Egyetemi doktori (PhD) értekezés tézisei

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

Hannusch Carolin

Témavezető: Dr. Lakatos Piroska

DEBRECENI EGYETEM
MATEMATIKA- ÉS SZÁMÍTÁSTUDOMÁNYOK DOKTORI ISKOLA

Debrecen, 2017

INTRODUCTION

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. If G is a finite abelian p-group, then $\mathbb{F}[G]$ is a modular group algebra and $\mathbb{F}[G]$ is a commutative ring of characteristic p. The Jacobson radical of such a group algebra is the unique maximal ideal. We will denote the Jacobson radical of $\mathbb{F}[G]$ by $\mathcal{J}(\mathbb{F}[G])$ or shortly by $\mathcal{J}$.

Our work is based on several classical results. In 1967, Berman [B] recognized that the binary Reed-Muller codes ($\mathcal{RM}$-codes) are ideals in the group algebra $\mathbb{F}_2[G]$, where G is an elementary abelian 2-group. Based on some properties of the Generalized Reed-Muller codes ($\mathcal{GRM}$-codes) discovered by Kasami et al. [KLP1] in 1968, Charpin [C] proved that a similar fact holds over $\mathbb{F}_p$.

Jennings [J] worked out the structure of the radical of a group algebra $\mathbb{F}[G]$. The relation between Jennings result and the results of Berman and Charpin was shown by Landrock and Manz [LM].

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. In this dissertation we construct and characterize linear codes which are ideals in the radical of the corresponding modular group algebras.

In Chapter 1 and Chapter 2 we introduce basic definitions and

properties of monomial codes and Reed-Muller codes, before we introduce our results in Chapter 3, Chapter 4 and Chapter 5.

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

- Hannusch, Lakatos [HL1]
- Hannusch, Lakatos [HL2]
- Hannusch [H].

We use the same numbering of theorems as in the dissertation.

SELF-DUAL CODES WITH GIVEN DISTANCE

Self-dual codes are a type of codes which is 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 $p = 2$. Drensky and Lakatos [DL] asked a question if for each possible minimum distance - which is always a power of 2 in this case - there exists an abelian group which defines a self-dual code with given distance. We give a positive answer to this question in the next theorem.

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 Theorem 3.2 is constructive and it is contained in Chapter 3 of the dissertation.

CONSTRUCTION OF SELF-DUAL $(2^{2k}, 2^{2k-1}, 2^k)$-CODES

In Chapter 4 we introduce new classes of binary abelian group codes which are self-dual. These codes are abelian group codes over elementary abelian 2-groups and they have similarly good parameters as the Reed-Muller codes. There exists a power of the radical defining a self-dual code if and only if the nilpotency index of the radical of the modular group algebra is even. If G is an elementary abelian 2-group of rank m, then the nilpotency index is even if and only if 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 $\mathbb{F}_2[G]$ if G is elementary abelian of even rank. We can give a positive answer to this question and we introduce a way to construct such codes. In order to describe the construction we need some definitions.

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.

The linear codes introduced in Chapter 4 and Chapter 5 are ideals in the radical of a group algebra $\mathbb{F}[G]$, where G is an elementary abelian p-group of rank m. For fix p and m, where $m \in \mathbb{N}$, 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

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

where $\mathbb{F}_p[x_1, x_2, \ldots, x_m]$ denotes the algebra of polynomials in m variables with coefficients in $\mathbb{F}_p$. We use the notation of $\mathscr{J}_{p,m}$ for the radical of $\mathscr{A}_{p,m}$.

With the notation $X_i = x_i - 1$ the following equation holds between $\mathcal{RM}$-codes and the powers of the radical:

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

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

$$x_1^{k_1} x_2^{k_2} \dots x_m^{k_m},\ k_i \in \{0,1\}.$$

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, i.e. codes defined by ideals of $\mathcal{J}_{2,m}$ which are generated by monomials of the X_i.

For $p = 2$ using the usual polynomial product in the monomial $X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}$ $(k_i \in \{0,1\})$ we have

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

Let $m = 2k$ and X be the set of all binary m-tuples with exactly k '0'-s and '1'-s. We denote by $\mathscr{X}$ the set of monomials corresponding to the set of exponents in X. Denote by $\mathscr{Y}$ the set with maximum number of pairwise orthogonal monomials in $\mathscr{X}$ and by Y their corresponding exponents in X.

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 $\mathcal{RM}(k-1,m-1)$.*

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

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

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.*

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* $\mathcal{Y}$*). Then we have the following isomorphism*

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

MONOMIAL GROUP CODES WITH VISIBLE BASES

In Chapter 5 we construct codes which are ideals in the radical of the modular group algebra $\mathcal{A}_{p,m}$. Let $\mathcal{C}$ be a monomial code generated by some monomials of the form

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

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 $\mathcal{C}$.

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

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 $\mathcal{C}_{m,k}$.

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

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

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 $\delta = \prod_{i=1}^{m}(a_i+1)$.

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 $k = m - 1$.*

In the last part of this dissertation we consider the codes defined in Theorem 5.8 for $p = 2$. We determine the automorphism groups of these binary codes. An automorphism of a linear code is a permutation of coordinates that stabilizes the code. 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.

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) it follows that* $Aut(C) = S_\delta \wr S_\lambda$.

BEVEZETÉS

Legyen p egy prímszám és $\mathbb{F}$ egy véges p karakterisztikájú test, i.e. $\mathbb{F} = GF(p^m)$ valamilyen m egész számra. A p elemű testet $\mathbb{F}_p$-vel jelöljük. Ha G véges Abel p-csoport, akkor az $\mathbb{F}[G]$ csoportalgebra moduláris, továbbá $\mathbb{F}[G]$ egy p karakterisztikájú kommutatív gyűrű. Egy ilyen csoportalgebra Jacobson-radikálja a csoportalgebra (egyetlen) maximális ideálja. A Jacobson radikált $\mathcal{J}(\mathbb{F}[G])$-vel vagy röviden $\mathcal{J}$-vel jelöljük.

Kutatásunk több klasszikus eredményen alapszik. Berman [B] mutatta meg 1967-ben, hogy a bináris Reed-Muller kódok ($\mathcal{RM}$-kódok) nevezetes ideálok (radikálhatványok) az $\mathbb{F}_2[G]$ csoportalgebrában, ahol G elemi Abel 2-csoport. 1968-ban Kasami et al. [KLP1] bevezette az Általánosított Reed-Muller kódokat ($\mathcal{GRM}$-kódok), amelyekre Charpin [C] hasonló kapcsolatot mutatott meg $\mathbb{F}_p$ felett.

Jennings [J] dolgozta ki az $\mathbb{F}[G]$ csoportalgebra radikáljának struktúráját. Később Landrock és Manz [LM] megmutatta a kapcsolatot Jennings eredménye és Berman és Charpin eredményei között.

A legtöbb eredményünk esetében $p = 2$, de a dolgozatban általános p-re vonatkozó állításokat is bizonyítunk. Esetünkben a G csoport mindig véges Abel p-csoport. Ebben a dolgozatban olyan lineáris kódokat konstruálunk és vizsgálunk, melyek ideálok a megfelelő moduláris csoportalgebra radikáljában. Továbbá vizsgáljuk ezen kódok tulajdonságait.

Az első és a második fejezetben monomiális kódok és Reed-Muller kódok definícióit és tulajdonságait vezetünk be. Eredményeinket bebizonyítjuk a harmadik, negyedik és ötödik fejezetben.

A dolgozatban szereplő eredmények megtalálhatók a következő publikációkban:

- Hannusch, Lakatos [HL1]
- Hannusch, Lakatos [HL2]
- Hannusch [H].

A tételek számozása ugyanaz mint a dolgozatban.

ADOTT TÁVOLSÁGÚ ÖNDUÁLIS KÓDOK

Az önduális kódok kombinatorikailag jól alkalmazhatók. Egy Abel p-csoport feletti moduláris csoportalgebra radikáljának valamely hatványa csak akkor lehet önduális kód, ha $p = 2$. Drensky és Lakatos ([DL]) tett fel egy kérdést azzal kapcsolatban, hogy minden lehetséges kódtávolsághoz konstruálható-e Abel csoport, mely adott távolságú önduális kódot határoz meg. Erre a kérdésre a következő pozitív választ adtuk:

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 $\jmath$ radikál-*

jának valamely hatványa egy önduális $(2^n, 2^{n-1}, 2^d)$*-kódot határoz meg.*

A tétel bizonyítása konstruktív. A bizonyítás a dolgozat harmadik fejezetében található.

ÖNDUÁLIS $(2^{2k}, 2^{2k-1}, 2^k)$-KÓDOK KONSTRUKCIÓJA

A disszertáció negyedik fejezetében új önduális bináris Abel csoportkód-osztályokat vezetünk be. Ezek a kódok Abel csoportkódok elemi Abel 2-csoportok felett, továbbá hasonlóan jó paraméterekkel rendelkeznek mint a Reed-Muller kódok. Egy moduláris csoportalgebra radikáljának pontosan akkor létezik olyan hatványa, mely önduális kód, ha a radikál nilpotencia indexe páros. Legyen G elemi Abel 2-csoport, melynek rangja m. Ekkor $\mathbb{F}_2[G]$ radikáljának nilpotencia indexe akkor és csak akkor páros, ha m páratlan. Tehát egy Reed-Muller kód önduális akkor és csak akkor ha egy $\mathcal{RM}(\frac{m-1}{2}, m)$-kód, i.e. m páratlan. Felmerül tehát a kérdés, hogy ha G rangja páros, akkor is létezik-e önduális kód az $\mathbb{F}_2[G]$ radikáljában. Erre a kérdésre pozitív választ adunk, miközben meg is adjuk az ilyen kódok konstrukcióját. A konstrukcióhoz néhány fogalomra van szükségünk.

4.1. Definíció *Legyen y egy bináris m-es. Azt mondjuk, hogy* $\mathbf{1} - y$ *az y komplemense, ahol* $\mathbf{1}$ *jelöli az* $\underbrace{(1, \ldots, 1)}_{m}$ *m*-est.

4.2. Definíció *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 halmaznak hívjuk.*

Azok a lineáris kódok, melyeket a negyedik és ötödik fejezetben bevezetünk ideálok egy $\mathbb{F}[G]$ moduláris csoportalgebrában, ahol G elemi Abel p-csoport, melynek rangja m. Rögzített m és p értékekre ($m \in \mathbb{N}$) az $\mathbb{F}_p[\underbrace{C_p \times \ldots \times C_p}_{m}]$ csoportalgebrát $\mathscr{A}_{p,m}$-mel jelöljük.

Legyen G elemi Abel csoport, és $\{g_1, g_2, \ldots g_m\}$ egy generátorrendszere. Tekintsük a következő leképezést $\mu : g_j \mapsto x_j$, ahol $1 \leq j \leq m$, ekkor megkapjuk a következő algebra izomorfizmust

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

ahol $\mathbb{F}_p[x_1, x_2, \ldots, x_m]$ jelölje az m változós, $\mathbb{F}_p$ együtthatós polinomok algebráját. $\mathscr{A}_{p,m}$ radikálját $\mathscr{J}_{p,m}$-mel jelöljük.

Továbbá jelöljük $X_i = x_i - 1$, ekkor a következő kapcsolat áll fenn $\mathcal{RM}$-kódok és a radikálhatványok között:

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

Tekintsük az

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

csoportalgebrát vektortérként, melynek egy bázisa

$$x_1^{k_1}x_2^{k_2}\dots x_m^{k_m},\ k_i \in \{0,1\}.$$

Az $X_i = x_i - 1 = x_i + 1$ monomok generálják a $\mathcal{J}_{2,m}$ radikált. Azok a kódok, melyeket mi tanulmányozunk, monomiális kódok.

Ha $p = 2$, akkor a szokásos polinomszorzást az $X_1^{k_1}X_2^{k_2}\dots X_m^{k_m}$ $(k_i \in \{0,1\})$ monomra alkalmazva azt kapjuk, hogy

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

Azon monomok halmazát, melyek kitevőiből álló $(k_1,\dots k_m)$ m-es X-ben van, $\mathscr{X}$-szel jelöljük. Azon monomok maximális halmazát $\mathscr{X}$-ben, melyek páronként ortogonálisak egymásra, $\mathscr{Y}$-nal jelöljük, és a megfelelő kitevők m-esekből álló halmazát X-ben Y-nal jelöljük.

4.6. Lemma *Ha m páros, és $m = 2k$, ekkor $\mathcal{RM}(k-1,m) = \mathcal{J}_{2,m}^{k+1}$ tartalmaz egy olyan altért, mely izomorf az $\mathcal{RM}(k-1,m-1)$ kóddal.*

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*

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

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

4.9. Tétel *Legyen* $\mathcal{C}$ *a Tétel 4.8-ban definiált kód. Tegyük fel, hogy* $k_i = 0$ *valamilyen* $i : 1 \leq i \leq m$*-re Y minden elemében (i.e. az* X_i *változó hiányzik minden monomból, ami* $\mathcal{Y}$*-ban van). Ekkor fennáll a következő izomorfizmus*

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

MONOMIÁLIS CSOPORTKÓDOK LÁTHATÓ BÁZISOKKAL

Az ötödik fejezetben olyan kódokat konstruálunk, melyek ideálok az $\mathscr{A}_{p,m}$ csoportalgebra radikáljában. Legyen $\mathcal{C}$ monomiális kód, azaz a

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

monomok egy részhalmaza által generált ideálnak megfelelő kód.

5.1. Definíció *Legyen $\mathcal{C}$ egy n hosszú lineáris kód $\mathbb{F}_p$ felett, azaz $\mathcal{C}$ tekinthető az $\mathbb{F}_p^n$ vektortér altereként. Azt mondjuk, hogy $\mathcal{C}$-nek egy bázisa látható bázis, ha a bázis elemei közül legalább egynek ugyanannyi a Hamming súlya, mint a $\mathcal{C}$ kódé.*

A továbbiakban monomiális kódokat konstruálunk az $\mathscr{A}_{p,m}$ csoportalgebrában, és mindegyiknek egy látható bázisát adjuk meg. Ezek a kódok ideálok a $\mathcal{J}_{p,m}$ radikálban.

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

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

Ekkor $B_{m,k}$ a $\mathcal{C}_{m,k}$ 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*

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

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 $\mathcal{C}_{a_1,\ldots,a_m}$ 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* $\delta=\prod_{i=1}^{m}(a_i+1)$.

5.10. Következmény *Legyen* $p=2$ *és* C *egy* $(2^m,2^k,2^d)$*-kód, melyet az 5.8. Tételben konstruáltunk, ahol* $0\leq k\leq m$. *Ekkor* C *mindig önortogonális és akkor és csak akkor önduális, ha* $k=m-1$.

A dolgozat utolsó részében azokat a kódokat tekintjük, melyeket az 5.8. Tételben konstruáltunk. Ezen kódok automorfizmus csoportjait határozzuk meg $p=2$ esetben. Egy lineáris kód automorfizmusa egy olyan permutáció a koordinátákon, mely stabilizálja a kódot. Egy C kód automorfizmusai csoportot alkotnak, és ezt a csoportot $Aut(C)$-vel jelöljük. Jelölje S_n az n-edfokú szimmetrikus csoportot. Ekkor jól ismert, hogy ha a C kód hossza ν, akkor $Aut(C)$ részcsoportja az S_ν-nek.

5.11. Tétel *Legyen* $p=2$ *és* m *egy tetszőleges pozitív egész szám. Legyen* C *az 5.8. Tételben definiált kód és legyen*

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

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

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

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

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

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

Registry number: DEENK/91/2017.PL
Subject: PhD Publikációs Lista

Candidate: Carolin Hannusch
Neptun ID: X4YY64
Doctoral School: Doctoral School of Mathematical and Computational Sciences
MTMT ID: 10036668

List of publications related to the dissertation

Foreign language scientific articles in international journals (3)

1. **Hannusch, C.**: On monomial codes in modular group algebras.
   Discret. Math. 340 (5), 957-962, 2017. ISSN: 0012-365X.
   DOI: http://dx.doi.org/10.1016/j.disc.2016.12.014
   IF: 0.6 (2015)

2. **Hannusch, C.**, Lakatos, P.: Construction of self-dual binary [2^(2k),2^(2k-1),2^k] -codes.
   Algebra Discrete Math. 21 (1), 59-68, 2016. ISSN: 1726-3255.

3. **Hannusch, C.**, Lakatos, P.: Construction of self-dual radical 2-codes of given distance.
   Discrete Math. Algorithm. Appl. 4 (4), 1250052-1-1250052-13, 2012. ISSN: 1793-8309.
   DOI: http://dx.doi.org/10.1142/S1793830912500528

List of other publications

Foreign language scientific articles in international journals (1)

4. Halasi, Z., **Hannusch, C.**, Nguyen, H. N.: The largest character degrees of the symmetric and alternating groups.
Proc. Amer. Math. Soc. 144 (5), 1947-1960, 2016. ISSN: 0002-9939.
DOI: http://dx.doi.org/10.1090/proc/12920
IF: 0.7 (2015)

Total IF of journals (all publications): 1,3
Total IF of journals (publications related to the dissertation): 0,6

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of Web of Science, Scopus and Journal Citation Report (Impact Factor) databases.

07 April, 2017

Nyilvántartási szám: DEENK/91/2017.PL
Tárgy: PhD Publikációs Lista

Jelölt: Hannusch, Carolin
Neptun kód: X4YY64
Doktori Iskola: Matematika- és Számítástudományok Doktori Iskola
MTMT azonosító: 10036668

A PhD értekezés alapjául szolgáló közlemények

Idegen nyelvű tudományos közlemények külföldi folyóiratban (3)

1. **Hannusch, C.**: On monomial codes in modular group algebras.
   Discret. Math. 340 (5), 957-962, 2017. ISSN: 0012-365X.
   DOI: http://dx.doi.org/10.1016/j.disc.2016.12.014
   IF: 0.6 (2015)

2. **Hannusch, C.**, Lakatos, P.: Construction of self-dual binary [2^(2k),2^(2k-1),2^k] -codes.
   Algebra Discrete Math. 21 (1), 59-68, 2016. ISSN: 1726-3255.

3. **Hannusch, C.**, Lakatos, P.: Construction of self-dual radical 2-codes of given distance.
   Discrete Math. Algorithm. Appl. 4 (4), 1250052-1-1250052-13, 2012. ISSN: 1793-8309.
   DOI: http://dx.doi.org/10.1142/S1793830912500528

További közlemények

Idegen nyelvű közlemények külföldi folyóiratban (1)

4. Halasi, Z., **Hannusch, C.**, Nguyen, H. N.: The largest character degrees of the symmetric and alternating groups.
Proc. Amer. Math. Soc. 144 (5), 1947-1960, 2016. ISSN: 0002-9939.
DOI: http://dx.doi.org/10.1090/proc/12920
IF: 0.7 (2015)

A közlő folyóiratok összesített impakt faktora: 1,3
A közlő folyóiratok összesített impakt faktora (az értekezés alapjául szolgáló közleményekre): 0,6

A DEENK a Jelölt által az iDEa Tudóstérbe feltöltött adatok bibliográfiai és tudománymetriai ellenőrzését a tudományos adatbázisok és a Journal Citation Reports Impact Factor lista alapján elvégezte.

Debrecen, 2017.04.07.