CONSTRUCTION OF SELF-DUAL BINARY CODES

C. Hannusch

Institute of Mathematics, University of Debrecen, Egyetem tër 1., H-4032, Debrecen, Hungary
carolin.hannusch@science.unideb.hu

Results stated in this talk were obtained by the author in a joint work with Piroska Lakatos (University of Debrecen, Hungary).

Let $K = GF(p)$ and G be an elementary abelian p-group of order p^m. We regard the p^k-dimensional subspaces C of the modular group algebra $K[G] = \mathcal{A}_{p,m}$ as linear codes. We will denote the Jacobson radical of $\mathcal{A}_{p,m}$ by J. The class of codes in the radical of the group algebra $\mathcal{A}_{p,m}$ has a significant practical value. If the minimum (Hamming) weight of a k-dimensional subspace C is d, then the linear code C is referred to as a (p^m, p^k, d)-code.

For abelian G Berman [1] initiated the study of the Jacobson radical of the group algebra $\mathcal{A}_{p,m}$. For $\mathcal{A}_{2,m}$ he has proved that the well known Reed-Muller (RM)-codes are the powers of the radical of the group algebra. A code C in $\mathcal{A}_{p,m}$ is called a *monomial code* [2] if it is generated by some monomials of the form $X_1^{b_1} X_2^{b_2} \dots X_m^{b_m}$, where $0 \le b_i \le p-1$. We will present codes which are ideals in J. These codes are monomial codes. Some of them are isomorphic to well-known codes and some of them are not. We give a new method to construct self-dual binary codes with parameters $(2^m, 2^{m-1}, 2^{\frac{m}{2}})$ for arbitrary even m. These codes are self-dual and they have some very good properties. The construction is introduced using "complement free" sets of binary m-tuples as the exponents of the generator elements. For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \dots, 2k\}$ by X. The elements of X can be described with the help of binary sequences $(k_1, k_2, \dots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$. We say that a subset Y of binary m-tuples in X is *complement free* if $y \in Y$ implies $\mathbf{1} - y \notin Y$, where $\mathbf{1} = (1, 1, \dots, 1)$. Then a maximal complement free subset of X has cardinality $\frac{1}{2}\binom{2k}{k} = \binom{2k-1}{k-1}$.

The construction is described in the following theorem:

Theorem. *Let C be a binary code with* $\mathrm{RM}(k-1, 2k) \subset C \subset \mathrm{RM}(k, 2k)$. *Suppose that a basis of the quotient space* $C/\mathrm{RM}(k-1, 2k)$ *is*

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

where the set of the exponents $(k_1, k_2, \dots, k_m)$ is a maximal complement free subset among the k-subsets of $\{1, 2, 3, \dots, 2k\}$.

Then C forms a $[2^{2k}, 2^{2k-1}, 2^k]$ *self-dual doubly-even code.*

Along with investigating these codes and pointing out their good properties, we will also provide some other codes in J.

References

1. Berman S.D. *On the theory of group codes* // Kibernetika. 1967. Vol. 3. No. 1. P. 31–39.

2. Drensky V., Lakatos P. *Monomial ideals, group algebras and error correcting codes* // Lecture Notes in Computer Science, Springer Verlag. 1989. Vol. 357. P. 181–188.