

## Construction of self-dual binary [ $2^{2k}, 2^{2k-1}, 2^k$ ]-codes

Carolin Hannusch\* and Piroska Lakatos

Communicated by V. I. Sushchansky

**ABSTRACT.** The binary Reed-Muller code  $\text{RM}(m - k, m)$  corresponds to the  $k$ -th power of the radical of  $GF(2)[G]$ , where  $G$  is an elementary abelian group of order  $2^m$  (see [2]). Self-dual RM-codes (i.e. some powers of the radical of the previously mentioned group algebra) exist only for odd  $m$ .

The group algebra approach enables us to find a self-dual code for even  $m = 2k$  in the radical of the previously mentioned group algebra with similarly good parameters as the self-dual RM codes.

In the group algebra

$$GF(2)[G] \cong GF(2)[x_1, x_2, \dots, x_m]/(x_1^2 - 1, x_2^2 - 1, \dots, x_m^2 - 1)$$

we construct self-dual binary  $C = [2^{2k}, 2^{2k-1}, 2^k]$  codes with property

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

for an arbitrary integer  $k$ .

In some cases these codes can be obtained as the direct product of two copies of  $\text{RM}(k - 1, k)$ -codes. For  $k \geq 2$  the codes constructed are doubly even and for  $k = 2$  we get two non-isomorphic  $[16, 8, 4]$ -codes. If  $k > 2$  we have some self-dual codes with good parameters which have not been described yet.

---

\*Research of the first author was partially supported by funding of EU's FP7/2007-2013 grant No. 318202.

**2010 MSC:** 94B05, 11T71, 20C05.

**Key words and phrases:** Reed–Muller code, Generalized Reed–Muller code, radical, self-dual code, group algebra, Jacobson radical.

## Introduction and Notation

Let  $K$  be a finite field of characteristic  $p$  and let  $V$  be a vector space over  $K$ , and  $C$  be a subspace of  $V$ . Then  $C$  is called a *linear code*. Let  $x, y \in C$ , then the Hamming weight of  $x$  is the number of its non-zero coordinates and the *Hamming distance* of  $x$  and  $y$  is the weight of  $x - y$ . The Hamming distance (or weight) of a linear code  $C$  is the minimum of all Hamming distances of its codewords.

In the study of binary codes  $C \subseteq V$  it is convenient that the space  $V$  has an additional algebraic structure. For example, if  $V$  is a group algebra  $K[G]$ , where  $G$  is a finite abelian  $p$ -group and  $C$  is an ideal of such a group algebra, then  $C$  is called an *abelian group code*.

The Hamming distance of a linear code determines the ability of error-correcting property of the code. The authors in [6] proved that for any  $1 \leq d \leq \left\lfloor \frac{m+1}{2} \right\rfloor$  there exists an Abelian 2-group  $G_d$  that a power of the radical is a self-dual code with parameters  $(2^m, 2^{m-1}, 2^d)$ . These codes are ideals in the group algebra  $GF(2)[G_d]$  and they are “monomial codes” in the sense of [5] as defined below.

Throughout,  $p$  will denote a prime and  $K$  a field of  $p$  elements. Let  $G = \langle g_1 \rangle \times \cdots \times \langle g_m \rangle \cong C_p^m$  be an elementary abelian  $p$ -group of order  $p^m$  i.e.  $K[G]$  is a modular group algebra, then the group algebra  $K[G]$  and  $K^n$  are isomorphic as vector spaces by the mapping

$$\varphi : K[G] \mapsto K^n, \text{ where } \varphi \left( \sum_{i=1}^n a_i g_i \right) \mapsto (a_1, a_2, \dots, a_n) := \mathbf{c} \in C.$$

Reed-Muller (RM) binary codes were introduced in [12] as binary functions. These codes are frequently used in applications and have good error correcting properties. Now we are looking for self-dual codes in the radical of  $K[G]$  with similarly good parameters as the RM codes.

If  $K$  is a field of characteristic 2 Berman [2] and in the general case Charpin [3] proved that all Generalized Reed-Muller (GRM) codes coincide with powers of the radical of the modular group algebra of  $K[G]$ , where  $G$  is an elementary abelian  $p$ -group. This group algebra is clearly isomorphic with the quotient algebra

$$GF(p)[x_1, x_2, \dots, x_m] / (x_1^p - 1, \dots, x_m^p - 1).$$

Self-dual RM-codes (i.e. some power of the radical of the group algebra  $GF(2)[G]$ ) exist only for odd  $m$ . They are  $(2^m, 2^{m-1}, 2^{\frac{m+1}{2}})$ -codes.

For any basis  $\{g_1, g_2, \dots, g_m\}$  of such a group  $G$  consider the algebra isomorphism  $\mu$  mapping  $g_j \mapsto x_j$  ( $1 \leq j \leq m$ ), and therefore we have the algebra isomorphism

$$\mathcal{A}_{p,m} \cong GF(p)[x_1, x_2, \dots, x_m]/(x_1^p - 1, x_2^p - 1, \dots, x_m^p - 1),$$

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

It is known ([7]) that the set of monomial functions ( $k_i \in \mathbb{N} \cup 0$ )

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

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

Introducing the notation

$$X_i = x_i - 1, \quad (1 \leq i \leq m)$$

(which will be used from now on) we have the following isomorphism

$$\mathcal{J}_{p,m} \simeq GF(p)[X_1, X_2, \dots, X_m]/(X_1^p, X_2^p, \dots, X_m^p). \quad (1)$$

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

$$\mathcal{J}_{p,m}^k = \text{GRM}(t - 1 - k, m) = \langle \prod_{i=1}^m (X_i)^{k_i} \mid \sum_{i=1}^m k_i \geq k \ (0 \leq k_i < p) \rangle. \quad (2)$$

Such a basis was exploited by Jennings [7].

By (2) the quotient space  $\mathcal{J}_{p,m}^k / \mathcal{J}_{p,m}^{k+1}$  has a basis

$$\left\{ \prod_{i=1}^m X_i^{k_i} + \mathcal{J}_{p,m}^{k+1}, \text{ where } 0 \leq k_i < p \text{ and } \sum_{i=1}^m k_i = k \right\}. \quad (3)$$

**Remark 1.** It is known [15] that the dual code  $C^\perp$  of an ideal  $C$  in  $\mathcal{A}_{p,m}$  coincides with the annihilator of  $C^*$ , where  $C^*$  is the image of  $C$  by the involution  $*$  defined on  $\mathcal{A}_{p,m}$  by

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

The annihilator of  $\mathcal{J}_{p,m}^k$  is obviously  $\mathcal{J}_{p,m}^{m(p-1)+1-k}$ . Thus the dual codes of GRM-codes are GRM-codes and

$$\text{GRM}(k, m)^\perp = \text{GRM}(m(p - 1) - k - 1, m).$$

It follows that for  $m = 2k + 1$  and  $p = 2$  the code  $\text{GRM}(k, m)$  is self-dual.

## 1. Construction of binary self-dual codes

Let us consider the group algebra

$$\mathcal{A}_{2,m} = GF(2)[x_1, \dots, x_m]/(x_1^2 - 1, x_2^2 - 1, \dots, x_m^2 - 1) \simeq GF(2)[C_2^m]$$

as a vector space with basis

$$x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}, \quad a_i \in \{0, 1\}. \quad (4)$$

It is known ([7]) that the radical  $\mathcal{J}_{2,m}$  of this group algebra is generated by the monomials  $X_i = x_i - 1 = x_i + 1$ .

**Definition 1** ([5]). The code  $C$  in  $\mathcal{J}_{2,m}$  (see (1)) is said to be a *monomial code* if it is an ideal in  $\mathcal{A}_{2,m}$  generated by some monomials of the form

$$X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}, \quad \text{where } 0 \leq k_i \leq 1 \quad (5)$$

The codes we intend to study are monomial codes.

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

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

and the Hamming weight in the basis (4) of this monomial equals  $\prod_{i=1}^m (1 + k_i)$ .

**Example.** Let  $G$  be an elementary abelian group of order  $2^m$ ,  $m \geq 2$ . Define the codes  $C_j$  as ideals in  $K[G]$  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  $C_j = C_j^\perp = \langle X_j \rangle$ . Further, this code is a direct sum of  $[2, 1, 2]$ -codes. The dimension of the code  $C_j$  is  $2^{m-1}$ , the same as the dimension of the radical of the group algebra  $GF(2)[H]$ , where  $H$  is an elementary abelian 2-group of rank  $m - 1$ . The minimal distance of  $C_j$  is  $d = 2$ . This follows from the fact that the element  $X_j = x_j + 1$  is included in the basis of  $C_j$ . Thus,  $C_j$  is a self-dual  $[2^m, 2^{m-1}, 2]$ -code.

By Remark 1 one can see that a power of the radical of a modular group algebra is self-dual if and only if the nilpotency index of the radical is even. In our case (when  $G$  is elementary abelian of order  $p^m$ ) the nilpotency index is even if and only if  $p = 2$  and  $m$  is odd.

If  $m$  is odd, the binary RM-codes with parameters  $[2^m, 2^{m-1}, 2^{\frac{m+1}{2}}]$  are self-dual and they are the  $\frac{m+1}{2}$ -th powers of the radical  $\mathcal{A}_{2,m}$ .

For  $m = 2k$  where  $k$  is an arbitrary integer, we have a new method to construct a doubly-even class of binary self-dual  $C$  codes with parameters  $[2^m, 2^{m-1}, 2^k]$ . For this code  $C$  we have  $\text{RM}(k-1, 2k) \subset C \subset \text{RM}(k, 2k)$ . In the case of  $m = 4$ , we get two known extremal  $[16, 8, 4]$  codes (listed in [14]) 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  $d = 4 \lfloor \frac{n}{24} \rfloor + 4$ , where  $n$  denotes the code length (see Definition 39 and Lemma 40 in [8]).

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

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

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

*Proof.* Recall, that the set of monomials in the basis (2) 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) is invariant under the permutation 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  $\mathcal{J}_{2,m-1}^k \cong \text{RM}(k-1, m-1)$ .  $\square$

For  $m = 2k$  denote the set of all  $k$ -subsets of  $\{1, 2, \dots, 2k\}$  by  $X$ . The elements of  $X$  can be described by binary sequences  $(k_1, k_2, \dots, k_m)$  consisting of  $k$  '0'-s and  $k$  '1'-s in any order. Clearly, the cardinality of the set  $X$  is  $\binom{2k}{k}$ .

We say that the subset  $Y$  of binary  $m$ -tuples in  $X$  is *complement free* if  $y \in Y$  implies  $\mathbf{1} - y \notin Y$ , where  $\mathbf{1} = (1, 1, \dots, 1)$ . Denote the set of monomials corresponding to the set of exponents in  $X$  by  $\mathcal{X}$ . Denote the set with maximum number of pairwise orthogonal monomials in  $\mathcal{X}$  by  $\mathcal{Y}$  and their corresponding exponents in  $X$  by  $Y$ .

**Example.** For  $m = 6$  the quotient space  $\mathcal{J}_{2,m}^3 / \mathcal{J}_{2,m}^4$  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:

$(1, 1, 1, 0, 0, 0)$	$(0, 0, 0, 1, 1, 1)$
$(1, 1, 0, 1, 0, 0)$	$(0, 0, 1, 0, 1, 1)$
$(1, 1, 0, 0, 1, 0)$	$(0, 0, 1, 1, 0, 1)$
$(1, 1, 0, 0, 0, 1)$	$(0, 0, 1, 1, 1, 0)$
$(1, 0, 1, 1, 0, 0)$	$(0, 1, 0, 0, 1, 1)$
$(1, 0, 1, 0, 1, 0)$	$(0, 1, 0, 1, 0, 1)$
$(1, 0, 1, 0, 0, 1)$	$(0, 1, 0, 1, 1, 0)$
$(1, 0, 0, 1, 1, 0)$	$(0, 1, 1, 0, 0, 1)$
$(1, 0, 0, 1, 0, 1)$	$(0, 1, 1, 0, 1, 0)$
$(1, 0, 0, 0, 1, 1)$	$(0, 1, 1, 1, 0, 0)$

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

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

**Theorem 1.** *Let  $C$  be a binary code with  $\text{RM}(k-1, 2k) \subset C \subset \text{RM}(k, 2k)$  with the following basis of the factorspace  $C/\text{RM}(k-1, 2k)$*

$$\left\{ \prod_{i=1}^m X_i^{k_i} + \text{RM}(k-1, 2k), \text{ where } k_i \in \{0, 1\} \text{ and } \sum_{i=1}^m k_i = k \right\}, \quad (6)$$

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

*Proof.* Let  $G$  be an elementary abelian group of order  $2^m$ , where  $m = 2k$ ,  $k \geq 2$ . By the group algebra representation of RM-codes and the definition of  $C$  we have the relation  $\mathcal{J}_{2,m}^{k+1} \subset C \subset \mathcal{J}_{2,m}^k$ .

For  $m = 2k$  the set  $\mathcal{X}$  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 (6).

Clearly, two monomials  $X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}$  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  $i : 1 \leq i \leq m$  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  $\mathcal{Y}$  are not orthogonal. Clearly  $Y$  is a complement free subset of  $X$  (given by (4)) with cardinality  $\frac{1}{2} \binom{2k}{k} = \binom{2k-1}{k-1}$ .

By definition,  $C = \langle \mathcal{J}_{2,m}^{k+1} \cup \mathcal{Y} \rangle$  is a subspace of the radical  $\mathcal{J}_{2,m}$  of the group algebra  $\mathcal{A}_{2,m}$  generated by the union of  $\mathcal{J}_{2,m}^{k+1}$  and  $\mathcal{Y}$ . For the dimension of  $C$  we have

$$\dim(C) = \dim(\text{RM}(k-1, m)) + \frac{1}{2} \binom{2k}{k} = 1 + \sum_{i=1}^{k-1} \binom{2k}{i} + \frac{1}{2} \binom{2k}{k} = 2^{2k-1}.$$

It follows that  $C$  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  $\mathcal{Y}$  has the same weight  $2^k$ , that is the minimal distance of  $C$ . 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  $C$  (which is subspace of  $\mathcal{J}_{2,m}$ ) is an ideal in the group algebra  $GF(2)[G]$ .  $\square$

**Theorem 2.** *Let  $Y$  and  $\mathcal{Y}$  be sets defined above and let  $C$  be the code defined in Theorem 1. Suppose that  $k_i = 0$  for some  $i : 1 \leq i \leq m$  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 isomorphism*

$$C \simeq \text{RM}(k-1, 2k-1) \oplus \text{RM}(k-1, 2k-1).$$

*Proof.* The elements of  $\mathcal{Y}$  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  $C = \langle \mathcal{J}_{2,m}^{k+1} \cup \mathcal{Y} \rangle$  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  $C_1$  of this projection is a self-dual RM( $k - 1, 2k - 1$ )-code with parameters  $[2^{2k-1}, 2^{2k-2}, 2^k]$ .

By Lemma 1 the elements of the basis of  $\mathcal{J}_{2,m}^{k+1}$  with  $k_i = 1$  generate a subspace  $C_2$  which is isomorphic to RM( $k - 1, 2k - 1$ ). The intersection of  $C_1$  and  $C_2$  is empty. Therefore  $C \simeq C_1 \oplus C_2$  and the statement follows.  $\square$

**Remark 2.** In particular, by Theorem 1 we get  $[16, 8, 4]$  self-dual codes for  $m = 4$ . These codes are extremal doubly-even codes. Using the SAGE computer algebra software we may check easily the classification of binary self-dual codes listed in [14].

There are two cases:

- 1) If  $k_i = 0$  for some  $i : 1 \leq i \leq m$  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 [14]).

These codes are formally self-dual. Both classes have the following weight function:

$$z^{16} + 28z^{12} + 198z^8 + 28z^4 + 1$$

**Remark 3.** It is known that for each odd  $m > 1$  there exists a self-dual affine-invariant code of length  $2^m$  over  $GF(2)$ , which is not a self-dual RM-code [4].

The factor space  $\mathcal{J}_{p,m}^k / \mathcal{J}_{p,m}^{k+1}$  is an irreducible  $AGL(m, GF(p))$  module. Thus the code  $C$  is not affine invariant (see [1] Theorem 4.17 ) as the powers of the radical of  $\mathcal{A}_{p,m}$  are. The code  $C$  cannot be an extended cyclic code by Corollary 1 in [4].

**Remark 4.** Using the inclusion-exclusion principle a formula can be given for the dimension of the RM( $k + 1, m$ )-code (see for example in [1] Theorem 5.5). If  $p = 2$  and  $0 \leq k \leq m$ , then we have

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

where  $i - 2j \geq 0$ .

The codes constructed in the current paper 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  $C$  in Theorem 1 is not affine-invariant and first computations show that the automorphism group of  $C$  with  $k_i = 0$  differs from the automorphism group of  $C$  with  $k_i = 1$  for some  $1 \leq i \leq m$ .

We can formulate the following open questions about the code  $C$  of Theorem 1:

- 1) Does there exist a classification for all complement-free sets for arbitrary even  $m$ ?
- 2) How many non-equivalent (in any sense) self-dual binary codes exist for fixed  $m$  and  $p$ ?
- 3) Compare the automorphism groups of the codes  $C$  defined in Theorem 1 with the automorphism group of RM-codes.
- 4) Find decoding algorithms for  $C$ .

### References

- [1] Assmus, E.F. Key, J.K., *Polynomial codes and finite geometries*, Chapter in Handbook of Coding Theory, edited by V. Pless and W. C. Huffman, Elsevier, 1995.
- [2] Berman, S.D., *On the theory of group code*, Kibernetika, **3**(1) (1967), 31–39.
- [3] Charpin, P., *Codes cycliques étendus et  $idA$  aux principaux d'une algèbre modulaire*, C.R. Acad. Sci. Paris, **295**(1) (1982), 313–315.
- [4] Charpin, P, Levy-Dit-Vehel, F., *On Self-Dual Affine-Invariant Codes* Journal Combinatorial Theory, Series A 67 (1994), 223–244.
- [5] Drensky, V., Lakatos, P., *Monomial ideals, group algebras and error correcting codes*, Lecture Notes in Computer Science, Springer Verlag, **357** (1989), 181–188.
- [6] Hannusch, C., Lakatos, P., *Construction of self-dual radical 2-codes of given distance*, Discrete Math., Algorithms and Applications, **4**(4) (2012).
- [7] Jennings, S. A., *The structure of the group ring of a  $p$ -group over modular fields*, Trans. Amer. Math. Soc. **50** (1941), 175–185.
- [8] Joyner, D., Kim, J.-L., *Selected unsolved problems in Coding Theory*, Birkhäuser, 2011.
- [9] Kasami, T. , Lin, S, Peterson, W.W., *New generalisations of the Reed-Muller codes*, IEEE Trans. Inform. Theory II-**14** (1968) 189–199.
- [10] Kelarev, A. V.; Yearwood, J. L.; Vamplew, P. W., *A polynomial ring construction for the classification of data*, Bull. Aust. Math. Soc. **79** , **2** (2009) 213–225.
- [11] Landrock, P., Manz, O., *Classical codes as ideals in group algebras*, Designs, Codes and Cryptography, **2**(3) (1992), 273–285.
- [12] Muller, D. E., *Application of boolean algebra to switching circuit design and to error detection*, IRE Transactions on Electronic Computers, 3:6–12 (1954).
- [13] MacWilliams, F.J., Sloane, N.J.A., *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1983.

- [14] Pless, V., *A classification of self-orthogonal codes over  $GF(2)$* , Discrete Mathematics **3** (1972), 209–246.
- [15] MacWilliams, F.J., *Codes and Ideals in group algebras*, Univ. of North Carolina Press, 1969.

## CONTACT INFORMATION

**C. Hannusch**, Institute of Mathematics, University of Debrecen, 4010  
**P. Lakatos** Debrecen, pf.12, Hungary  
*E-Mail(s)*: `carolin.hannusch@science.unideb.hu`,  
`lakatosp@science.unideb.hu`  
*Web-page(s)*: `www.mat.unideb.hu`

Received by the editors: 21.09.2015  
and in final form 16.12.2015.