Families of correcting codes with ideal group algebra structure

J.J. Bernal, Á. del Río, J.J. Simón

Universidad de Murcia

Aachen, March 22-26, 2010

S.D. Berman, On the theory of group codes, Kibernetika (1967).
J. Mac Williams, Codes and ideals in group algebra, Comb. Math. Appl. (1969).
P. Landrock and O. Manz, Classical codes as ideals in group algebras, Des. Codes Cryptogr. (1992).
F. Bernhardt, P. Landrock and O. Manz, The extended Golay does considered as ideal, J. Comb. Theory (1990).
A.V. Kelarev and P. Solé, Error correcting codes as ideal in group rings. Contemp. Math. (2001).
L. Zhu, Duadic group algebra codes, J. Stat. Planning and Inference (1996).
S. Aly, A. Klappenedra, P.K. Sarvepally, Duadic group algebra codes, Arxiv 070102. (2007).
E. Soljanin, E. Offer, LDPC codes: a group algebra formulation, Int. workshop on coding and cryptography, Paris (2001).
Handbook of coding theory. V.S. Pless and W.C. Huffman Editors (1998).

Theorem

C a q-ary Cauchy code of length $q-1$.

1. C is a left group code if and only one of the following conditions hold:
   (a) C is permutation equivalent to $\mathcal{C}_k(\alpha, f_m)$, with $L_\alpha = \mathbb{F}^*$ and $f_m(z) = z^m$.
   (b) $2 \nmid q$ and C permutation equivalent to $\mathcal{C}(\alpha, f_{m,m'})$, with $L_\alpha = \mathbb{F}^*$ and $f_{m,m'}(\xi^{2t+r}) = \xi^{2tm+rm'}$, $(\mathbb{F}^* = \langle\xi\rangle, t \in \mathbb{Z}, r \in \{0,1\}, 4m+k-1 \equiv 2m' \equiv 0 \mod (q-1))$.

Theorem

C a q-ary Cauchy code of length $q-1$.

1. C is a left group code if and only one of the following conditions hold:
   - (a) C is permutation equivalent to $\mathcal{C}_k(\alpha, f_m)$, with $L_\alpha = \mathbb{F}^*$ and $f_m(z) = z^m$.
   - (b) $2 \nmid q$ and C permutation equivalent to $\mathcal{C}(\alpha, f_{m,m'})$, with $L_\alpha = \mathbb{F}^*$ and $f_{m,m'}(\xi^{2t+r}) = \xi^{2tm+rm'}$,
   $(\mathbb{F}^* = \langle \xi \rangle, t \in \mathbb{Z}, r \in \{0,1\}, 4m+k-1 \equiv 2m' \equiv 0 \mod (q-1))$.
2. G group of order $q-1$.
   C is a left G-code if and only if either G is cyclic and condition (a) holds or G is dihedral and condition (b) holds.

Theorem

$C \subseteq \mathbb{F}\mathcal{I}$ non-trivial affine-invariant code. Let $a = a(C)$ and $b = b(C)$. G group.

1. C is a left G-code if and only if $G \simeq \mathcal{I}_\alpha$ for some map $\alpha : \mathcal{I} \to \mathcal{G}_{a,b}$ satisfying

$$\alpha(x+y) = \alpha(\alpha(y)(x))\alpha(y) \quad (x, y \in \mathcal{I}). \tag{1}$$

Theorem

$C \subseteq \mathbb{F}\mathcal{I}$ non-trivial affine-invariant code. Let $a = a(C)$ and $b = b(C)$. G group.

1. C is a left G-code if and only if $G \simeq \mathcal{I}_\alpha$ for some map $\alpha : \mathcal{I} \to \mathcal{G}_{a,b}$ satisfying

$$\alpha(x+y) = \alpha(\alpha(y)(x))\alpha(y) \quad (x, y \in \mathcal{I}). \tag{1}$$

2. C is a G-code if and only if $G \simeq \mathcal{I}_\alpha$ for some map $\alpha : \mathcal{I} \to \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ satisfying (1) and such that the map $\beta : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ given by $\beta(x, y) = \alpha(x)^{-1}(y) - y$ is $\mathbb{F}_{p^a}$-bilinear.