Visible codes in the radical of modular group algebras

Carolin Hannusch
Institute of Mathematics, University of Debrecen, Debrecen, Hungary

Let $K = GF(p)$ and G be an elementary abelian p-group G of order p^m. We consider the p^k-dimensional subspaces C of the modular group algebra $K[G] = \mathcal{A}_{p,m}$ as linear codes. The class of codes in the radical of group algebra $\mathcal{A}_{p,m}$ are of important practical values. If the minimum (Hamming) weight of the k-dimensional subspace 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 proved that the well known Reed-Muller (RM)-codes are the powers of the radical of the group algebra. The Generalized Reed-Muller (GRM) codes were introduced by Kasami, Lin, and Peterson [3] over an arbitrary finite field as the powers of the radical of group algebra.

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, and a linear code is called visible, if it has a visible basis.

The group algebra approach enables us to construct a class of binary self-dual codes and find some codes with visible basis. Since in our case $\mathcal{A}_{p,m}$ is isomorphic with $GF(p)[X_1, \dots, X_m]/(X_1^p, \dots X_m^p)$, the ambient space of the codes can be described by polynomials of m-variables.
The code C in $\mathcal{A}_{p,m}$ is called *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 $0 \le b_i \le p-1$.

The main objectives of our talk are to provide some visible codes in the radical of the modular group algebra $\mathcal{A}_{p,m}$. We describe a method for finding self-dual binary visible monomial codes (which are different to the known RM-codes). For $m = 2k$ we construct visible self-dual binary $(2^{2k}, 2^{2k-1}, 2^k)$-codes. For odd m they have better parameters than the self-dual RM-codes.
For $p > 2$ we have two new classes of visible monomial codes in the radical of $\mathcal{A}_{p,m}$, namely the following codes:

$$\left\langle \prod_{i=1}^{m} (X_i)^{b_i} \;\middle|\; \prod_{i=1}^{m} b_i \ge k, \text{ where } 0 < k \le (p-1)^m \right\rangle$$

and

$$\left\langle \prod_{i=1}^{m} (X_i)^{b_i} \;\middle|\; 0 \le b_i \le p-1 \right\rangle.$$

This is a joint work with Piroska Lakatos, Institute of Mathematics, University of Debrecen.

[1] S. D. Berman, On the theory of group codes, *Kibernetika* **3** (1967), no. 1 , 31–39.

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

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