \ldots, m_0$$
be two sequences of integers defined by

$$l_{a_1} = 0, \quad l_{a_1-1} = \cdots = l_{a_2} = s_1, \quad l_{a_2-1} = \cdots = l_{a_3} = s_1 + s_2, \ldots,$$

$$l_{a_m-1} = \cdots = l_{a_m} = s_1 + \cdots + s_{m-1}, \quad l_{a_m-1} = \cdots = l_0 = s_1 + \cdots + s_m,$$

and

$$m_i = l_i \cdot 2^i \quad \text{for} \quad 0 \leq i \leq a_1.$$

Further let $r$ be the largest positive integer such that

$$m_{a_1-1} + m_{a_1-2} + \cdots + m_{a_1-r} \leq j < m_{a_1-1} + m_{a_1-2} + \cdots + m_{a_1-r-1} \quad (1.1)$$

holds, where $0 \leq r \leq a_1 - 1$. With this notation the nilpotency index of the radical $R$ of abelian group algebra $K[G]$ is

$$T = s_1 2^{a_1} + \cdots + s_m 2^{a_m} - (s_1 + s_2 + \cdots + s_m) + 1$$
$$\quad = m_{a_1} + m_{a_1-1} + \cdots + m_0 + 1. \quad (1.2)$$
Construction of Self-Dual Radical 2-Codes of Given Distance

If \( T \) is even and \( j = \frac{T}{2} \) then the minimum distance of the \( j \)th power of \( R \) is \( 2^d \) with

\[
d = l_{a_1} + \cdots + l_{a_1-r} + \left[ \frac{j - (m_{a_1-1} + \cdots + m_{a_1-r}) + 2^{a_1-r-1} - 1}{2^{a_1-r-1}} \right].
\] (1.3)

1.2. Main result

Theorem 1.1. Let \( K \) be a field of characteristic 2. Then for each positive integer \( n \) and each integer \( d \) with \( 1 \leq d \leq \left\lfloor \frac{n+1}{2} \right\rfloor \) there exists an abelian group \( G \) of order \( 2^n \), such that some power of the radical of the group algebra \( K\left[G\right] \) defines a self-dual \( (2^n, 2^n-1, 2^d) \)-code.

Our proof is constructive. To construct the required codes it is enough to take abelian groups which are direct product of cyclic groups of at most three different orders. It is easy to see that if \( G \) is a 2-group, then some power of the radical of \( K[2^2] \) or \( K[G] \) is self-dual. This fact suggests to take abelian groups with one factor of order two. It turned out that in the construction of abovementioned group \( G \) with cyclic components \( C_2 \) and \( C_{2^2} \) satisfy the above-mentioned property.

This does not mean that there are no other groups with this property.

2. Lemmas

Examples show that there are integers \( n \) and \( d \) for which there are nonisomorphic abelian groups \( G_1 \) and \( G_2 \) of order \( 2^n \) such that if \( R_i \) \((i = 1, 2)\) denotes the radical of \( K[G_i] \) and \( T_i \) denotes the nilpotency index of \( R_i \), then both \( T_1 \) and \( T_2 \) are even and both \( R_{1/2} \) and \( R_{2/2} \) are self-dual \( [2^n, 2^{n-1}, 2^d] \)-codes. The difficulties of the construction of groups for each possible minimal distance is to control consecutive distances. It is easy to find groups with small \( d \) (is near to 1) and big distances \( d \) (is near to \( \left\lfloor \frac{n+1}{2} \right\rfloor \)), but it was not simple to find groups with corresponding \( d \) close to \( \frac{n}{4} \). It turned out that our groups can be expressed as the direct product of cyclic subgroups, which are of three different order:

\[
G = C_{2^{s_1}}^{s_1} \times C_{2^{s_2}}^{s_2} \times C_{2^{s_3}}^{s_3},
\] (2.1)

that is

\[
n = s_1 a_1 + 2 s_2 + s_3; \quad s_1, s_2, s_3 \geq 0.
\]

2.1. Notation

Our notation will be fixed throughout this paper. The largest integer not exceeding the number \( a \in \mathbb{R} \) will be denoted by \( \lfloor a \rfloor \). In the sequel \( K \) is a field of characteristic 2 and \( G \) is an abelian 2-group of order \( 2^n \) with decomposition (2.1). Set

\[
T = s_1(2^{s_1} - 1) + 3 s_2 + s_3 + 1 \quad \text{and} \quad j = \frac{T}{2}.
\] (2.2)

By Berman Theorem \( T \) is the nilpotency index of \( K[G] \), for \( G \) as in (2.1). Throughout the paper we assume \( T \) is even. Hence \( j \) is an integer.
The two integer sequences in Berman’s theorem have the form
\begin{align*}
\{ l_1 = 0; & \quad l_{a_1 - 1} = s_1; \ldots; l_2 = s_1; \quad l_1 = s_1 + s_2; \quad l_0 = s_1 + s_2 + s_3; \\
m_i = 2^i l_i & \text{ for } a_1 \geq i \geq 0.
\end{align*}
(2.3)

From (1.1) we get that

\begin{align*}
0 < j < s_1^{a_1 - 1}, \\
r = 1 & \iff s_1 \cdot 2^{a_1 - 1} \leq j < s_1 \cdot (2^{a_1 - 1} + 2^{a_1 - 2}), \\
& \quad \vdots \\
r = a_1 - 1 & \iff s_1 2^{a_1 - 1} + 2s_2 - 2s_1 \leq j,
\end{align*}
(2.4)

and the exponent \( d \) of Hamming distance is given by (1.3) (with the sequences (2.3)). Next we prove four lemmas which are needed in the proof of our main theorem. In the sequel we assume that \( n = a_1 s_1 + 2s_2 + s_3 \).

**Lemma 2.1.** The congruence

\[ n \equiv s_2 \pmod{2} \]  
(2.5)

holds if and only if \( a_1 \) is even and \( s_1 \) is odd.

**Proof.** We have

\[ n = a_1 s_1 + 2s_2 + s_3 \equiv a_1 s_1 + s_3 \pmod{2} \]

and as \( a_1 > 0 \) we have

\[ 0 \equiv T = s_1(2^{a_1 - 1} - 1) + 3s_2 + s_3 + 1 \equiv -s_1 - s_2 + s_3 + 1 \pmod{2}. \]

Thus

\[ s_3 \equiv s_1 + s_2 - 1 \pmod{2}, \]
\[ n \equiv a_1 s_1 + s_3 \pmod{2} \equiv (a_1 + 1)s_1 + s_2 - 1 \pmod{2}. \]

(1) If \( a_1 \) is even then \((a_1 + 1)s_1 \equiv s_1 \pmod{2}\), \( n \equiv s_2 + (s_1 - 1) \pmod{2} \) which shows that (2.5) holds if and only if \( s_1 \) is odd.

(2) If \( a_1 \) is odd then \((a_1 + 1)s_1 \equiv 0 \pmod{2}\), \( n \equiv s_2 - 1 \pmod{2} \), hence (2.5) cannot hold.

**Lemma 2.2.** Suppose \( a_1 \) is fixed and choose \( s_2 = 0 \) or \( s_2 = 1 \). Let \( s'_1 = s_1 + 1 \) choose \( s'_2 = 0 \) or \( s'_2 = 1 \) so that \( n \equiv 2 \) if and only if \( a_1 \) is even and \( s'_1 \) is odd. Let \( s'_3 = n - a_1 s'_1 - 2s'_2 \), \( j \) is given by (2.2) and \( j' = s'_1(2^{a_1 - 1} - 1) + 3s'_2 + s'_3 + 1 \). Then

\[ j' - j = 2^{a_1 - 1} - \frac{a_1 + h}{2}, \text{ where } h = \begin{cases} 
1, & \text{if } a_1 \text{ is odd} \\
2, & \text{if } a_1 \text{ and } n + s_1 \text{ are even} \\
0, & \text{if } a_1 \text{ is even and } n + s_1 \text{ is odd}. 
\end{cases} \]  
(2.6)

1250052-4
Proof. According to Lemma 2.1 by the parities of \( n, a_1, s_1 \), (i.e., \( s_2 = 0 \) if \( n, a_1 \) are even \( s_1 \) is odd, or if \( n \) is odd and either \( a_1 \) is odd or \( s_1 \) is even, and \( s_2 = 1 \) otherwise). By Lemma 2.1 for odd \( a_1 \) we have \( n \not\equiv s_2, n \not\equiv s'_2 \) (mod 2), thus \( s'_2 = s_2 \) for even \( a_1 \) either \( n \equiv s_2, n \not\equiv s'_2 \) (mod 2) or \( n \not\equiv s_2, n \not\equiv s'_2 \) (as the parities of \( s_1, s'_1 \) are different). Hence \( s_2 \neq s'_2 \), more precisely \( s_2 = 0, s'_2 = 1 \) if \( n + s_1 \) is odd and \( s_2 = 1, s'_2 = 0 \) if \( n + s_1 \) is even. Therefore

\[
j' - j = \frac{2^{a_1} - a_1 - 1 + s'_2 - s_2 + 1}{2} = \frac{2^{a_1} - a_1 + s_2 - s'_2 + 1}{2}
\]

and with \( h = s_2 - s'_2 + 1 \) we get (2.6).

Lemma 2.3. If \( r = a_1 - 1 \), then \( j + d = n + 1 \).

Proof. If \( a_1 = r - 1 \) then using (1.3) and (2.3)

\[
d = s_1(a_1 - 1) + s_2 + j - s_1(2^{a_1} - 2) - 2s_2.
\]

Hence, using (2.2)

\[
d + j = s_1(1 + a_1 - 2^{a_1}) - s_2 + 2j = s_1a_1 + 2s_2 + s_3 + 1 = n + 1.
\]

To the next lemma we choose some particular values for \( r \) and \( a_1 \) and increase either \( s_1 \) by 1 or \( s_2 \) by 2 and study how this change influences the value of \( d \).

Lemma 2.4. (a) Let \( r = 2, a_1 = 3 \) and \( s_1 \) be given. Increasing \( s_2 \) by 2 (if this is possible) the value of \( d \) decreases by 1.

(b) Let \( r = 2, a_1 = 4 \) and \( s_1 \) be given. Increasing \( s_2 \) by 2 (if this is possible) the value of \( d \) increases at most by 1.

(c) Let \( r = 1, a_1 > 3 \) be given and choose \( s_2 = 0 \) or \( s_2 = 1 \) according to Lemma 2.1 by the parities of \( n, a_1, s_1 \). Increasing \( s_1 \) by 1 (if this is possible) i.e., \( s'_1 = s_1 + 1 \) \( s'_2 = 0 \) or \( s'_2 = 1 \) according to Lemma 2.1 by the parities of \( n, a_1, s_1 \). Denote the values of \( j \) and \( d \) corresponding to \( s'_1, s'_2 \) by \( j' \) and \( d' \), respectively. Then either \( d' = d \) or \( d' = d + 1 \).

(d) Let \( r = 0, a_1 > 3 \) be given and choose \( s_2 = 0 \) or \( s_2 = 1 \) according to Lemma 2.1 by the parities of \( n, a_1, s_1 \). Increasing \( s_1 \) by 1 (if this is possible) i.e., \( s'_1 = s_1 + 1 \), \( s'_2 = 0 \) or \( s'_2 = 1 \) according to Lemma 2.1 by the parities of \( n, a_1, s_1 \). Then (using the notations of c) either \( d' = d \) or \( d' = d + 1 \).

Proof. (a) If \( s_2 \) is increased by 2 then \( s_3 \) has to decrease by 4 and by (2.2) the value of \( j \) increases by 1. Since \( r = a_1 - 1 \) by Lemma 2.3 \( d = n - j + 1 \). Therefore the increase of \( j \) by 1 results the decrease of \( d \) by 1.

(b) We have \( n = 4s_1 + 2s_2 + s_3 \) and by (2.3) \( m_3 = 8s_1, m_2 = 4s_1, m_1 = 2s_1 + 2s_2 \).

From (2.4) for \( r = 2 \) we have

\[
12s_1 \leq j < 14s_1 + 2s_2.
\]
Substituting \( j \) by (2.2) here and rearranging we get

\[
13s_1 - s_2 - 1 \leq n < 17s_1 + 3s_2 - 1.
\]

By (1.3) using again (2.2) for \( j \) we get

\[
d = 2s_1 + \left[ \frac{j - 12s_1 + 1}{2} \right] = \left[ \frac{-s_1 + 3s_2 + s_3 + 3}{4} \right].
\]  

(2.7)

We see that increasing \( s_2 \) by 2 the value of \( s_3 \) has to decrease by 4, hence the numerator of the last fraction increases by 2 therefore either \( d \) remains unchanged or it increases by 1.

(c) As \( r = 1 \) by (1.3) we have

\[
d = s_1 + \left[ \frac{j - s_12^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} \right],
\]

\[
d' = s_1' + 1 + \left[ \frac{j' - s_1'2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} \right].
\]  

(2.8)

By \( s_1' = s_1 + 1 \) and by (2.6) of Lemma 2.2 we can rewrite \( d' \) as

\[
d' = s_1 + \left[ \frac{j + 2^{a_1-1} - \frac{a_1+h}{2} - (s_1 + 1)2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} \right]
\]

\[
= s_1 + \left[ \frac{j - s_12^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} + \left( 1 - \frac{a_1 + h}{2^{a_1-1}} \right) \right] \leq d + 1,
\]

since for \( a_1 > 3 \) we have \( 0 < \frac{a_1 + h}{2^{a_1-1}} \leq \frac{a_1 + 2}{2^{a_1-2}} < 1 \) therefore \( 0 < 1 - \frac{a_1 + h}{2^{a_1-1}} < 1 \).

(d) As \( r = 0 \) by (1.3) we have

\[
d = \left[ \frac{j + 2^{a_1-1} - 1}{2^{a_1-1}} \right], \quad d' = \left[ \frac{j' + 2^{a_1-1} - 1}{2^{a_1-1}} \right].
\]  

(2.9)

By \( s_1' = s_1 + 1 \) and by (2.6) of Lemma (2.2) we can rewrite \( d' \) as

\[
d' = \left[ \frac{j + 2^{a_1-1} - 1}{2^{a_1-1}} + \left( 1 - \frac{a_1 + h}{2^{a_1}} \right) \right] \leq d + 1,
\]

Since, similarly to the proof of (c), \( 0 < 1 - \frac{a_1 + h}{2^{a_1}} < 1 \).

3. The Proof of Theorem 1.1

The main idea of the proof is to fix the values \( n, a_1, r \) and \( s_1 \) or \( s_2 \). Then we increase (by the smallest possible steps) the value \( s_1 \) or \( s_2 \). We consider only those situations, when the corresponding value of \( d \) is increasing or decreasing at most by 1.
3.1. Construction of the group for \([\frac{n}{2}] + t + 1 \leq d \leq [\frac{n+1}{2}],\) where
\[ t = 1 \text{ if } n \equiv 3, 6 \pmod{8}, \text{ and } t = 0 \text{ otherwise} \]

The largest possible distances can easily be constructed by (1.1)–(1.3).

If \(n\) is even and \(G = C_4 \times C_2 \times \cdots \times C_2\), then \(j = \frac{n+1}{2}\), and \(d = \frac{n}{2}\).

If \(n\) is odd and \(G = C_2 \times C_2 \times \cdots \times C_2\) elementary abelian then \(j = d = \frac{n+1}{2}\).

Let \(a_1 = 3, a_2 = 2, a_3 = 1, r = 2\) and \(s_2 = 0\) or \(s_2 = 2\) if \(n\) is odd, \(s_2 = 1\) and \(s_2 = 3\) if \(n\) is even.

In this case we have \(r = a_1 - 1\) and by Lemma 2.3, \(d = n + 1 - j\), hence from the value of \(j\) we can determine \(d\). By (2.2) if \(a_1 = 3\) and \(s_1\) are fixed and we increase \(s_2\) by 2 then the value of \(j\) is increasing by 1. We can use Lemma 2.4/(a) and get all consecutive values of \(d\) in the interval \([\frac{n}{2}] + t + 1, [\frac{n+1}{2}]\). We have to check the possible values of \(s_2\) for given \(s_1\) by Lemma 2.4/(a), when \(r = 2\) holds.

By Lemma 2.2 if \(s_1' = s_1 + 1\) and \(s_2 = 0\) or \(s_2 = 1\), then

\[ j' - j = 2^3 - 1 - \frac{a_1 + 1}{2} = 2. \]

Thus, for given \(s_1\) it is enough to check the value of \(j\) for the two smallest possible values of \(s_2\). Accordingly, we consider the value of \(j\) for each \(s_1\) only if \(s_2 = 0, 2\) or \(s_2 = 1, 3\), depending on the parity of \(n\) (by Lemma 2.1).

Now with (2.2) and \(s_3 = n - 3s_1 - 2s_2\), we have

\[ j = \frac{7s_1 + 3s_2 + s_3 + 1}{2} = \frac{4s_1 + s_2 + n + 1}{2}. \]

(3.1)

By (2.4) (since now \(r = a_1 - 1\)) we get

\[ 6s_1 + 2s_2 \leq j = \frac{4s_1 + s_2 + n + 1}{2} \]

or \(8s_1 + 3s_2 - 1 \leq n\), i.e.,

\[ s_1 \leq \frac{n - 3s_2 + 1}{8}. \]

(3.2)

When \(s_1\) and \(s_2\) are satisfying the condition (3.2) from Lemma 2.3 we have

\[ d = n - j + 1 = \frac{n - 4s_1 - s_2 + 1}{2}. \]

(3.3)

Thus, for each \(s_1\) satisfying (3.2) and for \(s_2 = 0, 2\) or \(s_2 = 1, 3\) we apply Lemma 2.4/(a) and see that \(d\) decreases by at most 1. If \(s_1\) increases, then \(j\) increases and \(d\) decreases.

If \(n\) is odd then for \(s_2 = 0\) and \(s_2 = 2\) from the inequality (3.2) it follows that \(s_1 \leq \frac{n+1}{4}\) and \(s_1 \geq \frac{n-3}{8}\). For even \(n\) with the values \(s_2 = 1\) and \(s_2 = 3\) we get the conditions \(s_1 \geq \frac{n-2}{8}\) and \(s_1 \leq \frac{n-7}{8}\) similarly. The smallest \(s_1\) with \(r = 2\) is \(2^1 = 0\).

If \(n\) is odd then for \(s_2 = 0\) we have \(j = \frac{n+1}{2}\) by (3.1) and \(d = \frac{n+1}{2}\). If \(n\) is even then \(s_2 = 1\) and \(j = \frac{n+1}{2}\) and \(d = n + 1 - \frac{n+2}{2} = \frac{n}{2}\).

If \(s_1'\) is the maximal value of \(s_1\) and \(s_2 = 0\) or \(s_2 = 1\) satisfy (3.2), then for each \(s_1 < s_1'\) and for the smallest possible value of \(s_2 (s_2' = 0, 2\) or \(s_2' = 1, 3)\) the condition (3.2) is also satisfied.
From the left side of (3.4) and from (2.2) we have

(1) If \( s_2 = 0 \), then from (3.5) we have \( s_1 \leq s_3 + 4 \) and from \( n = s_1a_1 + s_3 \geq s_1(a_1 + 1) - 1 \) the inequality \( s_1 \leq \frac{n + 3}{a_1 + 1} \) follows.

(2) Similarly, if \( s_2 = 1 \), then \( s_1 \leq s_3 + 4 \) and from \( n = s_1a_1 + 2 + s_3 \geq s_1(a_1 + 1) - 2 \) we have \( s_1 \leq \frac{n + 2}{a_1 + 1} \).
Substituting \( j = \frac{\log 2a_1 - n - 2a_1 + 1}{2} \) into (2.8) we get

\[
\overline{d} = \overline{s}_1 + \left[ \frac{j - \frac{2a_1 - 1 + 2a_1 - 1}{2}}{2a_1 - 2} \right] \overline{s}_1 + \left[ -\frac{2a_1 + 1 + 2a_1 - 1}{2a_1 - 1} \right] \overline{s}_1.
\]

By the condition of \( r = 1 \) and (1.3) we have \( d \geq s_1 \), so the equality \( \overline{d} = \overline{s}_1 \) holds.

To find the minimum of \( d \) (denoting it by \( \overline{d} \)) from the right side of (3.4) we get

\[
s_1 2a_1 - 1 > -s_1 + 3s_2 + s_3 + 1.
\]

With \( s_3 = n - a_1 s_1 - 2s_2 \) and \( s_2 = 0 \) or \( s_2 = 1 \) we get

\[
\Delta_1 > \frac{n + 1}{2a_1 - 1 + a_1 + 1} \quad \text{or} \quad \Delta_1 > \frac{n + 2}{2a_1 - 1 + a_1 + 1}.
\]

Thus, \( \Delta_1 = \left[ \frac{n + 1}{2a_1 - 1 + a_1 + 1} \right] + 1 \) or \( \Delta_1 = \left[ \frac{n + 2}{2a_1 - 1 + a_1 + 1} \right] + 1 \).

If \( s_2 = 0 \) then with (2.8) we get

\[
d = s_1 + \left[ \frac{j - \frac{2a_1 - 1 + 2a_1 - 1}{2}}{2a_1 - 2} \right] = s_1 + \left[ -\frac{2a_1 + 1 + 2a_1 - 1}{2a_1 - 1} \right] \geq s_1 + \left[ \frac{2a_1 - 1 - 2}{2a_1 - 1} \right] = 2s_1 - 1.
\]

If \( s_2 = 1 \) then we get analogously that \( \overline{d} \geq 2s_1 - 1 \).

By Lemma 2.4/(c) for \( a_1 > 3 \) we can construct groups for each \( d \) satisfying the inequalities

\[
2s_1 - 1 = 2 \left[ \frac{n + 1}{2a_1 - 1 + a_1 + 1} \right] \leq d \leq \left[ \frac{n + 1}{a_1 + 1} \right] = \overline{s}_1.
\]

If \( a_1 > \log_2(n) + 1 \), then \( n + 1 < 2a_1 - 1 + 1 < 2a_1 - 1 + a_1 + 1 \) and we have \( s_1 = 1 \) and \( d = 2 \).

It is easy to see that for \( a_1 = 4, 5, \ldots, \left[ \log_2(n) \right] + 1 \) these intervals overlap the closed interval \([2, [n+1]]\).

### 3.3. Construction of the group for \([n+1] < d \leq [\frac{5}{4}] - [\frac{n+40}{64}]\)

Let \( a_1 = 4, r = 0, s_2 = 0 \) or \( s_2 = 1 \) (depending on the parity of \( n \)).

By the previous part we have the largest \( d \) if \( a_1 = 4, \overline{s}_1 = \left[ \frac{n+1}{4} \right] \) and \( \overline{d} = \left[ \frac{n+1}{4} \right] \) or \( \overline{d} \leq \left[ \frac{n+2}{4} \right] \), corresponding to \( s_2 = 0 \) or \( s_2 = 1 \). Taking \( s_1 = \overline{s}_1 + 1 \) then \( j - 8s_1 \geq j - 8s_1' \) we have \( r = 0 \), otherwise \( \overline{s}_1 \) would not be the largest at \( r = 1 \). Next we show that \( d' - \overline{d} \leq 1 \), where \( d' \) denotes the value of \( d \) corresponding to \( s_1' \).

If \( j' \) denotes the \( j \) corresponding to \( s_1' \), then in Lemma 2.2 we have \( h = 0 \) or \( h = 2 \), and \( j' = \overline{f} + 5 \), or \( j' = \overline{f} + 6 \), and \( j' = \overline{f} + 8 - \frac{8a_1}{2} < 8s_1' = 8\overline{s}_1 + 8 \). Using
C. Hannusch & P. Lakatos

Table 2. Parameters for the largest $d$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$s_1$</th>
<th>$s_2$</th>
<th>$s_3$</th>
<th>$j$</th>
<th>$d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8$k$</td>
<td>2$k$</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>$15k - 5$</td>
</tr>
<tr>
<td>8$k$ + 1</td>
<td>2$k$</td>
<td>0</td>
<td>1</td>
<td>15$k + 1$</td>
<td></td>
</tr>
<tr>
<td>8$k$ + 2</td>
<td>2$k$</td>
<td>1</td>
<td>0</td>
<td>15$k + 2$</td>
<td></td>
</tr>
<tr>
<td>8$k$ + 3</td>
<td>2$k$</td>
<td>0</td>
<td>3</td>
<td>15$k + 2$</td>
<td></td>
</tr>
<tr>
<td>8$k$ + 4</td>
<td>2$k$</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>$15k + 10$</td>
</tr>
<tr>
<td>8$k$ + 5</td>
<td>2$k$</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>$15k + 10$</td>
</tr>
<tr>
<td>8$k$ + 6</td>
<td>2$k$</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>$15k + 9$</td>
</tr>
<tr>
<td>8$k$ + 7</td>
<td>2$k$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$15k + 10$</td>
</tr>
</tbody>
</table>

(2.9), we get for $d'$ that

$$d' = \left[ \frac{j' + 7}{8} \right] < \left[ \frac{8s_1 + 7}{8} \right] = \left[ \frac{8s_1 + 15}{8} \right] = s_1 + 1.$$  

The largest value of $s_1$, for which the condition $r = 0$ holds, is $\left[ \frac{n}{8} \right]$ or $\left[ \frac{n}{8} \right] - 1$, depending on the parity condition of Lemma 2.1 with $s_2 = 0$ or $s_2 = 1$ and $0 \leq s_3 \leq 3$. Since for arbitrary integers $a, k \geq 0$ we have $\left[ \frac{15k + a}{8} \right] = 2k - \left[ \frac{b - a + 7}{8} \right]$ in our case in Table 2 we have the following largest values of $d$.

Using Lemma 2.4/(d) we have all values of $s_1 + 1 = \left[ \frac{n + 1}{8} \right] + 1 \leq d \leq \left[ \frac{n}{8} \right] - \left( \frac{n + 40}{64} \right)$.

3.4. Construction of the group for $\left[ \frac{n}{8} \right] + 1 - \left( \frac{n + 40}{64} \right) \leq d \leq \left[ \frac{n}{8} \right] + t$, where $t = 1$, if $n \equiv 3, 6 \pmod{8}$, otherwise $t = 0$

In Table 3 we list the constructed and missing values of $d$. Here $\lambda_n = \left( \frac{n + 40}{64} \right) - 1$, $t = 1$ if $n \equiv 3, 6 \pmod{8}$ and $t = 0$ if $n \not\equiv 3, 6 \pmod{8}$.

Table 3. Missing values of $d$ close to $\left[ \frac{n}{8} \right]$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>Missing $d$</th>
<th>Constructed in part 3.1</th>
<th>Constructed in parts 3.2 and 3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n \leq 13$</td>
<td>none</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 1$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right]$</td>
</tr>
<tr>
<td>$15 \leq n \leq 23, t = 0$</td>
<td>none</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 1$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right]$</td>
</tr>
<tr>
<td>$14 \leq n \leq 23, t = 1$</td>
<td>$\left[ \frac{n}{8} \right] + 1$</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 2$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right]$</td>
</tr>
<tr>
<td>$24 \leq n \leq 87, t = 0$</td>
<td>$\left[ \frac{n}{8} \right]$</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 1$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right] - 1$</td>
</tr>
<tr>
<td>$24 \leq n \leq 87, t = 1$</td>
<td>$\left[ \frac{n}{8} \right], \left[ \frac{n}{8} \right] + 1$</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 2$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right] - 1$</td>
</tr>
<tr>
<td>$n \geq 87, t = 0$</td>
<td>$\left[ \frac{n}{8} \right] + 1 \leq d &lt; \left[ \frac{n}{8} \right] - \lambda_n + 1$</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 1$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right] - \lambda_n + 1$</td>
</tr>
<tr>
<td>$n \geq 87, t = 1$</td>
<td>$\left[ \frac{n}{8} \right] \leq d &lt; \left[ \frac{n}{8} \right] - \lambda_n$</td>
<td>$d \leq \left[ \frac{n}{8} \right] + 2$</td>
<td>$1 \leq d \leq \left[ \frac{n}{8} \right] - \lambda_n$</td>
</tr>
</tbody>
</table>
Let \( a_1 = 4, s_1 = \lceil \frac{n + 7}{18} \rceil, r = 2 \).

(1) If \( 14 \leq n \leq 23 \) then for the constructions of \( d = \lceil \frac{n}{4} \rceil + 1 \) we only need to consider the values of \( n = 14 \) and \( n = 19 \). One can check easily that for \( n = 14 \) (\( a_1 = 4 \)), we have \( s_1 = 1, s_2 = 4, d = 4 \) and for \( n = 19 \) (\( a_1 = 4 \)), we have \( s_1 = 1, s_2 = 3, d = 5 \).

(2) Now we suppose \( n > 23 \).

By Lemma 2.4/(b) we have to find at \( r = 2 \) the maximum of \( s_2 (\overline{s}_2) \) and minimum of \( s_2 (\underline{s}_2) \) and to estimate the minimum of the maximum of \( d \) (denoted by \( \overline{d} \)) and the maximum of the minimum of \( d \) (denote by \( \underline{d} \)) to cover the missing values of \( d \).

By \( n = 4s_1 + 2s_2 + s_3 \) and by (1.3) the condition \( r = 2 \) gives

\[
12s_1 \leq j < 14s_1 + 2s_2. 
\]

Substituting \( j \) (defined by (2.2)) into (3.6), we have

\[
13s_1 - s_2 - 1 \leq n < 17s_1 + 3s_2 - 1. 
\]

We have to estimate the minimum of the maximum of \( d \) (denoted by \( \overline{d} \)) and the maximum of the minimum of \( d \) (denote by \( \underline{d} \)) to cover the missing values of \( d \). It is easy to see that for \( n = 4 \lceil \frac{n + 7}{18} \rceil + 2s_2 + s_3 \) the left side of the inequality (3.7) holds for all \( s_2 \geq 0 \). Thus, for the maximum of \( s_2 \) (denoted by \( \overline{s}_2 \)) the value of \( s_3 \) is the smallest possible \( s_3 = 0, 1, 2, 3 \) depending on parities. Clearly \( \frac{n + 7}{18} \geq s_1 \geq \frac{a_1}{18} \). And \( s_3 \geq 0 \) we have \( n \geq 4s_1 + 2s_2 \) and \( \frac{n - 4s_1}{2} \geq \overline{s}_2 \geq \frac{n - 4s_1 - 3}{2} \). For the minimum of \( \overline{d} \) (at \( s_3 = 3 \)) by (2.7) we get

\[
\overline{d} \geq \left[ \frac{-s_1 + 3 \frac{n - 4s_1 - 3}{2} + 6}{4} \right] = \left[ \frac{3n - 14s_1 + 3}{8} \right].
\]

From this and by \( n > 23 \) we have

\[
\overline{d} \geq \left[ \frac{31n - 8}{120} \right] = \left[ \frac{n + \frac{n - 8}{10}}{4} \right] = \frac{n}{4}.
\]

The right-hand side of (3.7) gives \( s_2 > \frac{n - 17s_1 + 3}{18} \), thus the nearest integer is the minimum of \( s_2 \) (denoted by \( \underline{s}_2 \)),

\[
\underline{s}_2 \leq \left[ \frac{n - 17s_1 + 4}{3} \right] \leq \left[ \frac{n - 17 \frac{n - 8}{10} + 4}{3} \right] = \left[ \frac{-2n + 179}{45} \right].
\]

Since for \( n > 23 \) we have \( \frac{-2n + 179}{45} < 3 \), thus for \( \underline{s}_2 = 1 \) or \( \underline{s}_2 = 2 \) (depending on parity condition) we have \( r = 2 \).

In this case \( \overline{d} \) can be calculated by (2.7) \( (d = \left[ \frac{-s_1 + 3s_2 + ss_3 + 3}{2} \right]). \) Since the value \( d \) increases if \( s_2 \) increases and \( s_3 \) decreases, and at \( \underline{s}_2 = 1 \) or \( \underline{s}_2 = 2 \) we get

\[
12s_1 \leq j < 14s_1 + 2s_2. 
\]

Substituting \( j \) (defined by (2.2)) into (3.6), we have

\[
13s_1 - s_2 - 1 \leq n < 17s_1 + 3s_2 - 1. 
\]
Now, only the construction for \( d = \left\lfloor \frac{n}{4} \right\rfloor + 1 \) from Table 4 is needed.

The proof of Theorem 1.1 is completed.

The last inequality for \( 23 < n \leq 28 \) one can check directly and for \( n > 28 \) follows from

\[
\left\lfloor \frac{10n + 96}{60} \right\rfloor \leq \frac{10n + 96}{60} \leq \frac{15n - 24}{64} \\
\leq \frac{n - 3}{4} + 1 - \frac{n + 40}{64} \leq \left\lfloor \frac{n}{4} \right\rfloor + 1 - \left\lfloor \frac{n + 40}{64} \right\rfloor.
\]

Now, only the construction for \( d = \left\lfloor \frac{n}{4} \right\rfloor + 1 \) if \( n \equiv 3, 6 \pmod{8} \) is left.

If \( n = 8k + 3 \), and \( k \geq 5 \), we have \( d = \left\lfloor \frac{n}{4} \right\rfloor + 1 \) since \( \left\lfloor \frac{n}{4} \right\rfloor = \left\lfloor \frac{2k+3}{4} \right\rfloor = 2k \), \( \frac{n}{4} = 2k + 0, 75 \) and

\[
d \geq \left\lceil \frac{31n - 8}{120} \right\rceil = \left\lceil \frac{31 \cdot 4k + 8}{120} \right\rceil = \left\lceil \frac{124(2k + 0.75) - 8}{120} \right\rceil \\
= 2k + \left\lceil \frac{8k + 85}{120} \right\rceil \geq \left\lfloor \frac{n}{4} \right\rfloor + 1
\]

holds if \( 8k + 85 \geq 120 \), i.e., \( k \geq 5 \), and \( n \geq 43 \).

In similar manner, if \( n = 8k + 6 \), and \( k \geq 6 \), we get \( d = \left\lfloor \frac{n}{4} \right\rfloor + 1 \). If \( \frac{n}{4} = 2k + 1 \), then \( \frac{n}{4} = 2k + 1, 5 \), i.e.,

\[
d \geq \left\lceil \frac{31n - 8}{120} \right\rceil = \left\lceil \frac{31 \cdot 4k + 8}{120} \right\rceil = \left\lceil \frac{124(2k + 1, 5) - 8}{120} \right\rceil \\
= 2k + 1 + \left\lceil \frac{8k + 58}{120} \right\rceil \geq \left\lfloor \frac{n}{4} \right\rfloor + 1,
\]

if \( 8k + 58 \geq 120 \), and \( k \geq 8 \), thus \( n \leq 70 \).

If \( 24 \leq n < 43 \) and \( n = 8k + 3 \), i.e., \( n = 27, 35, 43 \) as well as if \( 24 \leq n > 70 \), and \( n = 8k + 6 \), i.e., \( n = 30, 38, 46, 54 \), and \( 62 \), then for \( a_1 = 4 \), \( s_1 = \left\lfloor \frac{n+4}{15} \right\rfloor \), \( r = 2 \) we can get \( d = \left\lfloor \frac{n}{4} \right\rfloor + 1 \) by the constructions listed in Table 4.

The proof of Theorem 1.1 is completed.
References


