On monomial codes in modular group algebras

Carolin Hannusch[1]

Institute of Mathematics, University of Debrecen, Hungary

Abstract

Let p be a prime number and K be the finite field of p elements, i.e. $K = GF(p)$. Further let G be an elementary abelian p-group of order p^m. Then the group algebra $K[G]$ is modular. We consider $K[G]$ as an ambient space and the ideals of $K[G]$ as linear codes. A basis of a linear space is called visible, if there exists a member of the basis with the minimum (Hamming) weight of the space. The group algebra approach enables us to find some linear codes with a visible basis in the Jacobson radical of $K[G]$. These codes can be generated by "monomials" [3]. For $p > 2$, some of our monomial codes have better parameters than the Generalized Reed-Muller codes. In the last part of the paper we determine the automorphism groups of some of the introduced codes.

Keywords: Error-correcting codes, modular group algebras, monomial codes, automorphism group

2010 MSC: 94B05, 11T71, 20C05, 20B25

1. Introduction and Notation

Reed-Muller codes were introduced as binary functions in [9]. Later the Generalized Reed-Muller (GRM) codes were defined over an arbitrary finite field by Kasami, Lin and Peterson in [6]. We will denote a cyclic group of p elements by C_p and C_p^m is the direct product of m copies of C_p. The radical of $K[C_p^m]$ is denoted by $J_{p,m}$. It turned out that the powers of $J_{p,m}$ coincide with the GRM-codes (see [1] for $p = 2$ and [2] for arbitrary p). Landrock and Manz [7] showed that GRM-codes are ideals in modular

Email address: `carolin.hannusch@science.unideb.hu` (Carolin Hannusch)

[1]The author was partially supported by the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202.

group algebras. In the current paper, we give some new classes of monomial codes which are ideals in modular group algebras but differ from the GRM-codes. If $p > 2$, then some of our codes have better parameters than the GRM-codes. All of the introduced codes have a visible basis, i.e. their minimum distance can be obtained by the minimum distance of such a basis.

This paper is organized as follows. In this section we summarize the algebraic concepts and introduce our notations. In Section 2 we construct monomial codes which have at least one visible basis and in Section 3 we determine the automorphism groups of some of the codes given previously for $p = 2$.

Throughout the paper p will denote a prime number and $K = GF(p)$ denotes the Galois-field of p elements. Further let G be an elementary abelian p-group of order p^m for some positive integer m. Thus the group algebra $K[G]$ is modular.

Let $n = p^m$ and $g_1, g_2, \ldots, g_n$ be a basis of $K[G]$. The elements of $K[G]$ are the formal sums

$$\sum_{i=1}^{n} \alpha_i g_i, \text{ where } \alpha_i \in K.$$

We use the usual operations in $K[G]$ (see [1] for more details).

The Jacobson radical of $K[G]$ is the kernel of the augmentation map $\sum_{i=1}^{n} \alpha_i g_i \mapsto \sum_{i=1}^{n} \alpha_i$. It is obvious that this map is an algebra homomorphism. We will refer to the Jacobson radical shortly as radical. Since $K[G]$ is local, its radical is unique.

Between $K[G]$ and K^n there exists a map

$$\varphi \colon K[G] \to K^n$$

such that

$$\varphi\left(\sum_{i=1}^{n} \alpha_i g_i\right) = (\alpha_1, \alpha_2, \ldots, \alpha_n) =: \mathbf{c}.$$

It can be easily verified that this map is an isomorphism, thus $K[G]$ and K^n are isomorphic as vector spaces. The ambient space of the linear codes we consider in this paper is $\varphi(K[G])$. The Hamming weight of codes in $J_{p,m}$ can be obtained from the basis formed by the elements of G i.e. the Hamming weight is the number of nonzero α_i's in $\mathbf{c}$.

Given a basis $g_{i_1}, g_{i_2}, \dots g_{i_m}$, $(1 \leq i_j \leq p^m, 1 \leq j \leq m)$ of the elementary abelian p-group G, we can consider the algebra isomorphism

$$\mu \colon K[G] \to K[x_1, \dots x_m]/\langle x_1^p - 1, \dots x_m^p - 1 \rangle, \text{ with } g_{i_j} \mapsto x_j.$$

Applying μ we may write any element $g_i \in G$ as

$$g_i = g_{i_1}^{a_1} g_{i_2}^{a_2} \dots g_{i_m}^{a_m} = x_1^{a_1} x_2^{a_2} \dots x_m^{a_m},\ 0 \leq a_j < p,$$

thus we obtain

$$K[G] \cong K[x_1, x_2, \dots, x_m]/\langle x_1^p - 1, x_2^p - 1, \dots x_m^p - 1 \rangle, \tag{1.1}$$

where $K[x_1, x_2, \dots, x_m]$ denotes the algebra of polynomials in m variables with coefficients in K.

The following set of monomial functions

$$\left\{ \prod_{i=1}^{m} (x_i - 1)^{a_i}, \text{ where } 0 \leq a_i \leq p-1 \text{ and } \sum_{i=1}^{m} a_i \geq 1 \right\}$$

forms a linear basis of the radical $J_{p,m}$ due to (1.1) (see [5] for more details).

Now we define $X_i := x_i - 1$, where $i = 1, \dots, m$. Then we have

$$K[G] \cong K[X_1, X_2, \dots, X_m]/\langle X_1^p, X_2^p, \dots X_m^p \rangle. \tag{1.2}$$

For $k \in \{0, \dots, m(p-1)\}$ the k-th power of the radical $J_{p,m}$ is defined as

$$J_{p,m}^k = \langle \prod_{i=1}^{m} (X_i)^{a_i} \mid \sum_{i=1}^{m} a_i \geq k\ , 0 \leq a_i \leq p-1 \rangle. \tag{1.3}$$

It is well-known that $J_{p,m}^k = \mathrm{GRM}(m(p-1) - k, m)$.

One can choose coset representations of $J_{p,m}^k / J_{p,m}^{k+1}$ of the form:

$$\left\{ \prod_{i=1}^{m} X_i^{a_i}, \text{ where } 0 \leq a_i \leq p-1 \text{ and } \sum_{i=1}^{m} a_i = k \right\}. \tag{1.4}$$

2. Monomial codes with visible bases

Definition 1 ([3]). *Let C be an ideal of $K[G]$ and a subspace of $J_{p,m}$. We say that C is a monomial code if it can be generated by some monomials of the form*

$$X_1^{a_1} X_2^{a_2} \dots X_m^{a_m}, \textit{ where } 0 \leq a_i \leq p-1, \textit{ and } i = 1, \dots, m.$$

Definition 2. *Let C be a linear code of length n over $K = GF(p)$, i.e. we consider C as a subspace of the vector space K^n. We say that C has a visible basis if at least one member of the basis has the same Hamming weight as C has. Further C will be denoted as an $[n,k,d]$-code, where n is the code length, k is its dimension and d is its minimum (Hamming) weight.*

It is known (Prop. 1.8 in [3]) that for $p = 2$ every monomial code has a visible basis.

Remark 1. *This definition of codes with visible bases is different from the definition of visible codes by Ward in [11]. He defined a set V to be 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.*

We construct monomial codes with at least one visible basis. The next theorem is a special case of Corollary 3.3 in [8].

Theorem 1. *Let p be an arbitrary prime. Then the principal ideal*

$$C = \langle X_1^{a_1} X_2^{a_2} \dots X_m^{a_m} \mid 0 \le a_i \le p-1 \ , \ \sum_{i=1}^{m} a_i \ge 1 \ , \ i = 1,2,\dots,m \rangle$$

determines a cyclic code. The set

$$B = \left\{ \prod_{i=1}^{m} X_i^{k_i} \mid a_i \le k_i \le p-1 \right\}$$

is a visible basis of C.
We have $C \subseteq J_{p,m}$ and C is a $[p^m, (p-a_1)\cdot(p-a_2)\cdot \dots \cdot (p-a_m), d]$-code, where $d = \prod_{i=1}^{m}(a_i+1)$.

Proof. Let C_{x_j} denote the ideal $\langle X_j^{a_j} \rangle = \langle (x_j-1)^{a_j} \rangle$ in the ring $K[x_j]/(x_j^p - 1)$ for $1 \le j \le m$. Then C is a tensor product $C \cong C_{X_1} \otimes C_{X_2} \otimes \dots \otimes C_{X_m}$ (Cor. 3.3 in [8]), where $C_{X_j} = \langle X_j^{a_j} \rangle$ ($1 \le j \le m$) is a cyclic code. Each code C_{X_j} has a visible basis, which is the set

$$\{X_j^{k_j} \mid a_j \le k_i \le p-1\}$$

with minimal distance $a_j + 1$. By the theorem of Ward [11], the tensor product C is visible. Thus, it has a visible basis. □

Remark 2. *The codes defined in Theorem 1 coincide with the GRM-codes only in the one-dimensional case, since*

$$C \cong J^k \Leftrightarrow k = m(p-1) \text{ and } C = \langle \prod X_i^{a_i} \mid a_i = p-1 \ \forall i \rangle.$$

The class of *maximal monomial codes* I_d in the group algebra $K[G]$ was defined by Drensky and Lakatos in [3] as

$$I_d = \langle \prod_{i=1}^{m} X_i^{a_i} \mid \prod_{i=1}^{m} (a_i+1) \geq d, 0 \leq a_i \leq p-1 \rangle.$$

The minimum distance of I_d is $d = \min\{\prod_{i=1}^{m}(a_i+1)\}$. Thus I_d has a visible basis.

For $p > 2$ some of the maximal monomial codes are better than the GRM-codes with the same minimum distance. For example if $d = 5$, then $\dim(I_d) = \dim(\mathrm{GRM}) + \binom{m}{2} + \binom{m}{3} + m(m-1)$.

Theorem 2. *Let $C_{m,k}$ be a monomial code generated by the set*

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

Then $B_{m,k}$ is a visible basis of $C_{m,k}$.

Proof.

The proof is similar to the proof of Lemma 1.9 in [1]. We use induction on the numbers of direct factors in the elementary abelian group G.

For $m = 1$ the statement follows from Theorem 1.1 in [1]. Suppose that the statement is true for $m = i$ and we prove it for the case $m = i+1$.

Let

$$\mathbf{x} = \sum_{a_1,\ldots,a_m} \lambda_{a_1,\ldots,a_m} (x_1-1)^{a_1} \cdots (x_m-1)^{a_m}, \tag{2.1}$$

where $\lambda_{a_1,\ldots,a_m} \in K$. If each $\lambda_{a_j} = 0$ or $a_j = 0$ for all $j \in \{1,\ldots,m\}$, then Theorem 2 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

$$\mathbf{x} = (x_m-1)^{l_m}(L_{l_m} + L_{l_m+1}(x_m-1) + L_{l_m+2}(x_m-1)^2 + \ldots L_{l_m+t}(x_m-1)^t), \tag{2.2}$$

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

$$L_{l_m} = \sum_{j_1, j_2, \ldots, j_{m-1}} \gamma_{j_1, j_2, \ldots, j_{m-1}} (x_1 - 1)^{j_1} \ldots (x_{m-1} - 1)^{j_{m-1}} \neq 0 \,, (1 \leq j_i \leq p-1). \quad (2.3)$$

Then we have

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

for each term in the equation of the right hand side of (2.3). By the induction hypothesis there exists a basis element $(x_1 - 1)^{a_1} \ldots (x_{m-1} - 1)^{a_{m-1}}$ in $C_{m-1, \frac{k}{l_m}}$ such that

$$d_m = wt((x_1 - 1)^{a_1} (x_2 - 1)^{a_2} \ldots (x_{m-1} - 1)^{a_{m-1}}) \leq wt(L_{i_m}),$$

where $wt(y)$ denotes the Hamming weight of the codeword $y \in C_{m,k}$. Express L_{l_m} in the monomial basis of $K[H]$, i.e.

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

Thus for the element $\mathbf{x}$ in (2.2) we have

$$\mathbf{x} = (x_m - 1)^{l_m} \left(\sum_{i_1, i_2, \ldots, i_{m-1}} \mu_{i_1, i_2, \ldots, i_{m-1}} + \mu^{(1)}_{i_1, i_2, \ldots, i_{m-1}} (x_m - 1) + \cdots + \mu^{(t)}_{i_1, i_2, \ldots, i_{m-1}} (x_m - 1)^t \right) \cdot$$

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

where $\Gamma_{i_1, i_2, \ldots, i_{m-1}} \in K[H_m]$ and $H_m = \langle x_m \rangle$. By Theorem 1.1 of Berman [1], there exists an element $(x_m - 1)^r$ such that $r \geq l_m$ and

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

It follows that

$$wt(\mathbf{x}) \geq d_m wt(x_m - 1)^r = wt\left((x_m - 1)^r (x_1 - 1)^{a_1} (x_2 - 1)^{a_2} \ldots (x_{m-1} - 1)^{a_{m-1}}\right),$$

while

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

This completes the proof. $\square$

Remark 3. *Let $P_m^{r_1,\ldots,r_i}$ denotes the number of permutations on m elements with $r_1,\ldots,r_i$ repititions. If $k = l_1 \cdots l_m$, then*

$$\dim(C_{m,k}) = \sum_{\substack{l_i \le p-1 \\ l_1 \cdots l_m \ge k}} P_m^{r_1,\ldots,r_i}.$$

3. Automorphism groups in the binary case

In this section we will consider the codes C defined in Theorem 1 for $p = 2$. We will determine their automorphism groups by using a combinatorial method which was introduced in [10]. Let G_C denote a generator matrix of C and S_n the symmetric group on n elements. It is well-known that if the length of C is n, then $Aut(C) \le S_n$.

Theorem 3. *Let $p = 2$ and m be an arbitrary positive integer. Let C be the code defined in Theorem 1 and*

$$C = \langle X_1 \cdots X_t \rangle,$$

where $1 \le t \le m$. Then C is a $[2^m, \lambda, d]$-code, where $\lambda = 2^{m-t}$ and $d = 2^t$. Then the automorphism group of C can be written as the semidirect product

$$Aut(C) = S_d^{\lambda} \rtimes S_{\lambda}.$$

Proof. Since C is an ideal in $GF(2)[G]$, we can use the identity

$$x_j(x_i - 1) = (x_j - 1)(x_i - 1) + (x_i - 1) = X_j X_i + X_i.$$

We use the basis B of the code C, which was also introduced in Theorem 1:

$$B = \{X_1X_2\ldots X_t, X_1X_2\ldots X_tX_{t+1}, X_1X_2\ldots X_tX_{t+2}, \ldots, X_1X_2\ldots X_tX_{t+1}X_{t+2}\ldots X_{m-2}X_{m-1}X_m\}.$$

Let $x_1,\ldots,x_m$ be a basis of the elementary abelian 2-group G. We construct a generator matrix G_C according to the basis B in lexicographical order, which means that for $b_i, c_i \in \{0,1\}$ and $1 \le i \le m$ we have

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

Keeping in mind that $X_i = x_i - 1$, we can write G_C as the following binary matrix.

$$G_C = \begin{pmatrix}
1\;1\;1\;1\;\dots\;1 & 0\;\dots\;0 & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 1\;\dots\;1 & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 0\;\dots\;0 & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 1\;\dots\;1 & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
 & \vdots & & & & & & & \\
1\;1\;1\;1\;\dots\;1 & 0\;\dots\;0 & 0\;\dots\;0 & \cdots & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 1\;\dots\;1 & 0\;\dots\;0 & \cdots & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 0\;\dots\;0 & 1\;\dots\;1 & \cdots & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
1\;1\;1\;1\;\dots\;1 & 1\;\dots\;1 & 1\;\dots\;1 & \cdots & 1\;\dots\;1 & \cdots & 0\;\dots\;0 & 0\;\dots\;0 & 0\;\dots\;0 \\
 & \vdots & & & & & & & \\
1\;1\;1\;1\;\dots\;1 & 1\;\dots\;1 & 1\;\dots\;1 & \cdots & 1\;\dots\;1 & \cdots & 1\;\dots\;1 & 0\;\dots\;0 & 1\;\dots\;1 \\
\underbrace{1\;1\;1\;1\;\dots\;1}_{d} & \underbrace{1\;\dots\;1}_{d} & \underbrace{1\;\dots\;1}_{d} & \cdots & \underbrace{1\;\dots\;1}_{d} & \cdots & \underbrace{1\;\dots\;1}_{d} & \underbrace{1\;\dots\;1}_{d} & \underbrace{1\;\dots\;1}_{d}
\end{pmatrix}$$

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 G_C is the tensor product of $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and A.

We can see that in G_C there is one row of weight $d = 2^t$, 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 G_C has 2^{m-t} rows.

Each row of G_C can be divided into d-tuples of 1-s and 0-s. The coordinates of each of the d-tuples can be permuted by S_d and it is easy to verify that the number of d-tuples in one row is $\lambda = 2^{m-t}$. Furthermore, the d-tuples can be permuted as d-tuples by all elements of S_λ.

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

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

which means that $\sigma_i^{-1} g_i \sigma_i \in S_d$ and σ_μ acts on the elements of $\{\sigma_1^{-1} g_1 \sigma_1, \dots, \sigma_\lambda^{-1} g_\lambda \sigma_\lambda\}$ as permutation. Thus $\sigma^{-1} g \sigma \in S_d^\lambda$.

We also show that S_λ is in general not normal in $Aut(C)$. Let $h \in S_\lambda$ and we take again $\sigma \in Aut(C)$ as previously. Further we will denote the d-tuples by $a_1, \dots a_\lambda$. Then

$$\sigma^{-1} h \sigma = (\sigma_1^{-1} a_1 \sigma_1, \dots, \sigma_\lambda^{-1} a_\lambda \sigma_\lambda)^{\sigma_\mu},$$

which means that σ_μ permutes the $\sigma_i^{-1}a_i\sigma_i$. Since $\sigma_i^{-1}a_i\sigma_i \neq a_i$ in general, this element cannot always be expressed as a permutation of $a_1,\ldots,a_\lambda$. Since S_d^λ and S_λ are both subgroups of $Aut(C)$, we have that the group $Aut(C)$ is an outer semidirect product of S_d^λ and S_λ.

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

Definition 3. *Let C be a monomial code in $K[G]$ and $c_1, c_2 \in C$ be two codewords. We say that c_1 is orthogonal to c_2 if their inner product is zero. The dual code of C is denoted by $C^\perp$ and it is the code containing all codewords which are orthogonal to all codewords of C. We say that C is self-orthogonal if $C \subseteq C^\perp$ and C is self-dual if $C = C^\perp$.*

Corollary 4. *Let $p = 2$ and C be a $[2^m, 2^k, d]$-code defined in Theorem 1, where $0 \leq k \leq m$. Then C is always self-orthogonal and it is self-dual if and only if $k = m-1$.*

Proof.

It is obvious by the construction of the generator matrix G_C in the proof of Theorem 3 that the difference of two arbitrary codewords has even weight. Thus all codewords are orthogonal to each other. In the example of page 4 in [4] it is shown that if $k = m-1$, then C is self-dual and it is a direct sum of $[2,1,2]$-codes. Further, the dimension of C implies self-duality if and only if $k = m-1$. □

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

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

[3] Drensky, V., Lakatos, P., *Monomial ideals, group algebras and error correcting codes,* Lecture Notes in Computer Science, Springer Verlag, **357,** 181–188, (1989)

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

[5] Jennings, S. A., *The structure of the group ring of a p-group over modular fields,* Trans. Amer. Math. Soc. **50,** 175–185, (1941)

[6] Kasami, T., Lin, S., Peterson, W.W., *New generalisations of the Reed-Muller codes,* IEEE Trans. Inform. Theory II-**14,** 189–199, (1968)

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

[8] Martinez-Moro, E., Ozadam, H., Ozbudak, F., Szabo, S., *On a class of repeated-root monomial-like abelian codes,* Journal of Algebra, Combinatorics, Discrete Structures and Applications **2** (2), (2015)

[9] Muller, D. E., *Application of boolean algebra to switching circuit design and to error detection* IRE Transactions on Electronic Computers, **3**, 6-12, (1954)

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

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