THERE ARE NOT NON-OBVIOUS CYCLIC AFFINE-INVARIANT CODES

JOSÉ JOAQUÍN BERNAL, ÁNGEL DEL RÍO, AND JUAN JACOBO SIMÓN

ABSTRACT. We show that an affine-invariant code C of length p^m is not permutation equivalent to a cyclic code except in the obvious cases: $m = 1$ or C is either $\{0\}$, the repetition code or its dual.

Affine-invariant codes were firstly introduced by Kasami, Lin and Peterson [KLP2] as a generalization of Reed-Muller codes. This class of codes has received the attention of several authors because of its good algebraic and decoding properties [D, BCh, ChL, Ho, Hu]. It is well known that every affine-invariant code can be seen as an ideal of the group algebra of an elementary abelian group in which the group is identified with the standard base of the ambient space. In particular, if C is a code of prime length then C is permutation equivalent to a cyclic code. Other obvious affine-invariant cyclic codes are the trivial code, $\{0\}$, the repetition code and the code form by all the even-like words, provided its length is a prime power. In this paper we prove that these are the only affine-invariant codes which are permutation equivalent to a cyclic code.

Our main tools are an intrinsical characterization of group codes obtained in [BRS] and a description of the group of permutation automorphisms of non-trivial affine-invariant codes given in [BCh]. These results are reviewed in Section 1, where we also recall the definition and main properties of affine-invariant codes. In Section 2 we prove the main result of the paper.

1. Preliminaries

In this section we recall the definition of (left) group code and the intrinsical characterization given in [BRS]. We also recall the definition of affine-invariant code and the description of its group of permutation automorphisms given in [BCh].

All throughout $\mathbb{F}$ is a field of order a power of p, where p is a prime number. The finite field with p^s elements is denoted by $\mathbb{F}_{p^s}$. For a group G, we denote by $\mathbb{F}G$ the group ring of G with coefficients in $\mathbb{F}$. All the group theoretical notions used in this paper can be easily founded in [R].

Definition 1. *If E is the standard basis of $\mathbb{F}^n$, $C \subseteq \mathbb{F}^n$ is a linear code and G is a group (of order n) then we say that C is a* G-code *if there is a*

Research supported by D.G.I. of Spain and Fundación Séneca of Murcia.

bijection $\phi : E \to G$ such that the linear extension of ϕ to an isomorphism $\phi : \mathbb{F}^n \to \mathbb{F}G$ maps C to an ideal of $\mathbb{F}G$.

A group code *is a linear code which is a G-code for some group G.*

A cyclic group code (respectively, abelian group code, solvable group code, etc) is a linear code which is G-code for some cyclic group G (respectively, abelian group, solvable group, etc).

Let S_n denote the group of permutations of n symbols. Every $\sigma \in S_n$ defines an automorphism of $\mathbb{F}^n$ in the obvious way, i.e. $\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. By definition, the group of permutation automorphisms of a linear code C of length n is

$$\mathrm{PAut}(C) = \{\sigma \in S_n : \sigma(C) = C\}.$$

An intrinsical characterization of group codes C in terms of $\mathrm{PAut}(C)$ has been obtained in [BRS]. Four our purposes we only need to consider abelian groups. So we record in the following theorem the specialization of [BRS, Theorem 1.2] to abelian groups.

Theorem 2. [BRS] *Let C be a linear code of length n over a field $\mathbb{F}$ and G a finite abelian group of order n. Then C is a G-code if and only if G is isomorphic to a transitive subgroup H of S_n.*

In the remainder of the paper we assume that $\mathcal{I} = \mathbb{F}_{p^m}$. Often we will be only using the underlying additive structure of $\mathcal{I}$; for example, $\mathbb{F}\mathcal{I}$ is the group algebra of this additive group with coefficients in $\mathbb{F}$. Let $S(\mathcal{I})$ denote the group of permutations of $\mathcal{I}$. Every element of $S(\mathcal{I})$ induces a unique $\mathbb{F}$-linear bijection of the group algebra $\mathbb{F}\mathcal{I}$. For an $\mathbb{F}$-subspace C of $\mathbb{F}\mathcal{I}$, let $\mathrm{PAut}(C) = \{\sigma \in S(\mathcal{I}) : \sigma(C) = C\}$.

An affine-invariant code is an $\mathbb{F}$-subspace C of $\mathbb{F}\mathcal{I}$ formed by even-like words such that $\mathrm{PAut}(C)$ contains the maps of the form $x \in \mathcal{I} \mapsto \alpha x + \beta$, with $\alpha \in \mathcal{I}^* = \{a \in \mathcal{I} : a \neq 0\}$ and $\beta \in \mathcal{I}$. These maps are called affine transformations of $\mathcal{I}$.

Observe that if $\mathbb{F}^{p^m}$ is identified with $\mathbb{F}\mathcal{I}$ via some bijection from $\{1, \ldots, p^m\}$ to $\mathcal{I}$, then the linear codes of length p^m correspond to subspaces of $\mathbb{F}\mathcal{I}$ in such a way that the groups of permutations automorphisms agree. Therefore if C is a subspace of $\mathbb{F}\mathcal{I}$ and G is a group then C is a left G-code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup H of $S(\mathcal{I})$ isomorphic to G and it is a G-code if H can be selected such that $C_{S(\mathcal{I})}(H) \subseteq \mathrm{PAut}(C)$.

Affine-invariant codes can be seen as extended cyclic codes. Recall that a cyclic code C of length n over $\mathbb{F}$ is a subspace of $\mathbb{F}^n$ which is closed under cyclic permutations, that is if $(x_1, x_2, \ldots, x_{n-1}, x_n)$ is an element of C then so is $(x_n, x_1, x_2, \ldots, x_{n-1})$. Cyclic codes are cyclic group codes via the bijection $\phi : E \to G$ given by $\phi(e_i) = g^{i-1}$, where $E = \{e_1, \ldots, e_n\}$ is the standard basis of $\mathbb{F}^n$ and G is a cyclic group of order n generated by g. Conversely, any ideal of the group algebra $\mathbb{F}G$, with G a cyclic group of order n can be seen as a cyclic code with a suitable identification of the elements of G with the coordinates.

The zeroes of a cyclic code C of length n are the n-th roots of unity α such that $x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{n-1}\alpha^{n-1} = 0$, for every $(x_0, x_1, \ldots, x_{n-1}) \in C$. It is well known that every cyclic code is uniquely determined by its zeroes and conversely, if ζ is a primitive n-th root of unity and D is a union of q-cyclotomic classes modulo n then there is a unique q-ary cyclic code of length n whose set of zeroes is $\{\zeta^i : i \in D\}$.

Let $C \subseteq \mathbb{F}\mathcal{I}$ be an affine-invariant code and let C^* denote the code obtained by puncturing C at the coordinate labelled by 0. The permutation automorphisms of C which fix 0 induces permutation automorphisms of C^*. In particular, $\mathrm{PAut}(C^*)$ contains the maps of the form $x \to \alpha x$, for $\alpha \in \mathcal{I}^*$. This maps form a cyclic group isomorphic to the group of units of the field $\mathcal{I}$. So, C^* is a cyclic group code and C is the extended code obtained by adding a parity check coordinate.

However not every code obtained by extending a cyclic code of length $p^m - 1$ is affine-invariant. We recall a characterization of Kasami, Lin and Peterson of the extended cyclic codes which are affine-invariant in terms of the roots of the cyclic code [KLP1].

The p-adic expansion of a non-negative integer x is the list of integers $(x_0, x_1, \ldots)$ with $0 \leq x_i < p$ and $x = \sum_{i \geq 0} x_i p^i$. The p-adic expansion yields a partial ordering in the set of positive integers by setting $x \preceq y$ if $x_i \leq y_i$, for every i, where (x_i) and (y_i) are the p-adic expansions of x and y, respectively.

Let $n = p^m - 1$ and let α be a primitive element of $\mathcal{I}$, i.e. a generator of $\mathcal{I}^*$. Identify the standard basis of $\mathbb{F}^n$, $E = \{e_1, \ldots, e_n\}$, with $\mathcal{I}^*$ via the map $e_i \mapsto \alpha^{i-1}$. A cyclic code C^* of length n is determined by the following set

$$D_{C^*} = \{i : 0 \leq i < n, \alpha^i \text{ is a zero of } C^*\}.$$

Since C^* is a q-ary cyclic code, with $q = p^r$, the set D_{C^*} is invariant under multiplication by q modulo n, that is, D_{C^*} is a union of q-cyclotomic classes modulo n. Conversely, every union D of q-cyclotomic classes modulo n, yields to a uniquely defined cyclic code C^* of length n with $D = D_{C^*}$. If C^* is a cyclic code and C is its corresponding extended code then the defining set of C is by definition $D_C = D_{C^*} \cup \{0\}$ if $0 \notin D_C$, and $D_C = D_{C^*} \cup \{n\}$ if $0 \in D_{C^*}$.

Proposition 3. [KLP1][Hu, Corollary 3.5] *Let C^* be a cyclic code of length $n = p^m - 1$ and C the extended code of C^*. Then C is affine-invariant if and only if D_C satisfy the following condition for every $1 \leq s, t \leq n$:*

$$s \preceq t \text{ and } t \in D_C \quad \Rightarrow \quad s \in D_C. \tag{1}$$

The trivial code and the repetition code of length n are cyclic with defining sets $\{0, 1, 2, \ldots, n-1\}$ and $\{1, 2, \ldots, n-1\}$ respectively. Their duals, i.e. $\mathbb{F}^n$ and the space of all the even-like words, are also cyclic with defining sets $\emptyset$ and $\{0\}$. Recall that a word $(x_1, \ldots, x_n)$ is even-like if $\sum_{i=1}^n x_i = 0$. When $n = p^m - 1$, except for the last one, all the others give rise to affine-invariant codes of length p^m: the trivial code, the repetition code and the

code formed by the even-like words. These three codes are known as the trivial affine-invariant codes.

For future use we describe the affine-invariant codes of length 4.

Example 4 (Affine-invariant codes of length 4)**.** Let D be the defining set of an affine-invariant code C of length 4 over $\mathbb{F}_{2^r}$. Then C is trivial as an affine-invariant code if and only if D is either $\{0\}, \{0,1,2\}$ or $\{0,1,2,3\}$. Since D is invariant by multiplication by 2^r modulo 3 and satisfies condition (1), if r is odd then there are not non trivial affine-invariant codes. However, if r is even then there are two non-trivial affine-invariant codes with defining sets $\{0,1\}$ and $\{0,2\}$ respectively.

If C is a trivial affine-invariant code then $\mathrm{PAut}(C) = S_n$, and therefore C is G-code for every group G of order p^m. So to avoid trivialities, in the remainder of the paper all the affine-invariant codes are suppose to be non-trivial. The group of permutations of a (non-trivial) affine-invariant code has been described by Berger and Charpin [BCh]. In order to present their description we need to introduce some notation.

We use the notation $N \rtimes G$ to represent a semidirect product of N by G via some action of G on N, which is going to be clear from the context. That is, N and G are groups and there is a group homomorphism $\sigma : G \to \mathrm{Aut}(N)$ associating $g \in G$ to σ_g. The underlying set of $N \rtimes G$ is the direct product $N \times G$ and the product is given by $(n_1, g_1)(n_2, g_2) = (n_1\sigma_{g_1}(n_2), g_1g_2)$.

For every $d|m$ let $\mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^d}})$ and $\mathrm{Aff}_d(\mathcal{I})$ denote the groups of linear and affine transformations of $\mathcal{I}$ as vector space over $\mathbb{F}_{p^d}$. The group of $\mathbb{F}_{p^d}$-automorphisms of the field $\mathcal{I}$ is denoted by $\mathrm{Gal}(\mathcal{I}/\mathbb{F}_{p^d})$. We identify every element $y \in \mathcal{I}$ with the translation $x \mapsto x+y$. Then $\mathrm{Aff}_d(\mathcal{I}) = \mathcal{I} \rtimes \mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^d}})$.

Given two divisors a and b of m with $b|a$, let

$$\mathcal{G}_{a,b} = \{f \in \mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^b}}) : f \text{ is } \tau - \text{semilinear for some } \tau \in \mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_{p^b})\}.$$

We claim that $\mathcal{G}_{a,b} = \langle \mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^a}}), \mathrm{Gal}(\mathcal{I}/\mathbb{F}_{p^b})\rangle$. Indeed, if f is τ-semilinear with $\tau \in \mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_{p^b})$ then τ is the restriction of σ for some $\sigma \in \mathrm{Gal}(\mathcal{I}/\mathbb{F}_{p^b})$ and $f\sigma^{-1} \in \mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^a}})$.

Theorem 5. [BCh, Corollary 2] *Let C be a non-trivial affine-invariant code of length p^m over $\mathbb{F}_q$, with $q = p^r$. Let*

$$\begin{aligned} a = a(C) &= \min\{d|m : \mathrm{Aff}_d(\mathcal{I}) \subseteq \mathrm{PAut}(C)\}, \\ b = b(C) &= \min\{d \geq 1 : p^d D_C = D_C\} \end{aligned}$$

Then $b|r$, $b|a|m$ and

$$\mathrm{PAut}(C) = \langle \mathrm{Aff}_a(\mathcal{I}), \mathrm{Gal}(\mathcal{I}/\mathbb{F}_{p^b})\rangle = \mathcal{I} \rtimes \mathcal{G}_{a,b}.$$

A method to compute $a(C)$ and $b(C)$ was firstly obtained by Delsarte [D]. Later, Berger and Charpin founded two alternative methods to calculate $a(C)$ and $b(C)$ which are sometimes computationally simpler [BCh].

2. Affine-invariant cyclic group codes

Let C be an affine-invariant code. Then C is an $\mathcal{I}$-code, since the group of translations of $\mathcal{I}$ (which we have identified with the additive group $\mathcal{I}$) is a transitive subgroup of $S(\mathcal{I})$ contained in $\mathrm{PAut}(C)$. So every affine-invariant code is an elementary abelian group code. In particular, if the length of C is prime then C is a cyclic group code. Next result shows that this one is the only type of non-trivial affine-invariant cyclic group codes.

Theorem 6. *A non-trivial affine-invariant code is permutation equivalent to a cyclic code if and only if it has prime length.*

Proof. Assume that C is a non trivial affine-invariant code of length p^m which is permutation equivalent to a cyclic code. Then C is a cyclic group code. By Theorem 2, this implies that $G = \mathrm{PAut}(C)$ contains a cyclic subgroup of order p^m or equivalently G contains an element of order p^m. Let $a = a(C)$, $b = b(C)$, as in Theorem 5 and $h = m/a$. Let p^t be the maximum p-th power dividing a/b, and p^u the minimum p-th power greater or equal than h. We first show that the existence of an element g of order p^m in G implies a strong relation on these parameters which reduces to some few cases.

By Theorem 5, $G = \mathcal{I} \rtimes \mathcal{G}_{a,b}$. Furthermore $H = \mathcal{I} \rtimes \mathrm{GL}(\mathcal{I}_{\mathbb{F}_{p^a}})$ is a normal subgroup of index a/b in G. Since the order of G is a p-th power and p^t is the maximum p-th power dividing a/b, g^{p^t} is an element of order p^{m-t} in H. Furthermore, H is isomorphic to $\mathbb{F}_{p^a}^h \rtimes \mathrm{GL}_h(\mathbb{F}_{p^a})$, where $\mathrm{GL}_h(\mathbb{F}_{p^a})$ is the group of invertible $h \times h$ matrices with entries in $\mathbb{F}_{p^a}$. Therefore there is an element $(x, A) \in \mathbb{F}_{p^a}^h \rtimes \mathrm{GL}_h(\mathbb{F}_{p^a})$ of order p^{m-t}. This implies that A has order p^k with $m-t-1 \leq k$. Since the order of A is a power of p, and the fields of characteristic p do not have elements of orden p, the only eigenvalue of A is 1. We may assume that A is given in Jordan form and hence $A = I + N$ where N is an upper triangular matrix with zeroes in the diagonal. Then $N^{p^u} = 0$ and therefore $A^{p^u} = I$. Thus $m - t - 1 \leq k \leq u = \lceil \log_p(h) \rceil$ and we conclude that

$$m \leq 1 + t + \lceil \log_p(h) \rceil < 2 + \log_p(a) + \log_p(h) = 2 + \log_p(m). \tag{2}$$

We have to prove that $m = 1$. Otherwise, (2) implies that either $m = 2$ or $m = 3$ and $p = 2$.

Case 1: $m = 2$. We claim that in this case $p = 2$. Indeed, if $p > 2$ then $0 < \log_p(2) < 1$ and $t = 0$, since p^t divides $m = 2$. Hence $2 = m \leq 1 + \lceil \log_p(h) \rceil \leq 1 + \lceil \log_p(m) \rceil = 2$ and so $h = 2$.

Hence (x, A) is an element of order p^2 in $\mathbb{F}_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p)$. Thus there are $x_1, x_2, y \in \mathbb{F}_p$ such that $((x_1, x_2), A)^p \neq (0, 1)$, where $A = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$.

However

$$\begin{aligned}((x_1,x_2),A)^p &= \left(\left(\sum_{i=0}^{p-1}(x_1+iyx_2),py\right),A^p\right)\\ &= \left(\left(\tfrac{p(p-1)}{2}yx_2,0\right),1\right)=(0,1),\end{aligned}$$

which is the desired contradiction.

Hence $p=2$ and so C has length 4. Since C is non-trivial as affine-invariant code, by Example 4, r is even and $D_C=\{0,1\}$ or $\{0,2\}$. By the definition of $b(C)$ we have $b=2$ and hence $a=2$. We deduce that $\mathrm{PAut}(C)=\mathcal{I}\rtimes\mathbb{F}_4^*$. Hence $\mathcal{I}\simeq\mathbb{F}_p^2$ is the only subgroup of order 4 of $\mathrm{PAut}(C)$ and we conclude that C is not cyclic group code.

Case 2: $m=3$ and $p=2$. Then $t=0$ and $3\leq 1+\lceil\log_2(h)\rceil\leq 1+\lceil\log_2(m)\rceil=3$, by (2). Thus $h=3$, or equivalently $a=1$ and hence $b=1$. Thus (x,A) is an element of order 8 in $\mathbb{F}_2^3\rtimes GL_3(\mathbb{F}_2)$. Then $u=\lceil\log_2(3)\rceil=2$ and so $A^4=1$. If $A^2=1$ then $x^4=1$, a contradiction. Therefore A is a Jordan matrix of order 4 and thus

$$A=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

However $I+A+A^2+A^3=0$. Then $(x,A)^4=((I+A+A^2+A^3)x,A^4)=(0,1)$, a contradiction. □

References

[BCh] T.P. Berger and P. Charpin, The Permutation group of affine-invariant extended cyclic codes, IEEE Trans. Inform. Theory 42 (1996) 2194-2209.

[BRS] J.J. Bernal, Á. del Río and J.J. Simón, An intrinsical description of group codes, Designs, Codes, Cryptog. (to appear). DOI 10.1007/s10623-008-9261-z.

[ChL] P. Charpin and F. Levy-Dit-Vehel, On Self-dual affine-invariant codes, J. Comb. Theory, Series A 67 (1994) 223-244.

[D] P. Delsarte, On cyclic codes that are invariant under the general linear group, IEEE Trans. Inform. Theory IT-16 (1970) 760-769.

[Ho] X-D Hou, Enumeration of certain affine invariant extended cyclic codes, J. Comb. Theory, Series A 110 (2005) 71-95.

[Hu] W.C. Huffman, Codes and groups, in Handbook of coding theory. Vol. II. 1345–1440. Edited by V. S. Pless, W. C. Huffman and R. A. Brualdi. North-Holland, Amsterdam, 1998.

[KLP1] T. Kasami, S. Lin, W.W. Peterson, *Some results on cyclic codes which are invariant under the affine group and their applications.* Information and Control 11 (1967) 475–496.

[KLP2] T. Kasami, S. Lin and W.W. Peterson, *New generalizations of the Reed-Muller codes part I: primitive codes*, IEEE Trans. Inform. Theory, IT-14 (1968) 189-199.

[R] D.J.S. Robinson, *A course in the theory of groups*, Springer, 1996.

Departamento de Matemáticas, Universidad de Murcia, Spain

E-mail address: josejoaquin.bernal@alu.um.es, adelrio@um.es, jsimon@um.es