AN INTRINSICAL DESCRIPTION OF GROUP CODES

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

Abstract. A (left) group code of length n is a linear code which is the image of a (left) ideal of a group algebra via an isomorphism $\mathbb{F}G \to \mathbb{F}^n$ which maps G to the standard basis of $\mathbb{F}^n$. Many classical linear codes have been shown to be group codes. In this paper we obtain a criterion to decide when a linear code is a group code in terms of its intrinsical properties in the ambient space $\mathbb{F}^n$, which does not assume an "a priori" group algebra structure on $\mathbb{F}^n$. As an application we provide a family of groups (including metacyclic groups) for which every two-sided group code is an abelian group code.

It is well known that Reed-Solomon codes are cyclic and its parity check extensions are elementary abelian group codes. These two classes of codes are included in the class of Cauchy codes. Using our criterion we classify the Cauchy codes of some lengths which are left group codes and the possible group code structures on these codes.

In this paper $\mathbb{F} = \mathbb{F}_q$ denotes the field with q elements where q is a power of a prime p. We consider $\mathbb{F}$ as the alphabet of linear codes of length n and so the ambient space is $\mathbb{F}^n$, the n-dimensional vector space. The standard basis of $\mathbb{F}^n$ is denoted by $E = \{e_1, \dots, e_n\}$. For any group G, we denote by $\mathbb{F}G$ the group algebra over G with coefficients in $\mathbb{F}$.

Recall that a linear code $C \subseteq \mathbb{F}^n$ is said to be cyclic if and only if C is closed under cyclic permutations, that is, $(x_1, \dots, x_n) \in C$ implies $(x_2, \dots, x_n, x_1) \in C$. For $C_n = \langle g \rangle$, the cyclic group of order n, the bijection $\pi : E \to C_n$ given by $\pi(e_i) = g^{i-1}$ extends to an isomorphism of vector spaces $\phi : \mathbb{F}^n \to \mathbb{F}C_n$ and the cyclic codes in $\mathbb{F}^n$ are the subsets C of $\mathbb{F}^n$ such that $\phi(C)$ is an ideal of $\mathbb{F}C_n$.

If G is a group of order n and $C \subseteq \mathbb{F}^n$ is a linear code then we say that C is a *left G-code* (respectively, a *right G-code*; a *G-code*) if there is a 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 a left ideal (respectively, a right ideal; a two-sided ideal) of $\mathbb{F}G$. A *left group code* (respectively, *group code*) is a linear code which is a left G-code (respectively, a G-code) for some group G. A (left) cyclic group code (respectively, abelian group code, solvable group code, etc.) is a linear code which is (left) G-code for some cyclic group (respectively, abelian group, solvable group, etc.). In general, if $\mathcal{G}$ is a class of groups then we say that a linear code C is a (left) $\mathcal{G}$ group code if and only if C is a (left) G-code for some G in $\mathcal{G}$.

Note that the cyclic codes of length n are C_n-codes. However, not every C_n-code is a cyclic code. For example, the linear code $\{(a, a, b, b) : a, b \in \mathbb{F}\}$ is not a cyclic code but it is a C_4-code via the map $\phi : \{e_1, \dots, e_4\} \to C_4$ given by $\phi(e_1) = 1$, $\phi(e_2) = g^2$, $\phi(e_3) = g$ and $\phi(e_4) = g^3$. If one fixes a bijection $\phi : E \to G$ to induce an isomorphism $\phi : \mathbb{F}^n \to \mathbb{F}G$ then the (left) G-codes are precisely those codes of $\mathbb{F}^n$ which are permutation equivalent to codes of the form $\phi^{-1}(I)$,

for I running on the (left) ideals of $\mathbb{F}G$. In particular, the cyclic group codes are the codes which are permutation equivalent to cyclic codes.

The aim of this paper is to give a criterion to decide if a linear code is a group code in terms of its intrinsical properties in the ambient space, which has not an "a priori" group algebra structure. More precisely we prove that a subspace C of $\mathbb{F}^n$ is a left group code if and only if $\mathrm{PAut}(C)$, the group of permutation automorphisms of C, contains a regular subgroup. Moreover, C is a group code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup H such that $C_{S_n}(H) \subseteq \mathrm{PAut}(C)$. Using this we prove that if $G = AB$, for A and B two abelian subgroups of G then every G-code is also an abelian group code. This extends a result of Sabin and Lomonaco [4]. We present some examples showing that this cannot be extended to left group codes. Finally, we study the class of Cauchy codes. This is a class of MDS codes introduced in [1], (see also [2]) which includes the class of generalized Reed-Solomon codes. We describe the possible left group code structures of some families of Cauchy codes.

1. Characterizing group codes

In this section we give necessary and sufficient conditions for a subspace C of $\mathbb{F}^n$ to be a (left) group code in terms of the group of permutation automorphisms of C. For this result we do not need to assume that $\mathbb{F}$ is finite.

Let S_n denote the group of permutations on n symbols, that is the group of bijections of $\mathbb{N}_n = \{1, \dots, n\}$ onto itself. Recall that a subgroup G of S_n is *regular* if and only if it is transitive and has order n (equivalently, $|G| = n$ and $\sigma(x) \neq x$ for every $1 \neq \sigma \in G$ and $x \in \mathbb{N}_n$). We consider S_n acting by linear transformations on $\mathbb{F}^n$ via the rule:

$$\sigma(e_i) = e_{\sigma(i)} \quad (\sigma \in S_n, i \in \mathbb{N}_n).$$

Two linear codes C and C' are permutation equivalent if $\sigma(C) = C'$ for some $\sigma \in S_n$. Following [2], we denote the group of permutation automorphisms of a linear code C by

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

For a group G, let $Z(G)$ denote the center of G and let $C_G(H)$ denote the centralizer of H in G, for each subgroup H of G.

We will need the following lemma which is possibly well known.

Lemma 1.1. *Let H be a regular subgroup of S_n and fix an element $i_0 \in \mathbb{N}_n$. Let $\psi : H \to \mathbb{N}_n$ be the bijection given by $\psi(h) = h(i_0)$. Then there is an anti-isomorphism $\sigma : H \to C_{S_n}(H)$, mapping $h \in H$ to σ_h, where*

$$\sigma_h(i) = \psi^{-1}(i)\,(h(i_0)) \quad (i \in \mathbb{N}_n).$$

Moreover $\sigma_h = h$ for every $h \in Z(H)$ and so $Z(H) = Z(C_{S_n}(H))$.

Proof. It is clear that ψ is a bijection, since H is regular. Furthermore $\psi^{-1}(i)(i_0) = i$, for every $i \in \mathbb{N}_n$ and $\psi^{-1}(h(i_0)) = h$, for $h \in H$. Therefore, if $h, k \in H$ then

$$\sigma_h k(i) = \sigma_h\left(k\left(\psi^{-1}(i)(i_0)\right)\right) = \psi^{-1}\left(\left[k\psi^{-1}(i)\right](i_0)\right)(h(i_0)) = \left[k\psi^{-1}(i)\right](h(i_0)) = k\sigma_h(i).$$

This shows that σ maps H into $C_{S_n}(H)$.

Now we prove that σ is an anti-homomorphism. If $h, k \in H$ and $i \in \mathbb{N}_n$ then

$$\sigma_{hk}(i) = \psi^{-1}(i)hk(i_0) = \psi^{-1}\left(\psi^{-1}(i)h(i_0)\right)k(i_0) = \sigma_k\left(\psi^{-1}(i)h(i_0)\right) = \sigma_k(\sigma_h(i)).$$

If $\sigma_h = 1$ then $\psi^{-1}(i)(i_0) = i = \sigma_h(i) = \psi^{-1}(i)h(i_0)$, for every $i \in \mathbb{N}_n$. Thus $\psi^{-1}(i) = \psi^{-1}(i)h$, since H is regular, and hence $h = 1$. This shows that σ is injective.

Finally we prove that $\sigma(H) = C_{S_n}(H)$. Indeed, for each $x \in C_{S_n}(H)$ let $h = \psi^{-1}(x(i_0)) \in H$. Then $h(i_0) = \psi^{-1}(x(i_0))(i_0) = x(i_0) = x\left(\left(\psi^{-1}(i)\right)^{-1}(i)\right) = \left(\psi^{-1}(i)\right)^{-1}x(i)$, for every $i \in \mathbb{N}_n$. Hence $x(i) = \psi^{-1}(i)h(i_0) = \sigma_h(i)$ for every $i \in \mathbb{N}$ and we have $x = \sigma_h$.

The last calculation also shows that if $x \in Z(H) = H \cap C_{S_n}(H)$ then $h = x = \sigma_h$. □

We are ready to present our intrinsical characterization of (left) group codes.

Theorem 1.2. *Let C be a linear code of length n over a field $\mathbb{F}$ and G a finite group of order n.*

1. *C is a left G-code if and only if G is isomorphic to a transitive subgroup of S_n contained in $\mathrm{PAut}(C)$.*
2. *C is a G-code if and only if G is isomorphic to a transitive subgroup H of S_n such that $H \cup C_{S_n}(H) \subseteq \mathrm{PAut}(C)$.*

Proof. Given a bijection $\phi : E \to G$, we also use ϕ to denote its linear extension $\mathbb{F}^n \to \mathbb{F}G$, and we define $f = f_\phi : G \to S_n$ by setting $e_{f(g)(i)} = \phi^{-1}(g\phi(e_i))$, for $g \in G$ and $i \in \mathbb{N}_n$. Then f is a group homomorphism. Furthermore, $f(g)(i) = i$ if and only if $\phi^{-1}(g\phi(e_i)) = e_i$ if and only if $g\phi(e_i) = \phi(e_i)$ if and only if $g = 1$. This shows that f is injective and $H = f(G)$ is a regular subgroup of S_n. Let $e_{i_0} = \phi^{-1}(1)$. By Lemma 1.1, there is an anti-isomorphism $\sigma : H \to C_{S_n}(H)$, defined by $\sigma_h(i) = \psi^{-1}(i)h(i_0)$, where $\psi : H \to \mathbb{N}_n$ is the bijection given by $\psi(h) = h(i_0)$. We will use several times the equality $\psi^{-1}(i)(i_0) = i$, for $i \in \mathbb{N}_n$.

For every $i \in \mathbb{N}_n$ one has

$$e_i = e_{\psi^{-1}(i)(i_0)} = e_{f(f^{-1}\psi^{-1}(i))(i_0)} = \phi^{-1}\left(f^{-1}\left(\psi^{-1}(i)\right)\cdot\phi(e_{i_0})\right) = \phi^{-1}f^{-1}\psi^{-1}(i).$$

Using this and the fact that $f : G \to H$ is an isomorphism, one has the following equalities for every $h \in H$:

$$\begin{aligned}\sigma_h(e_i) &= e_{\sigma_h(i)} = e_{(\psi^{-1}(i)h)(i_0)} = \phi^{-1}f^{-1}\psi^{-1}\left((\psi^{-1}(i)h)(i_0)\right)\\ &= \phi^{-1}f^{-1}(\psi^{-1}(i)h) = \phi^{-1}\left(f^{-1}(\psi^{-1}(i))\cdot f^{-1}(h)\right) = \phi^{-1}\left(\phi(e_i)\cdot f^{-1}(h)\right).\end{aligned}$$

This implies

$$\sigma_h(x) = \phi^{-1}(\phi(x)\cdot f^{-1}(h)) \tag{1.1}$$

for every $x \in \mathbb{F}^n$ and $h \in H$.

Assume now that C is a left G-code and let $\phi : E \to G$ be a bijection such that $\phi(C)$ is a left ideal of $\mathbb{F}G$ and $f = f_\phi$. By the previous paragraph $H = f(G)$ is a regular subgroup of S_n. Furthermore, by the definition of f, if $h \in H$ and $\alpha = \sum \alpha_i e_i \in \mathbb{F}^n$, then $h(\alpha) = \sum \alpha_i e_{h(i)} = \sum \alpha_i \phi^{-1}\left(f^{-1}(h)\cdot\phi(e_i)\right) = \phi^{-1}\left(f^{-1}(h)\cdot\phi(\alpha)\right)$. Hence $h(C) = \phi^{-1}\left(f^{-1}(h)\cdot\phi(C)\right) = C$, that is $H \subseteq \mathrm{PAut}(C)$. If, moreover, $\phi(C)$ is a two-sided ideal of $\mathbb{F}G$ and $x \in C_{S_n}(H)$ then, by

Lemma 1.1, there is $h \in H$ such that $x = \sigma_h$. Then $x(C) = \sigma_h(C) = \phi^{-1}\left(\phi(C) \cdot f^{-1}(h)\right) = C$, by (1.1). This gives the sufficiency part of (1) and (2).

Conversely, assume that G is isomorphic to a regular subgroup H of S_n contained in $\mathrm{PAut}(C)$. One may assume without loss of generality that $G = H$. Let $\phi : E \to G$ be the bijection given by $\phi^{-1}(g) = e_{g(1)}$. Then $h\phi(e_{g(1)}) = hg = \phi(e_{(hg)(1)}) = \phi(h(e_{g(1)}))$, for every $h, g \in G$. Therefore $h\phi(e_i) = \phi(h(e_i))$, for every $i \in \mathbb{N}_n$, since G is transitive. Using this we have $h\phi(C) = \phi(h(C)) = \phi(C)$, because $G \subseteq \mathrm{PAut}(C)$. Thus $\phi(C)$ is a left ideal of $\mathbb{F}G$.

Assume, additionally that $C_{S_n}(G) \subseteq \mathrm{PAut}(C)$ and let $f = f_\phi$. If $g \in G$ then $f(g)(e_i) = e_{f(g)(i)} = \phi^{-1}(g\phi(e_i)) = e_{(g\phi(e_i))(1)} = g(e_{\phi(e_i)(1)}) = g(e_i)$. Thus $f(g) = g$ for every $g \in G$. By (1.1), $\phi(C)g = \phi(C)f^{-1}(g) = \phi(\sigma_g(C)) = \phi(C)$, for every $g \in G$, and thus $\phi(C)$ is a two-sided ideal of $\mathbb{F}G$. □

Corollary 1.3. *Let C be a linear code of length n over a field and let $\mathcal{G}$ be a class of groups.*

(1) *C is a left $\mathcal{G}$ group code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup of S_n in $\mathcal{G}$.*
(2) *C is a $\mathcal{G}$ group code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup H of S_n in $\mathcal{G}$ such that $C_{S_n}(H) \subseteq \mathrm{PAut}(C)$.*

2. One-dimensional group codes

Even if one-dimensional codes are not relevant for applications, it is educating to see how one can use Theorem 1.2 to decide which one-dimensional codes are group codes.

Proposition 2.1. *Let $\mathbb{F}$ be a finite field, $n \geq 1$ and $0 \neq v \in \mathbb{F}^n$. Then $\mathbb{F}v$, the one-dimensional subspace spanned by v, is a left group code if and only if the entries of v are of the form $u, \xi u, \xi^2 u, \ldots, \xi^{h-1}u$, each of them appearing $s = n/h$ times in v, for some $u \in \mathbb{F}^*$ and ξ an h-th primitive root of unity.*

Assume that v satisfies the above conditions and let G be a group. Then $\mathbb{F}v$ is a left G-code if and only if G has a normal subgroup N of order s such that G/N is cyclic (of order h).

Proof. Write $v = (v_1, \ldots, v_n)$. We start describing $\mathrm{PAut}(\mathbb{F}v)$. Let $\sigma \in S_n$. Then $\sigma \in \mathrm{PAut}(\mathbb{F}v)$ if and only if $\sigma(v) = \lambda_\sigma v$, for some (necessarily unique) $\lambda_\sigma \in \mathbb{F}^*$. Moreover, $\sigma \mapsto \lambda_\sigma$ defines a group homomorphism $\lambda : \mathrm{PAut}(\mathbb{F}v) \to \mathbb{F}^*$. Let ξ be a generator of the image of λ and let $K = Ker\lambda$. Then $\sigma(v) = \xi v$ and hence, if $u \in \mathbb{F}$ appears exactly s times as an entry of v then ξu also appears exactly s times as an entry of v. Therefore, after permuting the entries of v, one may assume that v is of the form

$$\begin{aligned} v \;=\; & (u_1, \ldots, u_1, \xi u_1, \ldots, \xi u_1, \xi^2 u_1, \ldots, \xi^2 u_1, \xi^{h-1} u_1, \ldots, \xi^{h-1} u_1, \\ & u_2, \ldots, u_2, \xi u_2, \ldots, \xi u_2, \xi^2 u_2, \ldots, \xi^2 u_2, \xi^{h-1} u_2, \ldots, \xi^{h-1} u_2, \\ & \ldots, \\ & u_k, \ldots, u_k, \xi u_k, \ldots, \xi u_k, \xi^2 u_k \ldots, \xi^2 u_k, , \xi^{h-1} u_k, \ldots, \xi^{h-1} u_k). \end{aligned}$$

for $u_1, \ldots, u_k \in \mathbb{F}$ such that $u_x \neq \xi^z u_y$ for every $1 \leq x < y \leq k$ and $z \in \mathbb{Z}$, and each $\xi^z u_i$ appears s_i times as an entry of v. Then $K = (S_{s_1} \times \cdots \times S_{s_1}) \times (S_{s_2} \times \cdots \times S_{s_2}) \times \cdots \times (S_{s_k} \times \cdots \times S_{s_k})$, where the i-th block has h copies of S_{s_i} and the j-th S_{s_i} is identified with the subgroup of S_n

formed by the permutations which fix the coordinates k for which $v_k \neq \xi^j u_i$. Consider the permutation $\sigma \in S_n$ given by

$$\sigma(k) = \begin{cases} k + s_i, & \text{if } h(s_1 + \cdots + s_{i-1}) < k \leq h(s_1 + \cdots + s_{i-1}) + (h-1)s_i; \\ k - (h-1)s_i, & \text{if } h(s_1 + \cdots + s_{i-1}) + (h-1)s_i < k \leq h(s_1 + \cdots + s_i). \end{cases}$$

Clearly, σ has order h and $\lambda_\sigma = \xi$. Thus $\mathrm{PAut}(\mathbb{F}v) = K \rtimes \langle \sigma \rangle$. This provides the description of $\mathrm{PAut}(\mathbb{F}v)$.

Observe that, with the notation of the previous paragraph, $\mathrm{PAut}(\mathbb{F}v)$ is transitive if and only if $k = 1$. In that case (up to a permutation of coordinates)

$$v = (u, \ldots, u, \xi u, \ldots, \xi u, \xi^2 u, \ldots, \xi^2 u, \xi^{h-1} u, \ldots, \xi^{h-1} u) \tag{2.2}$$

for some $u \in \mathbb{F}^*$ and some h-th primitive root of unity ξ in $\mathbb{F}^*$ and each $\xi^j u$ is repeated $s = n/h$ times as a coordinate of v.

If $\mathbb{F}v$ is a left G-code, for G a group (of order n) then, by Theorem 1.2, we may assume that G is a transitive subgroup of S_n contained in $\mathrm{PAut}(\mathbb{F}v)$. Therefore v is as in (2.2) and G contains an element τ with $\tau(1) = h + 1$. This implies that $\tau = k\sigma$ for some $k \in K$. If $N = K \cap G$ then $G = \langle N, \tau \rangle$ and τ has order h modulo N. Thus N is a normal subgroup of index h in G and G/N is cyclic. This proves one implication for the two statements of the proposition.

Conversely, assume that v is as in (2.2) and let G be a group of order n with a normal subgroup N of index h in G such that G/N is cyclic. Let g be an element of G of order h modulo N. Fix a bijection $\varphi : \mathbb{N}_s \to N$, which we extend to obtain a bijection $\varphi : \mathbb{N}_n \to G$ by setting $\varphi(js + r) = \varphi(r)g^j$, for $1 \leq r \leq s$, and $0 \leq j < h$. Then φ induces an isomorphism of vectors spaces $\varphi : \mathbb{F}^n \to \mathbb{F}G$, such that $\varphi(v) = u \left(\sum_{n \in N} n\right) \left(\sum_{i=0}^{h-1} \xi^i g^i\right)$. Then $g\varphi(v) = \xi^{-1}\varphi(v)$ and $n\varphi(v) = \varphi(v)$ for every $n \in N$. Thus $\mathbb{F}\varphi(v)$ is a left ideal of $\mathbb{F}G$ and hence $\mathbb{F}v$ is a left G-code. □

Corollary 2.2. *If a one-dimensional vector space is a left group code then it is a cyclic group code.*

Proof. Assume that $\mathbb{F}v$ is a one-dimensional group code of length n. By Proposition 2.1, v has h different coordinates each of them repeated $s = n/h$ times. Then $\mathbb{F}v$ is a cyclic group code because the cyclic group of order n has a subgroup of order s. □

3. Group codes versus abelian group codes

In this section we present a class of groups $\mathcal{G}$, containing properly the class of abelian groups, such that every $\mathcal{G}$ group code is also an abelian group code. We also show that for every non-abelian finite group G there is a finite field $\mathbb{F}$ such that some left G-code over $\mathbb{F}$ is not an abelian group code.

Theorem 3.1. *Let G be a finite group. Assume that G has two abelian subgroups A and B such that every element of G can be written as ab with $a \in A$ and $b \in B$. Then every G-code is an abelian group code.*

Proof. Assume that C is a G-code of length n. Then, by Theorem 1.2, G is isomorphic to a regular subgroup H of S_n such that $H \cup C_{S_n}(H) \subseteq \mathrm{PAut}(C)$. One may assume without loss of generality that $G = AB = H$.

Let $\sigma : G \longrightarrow C_{S_n}(G)$ be the anti-isomorphism defined in Lemma 1.1, with respect to some $i_0 \in \mathbb{N}_n$. Set $A_1 = \sigma(A)$ and $B_1 = \sigma(B)$. Since σ is an anti-isomorphism, A_1 and B_1 are abelian groups and $C_{S_n}(G) = B_1A_1$.

Now, we consider the group $K = \langle A, B_1\rangle \leq \langle G, C_{S_n}(G)\rangle \leq \mathrm{PAut}(C)$. Then K is abelian, since A and B_1 are abelian subgroups, $A \subseteq G$ and $B_1 \subseteq C_{S_n}(G)$. By Theorem 1.2, it is enough to prove that K has order n and the stabilizer in K of every element of $\mathbb{N}_n$ is trivial. To prove the first it is sufficient to show that $[K : A] = [G : A]$. By Lemma 1.1, $B \cap Z(G) = \sigma(B \cap Z(G)) = B_1 \cap Z(C_{S_n}(G))$. Then $[B : B \cap Z(G)] = [B_1 : B_1 \cap Z(C_{S_n}(G))]$ and $[B \cap Z(G) : B \cap A] = [B_1 \cap Z(C_{S_n}(G)) : B_1 \cap A]$. Thus $[G : A] = [AB : A] = [B : B \cap A] = [B_1 : B_1 \cap A] = [AB_1 : A] = [K : A]$, as desired.

Finally, let $i \in \mathbb{N}_n$ and $k \in K$ with $k(i) = i$. Then $k = a\beta$ for some $a \in A$ and $\beta = \sigma_b \in B_1$ with $b \in B$. Moreover, $i = g(i_0)$ for a unique $g \in G$. Therefore $g(i_0) = i = k(i) = a\beta g(i_0) = a\sigma_b(\psi(g)) = agb(i_0)$, where ψ is the map defined in Lemma 1.1. Thus $agb = g$, because G is regular. Set $g = a'b'$, for $a' \in A$ and $b' \in B$. Then $a'abb' = aa'b'b = agb = g = a'b'$ and hence $ab = 1$. Thus $b^{-1} = a \in A \cap B \subseteq Z(G)$. Using the last part of Lemma 1.1 once more, we have $\beta = \sigma_b = b$ and so $a\beta = 1$. □

Recall that a group G is metacyclic if it has a cyclic normal subgroup N such that G/N is cyclic. Sabin and Lomonaco [4] have proved that if C is a G-code of a split metacyclic group G (i.e. G is a semidirect product of cyclic groups) then C is an abelian group code. Using the previous result this can be extended to arbitrary metacyclic group codes.

Corollary 3.2. *If C is a metacyclic group code then C is an abelian group code.*

Theorem 3.1 provides a family of groups $\mathcal{G}$ such that every two-sided $\mathcal{G}$ group code is also an abelian group code. We do not know any example of a group code which is not an abelian group code. For left group codes the situation is completely different.

Proposition 3.3. *For every non-abelian group G and every prime p not dividing the order of G there is a left G-code over some field of characteristic p which is not an abelian group code.*

Proof. Assume that p is a prime not dividing $|G|$. If c is the number of conjugacy classes of G then the number of ideals of $\mathbb{F}G$ is at most 2^c, for every field $\mathbb{F}$ of characteristic p. Therefore, there is a bound on the number of G-codes which is independent of the field. In particular, the number of abelian group codes of a given length is bounded by a number not depending on the field used. However, if G is non-abelian, then there is a field K such that a simple factor of KG is isomorphic to $M_m(K)$ for some $m \geq 2$. Then a simple factor of $\mathbb{F}G$ is isomorphic to $M_m(\mathbb{F})$

for every field extension $\mathbb{F}/K$. Since the left ideals of $M_m(\mathbb{F})$ generated by matrices of the form

$$\begin{pmatrix} 1 & a & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \quad (a \in \mathbb{F})$$

are all different, $\mathbb{F}^n$ has at least $|\mathbb{F}|$ different left G-codes. Thus, the number of left G-codes for the different fields of characteristic p increases with the order of the field and so it is not limited. □

Example 3.4. Since the proof of Proposition 3.3 is not constructive it is worth to present an example of a left group code which is not an abelian group code. Let $\mathbb{F} = \mathbb{F}_{11}$ be the field with 11 elements. Every 2-dimensional cyclic group code of length 6 over $\mathbb{F}$ is permutation equivalent to one of the following codes:

$$\begin{aligned} C_1 &= \{(\lambda, \mu, \mu-\lambda, -\lambda, -\mu, \lambda-\mu) \mid \lambda, \mu \in \mathbb{F}\}, \\ C_2 &= \{(\lambda, \mu, -\mu-\lambda, \lambda, \mu, -\mu-\lambda) \mid \lambda, \mu \in \mathbb{F}\}, \\ C_3 &= \{(\lambda, \mu, \lambda, \mu, \lambda, \mu) \mid \lambda, \mu \in \mathbb{F}\}. \end{aligned}$$

Then one can easily check that the subspace C of $\mathbb{F}^6$ generated by $u = (2, 5, -7, 2, -7, 5)$ and $v = (4, -3, -1, -4, 1, 3)$ is not an abelian group code. However C is a left S_3-code. Indeed, $A = (1, 2, 3)(4, 5, 6)$ and $B = (1, 4)(2, 6)(3, 5)$ belong to $\mathrm{PAut}(C)$, since $A(u) = 5u + 4v$, $B(u) = u$, $A(v) = 5(v - u)$ and $B(v) = -v$. Moreover, $\langle A, B\rangle$ is a regular subgroup of S_6 isomorphic to S_3 and the claim follows from Theorem 1.2.

4. Cauchy codes

In this section we give some necessary and sufficient conditions for some Cauchy codes to be left group codes and describe the possible left group code structures on such codes. Our main tool is a description of the group of permutation automorphisms due to Dür [1] (see also [2]) which we present in a slightly different form.

We first recall the definition of Cauchy codes. For that we need to introduce some notations. Let $\overline{\mathbb{F}}$ denote the projective line over $\mathbb{F}$. Each element of $\overline{\mathbb{F}}$ is represented either by its homogeneous coordinates, denoted $[x, y]$, or by an element of $\mathbb{F} \cup \{\infty\}$ in such a way that $x \in \mathbb{F}$ and $[x, 1]$ represent the same element in $\overline{\mathbb{F}}$, and ∞ and $[1, 0]$ also represent the same element in $\overline{\mathbb{F}}$. We use the coordinatization map $\varphi : \overline{\mathbb{F}} \to \mathbb{F}^2$ defined as follows:

$$\varphi(x) = \begin{cases} (x, 1), & \text{if } x \in \mathbb{F}; \\ (1, 0), & \text{if } x = \infty. \end{cases}$$

We evaluate a homogeneous polynomial $F \in \mathbb{F}[X, Y]$ on an element $z \in \overline{\mathbb{F}}$ by setting $F(z) = F(\varphi(z))$. For an element $\alpha = (\alpha_1, \dots, \alpha_n) \in \overline{\mathbb{F}}^n$ we denote the set of entries of α by L_α.

Definition 4.1. *Given $1 \le k < n$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \overline{\mathbb{F}}^n$, without repeated entries, and a map $f : L_\alpha \to \mathbb{F}^*$, the k-dimensional* Cauchy code *with location vector α and scaling map f is the*

code

$$\mathcal{C}_k(\alpha, f) = \{(f(\alpha_1)P(\alpha_1), \ldots, f(\alpha_n)P(\alpha_n)) : P \in \mathbb{F}[X,Y],\ \textit{homogeneous of degree } k-1\}.$$

Note that our notation is slightly different from that of [2]. The set L_α is called the location set of $\mathcal{C}_k(\alpha, f)$.

Every Cauchy code is MDS and its dual is another Cauchy code (see [2] for details). Moreover, if $\sigma \in S_n$ then $\sigma(\mathcal{C}_k(\alpha, f)) = \mathcal{C}(\sigma(\alpha), f)$ and in particular the class of Cauchy codes is closed under permutations.

Examples of Cauchy codes are the generalized Reed-Solomon codes which correspond to Cauchy codes with location set included in $\mathbb{F}$. In particular, the k-dimensional narrow sense Reed-Solomon codes are those Cauchy codes of the form $\mathcal{C}_k(\alpha, 1)$ with location vector $\alpha = (1, \xi, \xi^2, \ldots, \xi^{q-2})$, for ξ a primitive element of $\mathbb{F}$. Furthermore the parity check extension of the narrow sense Reed-Solomon code $\mathcal{C}_k(\alpha, 1)$ is the Cauchy code $\mathcal{C}_k(\overline{\alpha}, 1)$ with $\overline{\alpha} = (1, \xi, \xi^2, \ldots, \xi^{q-2}, 0)$. (Here 1 denotes the constant map $x \mapsto 1$.)

As mentioned at the beginning of this section our aim is to obtain criteria to decide when a Cauchy code $\mathcal{C}_k(\alpha, f)$ is a left G-code. Since a linear code and its dual have the same automorphism groups, they are (left) G-codes for the same groups G. Furthermore the dual of a Cauchy code is a Cauchy code too and $\mathcal{C}_1(\alpha, f)$ is the one-dimensional code generated by $(f(\alpha_1), \ldots, f(\alpha_n))$ (see [2] for details). This shows that the cases $k = 1$ and $k = n-1$ reduce to Proposition 2.1. Thus, in the remainder of this section, we assume that $2 \leq k \leq n-2$.

Let $\Gamma = \mathrm{PGL}_2(\mathbb{F})$, the 2-dimensional projective general linear group. We identify Γ with the group of homographies of $\overline{\mathbb{F}}$, so that $\mathrm{GL}_2(\mathbb{F})$ is considered acting on the left on $\overline{\mathbb{F}}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} [x, y] = [ax + by, cx + dy].$$

For a subset X of $\overline{\mathbb{F}}$ let $\Gamma_X = \{T \in \Gamma : T(X) = X\}$. For $a \in \overline{\mathbb{F}}$, let $\Gamma_a = \Gamma_{\{a\}}$. For example, Γ_∞ is formed by the classes represented by upper triangular invertible matrices and

$$\Gamma_\infty \simeq N \rtimes H, \text{ with } N = \left\{ U_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F} \right\} \text{ and } H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}^* \right\}. \tag{4.3}$$

Moreover N is an elementary abelian p-group of order q and H is cyclic of order $q-1$.

For every $T \in \mathrm{GL}_2(\mathbb{F})$, let $\theta_T : \overline{\mathbb{F}} \to \mathbb{F}^*$ be defined by

$$\theta_T(z) = \begin{cases} \text{second coordinate of } T(\varphi(z)), & \text{if it is non-zero;} \\ \text{first coordinate of } T(\varphi(z)), & \text{otherwise.} \end{cases}$$

Fix a subset L of $\overline{\mathbb{F}}$. If $T \in \mathrm{GL}_2(\mathbb{F})$ then we denote the restrictions of $T : \overline{\mathbb{F}} \to \overline{\mathbb{F}}$ and $\theta_T : \overline{\mathbb{F}} \to \mathbb{F}^*$ to L as T_L and $\theta_{T,L}$ respectively. If $f, g : L \to \mathbb{F}^*$ then let $f \cdot g : L \to \mathbb{F}^*$ be given by

$$(f \cdot g)(z) = f(z)g(z) \quad (z \in L).$$

We say that f and g are equivalent, denoted $f \equiv g$, if $g = \lambda f$ for some $\lambda \in \mathbb{F}^*$.

The following theorem describes when two Cauchy codes are equal.

Theorem 4.2. [2, Theorem 2.6] *Let $2 \leq k \leq n-2$ and consider two k-dimensional Cauchy codes. $C = \mathcal{C}_k(\alpha, f)$ and $C' = \mathcal{C}_k(\alpha', f')$ of length n. Then $C = C'$ if and only if there exists $T \in \mathrm{PGL}_2(\mathbb{F})$ such that $\alpha'_i = T(\alpha_i)$ and $f' \circ T_{L_\alpha} \equiv \theta_{T,L_\alpha}^{k-1} \cdot f$.*

In particular, C and C' are permutation equivalent if and only if there exists $T \in \mathrm{PGL}_2(\mathbb{F})$ such that $T(L_\alpha) = L_{\alpha'}$ and $f' \circ T_{L_\alpha} \equiv \theta_{T,L_\alpha}^{k-1} \cdot f$.

Note that the equivalence $f' \circ T_{L_\alpha} \equiv \theta_{T,L_\alpha}^{k-1} \cdot f$, in Theorem 4.2 does not depend on the representative of T in $\mathrm{GL}_2(\mathbb{F})$ used to calculate θ_T, because $\theta_{\lambda T} = \lambda \theta_T$, for every $\lambda \in \mathbb{F}^*$.

Given $f : L \to \mathbb{F}^*$ with $|L| = n$ we denote

$$\Gamma_{k,f} = \{T \in \Gamma_L : f \circ T_L \equiv \theta_{T,L}^{k-1} \cdot f\}$$

Proposition 4.3. *If C is a k-dimensional Cauchy code of length n with $2 \leq k \leq n-2$ and scaling map $f : L \to \mathbb{F}^*$ then the map $T \mapsto T_L$ is a group isomorphism $\Gamma_{k,f} \to \mathrm{PAut}(C)$.*

Proof. Let $C = \mathcal{C}_k(\alpha, f)$ with $L = L_\alpha$. If $\sigma \in S_n$ then $\sigma(C) = \mathcal{C}_k(\sigma(\alpha), f)$. Using this and Theorem 4.2 and identifying S_n with the permutations of L one has

$$\mathrm{PAut}(C) = \{T_L : T \in \Gamma_{L,f}\}. \tag{4.4}$$

The map $T \mapsto T_L$ is injective because $|L| = n > k \geq 2$ and an element of $\mathrm{PGL}_2(K)$ is uniquely determined by its action on three different elements of $\overline{\mathbb{F}}$. □

Now it is clear that we have the following consequence of Theorem 1.2.

Corollary 4.4. *Let $L \subseteq \overline{\mathbb{F}}$ with $n = |L|$ and $2 \leq k \leq n-2$. Let C be a Cauchy code with scaling map $f : L \to \mathbb{F}^*$. Then C is a left G-code if and only if G is isomorphic to a subgroup H of order n of $\Gamma_{k,f}$ whose action by homographies on L is transitive (equivalently, $h(x) \neq x$, for every $x \in L$ and $1 \neq h \in H$).*

As an application of Corollary 4.4 we characterize when some Cauchy codes with large location set are group codes.

Lemma 4.5. *Let L and L' be subsets of $\overline{\mathbb{F}}$ with $|L| = |L'| \geq q-2$. Then every Cauchy code with location set L is equal to a Cauchy code with location set L'.*

Proof. By assumption $|\overline{\mathbb{F}} \setminus L| = |\overline{\mathbb{F}} \setminus L'| \leq 3$. Since the action of Γ on $\overline{\mathbb{F}}$ is triply transitive there is $T \in \mathrm{GL}_2(\mathbb{F})$ such that $T(\overline{\mathbb{F}} \setminus L) = \overline{\mathbb{F}} \setminus L'$ and so $T(L) = L'$. Therefore, by Theorem 4.2, if C is a Cauchy code with scaling map $f : L \to \mathbb{F}^*$ then C is also a Cauchy code with scaling map $(\theta_{T,L}^{k-1} \cdot f) \circ T_L^{-1} : L' \to \mathbb{F}^*$. □

It is well known that the parity check extension of a narrow sense Reed-Solomon codes is a q-ary Cauchy G-code of length q, for G the p-elementary abelian group of order q (see e.g. [3]). Next theorem shows that this is the only possible structure of G-code on a q-ary Cauchy code of length q.

Theorem 4.6. *Let C be a q-ary Cauchy code of length q and dimension $2 \leq k \leq q-2$ and let G be a group of order q. Then C is a left G-code if and only if it is permutation equivalent to the parity check extended narrow sense Reed-Solomon code and G is p-elementary abelian.*

Proof. One implication was proved by Landrock and Manz [3]. Conversely, let C be a q-ary Cauchy code of length q with scaling map $f : L \to \mathbb{F}^*$. By Lemma 4.5, one may assume, without loss of generality, that $L = \mathbb{F}$. Then $\Gamma_{\mathbb{F}} = \Gamma_\infty = N \rtimes H$, with N and H as in (4.3). Thus N is a normal Sylow elementary abelian p-subgroup of $\Gamma_{\mathbb{F}}$ and hence it is the only subgroup of order q of $\Gamma_{\mathbb{F}}$. Therefore, if C is a G-code then $G \simeq N$. Moreover, N should be contained in $\Gamma_{k,f}$ and this implies that $f \circ U_b \equiv f$, for every $b \in \mathbb{F}$, because $\theta_{U_b}(z) = 1$ for every $b \in \mathbb{F}$ and $z \in \overline{\mathbb{F}}$. Thus, there is $\lambda \in \mathbb{F}^*$ with $f \circ U_b = \lambda f$. So, $f(0) = f(pb) = (f \circ U_b)((p-1)b) = \lambda f((p-1)b) = \cdots = \lambda^p f(0)$ and hence $\lambda^p = 1$. Then $\lambda = 1$, since $|\mathbb{F}^*| = q - 1$ is relatively prime with p. Hence $f(b) = (f \circ U_b)(0) = f(0)$, for every $b \in \mathbb{F}$, i.e. f is constant. Therefore C is permutation equivalent to the parity check extended narrow sense Reed-Solomon code. □

Now we turn our attention to Reed-Solomon like Cauchy codes. It is well known that the q-ary Reed-Solomon codes are cyclic of length $q - 1$.

Theorem 4.7. *Let $\mathbb{F} = \mathbb{F}_q$, the field of q elements, and let ξ be a primitive element of $\mathbb{F}$. Let C be a k-dimensional q-ary Cauchy code with scaling map $f : L \to \mathbb{F}^*$ and assume that $|L| = q - 1$ and $2 \le k \le q - 3$.*

Then C is a left group code if and only one of the following conditions hold for some (for all) $T \in \mathrm{PGL}_2(\mathbb{F})$ with $T(L) = \mathbb{F}^*$:

1. *there is an integer m such that $\left(\theta_{T,L}^{k-1} \cdot f\right) \circ T_L^{-1}$ is equivalent to the map $f_m : \mathbb{F}^* \to \mathbb{F}^*$ given by $f_m(z) = z^m$ for every $z \in \mathbb{F}^*$.*
2. *q is odd and there are integers m and m' such that $4m + 2(k-1) \equiv 2m' + k - 1 \equiv 0 \bmod (q-1)$ and $\left(\theta_{T,L}^{k-1} \cdot f\right) \circ T_L^{-1}$ is equivalent to the map $f_{m,m'} : \mathbb{F}^* \to \mathbb{F}^*$ given by*

$$f_{m,m'}(\xi^{2t+r}) = \xi^{2tm+rm'}, \qquad \text{for every } t \in \mathbb{Z} \text{ and } r = 0 \text{ or } 1.$$

Moreover, if G is a group of order $q - 1$ then C is a left G-code if and only if either G is cyclic and condition (1) holds or G is a dihedral group and condition (2) holds.

Proof. By Lemma 4.5 (and Theorem 4.2), it is enough to prove that if $L = \mathbb{F}^*$ and $f(1) = 1$ then C is a left G-code if and only if either G is cyclic and $f = f_m$, for some m, or $q - 1$ is even, G is the dihedral group of order $q - 1$ and $f = f_{m,m'}$, for some m and m' satisfying the conditions of (2).

So assume that $L = \mathbb{F}^*$ and $f(1) = 1$. Let $D = \Gamma_{\mathbb{F}^*} = \Gamma_{\{0,\infty\}} \supseteq \Gamma_{k,f}$. Then $D = \langle A, B\rangle$ with

$$A = \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

So, D is a dihedral group of order $2(q-1)$. If q is even then the only subgroup of D of order $q-1$ is $\langle A\rangle$. Otherwise, that is if q is odd then, the only subgroups of D of order $q-1$ are $\langle A\rangle$, $\langle A^2, B\rangle$ and $\langle A^2, AB\rangle$. By Corollary 4.4, C is a left G-code if and only if G is isomorphic to a subgroup H of order $q-1$ of $\Gamma_{k,f}$ which acts transitively on $\mathbb{F}^*$. However $B(1) = 1$, and this excludes the possibility $H = \langle A^2, B\rangle$. Thus C is a left G-code if and only if either G is cyclic

and $A \in \Gamma_{k,f}$, or q is odd, G is the dihedral group of order $q-1$ and A^2 and $M = AB$ belong to $\Gamma_{k,f}$.

Notice that $\theta_A(z) = 1$ for every $z \in \mathbb{F}$ and $(f_m \circ A)(z) = f_m(\xi z) = \xi^m f_m(z) = \xi^m(\theta_A \cdot f_m)(z)$ for every $z \in \mathbb{F}$. Thus $A \in \Gamma_{k,f_m}$ and hence if $f = f_m$ then C is a cyclic group code. Conversely, if C is a cyclic group code then $A \in \Gamma_{k,f}$, that is $f \circ A_{\mathbb{F}^*} \equiv f$. Hence there is $m = 0, 1, \ldots, q-2$ such that $f(\xi z) = \xi^m f(z)$ for every z. This implies, together with the assumption $f(1) = 1$, that $f(\xi^i) = \xi^{im}$ and so $f = f_m$.

Secondly assume that q is odd and let G be the dihedral group of order $q-1$. On the one hand, arguing as in the previous paragraph one deduces that $A^2 \in \Gamma_{k,f}$ if and only if there is an integer $0 \leq m_1 < q-1$ such that $f(\xi^{2t+r}) = \xi^{tm_1} f(\xi)^r$, for every $t \in \mathbb{Z}$ and $r = 0$ or 1. Moreover m_1 is even because $1 = f(1) = f\left(\xi^{2\frac{q-1}{2}}\right) = \xi^{\frac{q-1}{2}m_1}$. Set $m_1 = 2m$. On the other hand, $M(z) = \xi/z$ and $\theta_M(z) = z$, for every $z \in \mathbb{F}^*$. Hence $M \in \Gamma_{k,f}$ if and only if there is an integer $0 \leq m' < q-1$ such that $f(\xi/z) = \xi^{m'} z^{k-1} f(z)$, for every $z \in \mathbb{F}^*$. So, if C is a left G-code then there are integers m and m' such that

$$\begin{aligned} \xi^{m'+(2t+r)(k-1)+2tm} f(\xi)^r &= \xi^{m'+(2t+r)(k-1)} f(\xi^{2t+r}) = f\left(\tfrac{\xi}{\xi^{2t+r}}\right) = f(\xi^{2(-t)+(1-r)}) \\ &= \xi^{-2tm} f(\xi)^{1-r}, \end{aligned}$$

for every $t \in \mathbb{Z}$ and every $r = 0, 1$, or equivalently

$$\xi^{m'+(2t+r)(k-1)+4tm} = f(\xi)^{1-2r}.$$

Considering the two values $r = 0$ and $r = 1$ we deduce that $f(\xi) = \xi^{m'}$, hence $f = f_{m,m'}$, and $2(k-1)+4m \equiv 2m'+k-1 \equiv 0 \mod q-1$. Conversely, if m and m' satisfy the above conditions and $f = f_{m,m'}$ then, reversing the arguments, we deduce that $A^2, M \in \mathrm{PGL}_2(\mathbb{F})_{k,f}$ and so C is a left G-code. □

Remarks 4.8. Let $2 \leq k \leq q-3$ and let E_m and $E_{m,m'}$ denote k-dimensional Cauchy codes with scaling maps f_m and $f_{m,m'}$ respectively. By Theorem 4.7, every k-dimensional left group Cauchy code of length $q-1$ is permutation equivalent to either E_m, for some m, or $E_{m,m'}$, for m and m', satisfying the conditions in statement (2) of Theorem 4.7. Using Theorem 4.2 one can decide when two of these codes are permutation equivalent:

(1) On the one hand, by Theorem 4.2, E_m and $E_{m'}$ are permutation equivalent if and only if $f_{m'} \equiv f_m \circ T_{\mathbb{F}^*}$ for some $T \in \langle A, B \rangle$ (see the first part of the proof of Theorem 4.7). On the other hand, $f_m \circ A \equiv f_m$ and $f_m \circ B \equiv f_{-m}$. This proves that E_m and $E_{m'}$ are permutation equivalent if and only if $m' \equiv \pm m \mod (q-1)$.

(2) On the other hand, in the second case of Theorem 4.7, k is necessarily odd and $f_{m,m'}$ is determined by the values of $2m$ and m' modulo $q-1$. The equation $2X + k - 1 \equiv 0 \mod (q-1)$ has a unique solution modulo $\frac{q-1}{2}$, namely $\frac{1-k}{2}$.

   (a) If $q \equiv -1 \mod 4$ then the equation $4X+2(k-1) \equiv 0 \mod (q-1)$ has also a unique solution modulo $\frac{q-1}{2}$, namely $\frac{1-k}{2}$ and hence, in this case, $2m \equiv 1-k \mod q-1$. Thus $f_{m,m'}$ is either $f_{\frac{1-k}{2},\frac{1-k}{2}} = f_{\frac{1-k}{2}}$ or $f_{\frac{1-k}{2},\frac{q-k}{2}} = f_{\frac{q-k}{2}}$. We conclude that if $q \equiv -1 \mod 4$ then every left group Cauchy code is a cyclic group code.

(b) Otherwise, that is for $q \equiv 1 \mod 4$, the equation $4X+2(k-1) \equiv 0 \mod (q-1)$ has a unique solution modulo $\frac{q-1}{4}$, namely $\frac{1-k}{2}$. Therefore there are four possible dihedral group Cauchy codes of this form namely $E_{\frac{1-k}{2},\frac{1-k}{2}} = E_{\frac{1-k}{2}}$, $E_{\frac{1-k}{2},\frac{q-k}{2}} = E_{\frac{q-k}{2}}$, $E_{\frac{1+q-2k}{2},\frac{1-k}{2}}$ and $E_{\frac{1+q-2k}{2},\frac{q-k}{2}}$. The last two are not cyclic group codes. To see this it is enough to show that if $f_{m,m'} \equiv f_{m_1}$ then $2m \equiv 2m_1 \mod (q-1)$ and $m' \equiv m_1 \mod (q-1)$. This follows by straightforward calculations. This provides more examples of left group codes which are not abelian group codes.

Example 4.9. Let $C = \mathcal{C}_k(\alpha, 1)$ be a Cauchy code over $\mathbb{F} = \mathbb{F}_q$ with location set L. We have seen in Theorems 4.6 and 4.7 that if $L = \mathbb{F}$ or $\mathbb{F}^*$ then C is an abelian group code. More generally, if K is a subfield of $\mathbb{F}$ and $L = K$ then C is a $(K, +)$-code and if $L = K^*$ then C is a $(K^*, \cdot)$-code. This can be shown as in the proofs of Theorems 4.6 and 4.7.

We claim that the assumption $k \leq n-2$ implies that if C is a left group code then $|L|$ divides $q(q-1)$. Assume that C is a left G-code. Then G is isomorphic to a subgroup of $\Gamma_{k,1}$. If $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ represents an element of $\Gamma_{k,f}$, with $c \neq 0$ then there is $\lambda \in \mathbb{F}^*$ such that $(cz+d)^{k-1} = \theta_{T,L}^{k-1}(z) = \lambda_T$ for every $z \in L \setminus \{\infty, -\frac{d}{c}\}$. Thus the polynomial $(cz+d)^{k-1} - \lambda_T$ has at least $n-2 \geq k$ roots, a contradiction. This proves that $\Gamma_{k,1} \subseteq \Gamma_\infty$ and hence $|L| = |G|$ divides $|\Gamma_\infty| = q(q-1)$, as wanted. This argument, together with the description of $\Gamma_\infty = N \rtimes H$ given in (4.3), shows that if $|L|$ is coprime with $q-1$ then G is an elementary abelian p-group and if $|L|$ is coprime with q then G is cyclic.

Example 4.10. Theorems 4.6 and 4.7 describes the left group Cauchy codes over $\mathbb{F}_q$ of dimension $2 \leq k \leq n-2$ and length $n = q$ or $q-1$. Assume now that C is a Cauchy code of length $q-2$ and dimension $2 \leq k \leq q-4$. If $f : L \to \mathbb{F}^*$ is the scaling map of C then every element of $\Gamma_{k,f}$ permutes the three elements of $\overline{\mathbb{F}} \setminus L$. Since every element of Γ is determined by its action on three elements, we deduce that $\Gamma_{k,f}$ is isomorphic to a subgroup of S_3 and hence, if L is a left G-code then G is isomorphic to a subgroup of S_3. Therefore $q-2 = |L| = |G|$ divides 6. Since, by assumption $2 \leq n-2 = q-4$, we have $q \geq 6$. We then deduce that $q = 8$ and L is a left S_3-code.

References

[1] A. Dür, The automorphism groups of Reed-Solomon codes, J. Combin. Theory Ser. A. 44 (1987) 69–82.

[2] 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.

[3] P. Landrock and O. Manz, Classical codes as ideals in group algebras. Des. Codes Cryptogr. 2 (1992) 273–285.

[4] R.E. Sabin and S.J. Lomonaco, Metacyclic Error-Correcting Codes, AAECC, 6 (1995), 191–210.