Group code structures of affine-invariant codes ☆

José Joaquín Bernal, Ángel del Río, Juan Jacobo Simón

Departamento de Matemáticas Universidad de Murcia, Murcia, Spain

Abstract

A group code structure of a linear code is a description of the code as one-sided or two-sided ideal of a group algebra of a finite group. In these realizations, the group algebra is identified with the ambient space, and the group elements with the coordinates of the ambient space. It is an obvious consequence of the definition that every p^r-ary affine-invariant code of length p^m, with p prime, can be realized as an ideal of the group algebra $\mathbb{F}_{p^r}[(\mathbb{F}_{p^m},+)]$, where $(\mathbb{F}_{p^m},+)$ is the underlying additive group of the field $\mathbb{F}_{p^m}$ with p^m elements. In this paper we describe all the group code structures of an affine-invariant code of length p^m in terms of a family of maps from $\mathbb{F}_{p^m}$ to the group of automorphisms of $(\mathbb{F}_{p^m},+)$. We also present a familly of non-obvious group code structures in an arbitrary affine-invariant code.

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]. The length of an affine-invariant code is a prime power p^m, where p is the characteristic of the finite field $\mathbb{F}$ which plays the role of alphabet. Moreover, it is an obvious consequence of the definition of affine-invariant codes that C can be realized as an ideal of the group algebra $\mathbb{F}[(\mathbb{F}_{p^m},+)]$, where $(\mathbb{F}_{p^m},+)$ is the underlying additive group of the field with p^m elements. We refer to these realizations of codes as one-sided or two-sided

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

ideals in group algebras as group code structures of the given code. In this paper we study all the possible group code structures of an affine-invariant 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 describe all the group code structures of an affine-invariant code C in terms of a family of maps $\mathbb{F}_{p^m} \to \mathcal{G}_{a,b}$ where $\mathcal{G}_{a,b}$ is a subgroup of the group of automorphism of $(\mathbb{F}_{p^m}, +)$ depending on two integers a and b which are determined by the code C (see Theorem 6). Some methods to calculate a and b were given in [D] and [BCh]. As an application we exhibit in Section 3 a family of group code structures of any affine-invariant code C for which the integer a is different from m and characterize the affine-invariant codes C which have a non-abelian group code structure.

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 p is a positive prime integer and we use as alphabet the field $\mathbb{F} = \mathbb{F}_{p^r}$ with p^r elements. Instead of using the cartesian product $\mathbb{F}^n$ as the ambient space for p^r-ary linear codes of length n, we fix a finite set B of cardinality n and set $\mathbb{F}[B]$ as the ambient space for p^r-ary linear codes of length n, where $\mathbb{F}[B]$ denotes the set of formal sums

$$\sum_{b \in B} \alpha_b b, \quad (\alpha_b \in \mathbb{F}),$$

considered as vector space over $\mathbb{F}$. If $B = G$ is a group then $\mathbb{F}[G]$ is the group algebra of G with coefficients in $\mathbb{F}$.

A p^r-ary linear code C of length n is simply a subspace of $\mathbb{F}[B]$. We abbreviate this by saying that $C \subseteq \mathbb{F}[B]$ is a linear code. A linear code $C \subseteq \mathbb{F}[B]$ is said to be even-like if $\sum_{b\in B}\alpha_b = 0$ for every $\sum_{b\in B}\alpha_b b \in C$.

Definition 1. *Let $C \subseteq \mathbb{F}[B]$ be a linear code and let G be a group. We say that C is a* left G-code *(respectively, a* right G-code*, a* G-code*) if there is a bijection $\phi : B \to G$ such that the unique linear map $\mathbb{F}[B] \to \mathbb{F}[G]$ extending ϕ, maps C into a left ideal (respectively, a right ideal; a two-sided ideal) of $\mathbb{F}[G]$.*

A left group code *(respectively,* right group code, group code*) is a linear code which is a left G-code (respectively, a right G-code, G-code) for some group G.*

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

By the (left) group code structures of a linear code C we mean the different realizations of C as a (left) G-code.

Let S_B denote the set of bijections $B \to B$. Every element σ of S_B extends uniquely to a vector space automorphism $\mathbb{F}[B] \to \mathbb{F}[B]$ which we also denote by σ. The group of permutation automorphisms of a linear code $C \subseteq \mathbb{F}[B]$ is

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

An intrinsical characterization of (left) group codes C in terms of $\mathrm{PAut}(C)$ has been obtained in [BRS].

Theorem 2. *[BRS] Let $C \subseteq \mathbb{F}[B]$ be a linear code and let G be a finite group with the same cardinality than B.*

(a) *C is a left G-code if and only if G is isomorphic to a transitive subgroup of S_B contained in* $\mathrm{PAut}(C)$.

(b) *C is a G-code if and only if G is isomorphic to a transitive subgroup H of S_B such that $H \cup C_{S_B}(H) \subseteq \mathrm{PAut}(C)$, where $C_{S_B}(H)$ denotes the centralizer of H in S_B.*

Now we recall the definition of affine-invariant codes.

Definition 3. *Let $\mathbb{F} = \mathbb{F}_{p^r}$ and $\mathbb{K} = \mathbb{F}_{p^m}$ be the fields with p^r and p^m elements respectively. A p^r-ary affine invariant code of length p^m is an even-like linear code $C \subseteq \mathbb{F}[\mathbb{K}]$ such that* $\mathrm{PAut}(C)$ *contains all the affine maps of $\mathbb{K}$ (i.e. the maps $\mathbb{K} \to \mathbb{K}$ of the form $x \mapsto \alpha x + \beta$, with $\alpha \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$ and $\beta \in \mathbb{K}$).*

Observe that the multiplications of elements of $\mathbb{F}$ and $\mathbb{K}$ in $\mathbb{F}[\mathbb{K}]$ may be confused with the multiplication in a field containing both $\mathbb{F}$ and $\mathbb{K}$. To avoid this, an element $b \in \mathbb{K}$, considered as a basic element of $\mathbb{F}[\mathbb{K}]$, is denoted by

$\overline{b}$. Endowing $\mathbb{K}$ with the additive group structure $(\mathbb{K},+)$ of $\mathbb{K}$ we may consider $\mathbb{F}[\mathbb{K}]$ as the group algebra of $(\mathbb{K},+)$ with coefficients in $\mathbb{F}$.

If $C \subseteq \mathbb{F}[\mathbb{K}]$ is an affine-invariant code then C is an ideal of the group algebra $\mathbb{F}[(\mathbb{K},+)]$. To see this observe that if $h \in \mathbb{K}$ and $a = \sum_{g\in\mathbb{K}} a_g\overline{g} \in C$ then $ha = \sum_{g\in\mathbb{K}} a_g\overline{g+h} = T_h(a) \in C$, where $T_h : \mathbb{K} \to \mathbb{K}$ is the translation map $T_h : g \mapsto g+h$. Therefore every affine-invariant code $C \subseteq \mathbb{F}[\mathbb{K}]$ is a $(\mathbb{K},+)$-group code.

Affine-invariant codes can be seen as extended cyclic codes as follows: If $J \subseteq \mathbb{F}[\mathbb{K}^*]$ is a linear code then the parity check extension of J is

$$\left\{\sum_{g\in\mathbb{K}} a_g\overline{g} : \sum_{g\in\mathbb{K}^*} a_g\overline{g} \in J \text{ and } \sum_{g\in\mathbb{K}} a_g = 0\right\}.$$

We may now consider $\mathbb{F}[\mathbb{K}^*]$ as a group algebra over the multiplicative cyclic group $(\mathbb{K}^*,\cdot)$. If $C \subseteq \mathbb{F}[\mathbb{K}]$ is an affine-invariant code then $C^* = \{\sum_{g\in\mathbb{K}^*} a_g\overline{g} : \sum_{g\in\mathbb{K}} a_g\overline{g} \in C\}$ is an ideal of $\mathbb{F}[\mathbb{K}^*]$ and C is the parity check extension of C^*.

Now we recall a characterization of Kasami, Lin and Peterson of the parity check extensions of ideals of $\mathbb{F}[\mathbb{K}^*]$ which are affine-invariant in terms of the p-adic expansion of its defining set [KLP1]. Let $C \subseteq \mathbb{F}[\mathbb{K}]$ be the parity check extension of an ideal of $\mathbb{F}[\mathbb{K}^*]$. The defining set of C is

$$D_C = \left\{ i \ : \ 0 \le i < p^m \ \text{ and } \sum_{g\in\mathbb{K}} a_g g^i = 0 \text{ for every } \sum_{g\in\mathbb{K}} a_g\overline{g} \in C \right\},$$

where, by convention, $0^0 = 1$. As p^r is the cardinality of $\mathbb{F}$, the set $D_C \setminus \{p^m - 1\}$ is a union of p^r-cyclotomic classes modulo $p^m - 1$. Conversely, if D is a subset of $\{0, 1, \dots, p^m - 1\}$, such that $D \setminus \{p^m - 1\}$ is a union of p^r-cyclotomic classes modulo $p^m - 1$, then there is a unique ideal J of $\mathbb{F}[\mathbb{K}^*]$ such that D is the defining set of the parity check extension of J (see e.g. [Ch]).

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

Proposition 4. *[KLP1][Hu, Corollary 3.5] Let $C \subseteq \mathbb{F}[\mathbb{K}]$ be the parity check extension of an ideal of the group algebra $\mathbb{F}[\mathbb{K}^*]$. Then C is affine-invariant if and only if D_C satisfies the following condition for every $1 \le s, t \le p^m - 1$:*

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

Three obvious affine-invariant codes are the zero code, the repetition code and its dual, i.e. $\{0\}$, the ideal of $\mathbb{F}[\mathbb{K}]$ generated by $\sum_{g\in\mathbb{K}} \overline{g}$, and the augmentation ideal $\{\sum_{g\in\mathbb{K}} a_g\overline{g} : \sum_{g\in\mathbb{K}} a_g = 0\}$, respectively. Their defining sets are $\{0, 1, \ldots, p^m - 1\}$, $\{0, 1, \ldots, p^m - 2\}$ and $\{0\}$, respectively. These three codes are known as the trivial affine-invariant codes [BCh, Hu].

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

Example 5 (Affine-invariant codes of length 4)**.** Let D be the defining set of an affine-invariant code of length 4 over $\mathbb{F}_{2^r}$. Thus D satisfies condition (1) and $D \setminus \{3\}$ is a union of 2^r classes modulo 3. If r is odd then the 2^r-cyclotomic classes modulo 3 are $\{0\}$ and $\{1, 2\}$. This implies that if r is odd then $D = \{0\}$, $\{0, 1, 2\}$ or $\{0, 1, 2, 3\}$, i.e. C is trivial as affine-invariant code. However, if r is even then the cyclotomic classes modulo 3 are $\{0\}, \{1\}$ and $\{2\}$. So, in this case there are two additional possibilities for D, namely $\{0, 1\}$ and $\{0, 2\}$. Resuming, if r is odd then there are not 2^r-ary non-trivial affine-invariant codes of length 4 and if r is even then there are two 2^r-ary non-trivial affine invariant codes of length 4.

If $C \subseteq \mathbb{F}[\mathbb{K}]$ is a trivial affine-invariant code then $\mathrm{PAut}(C) = S_{\mathbb{K}}$, 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].

For every $d|m$ let $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_{p^d})$ denote the Galois group of $\mathbb{K}$ over $\mathbb{F}_{p^d}$. To refer to $\mathbb{K}$ as a vector space over $\mathbb{F}_{p^d}$ we write $\mathbb{K}_{\mathbb{F}_{p^d}}$. Accordingly $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^d}})$ denotes general linear group of $\mathbb{K}$ regarded as vector space over $\mathbb{F}_{p^d}$. Let $T_{\mathbb{K}}$ be the set of translations $T_h : \mathbb{K} \to \mathbb{K}$, $T_h(g) = g + h$ $(g, h \in \mathbb{K})$.

Theorem 6. *[BCh, Corollary 2] Let $C \subseteq \mathbb{F}[\mathbb{K}]$ be a p^r-ary non-trivial affine-invariant code of length p^m and let*

$$a = a(C) = \min\left\{d|m : \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^d}}) \subseteq \mathrm{PAut}(C)\right\} \text{ and}$$
$$b = b(C) = \min\left\{d \ge 1 : \begin{array}{l} D_C \setminus \{p^m - 1\} \text{ is a union of} \\ \text{cyclotomic } p^d - \text{classes modulo } p^m - 1 \end{array}\right\}.$$

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

$$\mathrm{PAut}(C) = \langle T_{\mathbb{K}}, \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}}), \mathrm{Gal}(\mathbb{K}/\mathbb{F}_{p^b})\rangle.$$

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

Now we present an alternative description of $\mathrm{PAut}(C)$, for C an affine-invariant code with $a = a(C)$ and $b = b(C)$ as in Theorem 6. Let

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

and consider the semidirect product $\mathbb{K} \rtimes \mathcal{G}_{a,b}$, with the natural action of $\mathcal{G}_{a,b}$ on $\mathbb{K}$. That is $\mathbb{K} \rtimes \mathcal{G}_{a,b}$ is the cartesian product $\mathbb{K} \times \mathcal{G}_{a,b}$, with multiplication given by $(x, f)(y, g) = (x + f(y), fg)$.

Corollary 7. *If C is a non-trivial affine-invariant code and $a = a(C)$ and $b = b(C)$ as in Theorem 6 then $(x, f) \mapsto T_x f$ defines a group isomorphism $\mathbb{K} \rtimes \mathcal{G}_{a,b} \to \mathrm{PAut}(C)$.*

Proof. We claim that $\mathcal{G}_{a,b} = \langle \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}}), \mathrm{Gal}(\mathbb{K}/\mathbb{F}_{p^b})\rangle$. 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 $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F}_{p^b})$. Then $f\sigma^{-1} \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$. This proves one inclusion; the other one is obvious, so that the claim is proved. Using the equality $fT_x f^{-1} = T_{f(x)}$, for $x \in \mathbb{K}$ and $f \in \mathcal{G}_{a,b}$, and $T_{\mathbb{K}} \cap \mathcal{G}_{a,b} = 1$ one deduces easily that the given map is an isomorphism. □

Remark 8. The map $\psi : \mathcal{G}_{a,b} \to \mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_{p^b})$ which associates f to τ, when f is τ-semilinear, is a surjective group homomorphism with kernel $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$.

In the remainder of the paper we use the isomorphism of Corollary 7 as an identification of $\mathrm{PAut}(C)$ with $\mathbb{K} \rtimes \mathcal{G}_{a,b}$. In particular, we identify $g \in \mathbb{K}$ with $T_g \in T_{\mathbb{K}}$.

2. Group code structures of affine-invariant codes

In this section we present the main result of the paper, namely a description of all the group code structures of a non-trivial affine-invariant code C with $a = a(C)$ and $b = b(C)$ in terms of some maps $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$.

Given a map $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$ let

$$\mathcal{I}_\alpha = \{(x, \alpha(x)^{-1}) : x \in \mathbb{K}\}.$$

The proof of the following lemma is straightforward.

Lemma 9. *$\mathcal{I}_\alpha$ is a subgroup of $\mathbb{K} \rtimes \mathcal{G}_{a,b}$ if and only if*

$$\alpha(x+y) = \alpha(\alpha(y)(x))\alpha(y) \tag{2}$$

for every $x, y \in \mathbb{K}$. In particular, if α satisfies (2) then $\{\alpha(x) : x \in \mathbb{K}\}$ is a p-subgroup of $\mathcal{G}_{a,b}$.

We need one more lemma which is an easy consequence of Sylow's Theorem [R, 1.6.16].

Lemma 10. *If P is a p-subgroup of $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ then $\sum_{\rho \in P} \mathrm{Im}(\rho - 1) \neq \mathbb{K}$.*

Proof. Select a basis $b_1, \dots, b_n$ of $\mathbb{K}_{\mathbb{F}_{p^a}}$, with $n = m/a$, and let U be the set of endomorphisms f of $\mathbb{K}_{\mathbb{F}_{p^a}}$ such that for every $i = 1, 2, \dots, n$, $f(b_i) - b_i$ belongs to the $\mathbb{F}_{p^a}$-subspace of $\mathbb{K}$ generated by the b_j's with $1 \leq j < i$. That is, U is the group of automorphisms of $\mathbb{K}_{\mathbb{F}_{p^a}}$ having upper unitriangular associated matrix in the given basis. An easy counting argument shows that $|U| = p^{a\frac{n(n-1)}{2}}$ and $|\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})| = (p^a - 1)(p^{na} - p^a)(p^{na} - p^{2a}) \dots (p^{na} - p^{(n-1)a}) = |U|(p^a - 1)(p^{(n-1)a} - 1)(p^{(n-2)a} - 1) \dots (p^a - 1)$. Then U is a Sylow's p-subgroup of $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$. By Sylow Theorem, there is $g \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ such that $P \subseteq gUg^{-1}$. Then $\sum_{\rho \in P} \mathrm{Im}(\rho - 1) \subseteq \sum_{u \in U} \mathrm{Im}(gug^{-1} - 1) \subseteq g(\sum_{u \in u} \mathrm{Im}(u - 1)) = g(\langle b_1, \dots, b_{n-1} \rangle) \neq \mathbb{K}$. $\square$

We are ready to present our main result.

Theorem 11. *Let $C \subseteq \mathbb{F}[\mathbb{K}]$ be a non-trivial affine-invariant code and let $a = a(C)$ and $b = b(C)$, as given in Theorem 6. Then the following assertions hold for every finite group G:*

(a) *C is a left G-code if and only if G is isomorphic to $\mathcal{I}_\alpha$ for some map $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$ satisfying condition (2).*

(b) *C is a G-code if and only if G is isomorphic to $\mathcal{I}_\alpha$ for some map $\alpha : \mathbb{K} \to \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ satisfying condition (2) 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.*

Proof. (a) First assume $G \cong \mathcal{I}_\alpha$ for some $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$ satisfying (2). Note that for every $0 \neq y \in \mathbb{K}$ there exist $(y, \alpha(y)^{-1}) \in \mathcal{I}_\alpha \subseteq S_\mathbb{K}$ such that $(y, \alpha(y)^{-1})(0) = y + \alpha(y)^{-1}(0) = y$. Hence $\mathcal{I}_\alpha$ is a transitive subgroup of $S_\mathbb{K}$. Since $|\mathcal{I}_\alpha| = |\mathbb{K}| = p^m$, the sufficiency follows from Theorem 2.

Conversely, assume that C is a left G-code for some group G, necessarily of order p^m. By Theorem 2 and Corollary 7, we may assume without loss of generality that G is a transitive subgroup of $S_{\mathbb{K}}$ contained in $\mathbb{K} \rtimes \mathcal{G}_{a,b}$. Thus, if (x,g) and (y,h) are two different elements of G with $x, y \in \mathbb{K}$ and $g, h \in \mathcal{G}_{a,b}$ then $x = (x,g)(0) \neq (y,h)(0) = y$, and this shows that the projection of G onto $\mathbb{K}$ is bijective. If $\mathbb{K} \to G, x \mapsto (x, \lambda(x))$, is the inverse of this projection, where $\lambda : \mathbb{K} \to \mathcal{G}_{a,b}$ is a mapping, then $G = \{(x, \lambda(x)) | x \in \mathbb{K}\}$. Define $\alpha(x) := \lambda(x)^{-1}$, for any $x \in \mathbb{K}$. Then $G = \mathcal{I}_\alpha$ and α satisfies condition (2), by Lemma 9.

(b) Let $\alpha : \mathbb{K} \to \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ satisfy the conditions of (b). By part (a) and Theorem 2 and Corollary 7, to prove that C is an $\mathcal{I}_\alpha$-code it is enough to show that $C_{S(\mathbb{K})}(\mathcal{I}_\alpha) \subseteq \mathbb{K} \rtimes \mathcal{G}_{a,b}$. In fact we are going to show that $C_{S(\mathbb{K})}(\mathcal{I}_\alpha) \subseteq \mathbb{K} \rtimes \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$.

For every $x \in \mathbb{K}$ we set $\lambda(x) = \alpha(x)^{-1}$. Since $\mathcal{I}_\alpha$ is a transitive subgroup of $S_{\mathbb{K}}$ of order $|\mathbb{K}| = p^m$, the centralizer of $\mathcal{I}_\alpha$ in $S_{\mathbb{K}}$ is $C_{S_{\mathbb{K}}}(\mathcal{I}_\alpha) = \{f(x) : x \in \mathbb{K}\}$, where

$$f(x)(y) = (y, \lambda(y))(x) = y + \lambda(y)(x).$$

(See [BRS, Lemma 1.1], specialized to $i_0 = 0$.) For every $x, y \in \mathbb{K}$ set

$$\lambda'(x)(y) = y + \lambda(y)(x) - x = y + \beta(y, x).$$

We claim that $\lambda'(x) \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$, for every $x \in \mathbb{K}$. Indeed, on the one hand $\lambda'(x)$ is the composition of $f(x)$ and the translation $y \mapsto y - x$. This shows that $\lambda'(x)$ is bijective. On the other hand, since β is $\mathbb{F}_{p^a}$-linear, if $y, y_1, y_2 \in \mathbb{K}$ and $\gamma \in \mathbb{F}_{p^a}$ then $\lambda'(x)(y_1 + y_2) = y_1 + y_2 + \beta(y_1 + y_2, x) = y_1 + \beta(y_1, x) + y_2 + \beta(y_2, x) = \lambda'(x)(y_1) + \lambda'(x)(y_2)$ and $\lambda'(x)(\gamma y) = \gamma y + \beta(x, \gamma y) = \gamma(y + \beta(x, y)) = \gamma \lambda'(x)(y)$. So $C_{S_{\mathbb{K}}}(\mathcal{I}_\alpha) = \{(x, \lambda'(x)) : x \in \mathbb{K}\} \subseteq \mathbb{K} \rtimes \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ as wanted.

Conversely, assume that C is a G-code. By Theorem 2 and the first part, $G \simeq \mathcal{I}_\alpha$ for a map $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$ satisfying condition (2) and such that $C_{S_{\mathbb{K}}}(\mathcal{I}_\alpha) \subseteq \mathrm{PAut}(C) = \mathbb{K} \rtimes \mathcal{G}_{a,b}$. We set $\lambda(x) = \alpha(x)^{-1}$ and $\beta(x, y) = \lambda(x)(y) - y$. We have to show that β is $\mathbb{F}_{p^a}$-bilinear. As in the previous paragraph the centralizer of $\mathcal{I}_\alpha$ in $S_{\mathbb{K}}$ is formed by the maps $f(x) : y \in \mathbb{K} \mapsto y + \lambda(y)(x)$, with $x \in \mathbb{K}$. So $f(x) \in \mathbb{K} \rtimes \mathcal{G}_{a,b}$, for every $x \in \mathbb{K}$. Since $f(x)(0) = x$, we have $f(x) = (x, \lambda'(x))$, with $\lambda'(x)(y) = y + \lambda(y)(x) - x$. In other words, $C_{S_{\mathbb{K}}}(\mathcal{I}_\alpha) = \mathcal{I}_{\alpha'}$ for $\alpha'(x) = \lambda'(x)^{-1}$. By Lemma 9, α' satisfies condition (2). Then $\mathcal{I}_\alpha$ and $\mathcal{I}_{\alpha'}$ are the centralizer of each other in $S_{\mathbb{K}}$ and their roles and the roles of λ and λ' can be interchanged. Since $\beta(x, y) = \lambda(x)(y) - y = \lambda'(y)(x) - x$, to prove that β is $\mathbb{F}_{p^a}$-bilinear it is enough to show that $\lambda(x), \lambda'(x) \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ for every x. By symmetry, we only prove that $\lambda'(x) \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$, for every $x \in \mathbb{K}$.

Using that $\lambda'(y)$ is additive for every $y \in \mathbb{K}$, we have the following equality for every $x_1, x_2 \in \mathbb{K}$:

$$\begin{aligned} x_1 + x_2 + \lambda(x_1 + x_2)(y) - y &= \lambda'(y)(x_1 + x_2) = \lambda'(y)(x_1) + \lambda'(y)(x_2) \\ &= x_1 + \lambda(x_1)(y) - y + x_2 + \lambda(x_2)(y) - y. \end{aligned}$$

Thus

$$\lambda(x_1 + x_2) + 1 = \lambda(x_1) + \lambda(x_2). \tag{3}$$

Let Q be the subgroup generated by the $\lambda(x)$'s. Since Q is a p-subgroup of $\mathcal{G}_{a,b}$, by Remark 8, $\psi(Q)$ is a p-subgroup of $\mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_{p^b})$. Let $P = Q \cap \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$. We fix a transversal $\mathcal{T}$ of P in Q containing 1, and for every $x \in \mathbb{K}$ we put $\delta(x) = \lambda(x) - t_x$, where t_x is the only element of $\mathcal{T}$ with $\lambda(x){t_x}^{-1} \in P$. Define $J = \sum_{x\in\mathbb{K}} \mathrm{Im}(\delta(x))$. Then

$$J = \sum_{x\in\mathbb{K}} \mathrm{Im}\left[\left(\lambda(x)t_x^{-1} - 1\right) t_x\right] \subseteq \sum_{\rho\in P} \mathrm{Im}(\rho - 1) \neq \mathbb{K}$$

by Lemma 10.

For every $x \in \mathbb{K}$, let $\tau_x = \psi(\lambda(x))$ and $\tau'_x = \psi(\lambda'(x))$, i.e. $\lambda(x)$ is τ_x-semilinear and $\lambda'(x)$ is τ'_x-semilinear. Observe that the condition $\lambda(x)t_x^{-1} \in P$ is equivalent to $\lambda(x){t_x}^{-1} \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ and hence t_x is τ_x-semilinear. Having in mind that $\lambda'(x)(y) = y + \lambda(y)(x) - x$ and $\lambda(x) = \delta(x) + t_x$ we have

$$\lambda'(x)(\gamma y) = \gamma y + \delta(\gamma y)(x) + t_{\gamma y}(x) - x$$

and

$$\lambda'(x)(\gamma y) = \tau'_x(\gamma)\lambda'(x)(y) = \tau'_x(\gamma)\left(y + \delta(y)(x) + t_y(x) - x\right)$$

for any $\gamma \in \mathbb{F}_{p^a}$, and $x, y \in \mathbb{K}$. Therefore

$$(\gamma - \tau'_x(\gamma))y = x - t_{\gamma y}(x) + \tau'_x(\gamma)(t_y(x) - x) + \delta(y)({\tau_y}^{-1}\tau'_x(\gamma)x) - \delta(\gamma y)(x). \quad (4)$$

Recall that the goal is proving that $\lambda'(x) \in \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$, or equivalently that $\tau'_x = 1$, for every $x \in \mathbb{K}$. By means of contradiction assume that this is not the case and fix an element x in $\mathbb{K}$ such that $\tau'_x \neq 1$. We also fix $\gamma \in \mathbb{F}_{p^a}$ with $\tau'_x(\gamma) \neq \gamma$. Observe that the order of τ'_x is a power of p because so is the order of G. Therefore p divides a/b.

For every $y \in \mathbb{K}$ let

$$z_y = x - t_{\gamma y}(x) + \tau'_x(\gamma)(t_y(x) - x)$$

and set

$$Z = Z_{x,\gamma} = \{z_y : y \in \mathbb{K}\}.$$

Using (4), we have

$$\mathbb{K} = \{(\gamma - \tau'_x(\gamma))y : y \in \mathbb{K}\} \subseteq \{z + j : (z, j) \in Z \times J\}.$$

Since the t_y's takes at most a/b different values and x and γ are fixed, $|Z| \leq (a/b)^2$. On the other hand J is a proper subspace of $\mathbb{K}_{\mathbb{F}_{p^a}}$. Thus $p^m \leq |Z \times J| \leq \frac{a^2p^{m-a}}{b^2}$ and so $p^a \leq (a/b)^2 \leq a^2$. This implies that $p = 2$, $b = 1$ and a is either 2 or 4 (recall that p divides a). Then, the index of J in $\mathbb{K}$, as an additive subgroup, is $|Z| = a^2 = 2^a$ and the elements of Z form a set of representatives of $\mathbb{K}$ modulo J. This implies that $\psi \circ \lambda'$ is surjective and hence we may choose x so that τ'_x is the Frobenius automorphism that maps $s \in \mathbb{F}_{2^a}$ to s^2. We also may choose $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Hence $\gamma - \tau'_x(\gamma) = 1$, so that $y \in z_y + J$, by (4). Therefore $y - y' \in J$ if and only if $z_y = z_{y'}$ if and only if $t_y = t_{y'}$ and $t_{\gamma y} = t_{\gamma y'}$, for every

$y, y' \in \mathbb{K}$. Given $u_1, u_2 \in \mathcal{T}$, let $K_{u_1,u_2} = x - u_1(x) + \tau'_x(\gamma)(u_2(x) - x) + J$. Then $\mathbb{K}/J = \{K_{u_1,u_2} : u_1, u_2 \in \mathcal{T}\}$ and $y \in K_{u_1,u_2}$ if and only if $t_y = u_2$ and $t_{\gamma y} = u_1$. Thus $\lambda^{-1}(P) = \{y \in \mathbb{K} : t_y = 1\} = \cup_{u\in\mathcal{T}} K_{u,1}$ and, by (3), $\lambda^{-1}(P)$ is a subgroup of $\mathbb{K}$. Hence $[\mathbb{K} : \lambda^{-1}(P)] = [\lambda^{-1}(P) : J] = a$.

We claim that if $u+v \in \lambda^{-1}(P)$ and $u \notin \lambda^{-1}(P)$ then $\lambda(u) = \lambda(v)$. By means of contradiction assume that $u+v \in \lambda^{-1}(P)$, $u \notin \lambda^{-1}(P)$ and $\lambda(u) \neq \lambda(v)$. Then $\lambda(u + v)$ is $\mathbb{F}_{p^a}$-linear, so that $\lambda(u) + \lambda(v)$ is also $\mathbb{F}_{p^a}$-linear, by (3). Thus for every $\zeta \in \mathbb{F}_{p^a}$ and $z \in \mathbb{K}$ we have

$$(\lambda(u) + \lambda(v))(\zeta z) = \zeta\lambda(u)(z) + \zeta\lambda(v)(z)$$

and

$$(\lambda(u) + \lambda(v))(\zeta z) = \tau_u(\zeta)\lambda(u)(z) + \tau_v(\zeta)\lambda(v)(z).$$

Therefore

$$(\zeta + \tau_u(\zeta))\lambda(u)(z) = (\zeta + \tau_v(\zeta))\lambda(v)(z). \tag{5}$$

From this equality and the assumption $\lambda(u) \neq \lambda(v)$ one deduces that $\tau_u \neq \tau_v$ and the fixed fields of τ_u and τ_v coincides. Therefore $a = 4$ and τ_u and τ_v are the two generators of $\text{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$. So one may assume that $\tau_u(\zeta) = \zeta^2$ and $\tau_v(\zeta) = \zeta^8$, for every $\zeta \in \mathbb{F}_{16}$. Now specializing (5) to $\zeta = \gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$ one deduces that $\lambda(u) = \lambda(v)$ because $\gamma + \tau_u(\gamma) = \gamma + \tau_v(\gamma) = 1$. This proves the claim.

By the previous paragraph $|P|(a - 1) = |Q \setminus P| = [\mathbb{K} : \lambda^{-1}(P)] - 1 = a - 1$ and hence $P = 1$. Therefore $J = 0$ and $m = a$, because J has codimension 1 as an $\mathbb{F}_{p^a}$-subspace of $\mathbb{K}$. If $a = 2$ then C is trivial as affine-invariant code, by Example 5. Here we use that $b = 1$, hence the defining set of C is a union of 2-cyclotomic classes modulo 3. Thus $a = 4$ and so $\mathcal{G}_{a,b} = \mathbb{F}_{16}^* \rtimes \text{Gal}\,(\mathbb{F}_{16}/\mathbb{F}_2)$. Let $\sigma \in \text{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$ be the Frobenius automorphism. Since $\psi \circ \lambda$ is surjective there exist $u, v \in \mathbb{K}$ such that $\lambda(u) = (\gamma_1, \sigma)$ and $\lambda(v) = (\gamma_2, \sigma^2)$, for some $\gamma_i \in \mathbb{F}_{16}^*$, $i = 1, 2$. Since $P = 1$ we have that $\lambda(u + v) = (\gamma_3, \sigma^3)$ for some $\gamma_3 \in \mathbb{F}_{16}$. Using (3) we conclude that every element of $\mathbb{F}_{16}$ is a root of the polynomial $p(X) = X + \gamma_1 X^2 + \gamma_2 X^4 + \gamma_3 X^8$, which yields the desired contradiction. □

Corollary 12. *Let C be a non-trivial affine-invariant code of length p^m and G be a finite group.*

(a) If $a(C) = m$, $m/b(C)$ is coprime with p and C is a left G-code then G is isomorphic to $(\mathbb{K}, +)$.

(b) If $a(C) = m$ and C is a G-code then G is isomorphic to to $(\mathbb{K}, +)$.

Proof. If $a(C) = m$ then $\text{GL}(\mathbb{K}_{\mathbb{F}_{p^a}}) = \text{GL}(\mathbb{K}_{\mathbb{K}}) \simeq \mathbb{K}^*$, a group of order coprime with p. Therefore, if $\alpha : \mathbb{K} \to \text{GL}(\mathbb{K}_{\mathbb{K}})$ satisfies condition (2) then $\alpha(x) = 1$ for every $x \in \mathbb{K}$. Now (b) follows from statement (b) of Theorem 11. The proof of (a) is similar using statement (a) of Theorem 11 and the fact that the order of $\mathcal{G}_{a,b}$ is $|\text{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})|a/b$, which is coprime with p under the assumptions of (a). □

Remark 13. For every $\alpha : \mathbb{K} \to \mathcal{G}_{a,b}$ satisfying (2), consider $\mathcal{I}_\alpha$ acting on $\mathbb{K}$ by conjugation inside $\mathbb{K} \rtimes \mathcal{G}_{a,b}$. Then the map $\pi : (x, \alpha(x)^{-1}) \mapsto x$ is a bijective 1-cocycle, i.e. $\pi(gh) = \pi(g) + g(\pi(h))$, for every $g, h \in \mathcal{I}_\alpha$. Groups acting on abelian groups with bijective 1-cocycles have received the attention of several authors by its connections with the set-theoretical solutions of the Yang-Baxter equation [CJR, ESS].

3. A class of group code structures

Theorem 11 describes all the (left) group code structures of a non-trivial affine-invariant code. The most obvious one is obtained for α the trivial map $x \mapsto 1$. In this case $\mathcal{I}_\alpha \simeq (\mathbb{K}, +)$ and this yields the group code structure given after Definition 3. In this section we exhibit a family of other group code structures of a fixed affine-invariant code C of length p^m under the assumption that $a(C) \neq m$.

We keep the notation of the previous sections, that is $\mathbb{F} = \mathbb{F}_{p^r}$ and $\mathbb{K} = \mathbb{F}_{p^m}$. Let C be a non-trivial affine-invariant code inside $\mathbb{F}[\mathbb{K}]$ and set $a = a(C)$ and $b = b(C)$. Let f and χ be as follows

$$\begin{array}{ll} \cdot & f : \mathbb{K} \to \mathbb{K} \text{ is an } \mathbb{F}_{p^a}\text{-linear map,} \\ \cdot & \chi : \mathbb{K} \to \mathbb{F}_{p^a} \text{ is an additive map (i.e. } \mathbb{F}_p\text{-linear),} \\ \cdot & \chi \neq 0 \neq f, \quad f^2 = 0 \quad \text{and} \quad \chi \circ f = 0. \end{array} \tag{6}$$

Observe that there are χ and f satisfying (6) if and only if $a < m$.

Consider the map

$$\begin{array}{rcl} \alpha = \alpha_{\chi,f} : \mathbb{K} & \longrightarrow & \mathcal{G}_{a,b} \\ x & \mapsto & 1 + \chi(x) \cdot f \end{array}$$

For $x, y \in \mathbb{K}$

$$\alpha\left(\alpha(y)(x)\right) = 1 + \left[\chi(x) + \chi\left(\chi(y) \cdot f(x)\right)\right] \cdot f = 1 + \chi(x) \cdot f = \alpha(x)$$

and hence

$$\begin{array}{rcl} \alpha\left(\alpha(y)(x)\right)\alpha(y) & = & \alpha(x)\alpha(y) = \left(1 + \chi(x) \cdot f\right)\left(1 + \chi(y) \cdot f\right) \\ & = & 1 + \chi(y) \cdot f + \chi(x) \cdot f = \alpha(x + y). \end{array}$$

Therefore α satisfies condition (2). Since $\alpha(x)^{-1} = 1 - \chi(x)f$, by Theorem 11, C is a left $\mathcal{I}_{\chi,f}$-code, where

$$\mathcal{I}_{\chi,f} = \{(x, 1 - \chi(x)f) : x \in \mathbb{K}\}.$$

Moreover, using the notation of Theorem 11, we have $\beta(x, y) = \alpha(x)^{-1}(y) - y = -\chi(x)f(y)$ and hence, if χ is $\mathbb{F}_{p^a}$-linear then C is $\mathcal{I}_{\chi,f}$-code.

Our next goal consist in describing the structure of $\mathcal{I}_{\chi,f}$. For that we need to introduce some group constructions from some vector spaces.

Notation 14. *Given an $\mathbb{F}_{p^a}$-vector space V and linear map $\mu : V \to \mathbb{F}_{p^a}$, we define the group $V_\mu = V \times V$ with the following product:*

$$(v_1, w_1)(v_2, w_2) = (v_1 + v_2 - \mu(w_1)w_2, w_1 + w_2),$$

for $v_1, w_1, v_2, w_2 \in V$.

If U is an additive subgroup of $\mathbb{F}_{p^a}$ then we consider the following action on V_μ:

$$u(v, w) = (v - uw, w), \quad (u \in U, v, w \in V).$$

The corresponding semidirect product is denoted by $V_\mu \rtimes U$ and its elements by $(v_1, v_2; u)$, with $v_1, v_2 \in V$ and $u \in U$.

Lemma 15. If (x_1, ρ_1) and (x_2, ρ_2) belong to $\mathbb{K} \rtimes \mathcal{G}_{a,b}$ then

$$(x_1, \rho_1)(x_2, \rho_2) = (x_2, \rho_2)(x_1, \rho_1) \quad \Leftrightarrow \quad x_1 + \rho_1(x_2) = x_2 + \rho_2(x_1) \text{ and } \rho_1\rho_2 = \rho_2\rho_1.$$

Proof. Straightforward. $\square$

Theorem 16. *Let χ and f be as in (6) and consider $\mathbb{K}$ as an $\mathbb{F}_p$-vector space. Then*

(a) *$\mathcal{I}_{\chi,f}$ is abelian if and only if χ is $\mathbb{F}_{p^a}$-linear and $\ker(\chi) \subseteq \ker(f)$. In this case $\ker(\chi) = \ker(f)$.*

(b) *If $\mathcal{I}_{\chi,f}$ is non-abelian then the center of $\mathcal{I}_{\chi,f}$ is $\{(z, 1) : z \in \ker(f) \cap \ker(\chi)\}$.*

(c) *If p is odd then $\mathcal{I}_{\chi,f}$ has exponent p. If $p = 2$ then the exponent of $\mathcal{I}_{\chi,f}$ is 4.*

(d) *Let $V = \mathrm{Im}(f)$, Z a complement of V in $\ker(\chi) \cap \ker(f)$ and U a complement of $\ker(\chi) \cap \ker(f)$ in $\ker(f)$. Then*

$$\mathcal{I}_{\chi,f} \simeq Z \times (V_{\chi\circ g} \rtimes \chi(U)).$$

where $g : V \to \mathbb{K}$ is an additive map satisfying $f \circ g = 1_V$ and $gf(\ker(\chi)) \subseteq \ker(\chi)$.

Proof. (a) Using Lemma 15, it is easy to see that $(x, \alpha(x)^{-1})$ and $(y, \alpha(y)^{-1})$ commute if and only if $\chi(x)f(y) = \chi(y)f(x)$. Using this and the assumption $\chi \neq 0$, one easily follows that if $\mathcal{I}_{\chi,f}$ is abelian then $\ker(\chi) \subseteq \ker(f)$. Furthermore, if $\gamma \in \mathbb{F}_{p^a}$ and $x, y \in \mathbb{K}$ then $\chi(\gamma y)f(x) = \chi(x)f(\gamma y) = \gamma\chi(x)f(y) = \gamma\chi(y)f(x)$. Using that $f \neq 0$ one deduces that χ is $\mathbb{F}_{p^a}$-linear. Therefore, $\ker(\chi) = \ker(f)$ because $\ker(\chi)$ has codimension 1 in $\mathbb{K}_{\mathbb{F}_{p^a}}$ and $\ker(f)$ is a proper subspace of $\mathbb{K}_{\mathbb{F}_{p^a}}$.

Conversely, assume that χ is $\mathbb{F}_{p^a}$-linear and $\ker(\chi) \subseteq \ker(f)$. Then the equality holds as above. Let $v \in \mathbb{K} \setminus \ker(\chi)$ and for every $x, y \in \mathbb{K}$ write $x = w_x + \beta_x v$ and $y = w_y + \beta_y v$ with $w_x, w_y \in \ker(\chi)$ and $\beta_x, \beta_y \in \mathbb{F}_{p^a}$. Then $\chi(x)f(y) = \beta_x\beta_y\chi(v)f(v) = \chi(y)f(x)$ and hence $\left(x, \alpha(x)^{-1}\right)$ and $\left(y, \alpha(y)^{-1}\right)$ commute.

(b) Assume that $\mathcal{I}_{\chi,f}$ is non-abelian. By Lemma 15, $(z, \alpha(z)^{-1})$ belongs to the center of $\mathcal{I}_{\chi,f}$ if and only if $\chi(x)f(z) = \chi(z)f(x)$, for every $x \in \mathbb{K}$. In particular, if $z \in \ker(f) \cap \ker(\chi)$ then $(z, \alpha(z)^{-1}) = (z, 1)$ belongs to the center of $\mathcal{I}_{\chi,f}$. Conversely, let $v = (z, \alpha(z)^{-1})$ belong to the center of $\mathcal{I}_{\chi,f}$. If $x_1 \in \mathbb{K} \setminus \ker(\chi)$ and $x_2 \in \mathbb{K} \setminus \ker(f)$ then from the equalities $\chi(x_1)f(z) = \chi(z)f(x_1)$ and $\chi(x_2)f(z) = \chi(z)f(x_2)$ one deduces that $z \in \ker(\chi)$ if and only if $z \in \ker(f)$. So it is enough to show that $f(z) = 0$ or $\chi(z) = 0$. By (a), either χ is not $\mathbb{F}_{p^a}$-linear or there is $y \in \ker(\chi) \setminus \ker(f)$. In the latter case, $0 = \chi(y)f(z) = \chi(z)f(y)$ and hence $\chi(z) = 0$. In the former case, there is $\gamma \in \mathbb{F}_{p^a}$ and $x \in \mathbb{K}$ with $\chi(\gamma x) \neq \gamma\chi(x)$. However, $\chi(\gamma x)f(z) = \chi(z)f(\gamma x) = \gamma\chi(z)f(x) = \gamma\chi(x)f(z)$ and hence $f(z) = 0$.

(c) Let $x \in \mathbb{K}$ and $v = (x, \alpha(x)^{-1}) = (x, 1-\chi(x)f) \in \mathcal{I}_{\chi,f}$. A straightforward calculation shows that

$$v^p = \left(-\sum_{i=0}^{p-1} i\chi(x)f(x), 1\right) = \left(\frac{p(p-1)}{2}\chi(x)f(x), 1\right).$$

Hence, if p is odd then $v^p = (0, 1)$ and if $p = 2$ then $v^2 \in \mathbb{K}$, so that $v^4 = 1$. By means of contradiction, assume that $p = 2$ and the exponent of $\mathcal{I}_{\chi,f}$ is 2. Then $\chi(x)f(x) = 0$, for every $x \in \mathbb{K}$. In particular, $f(x) = 0$ for every $x \in \mathbb{K} \setminus \ker(\chi)$. If $w \in \ker(\chi)$ and $x \in \mathbb{K} \setminus \ker(\chi)$ then $f(w) = f(x + w) - f(x) = 0$. This shows that $f = 0$, a contradiction.

(d) The existence of the map g follows by standard linear algebra arguments.

Let $W = g(f(\ker(\chi)))$ and $W' = g(H)$, where H is a complement of $f(\ker(\chi))$ in V. Clearly the restriction maps $f : W \oplus W' \to V$ and $g : V \to W \oplus W'$ are mutually inverse to each other.

Since $f \circ g = 1_V$, we have $W \cap \ker(f) = 0$. Furthermore, $\dim(\ker(\chi)) = \dim(\ker(\chi) \cap \ker(f)) + \dim f(\ker(\chi)) = \dim(\ker(\chi) \cap \ker(f)) + \dim(W)$. This shows that $\ker(\chi) = W \oplus (\ker(\chi) \cap \ker(f))$.

We claim that $\mathbb{K} = W' \oplus (\ker(\chi) + \ker(f))$. Indeed, if $x \in W' \cap (\ker(\chi) + \ker(f))$ then $x = u + v = g(h)$ for some $u \in \ker(\chi)$, $v \in \ker(f)$ and $h \in H$. So, $f(x) = f(u) = fg(h) = h$, and then $h \in f\left(\ker(\chi)\right) \cap H = \{0\}$. Thus $x = 0$.

Moreover,

$$\begin{aligned}
\dim \mathbb{K} &= \dim(V) + \dim(\ker(f)) \\
&= \dim(V) + \dim(\ker(f) + \ker(\chi)) + \\
&\quad \dim(\ker(\chi) \cap \ker(f)) - \dim(\ker(\chi)) \\
&= \dim(V) - \dim(f(\ker(\chi))) + \dim(\ker(f) + \ker(\chi)) \\
&= \dim(H) + \dim(\ker(f) + \ker(\chi)) \\
&= \dim(W') + \dim(\ker(f) + \ker(\chi)).
\end{aligned}$$

This proves the claim.

Then $\mathbb{K} = Z \oplus V \oplus W \oplus W' \oplus U$ and the product in $\mathcal{I}_{\chi,f}$ is given by

$$(x_1, 1-\chi(x_1)f)(x_2, 1-\chi(x_2)f) = (x_1+x_2-\chi(w_1'+u_1)f(w_2+w_2'), 1-\chi(x_1+x_2)f)$$

for $x_1 = z_1 + v_1 + w_1 + w_1' + u_1$ and $x_2 = z_2 + v_2 + w_2 + w_2' + u_2$, with $z_i \in Z, v_i \in V, w_i \in W, w_i' \in W'$ and $u_i \in U$. We conclude that the map $\mathcal{I}_{\chi,f} \to Z \times (V_{\chi\circ g} \rtimes \chi(U))$ given by

$$(z + v + w + w' + u, 1 - \chi(w' + u)f) \quad \mapsto \quad (z, (v, f(w + w'); \chi(u)))$$

is a bijection. The fact that this map is a group homomorphism follows by straightforward computations. □

As it was mentioned above, if χ is $\mathbb{F}_{p^a}$-linear then C is $\mathcal{I}_{\chi,f}$-code. In this case one can obtain a more friendly description of $\mathcal{I}_{\chi,f}$.

Let $\mathcal{F}_a = (\mathbb{F}_{p^a})_1$, i.e. $\mathcal{F}_a = \mathbb{F}_{p^a} \times \mathbb{F}_{p^a}$ with the product $(x_1, y_1)(x_2, y_2) = (x_1 + x_2 - y_1 y_2, y_1 + y_2)$ (see Notation 14). For an $\mathbb{F}_{p^a}$-vector space V consider the following action of $\mathcal{F}_a$ on $V \times V$:

$$(x, y) \cdot (u, v) = (u - yv, v), \quad (x, y \in \mathbb{F}_{p^a}, u, v \in V). \tag{7}$$

Let $(V \times V) \rtimes \mathcal{F}_a$ denote the corresponding semidirect product and denote its elements with $(v_1, v_2; x_1, x_2)$ for $v_i \in V$ and $x_i \in \mathbb{F}_{p^a}$.

Corollary 17. *Let χ and f be as in (6) and assume that χ is $\mathbb{F}_{p^a}$-linear. Let u denote the rank of f. Then we have:*

(a) *If $\ker(\chi) = \ker(f)$ and p is odd then $\mathcal{I}_{\chi,f}$ is p-elementary abelian.*
(b) *If $\ker(\chi) = \ker(f)$ and $p = 2$ then $\mathcal{I}_{\chi,f}$ is a direct product of $m - 2a$ copies of groups of order 2 and a copies of cyclic groups of order 4.*
(c) *If $\ker(f) \not\subseteq \ker(\chi)$ then $\mathcal{I}_{\chi,f}$ is isomorphic to the group*

$$\mathbb{F}_{p^a}^{\frac{m}{a}-2u-1} \times \left(\left(\mathbb{F}_{p^a}^u \times \mathbb{F}_{p^a}^u \right) \rtimes \mathbb{F}_{p^a} \right),$$

where the action is that given in Notation 14 with $V_0 = \mathbb{F}_{p^a}^u \times \mathbb{F}_{p^a}^u$ and $U = \mathbb{F}_{p^a}$.

(d) *If* $\ker(f) \subsetneq \ker(\chi)$ *then* $\mathcal{I}_{\chi,f}$ *is isomorphic to the group*

$$\mathbb{F}_{p^a}^{\frac{m}{a}-2u} \times \left(\left(\mathbb{F}_{p^a}^{u-1} \times \mathbb{F}_{p^a}^{u-1} \right) \rtimes \mathcal{F}_a \right).$$

Proof. (a) and (b). Assume that $\ker(\chi) = \ker(f)$. Then $\mathcal{I}_{\chi,f}$ is abelian, by statement (a) of Theorem 16. If p is odd then $\mathcal{I}_{\chi,f}$ is elementary abelian by statement (c) of the same proposition. Suppose that $p = 2$. Then $\mathcal{I}_{\chi,f}$ is a direct product of cyclic groups of order 2 or 4, by statement (d) of Theorem 16. If $x \in \mathbb{K}$ then $v = (x, 1 - \chi(x)f)$ has order ≤ 2 if and only if $(0,1) = v^2 = (-\chi(x)f(x), 1)$ if and only if $x \in \ker(\chi)$. Thus, if $\mathcal{I}_{\chi,f}$ is a direct product of k copies of groups of order 2 and l copies of cyclic groups of order 4 then $k + l = a \dim_{\mathbb{F}_{2^a}}(\ker(\chi)) = m - a$ and $m = k + 2l$. Solving this two equations we deduce that $k = m - 2a$ and $l = a$.

In the remainder of the proof we use the notation of Theorem 16 and its proof. So $\mathcal{I}_{\chi,f} \simeq Z \times (V_{\chi\circ g} \rtimes \chi(U))$. Notice that Z, V, U, W and W' can be selected as $\mathbb{F}_{p^a}$-subspaces of $\mathbb{K}$. Since $\ker(\chi)$ has codimension 1 in $\mathbb{K}_{\mathbb{F}_{p^a}}$ and $U \oplus W'$ is a complement of $\ker(\chi)$ in $\mathbb{K}$, either $U = 0$ or $W' = 0$.

(c) Suppose that $\ker(f) \not\subseteq \ker(\chi)$. Then $W' = 0$, $\chi(U) = \mathbb{F}_{p^a}$ and $\chi \circ g = 0$. By statement (d) of Theorem 16, $\mathcal{I}_{\chi,f} \simeq Z \times ((V \times V) \rtimes \mathbb{F}_{p^a})$. Furthermore $V \simeq \mathbb{F}_{p^a}^u$ and $Z \simeq \mathbb{F}_{p^a}^{\frac{m}{a}-2u-1}$.

(d) Assume now that $\ker(f) \subsetneq \ker(\chi)$. Then $U = 0$ and W and W' are $\mathbb{F}_{p^a}$-subspaces of $\mathbb{K}$ of dimensions $u - 1$ and 1 respectively. Using this one deduces that $X = \{(v_1, v_2) : v_1, v_2 \in f(W)\}$ and $X' = \{(v_1', v_2') : v_1', v_2' \in f(W')\}$ are subgroups of $V_{\chi\circ g}$ with $X \cap X' = 1$ and X normal in $V_{\chi\circ g}$. Then $V_{\chi\circ g} = X \rtimes X'$, so that $\mathcal{I}_{\chi,f} \simeq Z \times (X \rtimes X')$. Moreover $X = f(W) \times f(W)$, because $\chi \circ g$ vanishes on $f(W)$. On the other hand, the map $\phi : X' \to \mathcal{F}_a$, given by $\phi((v_1, v_2)) = (\chi g(v_1), \chi g(v_2))$, is a group isomorphism. Hence the action of X' on X by conjugation yields and action of $\mathcal{F}_a$ on X via ϕ. It is easy to see that this action is precisely the action defined in (7). So $\mathcal{I}_{\chi,f} \simeq Z \times ((f(W) \times f(W)) \rtimes \mathcal{F}_a)$. Finally, $Z \simeq \mathbb{F}_{p^a}^{\frac{m}{a}-2u}$ and $f(W) \simeq \mathbb{F}_{p^a}^{u-1}$. □

In the remainder of the section we fix a non-trivial affine-invariant code C with $a = a(C) \neq m$ and show how to obtain $\mathbb{F}_{p^a}$-linear maps χ and f satisfying (6) and yielding all the cases of Corollary 17. For that we start with an arbitrary non-zero linear form χ of $\mathbb{K}_{\mathbb{F}_{p^a}}$ and construct an endomorphism f of $\mathbb{K}_{\mathbb{F}_{p^a}}$ satisfying the conditions of (6). The existence of the endomorphism f in all the cases is clear.

To obtain an abelian group code structure on C with a given non-zero linear form χ we just need an endomorphism f of $\mathbb{K}_{\mathbb{F}_{p^a}}$ with $\ker(f) = \ker(\chi)$ and $0 \neq f(v) \in \ker(\chi)$ for a given $v \in \mathbb{K} \setminus \ker(\chi)$.

If $m > 2a$ then it is always possible to obtain a non-abelian group code structure on C. In fact, for every positive integer u with $2u \le \frac{m}{a} - 1$ there are endomorphisms f_1 and f_2 of $\mathbb{K}_{\mathbb{F}_{p^a}}$, satisfying the conditions of (6) such that $\mathcal{I}_{\chi,f_1}$ and $\mathcal{I}_{\chi,f_2}$ are as in statements (c) and (d) of Corollary 17 respectively. Indeed, in this case, the dimension of $\ker(\chi)$ as $\mathbb{F}_{p^a}$-vector space is $\frac{m}{a} - 1 \ge 2u$. Thus we have $\mathbb{K} = \ker(\chi) \oplus X$ and $\ker(\chi) = Z_1 \oplus V \oplus W_1 = Z_2 \oplus V \oplus W_2$, for $\mathbb{F}_{p^a}$-subspaces X, Z_1, Z_2, V, W_1 and W_2 of $\mathbb{K}$, where $\dim_{\mathbb{F}_{p^a}}(X) = 1$, $\dim_{\mathbb{F}_{p^a}}(V) = \dim_{\mathbb{F}_{p^a}}(W_1) = u$ and $\dim_{\mathbb{F}_{p^a}}(W_2) = u - 1$. Then we can construct the desired endomorphisms f_1 and f_2 of $\mathbb{K}$ by setting $f_i(W_i \oplus X) = V$ for $i = 1, 2$, $\ker(f_1) = Z_1 \oplus V \oplus X$ and $\ker(f_2) = Z_2 \oplus V$. Observe that, in case (d), we need $u > 1$. On the other hand, if $u = 1$ then $\ker(f_2) = \ker(\chi)$ and hence $\mathcal{I}_{\chi,f_2}$ is abelian.

However if $m = 2a$ then it is not possible to obtain a non-abelian group code structure by the following result.

Corollary 18. *Let C be a non-trivial affine-invariant code of length p^m. Then the following conditions are equivalent.*

(a) C is a G-code for some non-abelian group G.

(b) $2a(C) < m$.

Furthermore, if $2a(C) \ge m$ and C is a G-code then either $G \simeq \mathbb{K}$ or $p = 2$ and G is a direct product of a copies of cyclic groups of order 4.

Proof. (b) implies (a) is a consequence of the arguments given before the corollary.

(a) implies (b) Let $a = a(C)$ and assume that $2a \ge m$, so that m is either a or $2a$ and G is a group such that C is a G-code. By Theorem 11, G is isomorphic to $\mathcal{I}_\alpha$, for $\alpha : \mathbb{K} \to \mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$ a map satisfying condition (2) such that $\beta(x, y) = \alpha(x)^{-1}(y) - y$ is $\mathbb{F}_{p^a}$-bilinear. If $\alpha(x) = 1$ for every x then $G \simeq \mathbb{K}$ and so G is abelian as wanted. This happens, for example, if $m = a$ because in this case the order of $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}}) = \mathbb{K}^*$ is coprime with p and the order of $\alpha(x)$ is a p-th power. Assume now that $\alpha(x) \ne 1$ for some $x \in \mathbb{K}$. Then $m = 2a$ and, by Sylow's Theorem, we may assume that $\alpha(x)$ belongs to a prescribed Sylow p-subgroup of $\mathrm{GL}(\mathbb{K}_{\mathbb{F}_{p^a}})$. For example, we may fix a basis u_1, u_2 of $\mathbb{K}_{\mathbb{F}_{p^a}}$ and assume that $\alpha(x)(u_1) = u_1$ and $\alpha(x)(u_2) - u_2 = \chi(x) u_1$ for some $\chi(x) \in \mathbb{F}_{p^a}$ (see the proof of Lemma 10). Let f be the $\mathbb{F}_{p^a}$-linear endomorphism of $\mathbb{K}$ given by $f(u_1) = 0$ and $f(u_2) = u_1$. Then $\alpha(x)^{-1} = 1 - \chi(x) f$ and $\beta(x, y) = -\chi(x) f(y)$. Since β is $\mathbb{F}_{p^a}$-bilinear, χ is $\mathbb{F}_{p^a}$-linear. Furthermore,

$$1 + (\chi(x) + \chi(y)) f = 1 + \chi(x + y) f = \alpha(x + y) = \alpha(\alpha(y)(x))\alpha(y) =$$
$$(1 + \chi(x + \chi(y) f(x)) f)(1 + \chi(y) f) = 1 + (\chi(x) + \chi(y)) f + \chi(y)\chi(f(x)) f$$

and we conclude that $\chi \circ f = 0$, i.e. χ and f satisfy the conditions of (6) and $G \simeq \mathcal{I}_{\chi,f}$. Moreover $\dim_{\mathbb{F}_{p^a}}(\ker(\chi)) = 1$ and so $\ker(f) = f(\mathbb{K}) = \mathbb{F}_{p^a} v_1 = \ker(\chi)$. We conclude that $\mathcal{I}_{\chi,f}$ is abelian, by statement (a) of Theorem 16.

Finally, the last statement is a consequence of statements (a) and (b) of Corollary 17. $\square$

[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*, Des. Codes, Crypto. 51 (2009), 289–300.

[CJR] F. Cedó, E. Jespers and Á. del Río, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. to appear.

[Ch] P. Charpin, *Open problems on cyclic codes*, in *Handbook of Coding Theory* Vol. I. 963–1063. Edited by V. S. Pless, W. C. Huffman and R. A. Brualdi. North-Holland, Amsterdam, 1998.

[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.

[ESS] P. Etingof, T. Schedler and A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. 100 (1999), 169–209.

[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, 30100 Murcia. Spain.
email: josejoaquin.bernal@um.es, adelrio@um.es, jsimon@um.es