Additive multivariable codes over $\mathbb{F}_4$

E. Martínez-Moro, A. Piñera-Nicolás
Institute of Mathematics and Applied Math Department
University of Valladolid, Spain
{edgar,anicolas}@maf.uva.es

I. F. Rua
Department of Mathematics
University of Oviedo, Spain

Abstract

The structure of additive multivariable codes over $\mathbb{F}_4$ (the Galois field with 4 elements) is presented. This complete the study of the semisimple case that was specifically addressed by the same authors before. These codes extend in a natural way the abelian codes, of which additive are a particular case.

Keywords
Additive Multivariable Codes, Abelian Codes, Quantum Codes

Quantum codes are designed to detect and correct the errors produced in quantum computations [6, 7]. These codes can be constructed with the help of specific classical codes, called *additive*, over $\mathbb{F}_4$ (the Galois field with 4 elements) [1]. An additive code of length n is a subgroup of $\mathbb{F}_4^n$ under addition. The particular case of additive cyclic codes has been considered in [2]. An additive code $\mathcal{C}$ is called *cyclic* if, whenever $c = (c_1 \dots c_n) \in C$, then its cyclic shift $(c_2 \dots c_n c_1)$ is also a codeword in $\mathcal{C}$. These codes are related to properties of the ring $\mathbb{F}_4[X]/ < X^n - 1 >$. In the case n odd, the semisimple structure of this ring can be used to obtain a complete description of the codes [3]. The case n even has been also considered [4].

In this paper we describe additive multivariable codes over the finite field $\mathbb{F}_4$ viewed as ideals of the quotient ring $\mathbb{F}_4[X_1, \dots, X_r]/ < t_1(X_1), \dots, t_r(X_r) >$ (where $t_i(X_i)X_i^{n_i} - 1 \in \mathbb{F}_4[X_i]$ are fixed polynomials). In the semisimple case (no-repeated roots) this structure was studied in [5]. The structure of the rings $\mathcal{A}_4 = \mathbb{F}_4[X_1, \dots, X_r]/ < t_1(X_1), \dots, t_r(X_r) >$ and $\mathcal{A}_2 = \mathbb{F}_2[X_1, \dots, X_r]/ < t_1(X_1), \dots, t_r(X_r) >$ is fundamental is this description.

References

[1] A. Calderbank, E. Rains, P. Shor, and N. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.

[2] B. Dey and B. Rajan. $\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_q^m$. *Des. Codes Cryptogr.*, 34:89–116, 2005.

[3] W. C. Huffman. Additive cyclic codes over $\mathbb{F}_4$. *Adv. Math. Commun.*, 1(4):427–459, 2007.

[4] W. C. Huffman. Additive cyclic codes over $\mathbb{F}_4$. *Adv. Math. Commun.*, 2(3):309–343, 2008.

[5] E. Martínez-Moro, A.P. Nicolás and I. F. Rúa. Additive semisimple multivariable codes over $\mathbb{F}_4$. *Des. Codes Cryptogr.*, Accepted (Published Online) 45:1–20, 2012.

[6] P. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 52, 1995.

[7] A. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.