Discrete Mathematics 340 (2017) 957–962

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On monomial codes in modular group algebras

Carolin Hannusch

Institute of Mathematics, University of Debrecen, Hungary

ARTICLE INFO

Article history:
Received 19 April 2016
Received in revised form 10 November 2016
Accepted 15 December 2016
Available online 8 February 2017

Keywords:
Error-correcting codes
Modular group algebras
Monomial codes
Automorphism group

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" (Drensky & Lakatos, 1989). 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.

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 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 $g_1, g_2, \dots, g_n$ be a basis of $K[G]$. The elements of $K[G]$ are the formal sums

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

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

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

E-mail address: carolin.hannusch@science.unideb.hu.

http://dx.doi.org/10.1016/j.disc.2016.12.014
0012-365X/© 2016 Published by Elsevier B.V.

such that

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

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

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

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

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

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

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

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 kth power of the radical $J_{p,m}$ is defined as

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

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:

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

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

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

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].