Egyetemi doktori (PhD) értekezés

MONOMIAL CODES IN THE RADICAL OF MODULAR GROUP ALGEBRAS AND THEIR PROPERTIES

Hannusch Carolin

Témavezető: Dr. Lakatos Piroska

DEBRECENI EGYETEM
TERMÉSZETTUDOMÁNYI DOKTORI TANÁCS
MATEMATIKA- ÉS SZÁMÍTÁSTUDOMÁNYOK DOKTORI ISKOLA

Debrecen, 2017

Ezen értekezést a Debreceni Egyetem Természettudományi Doktori Tanács Matematika- és Számítástudományok Doktori Iskola *Gyűrűelmélet: csoportalgebrák és egységcsoportok* programja keretében készítettem a Debreceni Egyetem természettudományi doktori (PhD) fokozatának elnyerése céljából.

Debrecen, 2017. 08. 29.

Hannusch Carolin
jelölt

Tanúsítom, hogy Hannusch Carolin doktorjelölt 2012-2017 között a fent megnevezett Doktori Iskola *Gyűrűelmélet: csoportalgebrák és egységcsoportok* programjának keretében irányításommal végezte munkáját. Az értekezésben foglalt eredményekhez a jelölt önálló alkotó tevékenységével meghatározóan hozzájárult. Az értekezés elfogadását javasolom.

Debrecen, 2017. 08. 29.

Lakatos Piroska
témavezető

MONOMIAL CODES IN THE RADICAL OF MODULAR GROUP ALGEBRAS AND THEIR PROPERTIES

Értekezés a doktori (Ph.D.) fokozat megszerzése érdekében
matematika tudományágban

Írta: Hannusch Carolin okleveles matematikus

Készült a Debreceni Egyetem Matematika- és Számítástudományok Doktori Iskolája (Gyűrűelmélet: csoportalgebrák és egységcsoportok) keretében.

Témavezető: Dr. Lakatos Piroska

A doktori szigorlati bizottság:

elnök:	Dr. Pethő Attila	.....
tagok:	Dr. Pálfy Péter Pál	.....
	Dr. Horváth Gábor	.....

A doktori szigorlat időpontja: 2017.03.24.

Az értekezés bírálói:

	Dr.	.....
	Dr.	.....

A bírálóbizottság:

elnök:	Dr.	.....
tagok:	Dr.	.....
	Dr.	.....
	Dr.	.....
	Dr.	.....

Az értekezés védésének időpontja: 2017.

Acknowledgements

I want to thank my supervisor Piroska Lakatos for the enormous help and motivation I received from her during my years as student and later as PhD student and for always showing me an example of dedication to this profession in all cases of life. This thesis would not appear in the present form without her support and encouragement. I also thank my colleagues at the Institute of Mathematics for always being a great team with helpful and inspiring thoughts, just to point out some of them: Nóra Varga, Attila Bérczes, István Gaál, Lajos Hajdu, Gábor Horváth and Gábor Nyul. I want to thank Zoltán Halasi for so many patient and endless surveys in the deep theory of algebra and also for a lot of inspiring ideas. These were an essential part of my PhD studies. Last, but not least, I want to thank my family: my parents for supporting me while I was a student, my husband for his great understanding and support and every-day motivation and my sons for their patience and for the fact that they like the university's buildings at least as much as the playground yard.

To Anton and Vincent

Preface

Coding Theory is one of the youngest theory within the research areas of mathematics. Its start is considered to be the paper *A mathematical theory of communication* by Shannon in 1948 [S]. Since then a lot of researchers contributed to the theory and a very fast development has been started. First mention of error-correcting codes goes hand in hand with the invention of Reed-Muller codes in 1953 [MR]. Details on the development of Coding Theory in the 1950's can be found in [R]. In that time mathematicians like Reed, Muller, Golay and Fano shaped the Theory of Information and Coding fundamentally. Since then Coding Theory went through a great development, see for example [MS] and [PH]. Error-correcting codes build up an important class of codes. They have been used in digital communication, e.g. on CD's or other devices for saving data and information. Coding Theory is a beautiful mathematical theory. Some general surveys of linear codes are for example [AK] and [M]. Even nowadays it is an exciting area of applied mathematics with a lot of open problems, see for example [JK], [DKS]. In the current thesis we show some new results on linear codes and convey the theoretical background which is needed. We deal mainly with some problems on group codes, i.e. on codes which are ideals of group algebras. We investigate the properties of these codes related to the structure of modular group algebras.

Contents

Chapter 1

Introduction

The pictures are there, and you just take them.

Robert Capa

Let p be a prime number and $\mathbb{F}$ be a finite field of characteristic p, i.e. $\mathbb{F} = GF(p^m)$ for some integer m. We will use the notation $\mathbb{F}_p$ for the field of p elements. Some results in this thesis are concerning the binary case, i.e. $p = 2$, but we will also introduce some results for arbitrary prime numbers p. Further, if not stated otherwise, G is a finite abelian p-group. Then the group algebra $\mathbb{F}[G]$ is modular and $\mathbb{F}[G]$ is a commutative ring of characteristic p. The Jacobson radical is the intersection of all maximal ideals. The Jacobson radical was only introduced in 1945 in [Jac], whereas we use some basic theorems of Jennings, which were published in 1939 in [J]. Jennings then worked with the nilradical, which means he considered the radical to be an ideal containing all nilpotent elements of the group algebra. In our case the characteristic of $\mathbb{F}$ is p, where p is prime and G is a finite p-group. Thus the group algebra $\mathbb{F}[G]$ is local, Noetherian and Artinian. By Corollary 8.2 in [AM] the Jacobson radical

and the nilradical coincide in this case. The codes being constructed in this thesis are ideals of the underlying modular group algebra.

Definition 1.1. *Let G be a finite group of order n, $\mathbb{F}$ an arbitrary field. We denote the elements of G by $g_1, \ldots, g_n$. Then the group algebra $\mathbb{F}[G]$ is an algebra over $\mathbb{F}$ consisting of all possible linear combinations of $g_1, \ldots, g_n$ with coefficients $\theta_i \in \mathbb{F}$. Thus*

$$\mathbb{F}[G] = \{\sum_{i=1}^{n} \theta_i g_i, \text{ where } \theta_i \in \mathbb{F}\}.$$

If $\theta_i, \rho_j, \lambda \in \mathbb{F}$ and $g_i, g_j \in G$, then we have the following operations in $\mathbb{F}[G]$:

$$\sum_{i=1}^{n} \theta_i g_i + \sum_{i=1}^{n} \rho_i g_i = \sum_{i=1}^{n} (\theta_i + \rho_i) g_i,$$

$$\sum_{i=1}^{n} \theta_i g_i \cdot \sum_{j=1}^{n} \rho_j g_j = \sum_{\substack{i,j,k \\ g_i g_j = g_k}} (\theta_i \cdot \rho_j) g_k,$$

$$\lambda \sum_{i=1}^{n} \theta_i g_i = \sum_{i=1}^{n} \lambda \theta_i g_i.$$

In this dissertation we only consider modular group algebras, i.e. $\mathbb{F}$ is a finite field of characteristic p and G is a finite abelian p-group.

For an arbitrary integer ν we have that $\mathbb{F}^\nu$ is a vector space with the usual addition and multiplication. A κ-dimensional subspace of $\mathbb{F}^\nu$ is called **linear code** $\mathcal{C}$ of length ν and dimension κ. If $\mathbb{F}$ has characteristic 2, then $\mathcal{C}$ is called **binary code**. Let $\mathcal{C}$ be a linear code and $x, y \in \mathcal{C}$ two codewords. The **Hamming weight** of x is the number of its non-zero coordinates. The **Hamming distance** of x and y is the weight of $x - y$. The Hamming distance (or weight) of a linear code $\mathcal{C}$ is the minimum of all nonzero Hamming distances. A binary code is called **doubly even** if the

Hamming weight of all its codewords is divisible by 4. If $\mathcal{C}$ is a (ν, κ, δ)-code, where ν is the code length, κ its dimension as a vector space and δ its minimum distance, then we know by the Singleton bound ([MS], Theorem 11) that $\delta \leq \nu - \kappa + 1$. We will use Greek letters conventionally in the general case. In many results the code length, dimension and minimum distance occur to be powers of p. Then we denote the code as (p^n, p^k, p^d)-code. The **dual code** of a linear code $\mathcal{C}$ is denoted by $\mathcal{C}^\perp$ and is defined by

$$\mathcal{C}^\perp = \{x \in \mathbb{F}^\nu \mid \langle x, c \rangle = 0 \ \ \forall c \in \mathcal{C}\},$$

where $\langle x, c \rangle = \sum_{i=1}^{\nu} x_i c_i$ denotes the usual scalar product. We say that $\mathcal{C}$ is **self-orthogonal** if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and $\mathcal{C}$ is **self-dual** if $\mathcal{C} = \mathcal{C}^\perp$.

Throughout the dissertation, we use the notation of C_n for the cyclic group of order n and S_n for the symmetric group on a set with n elements.

A linear code $\mathcal{C}$ is called **group code** if it is an ideal in the group algebra $\mathbb{F}[G]$. If G is a p-group, then $\mathcal{C}$ is called **p-code**. If G is abelian, then $\mathcal{C}$ is called **abelian group code**.

Our work is based on several classical results. Berman showed in [B] the connection between Reed-Muller codes and the Jacobson radical of a group algebra $\mathbb{F}[G]$, where G is an elementary abelian 2-group and $char(\mathbb{F}) = 2$. Later, Charpin proved in [C] this connection for the Generalized Reed-Muller codes and the Jacobson radical of a group algebra $\mathbb{F}[G]$, where G is a finite p-group and $char(\mathbb{F}) = p$. Jennings worked out the structure of the radical of a group algebra $\mathbb{F}[G]$ in [J]. The relation between Jennings result and the results of Berman and Charpin was shown by Landrock and Manz in [LM].

If we have two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length ν, then we can compare the two codes in the following sense. If $\mathcal{C}_1$ is a $(\nu, \kappa_1, \delta_1)$-code and $\mathcal{C}_2$ is a $(\nu, \kappa_2, \delta_2)$-code, then we say that $\mathcal{C}_1$ has better parameters than $\mathcal{C}_2$ if $\kappa_1 < \kappa_2$ and $\delta_1 = \delta_2$, or if $\kappa_1 = \kappa_2$ and $\delta_1 > \delta_2$.

In this dissertation we consider abelian p-codes. The general case (when G is also allowed to be non-abelian) was treated by Ward in [W2]. If G is a p-group, then it is known (see [F] and [AK], p. 25-26) that the best codes arise if G is elementary abelian. In this thesis we also construct some radical p-codes, where G is not elementary abelian. It is clear that these codes are mainly theoretically interesting, since they can not have the "best" parameters, i.e. the dimension of these codes is not optimal compared to their minimum distance.

This thesis is built up in the following way. In Chapter 2 we introduce monomial codes and Reed-Muller codes. Although we work with Reed-Muller codes as monomial codes, we also introduce two other definitions because these may be more convenient to other equivalent definitions.

In Chapter 3 we construct codes which are powers of the radical of modular group algebras over abelian 2-groups. In this chapter we answer a question about self-dual binary abelian group codes with given distance which was asked by Drensky and Lakatos in [DL].

Afterwards we give new classes of binary abelian group codes which are self-dual in Chapter 4. These codes are abelian group codes over elementary abelian 2-groups and they have similarly good parameters as the Reed-Muller codes.

Finally, we introduce some other new classes of abelian group codes with special properties and study the automorphism groups of some of them in Chapter 5. The codes constructed here are ideals in modular group algebras of elementary abelian p-groups for an arbitrary prime p.

The results of this thesis are published in the following papers:

- Hannusch, Lakatos [HL1], which is the basis for Chapter 3
- Hannusch, Lakatos [HL2], which is the basis for Chapter 4
- Hannusch [H], which is the basis for Chapter 5.

Chapter 2

Linear codes as ideals in group algebras

2.1 Monomial codes

Jennings investigated in [J] the radical of $\mathbb{F}[G]$ when $\mathbb{F}$ is a field of characteristic p and G is a p-group. In this case the group algebra $\mathbb{F}[G]$ is not semi-simple (i.e. it can not be regarded as the direct sum of simple submodules). We consider modular group algebras $\mathbb{F}_p[G]$, where $\mathbb{F}_p$ denotes the field of p elements. We denote the Jacobson radical of $\mathbb{F}_p[G]$ by $\jmath$ or $\jmath(\mathbb{F}_p[G])$. Jennings gave a generating set of the radical and its powers. Since we will use this generating set in many places of this thesis, we recall some main theorems of [J] here. The main results of this dissertation are a contribution to the theory of abelian p-codes.

Theorem 2.1 (Theorem 1.2 in [J])**.** *Let G be a group of order p^m and let $\mathbb{F}_p$ be the field of p elements. Then $\jmath$ is of rank $p^m - 1$, which means it can be generated by $p^m - 1$ elements. Further it has a generating set with all its elements of the form $g_i - 1$, where $g_i \in G$, $g_i \neq 1$. Further let*

$\sum \theta_i g_i \in \mathbb{F}_p[G]$, *where* $\theta_i \in \mathbb{F}_p$. *Then* $\sum \theta_i g_i \in \mathcal{J} \Leftrightarrow \sum \theta_i = 0$.

Theorem 2.2 (Theorem 2.2 in [J]). *Let* $M_j = \{g_j \in G | g_j - 1 \equiv 0 \mod \mathcal{J}^j\}$. *We denote the nilpotency index of* $\mathcal{J}$ *by N, and we have*

$$\mathcal{J} \supset \mathcal{J}^2 \supset \ldots \supset \mathcal{J}^{N-1} \supset \mathcal{J}^N = 0.$$

Then the elements of M_j *can be written in the form* $1 + \eta_j$, *where* $\eta_j \in \mathcal{J}^j$. *Further, the* M_j*-s form a decreasing series of characteristic subgroups of G:*

$$G = M_1 \supseteq M_2 \supseteq \ldots \supseteq M_N = 1.$$

The previous series is called the M-series or Jennings-series or Brauer-Jennings-Zassenhaus-series and it is a chief series of G. The factor groups M_i/M_{i+1} are elementary abelian. Now, we are able to give generating sets for the M_j-s and afterwards a generating set for the powers of the radical.

Theorem 2.3 (Theorem 2.8 in [J]). *A minimal generating set* $\{x_{j,1}, \ldots, x_{j,d_j}\}$ *for* M_j *modulo* M_{j+1} *can be taken as any maximal set of elements*

$$\{x_{j,i} \in M_j | (x_{j,i} - 1) \text{ are linearly independent modulo } \mathcal{J}^{j+1}\}.$$

Theorem 2.4 (Theorem 3.2 in [J]). *Let* $1 \leq k \leq N-1$ *and we denote for fix k the following products*

$$B_j^k = \prod_{i,j} (x_{j,i} - 1)^{\theta_{j,i}},$$

where $0 \leq \theta_{j,i} \leq p-1$ *and* $\sum_{i,j}(j\theta_{j,i}) = k$. *Then the elements* B_j^h *with* $h \geq k$ *form a generating set of* $\mathcal{J}^k$.

In Chapter 3 we will construct binary self-dual abelian group codes of given length for all possible distances. These codes are powers of the

radical of the corresponding modular group algebra $\mathbb{F}[G]$, where G is an abelian p-group, but G is not necessarily elementary abelian. Whereas the linear codes introduced in Chapter 4 and Chapter 5 are ideals of a group algebra $\mathbb{F}[G]$, where G is an elementary abelian p-group of rank m. In order to point out the role of p and m in the second case, we denote the group algebra $\mathbb{F}_p[\underbrace{C_p \times \ldots \times C_p}_{m}]$ by $\mathscr{A}_{p,m}$.

Let G be an elementary abelian group with generating set $\{g_1, g_2, \ldots g_m\}$. Considering the correspondence $\mu : g_j \mapsto x_j$, where $1 \leq j \leq m$, we have the following algebra isomorphism

$$\mathscr{A}_{p,m} \cong \mathbb{F}_p[x_1, x_2, \ldots, x_m]/(x_1^p - 1, x_2^p - 1, \ldots, x_m^p - 1), \tag{2.1.1}$$

where $\mathbb{F}_p[x_1, x_2, \ldots, x_m]$ denotes the algebra of polynomials in m variables with coefficients from $\mathbb{F}_p$.

We will use the notation of $\mathscr{J}_{p,m}$ for the radical of $\mathscr{A}_{p,m}$.

By Theorem 2.4 we know that the set of monomial functions ($k_i \in \mathbb{N} \cup \{0\}$)

$$\left\{ \prod_{i=1}^{m} (x_i - 1)^{k_i}, \text{ where } 0 \leq k_i < p \right\} \tag{2.1.2}$$

form a linear generating set of the radical $\mathscr{J}_{p,m}$. Clearly the nilpotency index of $\mathscr{J}_{p,m}$ (i.e. the smallest positive integer N, such that $\mathscr{J}_{p,m}^N = 0$) is equal to $m(p-1)+1$.

Introducing the notation

$$X_i = x_i - 1, \ (1 \leq i \leq m) \tag{2.1.3}$$

(which will be used throughout the dissertation) we have the following

isomorphism

$$\mathscr{A}_{p,m} \cong \mathbb{F}_p[X_1, X_2, \ldots, X_m]/(X_1^p, X_2^p, \ldots, X_m^p). \tag{2.1.4}$$

The k-th power of the radical consists of m-variable (non-constant) polynomials of degree at least k, where $0 \leq k \leq m(p-1)$.

$$\mathscr{J}_{p,m}^k = \left\langle \prod_{i=1}^m (X_i)^{k_i} \mid \sum_{i=1}^m k_i \geq k,\ 0 \leq k_i < p \right\rangle. \tag{2.1.5}$$

Such a basis was exploited by Jennings [J].

By (2.1.5) the quotient space $\mathscr{J}_{p,m}^k/\mathscr{J}_{p,m}^{k+1}$ has a basis

$$\left\{ \prod_{i=1}^m X_i^{k_i} + \mathscr{J}_{p,m}^{k+1} \mid 0 \leq k_i < p, \sum_{i=1}^m k_i = k \right\}. \tag{2.1.6}$$

It is known (see [M]) that the dual code $\mathcal{C}^\perp$ of an ideal $\mathcal{C}$ in $\mathscr{A}_{p,m}$ coincides with the annihilator of $\mathcal{C}^*$, where $\mathcal{C}^*$ is the image of $\mathcal{C}$ by the involution $*$ defined on $\mathscr{A}_{p,m}$ by

$$*:\ g \mapsto g^{-1} \text{ for all } g \in G \text{ from } \mathscr{A}_{p,m} \text{ to itself.} \tag{2.1.7}$$

Berman introduced abelian group codes in [B] as ideals of modular group algebras for abelian groups. Further he showed that the Reed-Muller codes are special cases of abelian group codes. Now, we recall some main definitions and theorems of [B].

Throughout the dissertation, let G be an abelian p-group, i.e. it is isomorphic to a direct product of cyclic groups of prime power order, e.g.

$$G = \langle g_1 \rangle \times \ldots \times \langle g_m \rangle, \tag{2.1.8}$$

where each $\langle g_i \rangle$ has order p^{a_i} with $a_1 \geq \ldots \geq a_m > 0$. By (2.1.2) we have

a generating set for the radical $\mathcal{J}$ of the form

$$(x_1-1)^{k_1}\cdots(x_m-1)^{k_m}\text{ , where } k_j\in\{0,1,\ldots,p^{a_j}-1\}, j=1,\ldots,m. \tag{2.1.9}$$

Because of (2.1.5) the powers $\mathcal{J}^k$ of the radical have a generating set consisting of all products of the form (2.1.9) with $\sum k_j \geq k$.

Landrock and Manz gave a thorough survey of linear codes as ideals in group algebras in [LM].

Definition 2.5 ([DL])**.** *Let $\mathcal{C}$ be an ideal of $\mathcal{A}_{p,m}$. Then $\mathcal{C}$ is a subspace of $\mathcal{J}_{p,m}$. We say that $\mathcal{C}$ is a monomial code if it can be generated by some monomials of the form*

$$X_1^{k_1}X_2^{k_2}\ldots X_m^{k_m},\ \textit{where } 0\leq k_i\leq p-1.$$

Codes which are generated by a single monomial in the algebra of polynomials corresponding to modular abelian group algebras are studied in [MM]. In Chapter 5 we investigate codes generated by a single monomial if G is an elementary abelian p-group.

2.2 Reed-Muller codes

2.2.1 Definition by Boolean functions

First, we introduce Reed-Muller codes (in the sequel denoted by $\mathcal{RM}$-codes) as vector spaces over $\mathbb{F}_2$. This definition by Boolean functions can be found for example in ([MS], Chapter 13). Let $B=\{0,1\}$ and $m\geq 0$ an integer. A Boolean function is a function which maps B^m to B. Thus any binary sequence of length 2^m can be regarded as a Boolean function $f(x_1,\ldots,x_m)$ on m variables (which maps from $\mathbb{F}_2^m$ to $\mathbb{F}_2$). The basic representation of f is given by the output columns of its truth table

$(f_0,\ldots,f_{2^m-1})$, i.e. its a binary string of length 2^m. If $0 \le i \le 2^m-1$ and $i=\sum_{k=0}^{m-1} i_{k+1}2^k$, then $f_i = f(i_1,\ldots,i_m)$. Operations of these strings are the following. Addition is defined coordinatewise, as used in the space of $\mathbb{F}_2^m$ and multiplication is defined as the logical conjunction ("and": $\wedge$), again coordinatewise. There are two constant Boolean functions: $\mathbf{0} = (0,\ldots,0)$ and $\mathbf{1} = (1,\ldots,1)$.

Now, we define v_i to be the coordinate function which maps each element of $\mathbb{F}_2^m$ into the $m-i+1$-th coordinate of $(i_1,\ldots,i_m)$. For example, we have $v_1 = (\underbrace{0,\ldots 0}_{2^{m-1}},\underbrace{1,\ldots 1}_{2^{m-1}})$ and $v_m = (0,1,0,1,\ldots,0,1)$.

Example 2.6. *Let $m=3$ and we represent the integers i from 0 to 2^3-1 as binary strings. Then with the notations above we have*

$$\begin{array}{c} i \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Definition 2.7. *The linear space generated by the Boolean functions $f\colon \mathbb{F}_2^m \to \mathbb{F}_2$ of degree at most r are called Reed-Muller codes of degree r, where $0 \le r \le m$ and their length is $n = 2^m$, thus*

$$\mathcal{RM}(r,m) = \{v_1^{j_1}\ldots v_m^{j_m} | j_1+\ldots+j_m \le r\},$$

where $j_1,\ldots,j_m \in \mathbb{F}_2$.

By combinatorial computations, we can get the following properties of Reed-Muller codes.

1. $\dim(\mathcal{RM}(r,m)) = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$
2. If $1 \le r \le s \le m$, then $\mathcal{RM}(r,m) \subseteq \mathcal{RM}(s,m)$

3. For each $m \geq 1$ and $\mathcal{RM}(r,m)^{\perp} = \mathcal{RM}(m-r-1,m)$, where $\mathcal{RM}(r,m)^{\perp}$ denotes the dual space of $\mathcal{RM}(r,m)$.

Example 2.8. *We determine generator matrices for the Reed-Muller codes $\mathcal{RM}(k,4)$ for $k \in \{0,\ldots,4\}$. First, we define the following matrices $\mathscr{M}_k$.*

$$\mathscr{M}_0 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_0 \end{pmatrix},$$

$$\mathscr{M}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \mathbf{v}_3 \\ \mathbf{v}_4 \end{pmatrix},$$

$$\mathscr{M}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1\mathbf{v}_2 \\ \mathbf{v}_1\mathbf{v}_3 \\ \mathbf{v}_1\mathbf{v}_4 \\ \mathbf{v}_2\mathbf{v}_3 \\ \mathbf{v}_2\mathbf{v}_4 \\ \mathbf{v}_3\mathbf{v}_4 \end{pmatrix},$$

$$\mathscr{M}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1\mathbf{v}_2\mathbf{v}_3 \\ \mathbf{v}_1\mathbf{v}_2\mathbf{v}_4 \\ \mathbf{v}_1\mathbf{v}_3\mathbf{v}_4 \\ \mathbf{v}_2\mathbf{v}_3\mathbf{v}_4 \end{pmatrix},$$

and

$$\mathscr{M}_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1\mathbf{v}_2\mathbf{v}_3\mathbf{v}_4 \end{pmatrix}.$$

Now we can construct generator matrices for the following Reed-Muller codes from the rows of the matrices $\mathscr{M}_k$.

$$\mathcal{RM}(0,4) = \begin{pmatrix} \mathcal{M}_0 \end{pmatrix},\ \mathcal{RM}(1,4) = \begin{pmatrix} \mathcal{M}_0 \\ \mathcal{M}_1 \end{pmatrix},\ \mathcal{RM}(2,4) = \begin{pmatrix} \mathcal{M}_0 \\ \mathcal{M}_1 \\ \mathcal{M}_2, \end{pmatrix},$$

$$\mathcal{RM}(3,4) = \begin{pmatrix} \mathcal{M}_0 \\ \mathcal{M}_1 \\ \mathcal{M}_2 \\ \mathcal{M}_3 \end{pmatrix} \text{ and } \mathcal{RM}(4,4) = \begin{pmatrix} \mathcal{M}_0 \\ \mathcal{M}_1 \\ \mathcal{M}_2 \\ \mathcal{M}_3 \\ \mathcal{M}_4 \end{pmatrix}.$$

2.2.2 Reed-Muller codes as extended cyclic codes

A linear code $\mathcal{C}$ is **cyclic,** if for each codeword $(c_0, c_1, \ldots, c_{v-1}) \in \mathcal{C}$ we have $(c_1, \ldots, c_{v-1}, c_0) \in \mathcal{C}$. We get the **extended** code of $\mathcal{C}$ by adding a parity bit. It was shown by Kasami, Lin and Peterson in [KLP1] that all Reed-Muller codes can be regarded as extended cyclic codes. They used an original proof of Zierler [Z] that the first order punctured Reed-Muller codes are cyclic. Precisely, dropping a digit from a Reed-Muller code and reordering its coordinates will lead to a cyclic code. Considering Reed-Muller codes as extended cyclic codes Kasami, Lin and Peterson introduced a new generalization of these codes over $\mathbb{F}_p$, where p can be any prime number. They named these codes **Generalized Reed-Muller codes** - shortly $\mathcal{GRM}$-codes, which is still the usual notation. Later, Delsarte, Goethals and MacWilliams gave a formalization of Kasami's, Lin's and Peterson's approach and they collected more results on $\mathcal{GRM}$-codes, see [DGM] for more details. In this section we follow the approach of $\mathcal{RM}$-codes and $\mathcal{GRM}$-codes as it can be found in [KLP1] and [KLP2]. We give the generator polynomial of punctured Reed-Muller codes and their generalizations and we describe Kasami's, Lin's and Peterson's charac-

terization by Assmus and Key ([AK], Section 4.3).

Let p be a prime number, $\mathbb{F}_p$ the field of p elements and $\mathbb{F} = \mathbb{F}_{p^m}$ for some $m \in \mathbb{N}$. Let $\mathbb{F}^\star = \mathbb{F} \setminus \{0\}$ be the multiplicative group of $\mathbb{F}$.

Let α be a primitive element of $\mathbb{F}$, then $\alpha \in \mathbb{F}^\star$ is a generator of the multiplicative group of $\mathbb{F}$.

Set $n = p^m - 1$, then we have $\mathbb{F} = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$.

It is well known that all elements of $\mathbb{F}$ can be expressed as linear combinations of $1, \alpha, \ldots, \alpha^{m-1}$ with coefficients in $\mathbb{F}_p$. Thus

$$\alpha^j = \sum_{i=0}^{m-1} c_{i,j} \alpha^i,$$

where $c_{i,j} \in \mathbb{F}_p$, $0 \leq j \leq p^m - 2$ and $0 \leq i \leq m-1$. Then we can construct the following matrix

$$\mathscr{W} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ c_{0,0} & c_{0,1} & \ldots & c_{0,n-1} \\ c_{1,0} & c_{1,1} & \ldots & c_{1,n-1} \\ \vdots & & & \\ c_{m-1,0} & c_{m-1,1} & \ldots & c_{m-1,n-1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix}.$$

The vector product of two vectors is defined (as in Section 2.2.1) by the binary operation "and" componentwise. Now, we construct a matrix $\mathscr{W}_r$ for exponents k_λ, where $0 \leq k_\lambda \leq p-1$ and $\sum_{\lambda=0}^{m-1} k_\lambda \leq r$ in the following way:

$$\mathscr{W}_r = \begin{pmatrix} \mathbf{1} \\ w_1 \\ w_2 \\ \vdots \\ w_1^{k_0} w_2^{k_1} \dots w_m^{k_{m-1}} \end{pmatrix}.$$

In the binary case we can extend the row vectors of $\mathscr{W}_r$ by a parity bit. We will add the parity bit in the last column, and we denote this extended matrix by $\mathscr{W}_r^\star$. The linear codes generated by $\mathscr{W}_r^\star$ will be permutation equivalent to the linear codes which were described in Section 2.2.1.

For arbitrary p, the extended code generated by $\mathscr{W}_r^\star$ is called primitive Generalized Reed-Muller code of order r, denoted $\mathcal{GRM}$-code. Its dual code is generated by $\mathscr{W}_t$, where $t = m - r - 1$, i.e. the dual code of $\mathcal{GRM}(m(p-1) - r - 1, m)$ is $\mathcal{GRM}(r,m)$.

The code generated by $\mathscr{W}_r$ is called punctured Generalized Reed-Muller code. This code is cyclic which is proved in the Propositions 4.8 and 4.9 in [AK]. For our purposes we show the construction of $\mathcal{RM}(2,4)$ as extended cyclic code in the following example.

Example 2.9. *Let $m = 4$ and $\mathbb{F} = GF(2^4) = \mathbb{F}_2/(x^4 + x + 1)$, where α is a primitive element of the multiplicative group of $\mathbb{F}$. Further we fix $r = 2$. Then we have*

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} =$$

$$\begin{array}{c} \\ 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccc} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Now, we can construct $\mathscr{W}_2$ and extend it by a parity bit in the last column. We obtain

$$\mathscr{W}_2^\star = \begin{pmatrix} \mathbf{1} \\ w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_1w_2 \\ w_1w_3 \\ w_1w_4 \\ w_2w_3 \\ w_2w_4 \\ w_3w_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

The linear code generated by $\mathscr{W}_2^\star$ is permutation equivalent to the code
$\mathscr{RM}(2,4)$. It can be easily verified that applying the permutation

$$(1,9,11,15,10,6,7,4,2,5,13,16)(8,14,12)$$

on the columns of $\mathscr{W}_2^\star$ leads to the same generator matrix of $\mathscr{RM}(2,4)$ as given in Example 2.8.

More results on the generator polynomial, on the minimum weight of $\mathscr{GRM}$-codes and on the automorphism groups of $\mathscr{GRM}$-codes can be found in [KLP1].

2.2.3 Reed-Muller codes as monomial codes

Reed-Muller codes are binary codes, thus $p = 2$. With the notations introduced in Section 2.1, we have that $\mathcal{A}_{2,m}$ is the underlying group algebra and $\mathcal{J}_{2,m}$ is its radical. The powers of $\mathcal{J}_{2,m}$ are monomial codes and the k-th power of $\mathcal{J}_{2,m}$ coincides with the Reed-Muller code $\mathcal{RM}(m-k,m)$, which was shown in [B]. Thus

$$\mathcal{J}_{2,m}^k = \mathcal{RM}(m-k,m) = \left\langle \prod_{i=1}^{m} X_i^{k_i} \mid \sum_{i=1}^{m} k_i \geq k, k_i \in \{0,1\} \right\rangle.$$

Equivalence of all three definitions

The three introduced definitions of Reed-Muller codes are equivalent. This can be shown by a one-to-one correspondence between:

$$\text{coordinate functions} \leftrightarrow \text{powers of primitive element of } \mathbb{F}_{2^m} \leftrightarrow \text{monomials over } \mathbb{F}_2$$

The bijection between the first two is trivial, since the entries of coordinate functions and the powers of primitive elements differ only in a permutation of entries.

Let φ be a map (not necessarily a homomorphism) from $\mathbb{F}_2^m$ to $\mathbb{F}_2[G]$, where $G = \langle x_1 \rangle \times \ldots \times \langle x_m \rangle$. With the notation introduced in (2.1.3) we define

$$\varphi : \begin{array}{lll} v_0 & \mapsto & \prod_{i=1}^m X_i^{k_i} \mid k_i = 1 \\ v_1 & \mapsto & \prod_{i=1}^m X_i^{k_i} \mid k_1 = 0, k_i = 1 (i \neq 1) \\ \vdots & & \\ v_m & \mapsto & \prod_{i=1}^m X_i^{k_i} \mid k_m = 0, k_j = 1 (j \neq m) \end{array}$$

The coordinatewise multiplication of the elements of $\mathcal{J}_{2,m}$ can be writ-

ten in the following way:

$$X_1^{a_1}X_2^{a_2}\ldots X_m^{a_m}\cdot X_1^{b_1}X_2^{b_2}\ldots X_m^{b_m}=\prod_{i=1}^{m}X_i^{c_i},\ \text{where } c_i=a_i\wedge b_i.$$

It can be easily checked that φ is bijective.

Chapter 3

Self-dual codes with given distance

3.1 Motivation

In Chapter 2 we summarized how the vectorspace of a modular group algebra can be associated to a linear code. So it seems natural to ask questions about these codes and their properties in general. Berman investigated the minimum distance of abelian group codes which are powers of the radical of modular group algebras in [B]. He gave an algorithm which enables us to find the minimum distance of a linear code obtained from such a radical power. One could ask which minimum distances can occur in abelian group codes. Self-dual codes are a type of codes which are combinatorically well applicable. It turns out that a power of the Jacobson radical of a modular group algebra over an abelian p-group can only be self-dual if $p = 2$. The following problem is connected to this question and it was published by Drensky and Lakatos in [DL].

Problem 3.1 ([DL], Problem 2.6)**.** *Let n be an arbitrary positive integer*

and $d \leq \lceil \frac{n}{2} \rceil$. Does there exist an abelian 2-group G of order 2^n, such that some power of the Jacobson radical of the group algebra $\mathbb{F}_2[G]$ is a self-dual $(2^n, 2^{n-1}, 2^d)-$code?

The main theorem of this section is the following, which is published in [HL1].

Theorem 3.2 ([HL1])**.** *Let $\mathbb{F}$ be a field of characteristic 2. Let n be an arbitrary positive integer. Then for each integer d with $1 \leq d \leq \lceil \frac{n}{2} \rceil$ there exists an abelian group G of order 2^n, such that there exists a power of $\jmath(\mathbb{F}[G])$ which defines a self-dual $(2^n, 2^{n-1}, 2^d)$-code.*

The proof is constructive. The main tool is Berman's result for the minimum distance of codes which are powers of the radical (see [B]). We explain the algorithm of Berman in Section 3.2.

3.2 Minimum distance of abelian group codes (Berman's algorithm)

Let G be an abelian p-group of the form (2.1.8). Further let $\mathbb{F}$ be a finite field of characteristic p, $\mathbb{F}[G]$ its group algebra and $\jmath$ its Jacobson radical. If the group is

$$G = C_{p^{a_1}} \times \ldots \times C_{p^{a_m}},$$

then the nilpotency index of $\jmath$ is $p^{a_1} + \ldots + p^{a_m} - m + 1 = N$ ([B]). Therefore it is clear that if p is odd, then N is odd. The dual code of $\jmath^k$ is $\jmath^{N-k}$. Thus a power of the Jacobson radical can only be a self-dual code if $p = 2$. Further, for each possible group G the only power of $\jmath$ which will define a self-dual code is $\jmath^{\frac{N}{2}}$.

So we use Berman's algorithm in the case $p = 2$. For our purposes it is enough to introduce the algorithm for abelian 2-groups G of the form

$$G = C_{2^{a_1}}^{s_1} \times C_{2^2}^{s_2} \times C_2^{s_3},$$

where $a_1 > 0$, and s_1, s_2, s_3 are non-negative integers.

Theorem 3.3 ([B]). *We define two sequences of integers*

$$\begin{cases} l_{a_1} = 0,\ l_{a_1-1} = s_1,\ \ldots, l_2 = s_1,\ l_1 = s_1 + s_2,\ l_0 = s_1 + s_2 + s_3; \\ m_i = 2^i l_i, \text{ where } a_1 \geq i \geq 0. \end{cases} \tag{3.2.1}$$

After that let r be the unique positive integer with $0 \leq r \leq a_1 - 1$ fulfilling the following condition:

$$m_{a_1-1} + m_{a_1-2} + \ldots + m_{a_1-r} \leq \frac{N}{2} < m_{a_1-1} + \ldots + m_{a_1-r} + m_{a_1-r-1} \tag{3.2.2}$$

Thus the nilpotency index of $\mathcal{J}$ can be also given by

$$N = s_1 2^{a_1} + \ldots + s_m 2^{a_m} - (s_1 + \ldots s_m) + 1 = m_{a_1} + \ldots + m_0 + 1 \tag{3.2.3}$$

If N is even and $N = 2j$ for some integer j, then the minimum distance of the j-th power of $\mathcal{J}$ is 2^d, where

$$d = l_{a_1} + \ldots + l_{a_1-r} + \left\lceil \frac{j - (m_{a_1-1} + \ldots + m_{a_1-r}) + 2^{a_1-r-1} - 1}{2^{a_1-r-1}} \right\rceil. \tag{3.2.4}$$

3.3 Construction of suitable 2-groups

We want to find a way for the construction of G, such that if we change its parameters slightly, then the minimum distance of the linear self-dual

code defined by $\mathcal{J}^j$ will also change only slightly. Recall that $1 \leq d \leq \lceil \frac{n}{2} \rceil$. It is easy to find such groups for d close to the lower and to the upper bound. In contrast, it is not easy to find a group G such that the minimum distance of $\mathcal{J}^j$ is near to $\frac{n}{4}$. Finally it turned out that the following construction of G leads us to our aim and we achieve a code with minimum distance 2^d for all integers d between 1 and $\lceil \frac{n}{2} \rceil$. The group G is the direct product of cyclic subgroups which are of three different orders:

$$G = C_{2^{a_1}}^{s_1} \times C_{2^2}^{s_2} \times C_2^{s_3}, \tag{3.3.1}$$

that is

$$n = s_1 a_1 + 2s_2 + s_3; \;\; s_1, s_2, s_3 \geq 0.$$

In the sequel, the largest integer not exceeding the number $a \in \mathbb{R}$ is denoted by $[a]$. In the sequel $\mathbb{F}$ is a field of characteristic 2 and G is an abelian 2-group of order 2^n with decomposition (3.3.1). Set

$$N = s_1(2^{a_1} - 1) + 3s_2 + s_3 + 1 \text{ and } j = \frac{N}{2}. \tag{3.3.2}$$

It can be easily verified that N is the nilpotency index of $\mathbb{F}[G]$, for G as in (3.3.1). We assume that N is even. Hence j is an integer.

The two integer sequences in Berman's theorem have the form

$$\begin{cases} l_{a_1} = 0, \;\; l_{a_1 - 1} = s_1, \; \ldots, l_2 = s_1, \; l_1 = s_1 + s_2, \; l_0 = s_1 + s_2 + s_3, \\ m_i = 2^i l_i \text{ for } a_1 \geq i \geq 0. \end{cases} \tag{3.3.3}$$

By (3.2.2) we get that

$$\begin{array}{lll} r=0 & \iff & 0<j<s_1 2^{a_1-1}, \\ r=1 & \iff & s_1\cdot 2^{a_1-1}\le j<s_1\cdot(2^{a_1-1}+2^{a_1-2}), \\ \vdots & & \vdots \\ r=a_1-1 & \iff & s_1 2^{a_1}+2s_2-2s_1\le j, \end{array} \tag{3.3.4}$$

and the exponent d of Hamming distance is given by (3.2.4) (with the sequences (3.3.3)).

It was difficult to find direct products of cyclic groups for fixed n such that changing the cyclic groups slightly, the value of d would change only by 1. We will see that our construction of G makes it possible to follow the values $1\le d\le\lceil\frac{n}{2}\rceil$ divided into four intervals - applying different changes of parameters in each of them.

3.4 Auxiliary results

In this section we prove some lemmas which will be needed in the proof of Theorem 3.2. Throughout this chapter we assume that $n=a_1s_1+2s_2+s_3$.

Lemma 3.4. *Let $N=s_1(2^{a_1}-1)+3s_2+s_3+1$ and we assume that N is even. The congruence*

$$n\equiv s_2 \pmod 2 \tag{3.4.1}$$

holds if and only if a_1 is even and s_1 is odd.

Proof. We have

$$n=a_1s_1+2s_2+s_3\equiv a_1s_1+s_3 \pmod 2$$

and as $a_1 > 0$ we have

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

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 (3.4.1) 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 (3.4.1) cannot hold.

□

Lemma 3.5. *Suppose a_1 is fixed and choose $s_2 = 0$ or $s_2 = 1$. Let $s_1' = s_1 + 1$ and choose $s_2' = 0$ or $s_2' = 1$ so that $n \equiv s_2$ 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* (3.3.2)
and

$$j' = \frac{s_1'(2^{a_1}-1) + 3s_2' + s_3' + 1}{2}.$$

Then

$$j' - j = 2^{a_1-1} - \frac{a_1 + h}{2}, \text{ where } h = \begin{cases} 1, \text{ if } a_1 \text{ is odd} \\ 2, \text{ if } a_1 \text{ and } n + s_1 \text{ are even} \\ 0, \text{ if } a_1 \text{ is even, } n + s_1 \text{ is odd.} \end{cases} \tag{3.4.2}$$

Proof. According to Lemma 3.4 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 3.4 for odd a_1 we have $n \not\equiv$

$s_2,\ n \not\equiv s_2' \pmod 2$, thus $s_2' = s_2$. For even a_1 we have either $n \equiv s_2,\ n \not\equiv s_2' \pmod 2$ or $n \not\equiv s_2,\ n \equiv s_2' \pmod 2$ (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

$$j' - j = \frac{2^{a_1} - a_1 - 1 + s_2' - s_2 + 1}{2} = 2^{a_1 - 1} - \frac{a_1 + s_2 - s_2' + 1}{2}$$

and with $h = s_2 - s_2' + 1$ we get (3.4.2). □

Lemma 3.6. *If $r = a_1 - 1$, then $j + d = n + 1$.*

Proof. If $r = a_1 - 1$ then using (3.2.4) and (3.2.1)

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

Hence, using (3.3.2)

$$d + j = s_1(1 + a_1 - 2^{a_1}) - s_2 + 2j = s_1 a_1 + 2s_2 + s_3 + 1 = n + 1.$$

□

In 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, keeping n fixed. We study how this change influences the value of d.

Lemma 3.7. *(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 3.4 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 3.4 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 3.4 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 3.4 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 (3.3.2) the value of j increases by 1. Since $r = a_1 - 1$ by Lemma 3.6 $d = n - j + 1$. 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 (3.2.1) $m_3 = 8s_1$, $m_2 = 4s_1, m_1 = 2s_1 + 2s_2$. From (3.3.4) for $r = 2$ we have

$$12s_1 \leq j < 14s_1 + 2s_2.$$

Substituting j by (3.3.2) here and rearranging we get

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

By (3.2.4) using again (3.3.2) for j we get

$$d = 2s_1 + \left[\frac{j - 12s_1 + 1}{2}\right] = \left[\frac{-s_1 + 3s_2 + s_3 + 3}{4}\right]. \qquad (3.4.3)$$

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 $r = 1$ we have by (3.2.4)

$$\begin{aligned} d &= s_1 + \left\lceil \frac{j - s_1 2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} \right\rceil, \\ d' &= s_1' + 1 + \left\lceil \frac{j' - s_1' 2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} \right\rceil. \end{aligned} \tag{3.4.4}$$

By $s_1' = s_1 + 1$ and by (3.4.2) of Lemma 3.5 we can rewrite d' as

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

$$= s_1 + \left\lceil \frac{j - s_1 2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}} + \left(1 - \frac{a_1+h}{2^{a_1-1}}\right) \right\rceil \leq d + 1,$$

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

(d) As $r = 0$ by (3.2.4) we have

$$d = \left\lceil \frac{j + 2^{a_1-1} - 1}{2^{a_1-1}} \right\rceil, \;\; d' = \left\lceil \frac{j' + 2^{a_1-1} - 1}{2^{a_1-1}} \right\rceil. \tag{3.4.5}$$

By $s_1' = s_1 + 1$ and by (3.4.2) of Lemma 3.5 we can rewrite d' as

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

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

□

3.5 Proof of Theorem 3.2

The main idea of the proof is to fix the values of n, a_1, r and s_1 or s_2. Then we increase (by the smallest possible steps) the value of s_1 or s_2.

We consider only those situations, when the corresponding value of d is increasing or decreasing by at most 1.

I) G **for** $\left[\frac{n}{4}\right]+t+1 \leq d \leq \left[\frac{n+1}{2}\right]$**, where** $t=1$ **if** $n \equiv 3,6 \pmod 8$**, and** $t=0$ **otherwise**

The largest possible distances can be easily constructed by (3.2.2),(3.2.3) and (3.2.4).
If n is even and $G = C_4 \times C_2 \times \cdots \times C_2$, then $j = \frac{n+2}{2}$, 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 3.6, $d = n+1-j$, hence from the value of j we can determine d. By (3.3.2) 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 3.7/(a) and get all consecutive values of d in the interval $\left[\left[\frac{n}{4}\right]+t+1, \left[\frac{n+1}{2}\right]\right]$. We have to check the possible values of s_2 for given s_1 by Lemma 3.7/(a), when $r = 2$ holds.

By Lemma 3.5 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 3.4).

Now with (3.3.2) and $s_3 = n - 3s_1 - 2s_2$, we have

$$j = \frac{7s_1+3s_2+s_3+1}{2} = \frac{4s_1+s_2+n+1}{2}. \tag{3.5.1}$$

By (3.3.4) (since now $r = a_1 - 1$) we get

$$6s_1 + 2s_2 \leq j = \tfrac{4s_1+s_2+n+1}{2}$$

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

$$s_1 \leq \frac{n - 3s_2 + 1}{8}. \tag{3.5.2}$$

If s_1 and s_2 satisfy the condition (3.5.2), then we have by Lemma 3.6

$$d = n - j + 1 = \frac{n - 4s_1 - s_2 + 1}{2}. \tag{3.5.3}$$

Thus, for each s_1 satisfying (3.5.2) and for $s_2 = 0,2$ or $s_2 = 1,3$ we apply Lemma 3.7/(a) and see that d decreases at most by 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 (3.5.2) it follows that $s_1 \leq \frac{n+1}{8}$ and $s_1 \leq \frac{n-5}{8}$. For even n with the values $s_2 = 1$ and $s_2 = 3$ we get the conditions $s_1 \leq \frac{n-2}{8}$ and $s_1 \leq \frac{n-8}{8}$ similarly. The smallest s_1 with $r = 2$ is $\underline{s}_1 = 0$. If n is odd, then for $\underline{s}_2 = 0$ we have $\underline{j} = \frac{n+1}{2}$ by (3.5.1) and $\overline{d} = \frac{n+1}{2}$. If n is even, then $\underline{s}_2 = 1$ and $\underline{j} = \frac{n+2}{2}$ and $\overline{d} = n + 1 - \frac{n+2}{2} = \frac{n}{2}$.

If s_1' is the maximal value of s_1 and $s_2 = 0$ or $s_2 = 1$ satisfy (3.5.2), 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 (3.5.2) is also satisfied.

We list the precise maximum value of j (denoted by j') and by (3.5.2) the minimum value of d (denoted by d') in Table 3.1. Thus, we obtain each d on the interval $\left[\left[\frac{n}{2}\right], d'\right]$.

Table 3.1: Parameters defining the smallest values of d

n	s_1'	$s_2'=0$	$s_2'=2$	$s_2'=1$	$s_2'=3$	s_2'	j'	d'
$8k$	$\frac{n}{8}-1$				$s_1'=\frac{n-8}{8}$	3	$\frac{3}{4}n$	$\frac{n}{4}+1$
$8k+1$	$\frac{n-1}{8}$	$s_1'<\frac{n+1}{8}$				0	$\frac{3n+1}{4}$	$\lceil\frac{n}{4}\rceil+1$
$8k+2$	$\frac{n-2}{8}$			$s_1'=\frac{n-2}{8}$		1	$\frac{3n+2}{4}$	$\lceil\frac{n}{4}\rceil+1$
$8k+3$	$\frac{n-3}{8}$	$s_1'<\frac{n+1}{8}$				0	$\frac{3n-3}{4}$	$\lceil\frac{n}{4}\rceil+2$
$8k+4$	$\frac{n-4}{8}$			$s_1'<\frac{n+1}{8}$		1	$\frac{3n}{4}$	$\lceil\frac{n}{4}\rceil+1$
$8k+5$	$\frac{n-5}{8}$		$s_1'=\frac{n-5}{8}$			2	$\frac{3n+1}{4}$	$\lceil\frac{n}{4}\rceil+1$
$8k+6$	$\frac{n-6}{8}$			$s_1'<\frac{n-2}{8}$		1	$\frac{3n-2}{4}$	$\lceil\frac{n}{4}\rceil+2$
$8k+7$	$\frac{n+1}{8}$	$s_1'=\frac{n+1}{8}$				0	$\frac{3n+3}{4}$	$\lceil\frac{n}{4}\rceil+1$

II) G **for** $1 \le d \le \left\lceil \frac{n+1}{5} \right\rceil$

Let $r=1$ *and* $3<a_1 \le [log_2(n)]+1$ *as well as* $s_2=0$ *or* $s_2=1$, *depending on the parity of* n.

If G is a cyclic group of order 2^n and $\mathbb{F}$ is a field with characteristic 2, then

$a_1=n$, $s_1=1$, $s_2=s_3=0$, $m_{n-1}=j=2^{n-1}$, $l_{n-1}=1$, and $d=l_{n-1}=1$.

Thus we have $d=1$ (see also [B]).

If G is not a cyclic group, then we get from (3.3.4)

$$s_1 2^{a_1-1} \le j < s_1(2^{a_1-1}+2^{a_1-2}). \tag{3.5.4}$$

From the lefthand side of (3.5.4) and from (3.3.2) we have

$$s_1 2^{a_1} \le s_1(2^{a_1}-1)+2s_2+s_3+1$$

hence

$$-s_1+3s_2+s_3+1 \ge 0. \tag{3.5.5}$$

Now we use Lemma 3.7/(c) and determine the minimum and maximum value of s_1 (denoting them by $\underline{s}_1$ and by $\overline{s}_1$).

1. If $s_2 = 0$, then from (3.5.5) we have $s_1 \le s_3 + 4$ and from $n = s_1 a_1 + s_3 \ge s_1(a_1+1) - 1$ the inequality $s_1 \le \frac{n+1}{a_1+1}$ follows.

2. Similarly, if $s_2 = 1$, then $s_1 \le s_3 + 4$ and from $n = s_1 a_1 + 2 + s_3 \ge s_1(a_1+1) - 2$ we have $s_1 \le \frac{n+2}{a_1+1}$.

Substituting $j = \frac{\overline{s}_1 2^{a_1} - \overline{s}_1 + n - a_1 \overline{s}_1 + 1}{2}$ into (3.4.4) we get

$$\overline{d} = \overline{s}_1 + \left[\frac{j - \overline{s}_1 2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}}\right] \overline{s}_1 + \left[\frac{-\overline{s}_1(1+a_1) + n + 2^{a_1-1} - 1}{2^{a_1-1}}\right]$$

$$\le \overline{s}_1 + \left[\frac{2^{a_1-1} - 2}{2^{a_1-1}}\right] = \overline{s}_1.$$

By the condition of $r = 1$ and (3.2.4) we have $d \ge s_1$, so the equality $\overline{d} = \overline{s_1}$ holds.

To find the minimum of d (denoting it by $\underline{d}$) from the right-hand side of (3.5.4) we get $s_1 2^{a_1-1} > -s_1 + 3s_2 + s_3 + 1$. With $s_3 = n - a_1 s_1 - 2s_2$ and $s_2 = 0$ or $s_2 = 1$ we get

$$\underline{s}_1 > \frac{n+1}{2^{a_1-1} + a_1 + 1} \text{ or } \underline{s}_1 > \frac{n+2}{2^{a_1-1} + a_1 + 1}.$$

Thus, $\underline{s}_1 = \left[\frac{n+1}{2^{a_1-1}+a_1+1}\right] + 1$ or $\underline{s}_1 = \left[\frac{n+2}{2^{a_1-1}+a_1+1}\right] + 1$.
If $s_2 = 0$, then we have by (3.4.4)

$$\underline{d} = \underline{s}_1 + \left[\frac{j - \underline{s}_1 2^{a_1-1} + 2^{a_1-2} - 1}{2^{a_1-2}}\right] =$$

$$s_1 + \left[\frac{-\underline{s}_1(1 + a_1 + 2^{a_1-1}) + \underline{s}_1(2^{a_1-1}) + n - 1}{2^{a_1-1}}\right] \ge$$

$$\underline{s}_1 + \left[\frac{\underline{s}_1 2^{a_1-1} - 2}{2^{a_1-1}}\right] = 2\underline{s}_1 - 1.$$

If $s_2 = 1$, then we get analogously that $\underline{d} \geq 2\underline{s}_1 - 1$.

By Lemma 3.7/(c) for $a_1 > 3$ we can construct groups for each d satisfying the inequalities

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

If $a_1 > [\log_2(n)]+1$, then $n+1 < 2^{a_1-1}+1 < 2^{a_1-1}+a_1+1$ and we have $s'_1 = 1$ and $d = 2$.

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

III) G **for** $\left[\frac{n+1}{5}\right] < d \leq \left[\frac{n}{4}\right] - \left[\frac{n+40}{64}\right]$

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 $a_1 = 4$, $\overline{s}_1 = \left[\frac{n+1}{5}\right]$ and $\overline{d} = \left[\frac{n+1}{5}\right]$ or $\overline{d} \leq \left[\frac{n+2}{5}\right]$, corresponding to $s_2 = 0$ or $s_2 = 1$. Taking $s'_1 = \overline{s}_1 + 1$ then $j - 8\overline{s}_1 \geq j - 8s'_1$ 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 3.5 we have $h = 0$ or $h = 2$, and $j' = \overline{j}+5$, or $j' = \overline{j}+6$, and $j' = \overline{j}+8-\frac{4+h}{2} < 8s'_1 = 8\overline{s}_1 + 8$. Using (3.4.5), we get for d' that

$$d' = \left[\frac{j'+7}{8}\right] < \left[\frac{8s'_1+7}{8}\right] = \left[\frac{8\overline{s}_1+15}{8}\right] = \overline{s}_1 + 1.$$

The largest value of s_1, for which the condition $r = 0$ holds, is $[\frac{n}{4}]$ or $[\frac{n}{4}]-1$, depending on the parity condition of Lemma 3.4 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 $\left[\frac{15k+a}{8}\right] = 2k - \left[\frac{k-a+7}{8}\right]$ in our case in Table 3.2 we have the following largest values of d.

Table 3.2: Parameters for the largest d

n	s_1	s_2	s_3	j	d
$8k$	$2k-1$	0	4	$15k-5$	$\left\lfloor\frac{15k+2}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n+40}{64}\right\rfloor$
$8k+1$	$2k$	0	1	$15k+1$	$\left\lfloor\frac{15k+8}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n-9}{64}\right\rfloor$
$8k+2$	$2k$	1	0	$15k+2$	$\left\lfloor\frac{15k+9}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n-18}{64}\right\rfloor$
$8k+3$	$2k$	0	3	$15k+2$	$\left\lfloor\frac{15k+9}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n-19}{64}\right\rfloor$
$8k+4$	$2k+1$	1	2	$15k+3$	$\left\lfloor\frac{15k+10}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n+26}{64}\right\rfloor$
$8k+5$	$2k$	0	5	$15k+3$	$\left\lfloor\frac{15k+10}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n+35}{64}\right\rfloor$
$8k+6$	$2k+1$	0	2	$15k+9$	$\left\lfloor\frac{15k+16}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n-14}{64}\right\rfloor$
$8k+7$	$2k+1$	1	1	$15k+10$	$\left\lfloor\frac{15k+17}{8}\right\rfloor = \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n-23}{64}\right\rfloor$

Using Lemma 3.7/(d) we have all values of $\bar{s}_1+1 = \left\lfloor\frac{n+1}{5}\right\rfloor + 1 \le d \le \left\lfloor\frac{n}{4}\right\rfloor - \left\lfloor\frac{n+40}{64}\right\rfloor$.

IV) G **for** $\left\lfloor\frac{n}{4}\right\rfloor + 1 - \left\lfloor\frac{n+40}{64}\right\rfloor \le d \le \left\lfloor\frac{n}{4}\right\rfloor + t$, **where** $t = 1$, **if** $n \equiv 3,6 \pmod 8$, **otherwise** $t = 0$

In Table 3.3 we list the constructed and missing values of d. Here $\lambda_n = \left\lfloor\frac{n+40}{64}\right\rfloor - 1$, $t = 1$ if $n \equiv 3,6 \pmod 8$ and $t = 0$ if $n \not\equiv 3,6 \pmod 8$.
Let $a_1 = 4, s_1 = \left\lfloor\frac{n+7}{15}\right\rfloor$, $r = 2$.

1. If $14 \le n \le 23$ then for the constructions of $d = \left\lfloor\frac{n}{4}\right\rfloor + 1$ 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 3.7/(b) we have to find at $r = 2$ the maximum of s_2 ($\bar{s}_2$) 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 (3.2.4) the

Table 3.3: Missing values of d close to $\frac{n}{4}$

n	missing d	constructed in part I	constructed in part II and III
$n \le 13$	*none*	$d \le \left[\frac{n}{4}\right]+1$	$1 \le d \le \left[\frac{n}{4}\right]$
$15 \le n < 23$, $t=0$	*none*	$d \le \left[\frac{n}{4}\right]+1$	$1 \le d \le \left[\frac{n}{4}\right]$
$14 \le n \le 23$, $t=1$	$\left[\frac{n}{4}\right]+1$	$d \le \left[\frac{n}{4}\right]+2$	$1 \le d \le \left[\frac{n}{4}\right]$
$24 \le n \le 87$, $t=0$	$\left[\frac{n}{4}\right]$	$d \le \left[\frac{n}{4}\right]+1$	$1 \le d \le \left[\frac{n}{4}\right]-1$
$24 \le n \le 87$, $t=1$	$\left[\frac{n}{4}\right], \left[\frac{n}{4}\right]+1$	$d \le \left[\frac{n}{4}\right]+2$	$1 \le d \le \left[\frac{n}{4}\right]-1$
$n \ge 87$, $t=0$	$\left[\frac{n}{4}\right]+1 \le d < \left[\frac{n}{4}\right]-\lambda_n+1$	$d \le \left[\frac{n}{4}\right]+1$	$1 \le d \le \left[\frac{n}{4}\right]-\lambda_n+1$
$n \ge 87$, $t=1$	$\left[\frac{n}{4}\right] \le d < \left[\frac{n}{4}\right]-\lambda_n$	$d \le \left[\frac{n}{4}\right]+2$	$1 \le d \le \left[\frac{n}{4}\right]-\lambda_n$

condition $r=2$ gives

$$12s_1 \le j < 14s_1 + 2s_2. \tag{3.5.6}$$

Substituting j (defined by (3.3.2)) into (3.5.6), we have

$$13s_1 - s_2 - 1 \le n < 17s_1 + 3s_2 - 1. \tag{3.5.7}$$

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 $n = 4\left[\frac{n+7}{15}\right] + 2s_2 + s_3$ the left side of the inequality (3.5.7) holds for all $s_2 \ge 0$. 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 $\frac{n+7}{15} \ge s_1 \ge \frac{n+7}{15}$. and $s_3 \ge 0$ we have $n \ge 4s_1 + 2s_2$ and $\frac{n-4s_1}{2} \ge \overline{s}_2 \ge \frac{n-4s_1-3}{2}$. For the minimum of $\overline{d}$ (at $s_3 = 3$) by (3.4.3) we get

$$\overline{d} \ge \left[\frac{-s_1+3\frac{n-4s_1-3}{2}+6}{4}\right] = \left[\frac{3n-14s_1+3}{8}\right] \ge \left[\frac{3n-14\frac{n+7}{15}+3}{8}\right] = \left[\frac{31n-8}{120}\right].$$

From this and by $n > 23$ we have

$$\overline{d} \geq \left[\tfrac{31n-8}{120}\right] \geq \tfrac{31n-127}{120} > \tfrac{n}{4} \geq \left[\tfrac{n}{4}\right].$$

The right-hand side of (3.5.7) gives $s_2 > \frac{n-17s_1+1}{3}$, thus the nearest integer is the minimum of s_2 (denoted by $\underline{s_2}$),

$$\underline{s_2} \leq \left[\tfrac{n-17s_1+4}{3}\right] \leq \left[\tfrac{n-17\frac{n-7}{15}+4}{3}\right] = \left[\tfrac{-2n+179}{45}\right].$$

Since for $n > 23$ we have $\left[\frac{-2n+179}{45}\right] < 3$, thus for $\underline{s_2} = 1$ or $\underline{s_2} = 2$ (depending on parity condition) we have $r = 2$.

In this case $\underline{d}$ can be calculated by (3.4.3) ($d = \left[\frac{-s_1+3s_2+s_3+3}{4}\right]$). 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 $s_3 \leq n-2-4s_1 \leq n-2-4\frac{n-7}{15} \leq \frac{11n-2}{15}$, and by (3.4.3) and $n > 23$ we have

$$\underline{d} \leq \left[\tfrac{-\frac{n+7}{15}+6+\frac{11n-2}{15}+3}{4}\right] = \left[\tfrac{10n+96}{60}\right] \leq \left[\tfrac{n}{4}\right] + 1 - \left[\tfrac{n+40}{64}\right].$$

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

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

Now, only the construction for $d = \left[\frac{n}{4}\right] + 1$ if $n \equiv 3,6 \pmod 8$ is left.
If $n = 8k+3$, and $k \geq 5$, we have $d = \left[\frac{n}{4}\right] + 1$ since $\left[\frac{n}{4}\right] = \left[\frac{8k+3}{4}\right] = 2k$, $\frac{n}{4} = 2k + 0,75$ and

$$\overline{d} \geq \left[\tfrac{31n-8}{120}\right] = \left[\tfrac{31\cdot 4\frac{n}{4}-8}{120}\right] = \left[\tfrac{124(2k+0,75)-8}{120}\right] = 2k + \left[\tfrac{8k+85}{120}\right] \geq \left[\tfrac{n}{4}\right] + 1$$

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 $d = \left[\frac{n}{4}\right] + 1$. If $\left[\frac{n}{4}\right] = 2k+1$, then $\frac{n}{4} = 2k+1,5$, i.e.

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

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 $a_1 = 4$, $s_1 = \left[\frac{n+4}{15}\right]$, $r = 2$ we can get $d = \left[\frac{n}{4}\right] + 1$ by the constructions listed in Table 3.4.

Table 3.4: Constructions of $d = \left[\frac{n}{4}\right] + 1$

n	s_1	s_2	s_3	j	d	n	s_1	s_2	s_3	j	d
27	2	8	7	28	7	30	2	9	4	31	8
35	2	8	11	33	9	38	2	11	8	36	10
43	3	13	5	45	11	46	3	14	6	47	12
54	4	19	0	59	14	62	4	19	8	63	16

The proof of Theorem 3.2 is completed. □

Chapter 4

Construction of self-dual $(2^{2k}, 2^{2k-1}, 2^k)$-codes

4.1 Complement-free sets

In this chapter, we fix G to be an elementary abelian p-group, i.e.

$$G = \underbrace{C_p \times \ldots \times C_p}_{m}.$$

Furthermore we will use the notation $\mathscr{A}_{p,m}$ for the modular group algebra as defined in equation (2.1.1). Our aim is to find self-dual codes in the radical of $\mathscr{A}_{p,m}$. As it is mentioned in the beginning of Section 3.2 there is a power of the radical defining a self-dual code, if the nilpotency index of $\mathcal{J}_{p,m}$ is even. Since G is elementary abelian, the nilpotency index of $\mathcal{J}_{p,m}$ is even if and only if $p = 2$ and m is odd. Thus a Reed-Muller code is self-dual if and only if it is an $\mathcal{RM}(\frac{m-1}{2}, m)$-code, i.e. m has to be odd.

It clearly rises the question if there exist binary self-dual codes in the radical of $\mathscr{A}_{2,m}$ if m is even. We can give a positive answer to this ques-

tion and we will introduce a way to construct such codes. The codes constructed in this chapter are ideals in the radical of $\mathscr{A}_{2,m}$, i.e. in this chapter $p = 2$.

For $m = 2k$, where k is an arbitrary integer, we have a new method to construct a doubly even class of binary self-dual codes with length 2^m, dimension 2^{m-1} and minimum distance 2^k. For such a code $\mathcal{C}$ we have

$$\mathcal{RM}(k-1,2k) \subset \mathcal{C} \subset \mathcal{RM}(k,2k).$$

In [HL2] we introduce the following sets of binary m-tuples, where $m = 2k$ for some integer k.

Definition 4.1. *Let y be a binary m-tuple. We say that $\mathbf{1} - y$ is the complement m-tuple of y, where $\mathbf{1}$ denotes the all-1 tuple $(\underbrace{1,\ldots,1}_{m})$.*

Definition 4.2. *Let $m = 2k$ and X be the set of all binary m-tuples with exactly k '0'-s and '1'-s. Further, let Y be a subset of X such that if $y \in Y$, then $\mathbf{1} - y \notin Y$. Then Y is called a complement-free set of binary m-tuples.*

Remark 4.3. *The cardinality of the set X is $\binom{2k}{k}$ and the maximum cardinality of Y is $\frac{1}{2}\binom{2k}{k}$.*

Example 4.4. *If $m = 4$, then we have exactly eight possible complement-free sets, which can be seen in Table 4.1 below.*

Table 4.1: Complement-free sets for $m = 4$

1	1	0	0	0	1	1	0	0	1	1	0	1	0	0	1
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1
1	0	0	1	1	1	0	0	0	0	1	1	0	0	1	1
0	1	1	0	0	0	1	1	1	1	0	0	1	1	0	0
0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
0	0	1	1	1	0	0	1	1	0	0	1	0	1	1	0

It is easy to see that the number of possible complement-free sets increases exponentially when k increases. Imagine we write the elements of X in two columns such that if y is in the first column, then $\mathbf{1}-y$ is in the second column, but in the same row. Then we can get a complement-free set Y by choosing exactly one element from each row, either from the first or from the second column. Therefore there exist $2^{\frac{1}{2}\binom{2k}{k}}$ different sets Y.

4.2 Description of self-dual $(2^{2k}, 2^{2k-1}, 2^k)$-codes

Let us consider the group algebra

$$\mathscr{A}_{2,m} \cong \mathbb{F}_2[x_1, \ldots x_m]/(x_1^2-1, x_2^2-1, \ldots, x_m^2-1)$$

as a vector space with basis

$$\left\{ x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m} \mid \; k_i \in \{0,1\} \right\}. \tag{4.2.1}$$

Applying (2.1.5) for $p=2$ we have that the radical $\mathcal{J}_{2,m}$ of this group algebra is generated by the monomials $X_i = x_i - 1 = x_i + 1$. The codes we intend to study are monomial codes.

If $p=2$, then applying the usual polynomial product on the monomials $X_1^{k_1} X_2^{k_2} \ldots X_m^{k_m}$ $(k_i \in \{0,1\})$ leads to

$$X_1^{k_1} X_2^{k_2} \ldots X_m^{k_m} = (x_1+1)^{k_1} (x_2+1)^{k_2} \ldots (x_m+1)^{k_m}$$

and the Hamming weight of this monomial in the basis (4.2.1) equals $\prod_{i=1}^{m} (1+k_i)$. We will denote by $\mathscr{X}$ the set of monomials corresponding to the set of exponents from X.

Denote the set with maximum number of pairwise orthogonal monomials in $\mathscr{X}$ by $\mathscr{Y}$ and their corresponding exponents in X by Y. The cardinality of $\mathscr{X}$ is $\binom{2k}{k}$ and the cardinality of $\mathscr{Y}$ is $\frac{1}{2}\binom{2k}{k}$.

Example 4.5. *Let $\mathscr{A}_{2,m}$ be a group algebra ($m \geq 2$, see (4.2.1)). Define the codes $\mathcal{C}_j$ as ideals in $\mathscr{A}_{2,m}$ generated by $X_j = x_j - 1$. These codes are binary self-dual $(2^m, 2^{m-1}, 2)$-codes and they are self-dual since $\mathcal{C}_j = \mathcal{C}_j^{\perp} = \langle X_j \rangle$. Further, this code is a direct sum of $(2,1,2)$-codes. The dimension of the code $\mathcal{C}_j$ is 2^{m-1}, the same as the dimension of the radical of the group algebra $\mathscr{A}_{2,m-1}$. The minimal distance of $\mathcal{C}_j$ is $d = 2$. This follows from the fact that the element $X_j = x_j + 1$ is included in the basis of $\mathcal{C}_j$. Thus, $\mathcal{C}_j$ is a self-dual $(2^m, 2^{m-1}, 2)$-code.*

In the case of $m = 4$, we get two known extremal $(16,8,4)$-codes (listed in [P2]) and for $m > 4$ these codes are not extremal. A doubly even (i.e. its minimum distance is divisible by 4) self-dual code is called extremal, if we have for its minimum distance $d = 4\left[\frac{n}{24}\right] + 4$, where n denotes the code length (see Definition 39 and Lemma 40 in [JK]).

To abbreviate the description of our codes, we will refer to the monomial $X_1^{k_1} \dots X_m^{k_m}$ by the m-tuple $(k_1, k_2, \dots, k_m) \in \{0, 1, \dots, p-1\}^m$ of exponents.

Using Plotkin's construction of $\mathcal{RM}$-codes (see [M], Ch.13 §3, Theorem 2) we obtain the following property of $\mathcal{RM}$-codes.

Lemma 4.6. *If m is even and $m = 2k$, then $\mathcal{RM}(k-1, m) = \mathcal{J}_{2,m}^{k+1}$ contains a proper subspace which is isomorphic to $\mathcal{RM}(k-1, m-1)$.*

Proof. Recall, that the set of monomials in the basis (2.1.5) of $\mathcal{J}_{2,m}^{k+1}$ is invariant under the permutations of the variables X_i, i.e. the set of binary m-tuples $(k_1, k_2, \dots, k_m)$ assigned to the basis (2.1.5) is invariant under the

permutations of all elements of the symmetric group S_m. Take the basis elements with $k_m = 1$. Then the monomials $X_1^{k_1} \dots X_m^{k_m}$ of degree m can be projected by

$$\pi : (k_1, k_2, \dots, k_{m-1}, 1) \mapsto (k_1, k_2, \dots, k_{m-1}).$$

In this way we get a basis of $\mathcal{J}^k_{2,m-1} \cong \mathcal{RM}(k-1, m-1)$. □

Example 4.7. *For $m = 6$ the quotient space $\mathcal{J}^3_{2,m}/\mathcal{J}^4_{2,m}$ has a basis with $\binom{6}{3} = 20$ elements, where the binary 6-tuples corresponding to the coset representative monomials (the set X) are listed in pairs of complements:*

$$\begin{array}{ll}
(1,1,1,0,0,0) & (0,0,0,1,1,1) \\
(1,1,0,1,0,0) & (0,0,1,0,1,1) \\
(1,1,0,0,1,0) & (0,0,1,1,0,1) \\
(1,1,0,0,0,1) & (0,0,1,1,1,0) \\
(1,0,1,1,0,0) & (0,1,0,0,1,1) \\
(1,0,1,0,1,0) & (0,1,0,1,0,1) \\
(1,0,1,0,0,1) & (0,1,0,1,1,0) \\
(1,0,0,1,1,0) & (0,1,1,0,0,1) \\
(1,0,0,1,0,1) & (0,1,1,0,1,0) \\
(1,0,0,0,1,1) & (0,1,1,1,0,0)
\end{array}$$

and we have $2^{\frac{1}{2}\binom{6}{3}} = 2^{10}$ complement-free sets. For example the following

complement-free set Y and the set $\mathscr{Y}$, each consisting of 10 *elements:*

Y	$\mathscr{Y}$
$(1,1,1,0,0,0)$,	$X_1X_2X_3$
$(0,0,1,0,1,1)$,	$X_3X_5X_6$
$(1,1,0,0,1,0)$,	$X_1X_2X_5$
$(0,0,1,1,1,0)$,	$X_3X_4X_5$
$(1,0,1,1,0,0)$,	$X_1X_3X_4$
$(0,1,0,1,0,1)$,	$X_2X_4X_6$
$(0,1,0,1,1,0)$,	$X_2X_4X_5$
$(0,1,1,0,0,1)$,	$X_2X_3X_6$
$(1,0,0,1,0,1)$,	$X_1X_4X_6$
$(1,0,0,0,1,1)$,	$X_1X_5X_6$

Theorem 4.8. *Let $\mathcal{C}$ be a binary code with*

$$\mathcal{RM}(k-1,2k) \subset \mathcal{C} \subset \mathcal{RM}(k,2k)$$

and the following basis of the quotient $\mathcal{C}/\mathcal{RM}(k-1,2k)$

$$\left\{ \prod_{i=1}^{m} X_i^{k_i} + \mathcal{RM}(k-1,2k), \text{ where } k_i \in \{0,1\} \text{ and } \sum_{i=1}^{m} k_i = k \right\}, \quad (4.2.2)$$

where the set of the exponent m-tuples $(k_1,k_2,\ldots,k_m)$ is a maximal (with cardinality $2^{\frac{1}{2}\binom{2k}{k}}$) complement-free subset of X. Then $\mathcal{C}$ forms a doubly even self-dual $(2^{2k},2^{2k-1},2^k)$-code.

Proof. For the group algebra $\mathscr{A}_{2,m}$ suppose m is even, i.e. $m = 2k$ for some positive integer k. By the group algebra representation of $\mathcal{RM}$-codes and the definition of $\mathcal{C}$ we have the relation $\mathcal{J}_{2,m}^{k+1} \subset \mathcal{C} \subset \mathcal{J}_{2,m}^{k}$. For $m = 2k$ the set $\mathscr{X}$ is the set of coset representatives of the quotient space $\mathcal{J}_{2,m}^{k}/\mathcal{J}_{2,m}^{k+1}$, i.e. the set of monomials satisfying (2.1.6). Clearly, two mono-

mials $X_1^{k_1}X_2^{k_2}\dots X_m^{k_m}$ and $X_1^{l_1}X_2^{l_2}\dots X_m^{l_m}$ are orthogonal, i.e. their product is zero, if for some $i: 1 \le i \le m$ we have $k_i = l_i$. Thus, the elements in the radical corresponding to these monomials are orthogonal if their exponent m-tuples belong to a complement-free set. The m-tuples $(k_1, k_2 \dots k_m)$ have to be complement-free in Y, otherwise the corresponding monomials in $\mathscr{Y}$ are not orthogonal. Clearly Y is a complement-free subset of X (given by (4.2.1)) with cardinality $\frac{1}{2}\binom{2k}{k} = \binom{2k-1}{k-1}$. By definition, $\mathcal{C} = \langle\, \mathcal{J}_{2,m}^{k+1} \bigcup \mathscr{Y} \,\rangle$ is a subspace of the radical $\mathcal{J}_{2,m}$ of the group algebra $\mathscr{A}_{2,m}$ generated by the union of $\mathcal{J}_{2,m}^{k+1}$ and $\mathscr{Y}$. For the dimension of $\mathcal{C}$ we have

$$\begin{aligned} \dim(\mathcal{C}) = \dim(\mathcal{RM}(k-1,m)) + \frac{1}{2}\binom{2k}{k} = \\ 1 + \sum_{i=1}^{k-1}\binom{2k}{i} + \frac{1}{2}\binom{2k}{k} = 2^{2k-1}. \end{aligned} \tag{4.2.3}$$

It follows that $\mathcal{C}$ is self-dual. Since a binary self-dual code contains a word of weight 2 if and only if the generator matrix has two equal columns, we have our self-dual code to be doubly even. Each monomial in $\mathscr{Y}$ has the same weight 2^k, that is the minimal distance of $\mathcal{C}$. Using the identities for the monomials involved in the basis of our codes

$$x_i(x_j+1) = (x_i+1)(x_j+1) + (x_j+1) \text{ and } (x_i+1)^2 = 0,$$

we easily obtain that $\mathcal{C}$ (which is a subspace of $\mathcal{J}_{2,m}$) is an ideal in the group algebra $\mathscr{A}_{2,m}$. □

Theorem 4.9. *Let $\mathcal{C}$ be the code defined in Theorem 4.8. Suppose that $k_i = 0$ for some $i: 1 \le i \le m$ in each element of the subset Y, (i.e. the variable X_i is missing in each monomial of $\mathscr{Y}$). Then we have the following*

isomorphism

$$\mathcal{C} \cong \mathcal{RM}(k-1,2k-1) \oplus \mathcal{RM}(k-1,2k-1).$$

Proof. The elements of $\mathscr{Y}$ are of the form

$$X_1^{k_1} \dots X_m^{k_m} = (x_1+1)^{k_1}(x_2+1)^{k_2} \dots (x_m+1)^{k_m}, \text{ where } \sum_{i=1}^{m} k_i = k$$

and their weight is 2^k. Project the set of monomials with $k_i = 0$ in $\mathcal{C} = \langle\, \mathcal{J}_{2,m}^{k+1} \bigcup \mathscr{Y} \,\rangle$ onto the monomials $X_1^{k_1}, \dots, X_{i-1}^{k_{i-1}}, X_{i+1}^{k_{i+1}}, \dots, X_m^{k_m}$. The image $\mathcal{C}_1$ of this projection is a self-dual $\mathcal{RM}(k-1,2k-1)$-code with parameters $(2^{2k-1}, 2^{2k-2}, 2^k)$.

Now we consider all those elements of the basis of $\mathcal{J}_{2,m}^{k+1}$ which fulfill $k_i = 1$ for some $i \in \{1, \dots, m\}$. By Lemma 4.6 we know that the subspace $\mathcal{C}_2$ generated by these elements is isomorphic to $\mathcal{RM}(k-1,2k-1)$. The intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$ is empty. Therefore $\mathcal{C} \cong \mathcal{C}_1 \oplus \mathcal{C}_2$ and the statement follows. □

Properties

In this section we mention briefly some properties of the codes constructed in Theorem 4.8 without any claim to completeness.

Remark 4.10. In particular, we get $(16,8,4)$ self-dual codes for $m = 4$ in Theorem 4.8. These codes are extremal doubly even codes. One can easily check the classification of binary self-dual codes listed in [P2]. There are two cases:

1. If $k_i = 0$ for some $i : 1 \le i \le m$ in each element of the set Y, then we get the direct sum $E_8 \oplus E_8$, where E_8 is the extended Hamming code.

2. otherwise we get an indecomposable $(16,8,4)$-code (which is denoted by E_{16} in [P2]).

These codes are formally self-dual. Both classes have the weight function $z^{16}+28z^{12}+198z^8+28z^4+1$, where αz^w means there are α codewords which have weight w.

Remark 4.11. Using the inclusion-exclusion principle a formula can be given for the dimension of the $\mathcal{RM}(k+1,m)$-code (see for example in [AK] Theorem 5.5). If $p=2$ and $0\le k\le m$, then we have

$$\dim \mathcal{C} = \tfrac{1}{2}\binom{2k}{k} + \sum_{i=k+1}^{m}\sum_{j=0}^{2k}(-1)^j\binom{2k}{j}\binom{2k-2j+i-1}{i-2j} = \sum_{i=k+1}^{m}\binom{2k}{i} + \tfrac{1}{2}\binom{2k}{k},$$

where $i-2j\ge 0$. This is the same quantity as in (4.2.3).

The codes constructed in this chapter are worth to be studied further. Already for $k=2$ we get two non-isomorphic codes with the same parameters. It would be interesting to determine all classes of codes up to isomorphism for each arbitrary integer k and to determine their automorphism group. The code $\mathcal{C}$ in Theorem 4.8 is not affine-invariant, i.e. the automorphism group does not contain the affine group $AGL(m,2)$. For $m\le 6$ our computations show that the automorphism group of $\mathcal{C}$ with $k_i=0$ differs from the automorphism group of $\mathcal{C}$ with $k_i=1$ for some $1\le i\le m$, which implies that these codes are not isomorphic.

Chapter 5

Monomial group codes with visible bases

5.1 Linear codes with visible bases

In this chapter, we construct codes which are ideals in the radical of the modular group algebra $\mathscr{A}_{p,m}$ for arbitrary prime p. In some places we want to point out that a code $\mathcal{C}$ is an ideal, then we use for generating sets the () brackets. Let $\mathcal{C}$ be a monomial code generated by some monomials of the form

$$X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}, \text{ where } 0 \leq k_i \leq p-1.$$

Similar to the notation in the previous chapters we will refer to the monomial $X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}$ by the m-tuple of exponents

$$(k_1, k_2, \dots, k_m) \in \{0, 1, \dots, p-1\}^m.$$

Definition 5.1. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_p$, i.e. we consider $\mathcal{C}$ as a subspace of the vector space $\mathbb{F}_p^n$. We say that a basis of $\mathcal{C}$ is a visible basis if at least one member of the basis has the same Hamming weight*

as $\mathcal{C}$.

It is known (Prop. 1.8 in [DL]) that for $p = 2$ every monomial code has a visible basis.

Remark 5.2. *This definition of codes with visible bases is different from the definition of visible codes by Ward in [W2]. He defined that a set V is visible, if each subspace generated by a non-empty subset of V has the same weight as the generator set, i.e. the weight of at least one member of the basis equals the weight of the generated code. Obviously, if a code is visible in the sense of Ward, then it also has a visible basis.*

The class of *maximal monomial codes* I_d in the group algebra $\mathscr{A}_{p,m}$ were defined in [DL] as

$$I_d = \left(\prod_{i=1}^{m} X_i^{k_i} \mid \prod_{i=1}^{m} (k_i + 1) \geq d, 0 \leq k_i < p \right).$$

These codes have length p^m. If $p = 2$, then these codes coincide with the powers of $J_{2,m}$, i.e. they are Reed-Muller codes.

The maximal monomial code is uniquely defined. The minimum distance of I_d is $d = \min\{\prod_{i=1}^{m}(k_i+1)\}$, see [DL]. Thus, I_d has a visible basis.

For $p > 2$ some of the maximal monomial codes have better parameters than the $\mathcal{GRM}$-codes. For example if $p = 5$ and $m = 3$ the code I_{20} is a $(125, 63, 20)$ code, and $\mathcal{J}^{20}$ is a $(125, 53, 20)$-code.

We will denote the dimension of the ideal I_d by $\dim(I_d)$ and the dimension of the corresponding $\mathcal{GRM}$ code with the same minimum distance by $\dim(\mathcal{GRM})$.

It is not too hard to compute the dimension of the codes I_d. For $p > d$ we have the following relations of $\dim(I_d)$ and $\dim(\mathcal{GRM})$:

Table 5.1: Relations of $\dim(I_d)$ and $\dim(\mathcal{GRM})$

$d=3$	$\dim(I_d)=\dim(\mathcal{GRM})$
$d=4$	$\dim(I_d)=\dim(\mathcal{GRM})+\binom{m}{2}$
$d=5$	$\dim(I_d)=\dim(\mathcal{GRM})+\binom{m}{2}+\binom{m}{3}+m(m-1)$
$d=6$	$\dim(I_d)=\dim(\mathcal{GRM})+\sum_{i=2}^{4}\binom{m}{i}+m(m-1)+m\binom{m-1}{2}$

Monomially equivalent codes were introduced by Drensky and Lakatos in [DL] as follows:

Definition 5.3. *Two codes are monomially equivalent if one code can be obtained by permuting the variables $X_1,\ldots,X_m$ of the other one.*

Definition 5.4. *A code generated by monomials is called monomially self-equivalent if it is invariant under all permutations of the variables $X_i = x_i - 1$ for $1 \leq i \leq m$.*

Remark 5.5. *The maximal monomial codes are monomially self-equivalent codes.*

In the sequel we construct monomial codes in the group algebra $\mathscr{A}_{p,m}$ by giving one visible basis for each of them.

Theorem 5.6. *Let $\mathcal{C}_{m,k}$ be a monomial code generated by the set*

$$B_{m,k}=\{\prod(X_i)^{k_i} \mid \prod_{i=1}^{m} k_i \geq k, \text{ where } 0\leq k_i<p,\ 0<k\leq(p-1)^m\}.$$

Then $B_{m,k}$ is a visible basis of $\mathcal{C}_{m,k}$.

Proof. The proof is similar to the proof of Lemma 1.9 in [B], it goes by induction on the numbers of direct factors in the elementary abelian group G.

For $m = 1$ the statement follows from Theorem 1.1 in [B]. In our case, the statement of Theorem 1.1 in [B] says if $\mathcal{C}_{1,i} = \left(X^i\right)$, where $1 \le i \le p-1$, then $\delta = i+1$. This δ equals the minimum of the weights of all elements from $B_{1,i}$. Thus $B_{1,i}$ is a visible basis for $\mathcal{C}_{1,i}$. Suppose that the statement is true for $m = i$ and we prove it for the case $m = i+1$.

Let $\mathbf{x}$ be an arbitrary codeword in $\mathcal{C}_{m,k}$. Then $\mathbf{x}$ can be written in the form

$$\mathbf{x} = \sum_{k_1,\ldots,k_m} \lambda_{k_1,\ldots,k_m} (x_1-1)^{k_1} \cdots (x_m-1)^{k_m}, \tag{5.1.1}$$

where $\lambda_{k_1,\ldots,k_m} \in \mathbb{F}$. If each $\lambda_{a_j} = 0$ or $a_j = 0$ for all $j \in \{1,\ldots,m\}$, then Theorem 5.6 holds. Thus we may assume, that $\mathbf{x}$ contains terms with $\lambda_{a_j} \neq 0$ and $a_j \neq 0$ for some $j \in \{1,\ldots,m\}$. Let $(x_m-1)^{l_m}$ be the lowest power of the element (x_m-1) in $\mathbf{x}$.

Then we have

$$\mathbf{x} = (x_m-1)^{l_m}(L_{l_m} + L_{l_m+1}(x_m-1) + L_{l_m+2}(x_m-1)^2 + \ldots L_{l_m+t}(x_m-1)^t), \tag{5.1.2}$$

where $0 \le t \le min(p-1, \frac{k}{l_m})$, $L_j \in \mathbb{F}[H]$, $l_m \le j \le l_m + t$, $H = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_{m-1} \rangle$. Since L_{l_m} is an element of the radical of $\mathbb{F}[H]$, we can write it in the form

$$L_{l_m} = \sum_{j_1,j_2,\ldots,j_{m-1}} \gamma_{j_1,j_2,\ldots,j_{m-1}} (x_1-1)^{j_1} \ldots (x_{m-1}-1)^{j_{m-1}} \neq 0\,, \quad (1 \le j_i \le p-1). \tag{5.1.3}$$

Then we have

$$\prod_{i=1}^{m-1} j_i \ge \frac{k}{l_m}, \text{ where } 0 < k \le (p-1)^m$$

for each term in the equation of the right-hand side of (5.1.3). By the

induction hypothesis there is a basis element $(x_1-1)^{k_1}\dots(x_{m-1}-1)^{k_{m-1}}$ in $\mathcal{C}_{m-1,\frac{k}{l_m}}$ such that

$$\delta_m = wt((x_1-1)^{k_1}(x_2-1)^{k_2}\dots(x_{m-1}-1)^{k_{m-1}}) \le wt(L_{i_m}),$$

where wt(y) denotes the Hamming weight of the codeword $y \in \mathcal{C}_{m,k}$.

Express L_{l_m} in the monomial basis of $\mathbb{F}[H]$, i.e.

$$L_{l_m} = \sum_{i_1,\dots i_{m-1}} \mu_{i_1,i_2,\dots,i_{m-1}} x_1^{i_1}\dots x_{m-1}^{i_{m-1}}.$$

Thus for the element $\mathbf{x}$ in (5.1.2) we have

$$\mathbf{x} = (x_m-1)^{l_m}.$$

$$\cdot\left(\sum_{i_1,i_2,\dots,i_{m-1}} \mu_{i_1,i_2,\dots,i_{m-1}} + \mu^{(1)}_{i_1,i_2,\dots,i_{m-1}}(x_m-1) + \dots + \mu^{(t)}_{i_1,i_2,\dots,i_{m-1}}(x_m-1)^t\right)\cdot$$

$$\cdot x_1^{i_1}\dots x_{m-1}^{i_{m-1}} = (x_m-1)^{l_m}\sum_{i_1,i_2,\dots,i_{m-1}} \Gamma_{i_1,i_2,\dots,i_{m-1}} x_1^{i_1}\dots x_{m-1}^{i_{m-1}},$$

where $\Gamma_{i_1,i_2,\dots,i_{m-1}} \in \mathbb{F}[\langle x_m\rangle]$. By Theorem 1.1 of Berman [B], there exists an element $(x_m-1)^r$ such that $r \ge l_m$ and

$$wt((x_m-1)^{l_m}\Gamma_{i_1,i_2,\dots,i_{m-1}}) \ge wt(x_m-1)^r.$$

It follows that

$$wt(\mathbf{x}) \ge d_m wt(x_m-1)^r = wt\left((x_m-1)^r(x_1-1)^{k_1}(x_2-1)^{k_2}\dots(x_{m-1}-1)^{k_{m-1}}\right),$$

while

$$r\prod_{i=1}^{m-1}(k_i) \geq r\frac{k}{l_m} \geq k.$$

This completes the proof. □

Remark 5.7. *The dimension of $\mathcal{C}_{m,k}$ can be calculated in the following way. Let $P_m^{r_1,\ldots,r_i}$ denote the number of permutations on m elements with $r_1,\ldots,r_i$ repititions. If $k = l_1 \cdot \ldots \cdot l_m$, then*

$$\dim(\mathcal{C}_{m,k}) = \sum_{\substack{l_i \leq p-1 \\ l_1 \cdot \ldots \cdot l_m \geq k}} P_m^{r_1,\ldots,r_i}.$$

5.2 Principal ideal code

The next theorem is a consequence of Corollary 3.3 in [MM], where the "monomial-like" abelian code is a principal ideal of a modular groupring over an arbitrary finite field of characteristic p. At the visibility we restrict ourself to the group algebra $\mathscr{A}_{p,m}$ with its radical $\mathcal{J}_{p,m}$.

Theorem 5.8. *Let p be an arbitrary prime. We fix values $a_1,\ldots,a_m$ each fulfilling $0 \leq a_i < p$, where $i \in \{1,\ldots,m\}$, and at least one of them is nonzero. Then the principal ideal*

$$\mathcal{C}_{a_1,\ldots,a_m} = \left(X_1^{a_1}X_2^{a_2}\ldots X_m^{a_m}\right)$$

in $\mathcal{J}_{p,m}$ determines a cyclic code. The set

$$B = \{\prod_{i=1}^{m} X_i^{k_i} \mid a_i \leq k_i < p,\ i = 1,2,\ldots,m\}$$

is a visible basis of $\mathcal{C}_{a_1,\ldots,a_m}$.

Furthermore, $\mathcal{C}_{a_1,\ldots,a_m}$ *is a* $(p^m,(p-a_1)\cdot(p-a_2)\cdot\ldots\cdot(p-a_m),\delta)$*-code, where* $\delta=\prod_{i=1}^{m}(a_i+1)$.

Proof. Denote the ideal $\left(X_j^{a_j}\right)=\left((x_j-1)^{a_j}\right)$ in the ring $\mathbb{F}[x_j]/(x_j^p-1)$ for $1\leq j\leq m$ by $\mathcal{C}_{X_j}$. Then $\mathcal{C}_{a_1,\ldots,a_m}$ is a tensor product $\mathcal{C}\cong\mathcal{C}_{X_1}\otimes\mathcal{C}_{X_2}\otimes\cdots\otimes\mathcal{C}_{X_m}$ (see [MM], Corollary 3.3), where $\mathcal{C}_{X_j}=\left(X_j^{a_j}\right)$ $(1\leq j\leq m)$ is a cyclic code. Each code $\mathcal{C}_{X_j}$ has a visible basis, which is the set

$$\{X_j^{k_j}|a_j\leq k_i<p\}$$

with minimal distance a_j+1. By the theorem of Ward [W2], the tensor product $\mathcal{C}_{a_1,\ldots,a_m}$ is visible. Thus, it has a visible basis. □

Remark 5.9. *The codes* $\mathcal{C}_{a_1,\ldots,a_m}$ *are different from the* $\mathcal{GRM}$*-codes. We know that the* $\mathcal{GRM}$*-codes coincide with the powers of the Jacobson radical* $\mathcal{J}^k$ *for some* $1\leq k\leq m(p-1)$. *We have*

$$\mathcal{C}_{a_1,\ldots,a_m}\cong\mathcal{J}^k\Leftrightarrow k=m(p-1)\text{ and }a_i=p-1\ \forall i\in\{1,\ldots,m\}.$$

Corollary 5.10. *Let* $p=2$ *and* $\mathcal{C}$ *be a* $(2^m,2^k,2^d)$*-code defined in Theorem 5.8, where* $0\leq k\leq m$. *Then* $\mathcal{C}$ *is always self-orthogonal and it is self-dual if and only if* $k=m-1$.

Proof. The difference of two arbitrary codewords has even weight (see e.g. the generator matrix $\mathscr{M}_C$ in the proof of Theorem 5.11). Thus all codewords are orthogonal to each other. In the example of page 4 in [HL2] it is shown that if $k=m-1$, then $\mathcal{C}$ is self-dual and it is a direct sum of $(2,1,2)$-codes. Further, the dimension of $\mathcal{C}$ implies self-duality if and only if $k=m-1$. □

5.3 Automorphism groups of principal ideal codes

In this part of the dissertation we will consider the codes defined in Theorem 5.8 for $p = 2$. We will determine their automorphism groups. In the following we will denote a generator matrix of the code $\mathcal{C}$ by $\mathscr{M}_{\mathcal{C}}$. An automorphism of a linear code is a permutation of coordinates that stabilizes the code. In other words, an automorphism of $\mathcal{C}$ is a permutation of the columns of $\mathscr{M}_{\mathcal{C}}$, such that the code generated by the permuted generator matrix coincides with $\mathcal{C}$. The automorphisms of a code $\mathcal{C}$ form a group and this group is denoted by $Aut(\mathcal{C})$. Let S_n denote the symmetric group on n elements. It is well known that if $\mathcal{C}$ is a code of length ν, then $Aut(\mathcal{C})$ is a subgroup of S_ν. Automorphism groups of binary codes were determined by the combinatorial method we use for example in [P2]. The author used the program packages GAP and MAGMA in order to show some examples.

Theorem 5.11. *Let $p = 2$ and m be an arbitrary positive integer. Let $\mathcal{C}$ be the code defined in Theorem 5.8 and*

$$\mathcal{C} = (X_1 \cdots X_t),$$

where $1 \leq t \leq m$. We will denote the dimension of $\mathcal{C}$ by λ and its minimum distance by δ. Then $\mathcal{C}$ is a $(2^m, \lambda, \delta)-$code, where $\lambda = 2^{m-t}$ and $\delta = 2^t$. Then the automorphism group of $\mathcal{C}$ can be written as the following semidirect product

$$Aut(\mathcal{C}) = S_\delta^\lambda \rtimes S_\lambda,$$

where S_δ^λ means $\underbrace{S_\delta \times \ldots \times S_\delta}_{\lambda}$ and S_i (for $i = \delta, \lambda$) denotes the symmetric group on i elements.

Remark 5.12. *From the definition of the wreath product of permutation*

groups (see [KK], or [Cam] Sec. 1.10) follows $Aut(C) = S_\delta \wr S_\lambda$.

Before we prove Theorem 5.11 and Remark 5.12, let us consider an example.

Example 5.13. *Let* $m = 4$ *and* $C_{1,1,0,0} = (X_1X_2)$. *Then*

$$\mathscr{M}_C = \begin{pmatrix} X_1X_2 \\ X_1X_2X_3 \\ X_1X_2X_4 \\ X_1X_2X_3X_4 \end{pmatrix} =$$

$$\left(\begin{array}{cccc}
\underbrace{1 \quad x_1 \quad x_2 \quad x_1x_2}_{\alpha_1} & \underbrace{x_3 \quad x_1x_3 \quad x_2x_3 \quad x_1x_2x_3}_{\alpha_2} & \underbrace{\quad\ldots\quad}_{\alpha_3} & \underbrace{x_3x_4 \quad x_1x_3x_4 \quad x_2x_3x_4 \quad x_1x_2x_3x_4}_{\alpha_4} \\
\hline
\begin{array}{cccc} \underbrace{1\ 1\ 1\ 1}_{\alpha_1} & \underbrace{0\ 0\ 0\ 0}_{\alpha_2} & \underbrace{0\ 0\ 0\ 0}_{\alpha_3} & \underbrace{0\ 0\ 0\ 0}_{\alpha_4} \\ \underbrace{1\ 1\ 1\ 1}_{\alpha_1} & \underbrace{1\ 1\ 1\ 1}_{\alpha_2} & \underbrace{0\ 0\ 0\ 0}_{\alpha_3} & \underbrace{0\ 0\ 0\ 0}_{\alpha_4} \\ \underbrace{1\ 1\ 1\ 1}_{\alpha_1} & \underbrace{0\ 0\ 0\ 0}_{\alpha_2} & \underbrace{1\ 1\ 1\ 1}_{\alpha_3} & \underbrace{0\ 0\ 0\ 0}_{\alpha_4} \\ \underbrace{1\ 1\ 1\ 1}_{\alpha_1} & \underbrace{1\ 1\ 1\ 1}_{\alpha_2} & \underbrace{1\ 1\ 1\ 1}_{\alpha_3} & \underbrace{1\ 1\ 1\ 1}_{\alpha_4} \end{array}
\end{array}\right)$$

is a generator matrix of $C_{1,1,0,0}$.

Here $\delta = 4$ *and* $\lambda = 4$. *We can divide each row into* 4 *pieces of* 4*-tuples, denote these by* $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. *Each* 4*-tuple either consists only of* 1*-s or only of* 0*-s.* S_4 *acts on the coordinates of each* 4*-tuple and* S_4 *acts on the set* $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. *By Theorem 5.11 we have* $Aut(C) = S_4^4 \rtimes S_4$, *which can be easily verified by computation with some algebraic program package like MAGMA or GAP. The construction of the generator matrix* $\mathscr{M}_C$ *is also used in the proof of Theorem 5.11.*

Proof. Using the identity

$$x_j(x_i-1) = (x_j-1)(x_i-1) + (x_j-1) = X_jX_i + X_j,$$

we can see that $\mathcal{C}$ is an ideal in $\mathscr{A}_{p,m}$. We construct the following matrix $\mathscr{M}_{\mathcal{C}}$ of size $2^{m-t} \times 2^m$, which is a generator matrix of the code $\mathcal{C}$. The rows of $\mathscr{M}_{\mathcal{C}}$ are multiples of $X_1 \dots X_t$. More precisely we choose each subset of $\{X_{t+1}, \dots, X_m\}$ and multiply the variables of these subsets with the monomial $X_1 \dots X_t$.

$$\mathscr{M}_{\mathcal{C}} = \begin{pmatrix} X_1X_2 \dots X_t \\ X_1X_2 \dots X_tX_{t+1} \\ X_1X_2 \dots X_tX_{t+2} \\ X_1X_2 \dots X_tX_{t+1}X_{t+2} \\ \vdots \\ X_1X_2 \dots X_tX_m \\ X_1X_2 \dots X_tX_{t+1}X_m \\ X_1X_2 \dots X_tX_{t+2}X_m \\ X_1X_2 \dots X_tX_{t+1}X_{t+2}X_m \\ \vdots \\ X_1X_2 \dots X_tX_{t+1}X_{t+2} \dots X_{m-2}X_m \\ X_1X_2 \dots X_tX_{t+1}X_{t+2} \dots X_{m-2}X_{m-1}X_m \end{pmatrix}$$

Let $x_1, \dots, x_m$ be a basis of the elementary abelian 2-group G. We write the elements of the rows of the binary matrix $\mathscr{M}_{\mathcal{C}}$ in the basis of G in lexicographical order. The lexicographical order means that for $b_i, c_i \in \{0,1\}$, $1 \leq i \leq m$ we have

$$x_1^{b_1}x_2^{b_2} \dots x_m^{b_m} < x_1^{c_1}x_2^{c_2} \dots x_m^{c_m} \iff \sum_{j=1}^{m} b_j 2^{j-1} < \sum_{j=1}^{m} c_j 2^{j-1}.$$

Keeping in mind $X_i = x_i - 1$, we can now write down the matrix $\mathscr{M}_C$ as the following binary matrix.

$$\mathscr{M}_C =$$

$$\begin{pmatrix}
1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 & \dots & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
 & & & \vdots & & & & & & & & & & & & & & & & & & & \\
1 & \dots & 1 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 1 & \dots & 1 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 1 & \dots & 1 & 0 & \dots & 0 & \dots & 1 & \dots & 1 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\
 & & & \vdots & & & & & & & & & & & & & & & & & & & \\
1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 1 & 0 & \dots & 0 & 1 & \dots & 1 \\
1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 1 & \dots & 1 & 1 & \dots & 1 & 1 & \dots & 1 \\
\underbrace{}_{\delta} & & & \underbrace{}_{\delta} & & & \underbrace{}_{\delta} & & & & \underbrace{}_{\delta} & & & & \underbrace{}_{\delta} & & & \underbrace{}_{\delta} & & & \underbrace{}_{\delta} & &
\end{pmatrix}$$

That means G_C is of the form $\begin{pmatrix} A & 0 \\ A & A \end{pmatrix}$ for some binary matrix A of size $2^{m-t-1} \times 2^{m-1}$. Thus $\mathscr{M}_C$ is a tensor product of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and A.

We can see that in $\mathscr{M}_C$ there is one row of weight $\delta = 2^t$, there are $m-t$ rows of weight 2^{t+1}, $\binom{m-t}{2}$ rows with weight 2^{t+2}, etc. Finally we have one row with weight 2^m. Thus $\mathscr{M}_C$ has 2^{m-t} rows.

Each row of $\mathscr{M}_C$ can be divided into δ-tuples of 1-s and 0-s. The coordinates of each of the δ-tuples can be permuted by S_δ and the number of δ-tuples in one row is $\lambda = 2^{m-t}$. Furthermore, the δ-tuples can be permuted as δ-tuples by all elements of S_λ.

We still have to show that there are no other automorphisms of C. Let us suppose that there exists $\psi \notin S_\delta^\lambda \rtimes S_\lambda$, which is an automorphism of C. That means ψ does not only act on the coordinates of the δ-tuples or on the set of δ-tuples (which has cardinality λ). Thus ψ cuts apart at least one of the δ-tuples. Thus, if $\mathscr{M}_C$ is the generator matrix of C, then the code generated by $\mathscr{M}_C^\psi$ is not identical to the code C, although they are permutation equivalent.

Now we will show that S_δ^λ is normal in $Aut(\mathcal{C})$. Let $g \in S_\delta^\lambda$ and $\sigma \in Aut(\mathcal{C})$ be arbitrary. Then $\sigma = (\sigma_1, \ldots, \sigma_\lambda, \sigma_\mu)$, where $\sigma_1, \ldots, \sigma_\lambda \in S_\delta$ and $\sigma_\mu \in S_\lambda$, further $g = (g_1, \ldots, g_\lambda)$, where $g_1, \ldots, g_\lambda \in S_\delta$. We have

$$\sigma^{-1} g \sigma = (\sigma_1^{-1} g_1 \sigma_1, \ldots, \sigma_\lambda^{-1} g_\lambda \sigma_\lambda)^{\sigma_\mu},$$

which means that $\sigma_i^{-1} g_i \sigma_i \in S_\delta$ and σ_μ acts on $\sigma_1^{-1} g_1 \sigma_1, \ldots, \sigma_\lambda^{-1} g_\lambda \sigma_\lambda$ as permutation. Thus $\sigma^{-1} g \sigma \in S_\delta^\lambda$.

We also show that S_λ is in general not normal in $Aut(\mathcal{C})$. Let $h \in S_\lambda$ and we take again $\sigma \in Aut(\mathcal{C})$ as previously. Further we will denote the δ-tuples by $\alpha_1, \ldots \alpha_\lambda$. Then

$$\sigma^{-1} h \sigma = (\sigma_1^{-1} \alpha_1 \sigma_1, \ldots, \sigma_\lambda^{-1} \alpha_\lambda \sigma_\lambda)^{\sigma_\mu},$$

which means that σ_μ permutes the $\sigma_i^{-1} \alpha_i \sigma_i$. Since $\sigma_i^{-1} a_i \sigma_i \neq \alpha_i$ in general, this element cannot always be expressed as a permutation of $\alpha_1, \ldots, \alpha_\lambda$. Since S_δ^λ and S_λ are both subgroups of $Aut(\mathcal{C})$, we have that the group $Aut(\mathcal{C})$ is an outer semidirect product of S_δ^λ and S_λ. This completes the proof. □

Example 5.14. *We denote a cyclic group of two elements by C_2 and let $\mathcal{C}$ be the code $\mathcal{C} = (X_1)$. Then $\mathcal{C}$ is a $(2^m, 2^{m-1}, 2)$-code. We fix $s := 2^{m-1}$, thus $Aut(\mathcal{C}) = C_2^s \rtimes S_s$, where $C_2^s = \underbrace{C_2 \times \ldots \times C_2}_{s}$.*

Summary

In this dissertation we introduce some new results in the area of Algebraic Coding Theory. Let p be a prime number and $\mathbb{F}$ a field of characteristic p. If G is a finite abelian p-group, then $\mathbb{F}[G]$ is a modular group algebra. We use some well-known facts about the Jacobson radical of $\mathbb{F}[G]$, which were proved by Jennings in [J]. Berman [B] proved that Reed-Muller codes are powers of the radical of $\mathbb{F}[G]$ if G is elementary abelian and $p = 2$. Charpin proved the general case for arbitrary p. Landrock and Manz showed in [LM] the connection between these results and the classical result of Jennings related to the structure of the Jacobson radical of $\mathbb{F}[G]$, where G is a finite p-group.

Berman gave an algorithm to determine the minimum distance of codes which are radical powers. We use this algorithm in Chapter 3 to construct self-dual codes with given distance.

We denote the Jacobson radical of $\mathbb{F}[G]$ by $\jmath$. If p is odd and G is abelian, then the nilpotency index of $\jmath$ is odd. It follows that there is no self-dual code which is a power of the radical. Naturally arises the question of Drensky and Lakatos [DL]:

Problem 3.1 Let n be an arbitrary positive integer and $d \leq \lceil \frac{n}{2} \rceil$. Does there exist an abelian 2-group G of order 2^n, such that some power of the Jacobson radical of the group algebra $\mathbb{F}_2[G]$ is a self-dual $(2^n, 2^{n-1}, 2^d)-$code?

The first result of this dissertation is the construction of abelian 2-groups which are solutions to Problem 3.1. The result is published in [HL1].

Theorem 3.2 *Let $\mathbb{F}$ be a field of characteristic 2. Let n be an arbitrary positive integer. Then for each integer d with $1 \leq d \leq \lceil \frac{n}{2} \rceil$ there exists an abelian group G of order 2^n, such that there exists a power of $\jmath(\mathbb{F}[G])$ which defines a self-dual $(2^n, 2^{n-1}, 2^d)$-code.*

The proof of this theorem is constructive.

Reed-Muller codes play an important role in connection to our results, so we introduce three convenient definitions in Chapter 2, but we use and generalize the monomial representation of these well-known codes in the Chapters 4 and 5.

If $p = 2$ and G is elementary abelian, then the radical of $\mathbb{F}[G]$ has a power which is a self-dual code if and only if G has odd rank. In Chapter 4 we construct self-dual binary codes for even rank of G. These codes are between two consecutive powers of the radical. We introduce complement-free sets for the construction of these codes.

Let y be a binary m-tuple. We say that $\mathbf{1} - y$ is the complement m-tuple of y, where $\mathbf{1}$ denotes the all-1 tuple $(\underbrace{1, \ldots, 1}_{m})$. Let $m = 2k$ and X be the set of all binary m-tuples with exactly k '0'-s and '1'-s. Further, let Y be a subset of X such that if $y \in Y$, then $\mathbf{1} - y \notin Y$. Then Y is called a *complement-free* set of binary m-tuples.

We prove the following theorem, which gives a construction of self-dual $(2^{2k}, 2^{2k-1}, 2^k)$-codes.

Theorem 4.8 *Let $\mathcal{C}$ be a binary code with*

$$\mathcal{RM}(k-1, 2k) \subset \mathcal{C} \subset \mathcal{RM}(k, 2k)$$

and the following basis of the quotient $\mathcal{C}/\mathcal{RM}(k-1,2k)$

$$\left\{\prod_{i=1}^{m} X_i^{k_i} + \mathcal{RM}(k-1,2k),\ \textit{where } k_i \in \{0,1\} \textit{ and } \sum_{i=1}^{m} k_i = k\right\}, \quad (5.3.1)$$

where the set of the exponent m-tuples $(k_1,k_2,\ldots,k_m)$ *is a maximal (with cardinality* $2^{\frac{1}{2}\binom{2k}{k}}$*) complement-free subset of* X*. Then* $\mathcal{C}$ *forms a doubly even self-dual* $(2^{2k},2^{2k-1},2^k)$*-code.*

Furthermore we prove that if there exists one element $i \in \{1,\ldots,m\}$, such that $k_i = 0$ for each element of the maximal complement-free subset, then the constructed self-dual $(2^{2k},2^{2k-1},2^k)$-code is the direct sum of two copies of the Reed-Muller code $\mathcal{RM}(k-1,2k-1)$. This is Theorem 4.9 of this dissertation.

The monomial codes introduced in [DL] are ideals generated by monomials in modular group algebras over elementary abelian p-groups. In Chapter 5 we investigate monomial codes over an elementary abelian p-group G.

The minimum distance of linear codes is very important for the error correction capability. It is usually more difficult to determine the minimum distance than in Berman's case, i.e. if the code is a power of the radical in a modular group algebra. The simplest case is to determine the minimal distance from its basis if there exists an element in the basis having the weight equal to the minimum distance of the code. We introduce the following group codes which have such a basis.

Theorem 5.6 *Let* $\mathcal{C}_{m,k}$ *be a monomial code generated by the set*

$$B_{m,k} = \{\prod (X_i)^{k_i} \mid \prod_{i=1}^{m} k_i \geq k,\ \textit{where } 0 \leq k_i < p,\ 0 < k \leq (p-1)^m\}.$$

Then $B_{m,k}$ *is a visible basis of* $\mathcal{C}_{m,k}$*.*

Theorem 5.8 *Let p be an arbitrary prime. We fix values $a_1,\dots,a_m$ each fulfilling $0 \le a_i < p$ and at least one of them is nonzero. Then the principal ideal*

$$C_{a_1,\dots,a_m} = \left(X_1^{a_1} X_2^{a_2} \dots X_m^{a_m}\right)$$

in $\mathcal{I}_{p,m}$ determines a cyclic code. The set

$$B = \{\prod_{i=1}^{m} X_i^{k_i} \mid a_i \le k_i < p,\ i = 1,2,\dots,m\}$$

is a visible basis of $C_{a_1,\dots,a_m}$.
Furthermore, $C_{a_1,\dots,a_m}$ is a $(p^m,(p-a_1)\cdot(p-a_2)\cdot\ldots\cdot(p-a_m),\delta)$-code, where $\delta = \prod_{i=1}^{m}(a_i+1)$.

The proof of Theorem 5.6 goes by induction on the numbers of direct factors in the elementary abelian group G. For the proof of Theorem 5.8 we use the fact that C can be regarded as a tensor product of smaller codes.

We also investigate the automorphism groups of the codes defined in Theorem 5.6 and we prove the following theorem.

Theorem 5.11 *Let $p = 2$ and m be an arbitrary positive integer. Let C be the code defined in Theorem 5.8 and*

$$C = (X_1 \cdots X_t),$$

where $1 \le t \le m$. We will denote the dimension of C by λ and its minimum distance by δ. Then C is a $(2^m,\lambda,\delta)-$code, where $\lambda = 2^{m-t}$ and $\delta = 2^t$. Then the automorphism group of C can be written as the following semidirect product

$$Aut(C) = S_\delta^\lambda \rtimes S_\lambda,$$

where S_δ^λ *means* $\underbrace{S_\delta \times \ldots \times S_\delta}_{\lambda}$ *and* S_i *(for* $i = \delta, \lambda$*) denotes the symmetric group on* i *elements.*

Remark 5.12 *From the definition of the wreath product of permutation groups (see [KK], or [Cam] Sec. 1.10) it follows that* $Aut(C) = S_\delta \wr S_\lambda$.

The proof of Theorem 5.11 is theoretical, we use a combinatorial method which was introduced by Pless in [P2] in order to determine the automorphism group of C.

Összefoglaló

Ebben a disszertációban moduláris csoportalgebrák radikáljaiban szereplő ideálokat mint lineáris kódokat vizsgálunk.

Legyen p egy prímszám és $\mathbb{F}$ egy p-karakterisztikájú test, továbbá legyen G egy véges Abel p-csoport. Ekkor az $\mathbb{F}[G]$ csoportalgebra moduláris. A dolgozatban a Jacobson radikálra vonatkozó Jennings [J] által bebizonyított eredményeket használjuk. Berman [B] mutatta meg, hogy a Reed-Muller kódok éppen az $\mathbb{F}[G]$ radikáljának hatványai, ha G elemi Abel és $\mathbb{F} = \mathbb{F}_2$. Charpin bebizonyította az általános esetet tetszőleges p-re. Berman és Charpin eredményeit felhasználva dolgozta ki Landrock és Manz [LM] az $\mathbb{F}[G]$ Jacobson radikáljának struktúráját. Az első két fejezetben a disszertációhoz fontos eredményeket, főként a Reed-Muller kódok leírását ismertetjük.

Az $\mathbb{F}[G]$ csoportalgebra radikálját $\jmath$-vel jelöljük. Ha p páratlan prím és G Abel csoport, akkor $\jmath$ nilpotencia foka páratlan. Ebből következik, hogy páratlan p-re nincs önduális kód, mely radikálhatványként áll elő.

A következő kérdést Drensky és Lakatos tette fel [DL]-ben:

3.1. Probléma Legyen n tetszőleges pozitív egész szám, és $d \leq \lceil \frac{n}{2} \rceil$. Létezik-e olyan G Abel 2-csoport, melynek rendje 2^n úgy, hogy $\mathbb{F}_{2^m}[G]$ Jacobson radikáljának valamilyen hatványa meghatároz egy $(2^n, 2^{n-1}2^d)$-kódot?

Az első eredmény ebben a disszertációban olyan Abel 2-csoportok konstrukciója, melyek megoldások a 3.1. Problémára. A harmadik fejezetben a Berman [B] által megadott algoritmust az adott távolságú önduális kódok konstrukciójához használjuk. Ez az eredmény megjelent a [HL1] publikációban.

3.2. Tétel *Legyen $\mathbb{F}$ egy 2-karakterisztikájú test. Ekkor minden n pozitív egész számhoz és $1 \leq d \leq \lceil \frac{n}{2} \rceil$ számhoz létezik olyan 2^n-rendű G Abel csoport, melyhez tartozó $\mathbb{F}[G]$ csoportalgebra $\jmath$ radikáljának valamely hatványa egy önduális $(2^n, 2^{n-1}, 2^d)$-kódot határoz meg.*

A 3.2. Tétel bizonyítása konstruktív.

A Reed-Muller kódok - mint a megfelelő monomiális csoportalgebra radikálhatványai - fontos szerepet játszanak a disszertációban, ezért bevezetünk három jól ismert definíciót a második fejezetben. Az eredményeinkkel kapcsolatosan a Reed-Muller kódok monomiális reprezentációját használjuk a negyedik és ötödik fejezetben.

Ha $p = 2$ és G elemi Abel csoport, akkor $\mathbb{F}[G]$ radikáljának valamely hatványa akkor és csak akkor definiál önduális kódot, ha G rangja páratlan. A negyedik fejezetben önduális bináris kódokat konstruálunk a radikálban ha G rangja páros. Mivel a konstruált kódok monomiálisak, a monomokban szereplő kitevők jellemzéséhez bevezetjük a komplemens-mentes halmaz fogalmát.

Legyen y egy bináris m-es. Azt mondjuk, hogy $\mathbf{1} - y$ az y komplemense, ahol $\mathbf{1}$ jelöli a tiszta 1-es m-es $\underbrace{(1, \ldots, 1)}_{m}$. Legyen $m = 2k$ és X legyen az a halmaz, mely az összes olyan m-esből áll, melyben pontosan k darab '0' és k darab '1' van. Továbbá legyen Y egy olyan részhalmaza X-nek, hogy ha $y \in Y$, akkor $\mathbf{1} - y \notin Y$. Ekkor Y-t bináris m-esekből álló *komplemens-mentes halmaz*nak hívjuk.

A következő tételt bizonyítjuk be, melyben konstruálunk önduális $(2^{2k}, 2^{2k-1}, 2^k)$-kódokat.

4.8. Tétel *Legyen $\mathcal{C}$ egy bináris kód, melyre*

$$\mathcal{RM}(k-1,2k) \subset \mathcal{C} \subset \mathcal{RM}(k,2k)$$

és a $\mathcal{C}/\mathcal{RM}(k-1,2k)$ faktortér egy következő bázisával

$$\left\{ \prod_{i=1}^{m} X_i^{k_i} + \mathcal{RM}(k-1,2k), \text{ ahol } k_i \in \{0,1\} \text{ és } \sum_{i=1}^{m} k_i = k \right\},$$

ahol a kitevőkből álló $(k_1,\ldots,k_m)$ m-esek halmaza egy maximális (tehát $2^{\frac{1}{2}\binom{2k}{k}}$ ele-mű) komplemens-mentes részhalmaza X-nek. Ekkor $\mathcal{C}$ egy duplán páros önduális $(2^{2k}, 2^{2k-1}, 2^k)$-kód.

A 4.9. Tételben bebizonyítjuk, hogy ha létezik olyan $i \in \{1,\ldots,m\}$, hogy $k_i = 0$ a maximális komplemens-mentes halmaz minden elemében, akkor a konstruált önduális $(2^{2k}, 2^{2k-1}, 2^k)$-kód két $\mathcal{RM}(k-1,2k-1)$ Reed-Muller kód direkt összege.

Monomiális kódokat bevezették [DL]-ben, és ezek a kódok ideálok, melyeket moduláris csoportalgebrák radikáljaiban lévő elemeknek megfelelő monomok generálnak. Mi elemi Abel p-csoport feletti monomiális kódokat vizsgálunk az ötödik fejezetben.

Egy lineáris kód minimális távolsága nagyon fontos - erősen befolyásolja a kód hibajavítóképességét. Általános esetben nehezebb a minimális távolságot meghatározni, mint Berman esetében, tehát ha a kód egy hatványa a csoportalgebra radikáljának. A legegyszerűbb eset az, amikor egy kód minimális távolságát meg lehet határozni egy bázisából, tehát ha létezik olyan elem a bázisban, melynek a súlya ugyanannyi mint a kód minimális távolsága. Mi olyan csoportkódokat keresünk, melyek

rendelkeznek ilyen bázissal.

5.6. Tétel *Legyen $C_{m,k}$ egy monomiális kód, melyet a következő halmaz generál:*

$$B_{m,k} = \{\prod (X_i)^{k_i} \mid \prod_{i=1}^{m} k_i \geq k, \text{ ahol } 0 \leq k_i < p,\ 0 < k \leq (p-1)^m\}.$$

Ekkor $B_{m,k}$ a $C_{m,k}$ egy látható bázisa.

5.8. Tétel *Legyen p tetszőleges prím. Legyenek $a_1, \ldots, a_m$ fix számok, melyekre $0 \leq a_i < p$ és legalább az egyik a_i nem nulla. Ekkor a következő $\mathcal{J}_{p,m}$-ben lévő főideál*

$$C_{a_1,\ldots,a_m} = \left(X_1^{a_1} X_2^{a_2} \ldots X_m^{a_m}\right)$$

határoz meg egy ciklikus kódot. A következő halmaz

$$B = \{\prod_{i=1}^{m} X_i^{k_i} | a_i \leq k_i < p,\ i = 1, 2, \ldots, m\}$$

a $C_{a_1,\ldots,a_m}$ kódnak egy látható bázisa.
Továbbá $C_{a_1,\ldots,a_m}$ egy $(p^m, (p-a_1)\cdot(p-a_2)\cdot\ldots\cdot(p-a_m), \delta)$-kód, ahol $\delta = \prod_{i=1}^{m}(a_i+1)$.

Az 5.6. Tétel bizonyításában teljes indukciót alkalmazunk a G elemi Abel csoport direkt faktorainak száma szerint.

Az 5.8. Tétel bizonyításához Ward [W2] eredményét kihasználjuk, hogy C előáll ciklikus kódok tenzorszorzataként.

Ezután az 5.6. Tétel-ben konstruált kódok automorfizmus csoportjait vizsgáljuk és a következő tételt bizonyítjuk be.

5.11. Tétel *Legyen $p = 2$ és m egy tetszőleges pozitív egész szám. Legyen $\mathcal{C}$ az 5.8. Tétel-ben definiált kód és legyen*

$$\mathcal{C} = (X_1 \cdots X_t),$$

ahol $1 \leq t \leq m$. A $\mathcal{C}$ dimenzióját λ-val jelöljük és δ-val a minimális távolságát. Ekkor $\mathcal{C}$ egy $(2^m, \lambda, \delta)-$kód, ahol $\lambda = 2^{m-t}$ és $\delta = 2^t$. Ekkor $\mathcal{C}$ automorfizmus csoportját felírhatjuk a következő szemidirekt szorzatként

$$Aut(\mathcal{C}) = S_\delta^\lambda \rtimes S_\lambda,$$

ahol S_δ^λ jelölje $\underbrace{S_\delta \times \ldots \times S_\delta}_{\lambda}$-t és S_i (ha $i = \delta, \lambda$) jelöli az i-edfokú szimmetrikus csoportot.

5.12. Megjegyzés *A koszorúszorzat definíciójából (lsd. [KK], vagy [Cam] Sec. 1.10) azt kapjuk, hogy $Aut(\mathcal{C}) = S_\delta \wr S_\lambda$.*

Az 5.11. Tétel bizonyítása elméleti. A $\mathcal{C}$ kód automorfizmus csoportja meghatározásához egy kombinatorikai módszert használunk, melyet Pless bevezetett [P2]-ben.

Bibliography

[AK] E. F. Assmus, Jr., J. D. Key, *Polynomial codes and finite geometries*, in Handbook of Coding Theory, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, 1269-1343

[AM] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Westview Press, 1994

[B] S. D. Berman, *On the theory of group codes*, Kibernetika **3** (1), 1967, 31-39.

[Cam] P. J. Cameron, *Permutation Groups*, Cambridge University Press, 1999

[C] P. Charpin, *Codes cycliques étendus et idéaux principaux d'une algébre modulaire*, C.R. Acad. Sci. Paris **295** (1), 1982, 313-315

[DGM] P. Delsarte, J. M. Goethals and F. J. MacWilliams, *On Generalized Reed-Muller Codes and Their Relatives*, Information and Control **16**, 1970, 403-442

[DKS] S. Dougherty, J.-L. Kim, P. Solé, *Open Problems in Coding Theory*, Contemporary Mathematics **634**, 2015, 79-99.

[DL] V. Drensky, P. Lakatos, *Monomial Ideals, Group Algebras and Error Correcting Codes*, Applied Algebra, Algebraic Algorithms

and Error-Correcting Codes, ed. T. Mora, Lecture Notes in Computer Science **357**, 1989, 181-188.

[F] A. Faldum, *Reed-Muller Codes are Optimal in the Class of the Radical Codes*, manuscript

[H] C. Hannusch, *On monomial codes in modular group algebras*, Discrete Mathematics **340** (5), 2017, 957-962

[HL1] C. Hannusch, P. Lakatos, *Construction of self-dual radical 2-codes of given distance*, Discrete Mathematics, Algorithms and Applications **4** (4), 2012, 1250052.

[HL2] C. Hannusch, P. Lakatos, *Construction of self-dual binary* $[2^{2k}, 2^{2k-1}, 2^k]$*-codes*, Algebra and Discrete Mathematics **21** (1), 2016, 59-68

[Jac] N. Jacobson, *The radical and semi-simplicity for arbitrary rings*, American Journal of Mathematics **67**, 1945, 300–320

[J] S. A. Jennings, *The structure of the group ring of a p-group over modular fields*, Trans. Amer. Math. Soc. **50**, 1947, 175-185.

[JK] D. Joyner, J. L. Kim, *Selected unsolved problems in Coding Theory*, Birkhäuser Verlag, 2011

[KLP1] T. Kasami, S. Lin, W. W. Peterson, *New Generalizations of the Reed-Muller Codes - Part I: Primitive Codes*, IEEE Trans. Information Theory **IT-14** (2), 1968, 189-199

[KLP2] T. Kasami, S. Lin, W. W. Peterson, Polynomial Codes, *IEEE Trans. Information Theory* **IT-14** (6), 1968, 807-814

[KK] M. Krasner, L. Kaloujnine, *Produit complet des groupes de permutations et le problème d'extension de groupes III*, Acta Sci. Math. Szeged **14**, 1951, 69-82

[LM] P. Landrock, O. Manz, *Classical codes as ideals in group algebras*, Designs, Codes and Cryptography **2** (3), 1992, 273-285

[M] F.J. MacWilliams, *Codes and Ideals in group algebras*, Univ. of North Carolina Press, 1969

[MR] D. Muller, I.S. Reed, *A Class of Multiple Error Correcting Codes and the Decoding Scheme*, MIT Lincoln Laboratory Report **44**, 1953

[MS] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science Publishers B.V., Eight impression, 1993

[MM] E. Martinez-Moro, H. Özadam, F. Özbudak, S. Szabo, *On a class of repeated-root monomial-like abelian codes*, J. Algebra Comb. Discrete Appl. **2** (2), 2015, 75-84

[P1] V. S. Pless, *An introduction to algebraic codes*, in Handbook of Coding Theory, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, 3-139

[P2] V. S. Pless, *A classification of self-orthogonal codes over GF(2)*, Discrete Mathematics **3**, 1972, 209-246

[PH] V. S. Pless, W. C. Huffman (editors), *Handbook of Coding Theory*, Elsevier, 1998

[R] I. S. Reed, *A brief history of the development of Error Correcting Codes*, Computers and Mathematics with Applications, **39**, 2000, 89-93

[S] C. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27**, 1948, 379-423 and 623-656

[W1] H. N. Ward, *Quadratic residue codes and divisibility*, in Handbook of Coding Theory, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, 827-870

[W2] H. N. Ward, *Visible codes*, Arch. Math. (Basel) **54** (3), 1990, 307-312

[Z] N. Zierler, *On a variation of the first-order Reed-Muller codes*, M.I.T. Lincoln Lab, Lexington, Mass., 1958, 34-80

Appendix

List of papers of the author

1. C. Hannusch, P. Lakatos, Construction of self-dual radical 2-codes of given distance, Discrete Mathematics, Algorithms and Applications 4 (2012), 1250052.

2. Z. Halasi, C. Hannusch, H. N. Nguyen, The largest character degrees of the symmetric and alternating groups, arXiv:1410.3055, Proc. Amer. Math. Soc. 144 (2016), 1947-1960

3. C. Hannusch, P. Lakatos, Construction of self-dual binary $[2^{2k}, 2^{2k-1}, 2^k]$-codes, Algebra and Discrete Mathematics Vol. 21 No. 1 (2016), 59-68

4. C. Hannusch, On monomial codes in modular group algebras, Discrete Mathematics Vol. 350 No. 5 (2017), 957-962

List of conference talks of the author

1. Visible codes in the radical of modular group algebras, Third Conference of PhD Students in Mathematics, 30th June - 2nd July 2014, Szeged

2. Bounds for the largest character degree of the symmetric and alternating groups, Groups and Topological Groups, 13th - 14th February 2015, Debrecen

3. On self-dual binary codes, Joint Austrian-Hungarian Mathematical Conference, 25th-27th August 2015, Győr

4. Construction of self-dual codes, Discrete Mathematics, Algebra and Their Applications, 14th-18th September 2015, Minsk, Belarus

5. On monomial group codes, Alfréd Rényi Institute of Mathematics, 23rd November 2015, Budapest

6. On the automorphism groups of some classes of binary codes, Groups and Topological Groups, 3rd - 4th February 2017, Budapest