GROUP CODES*

Santos González[1], Victor Markov[2], Olga Markova[2], and Consuelo Martínez[1]

[1] Department of Mathematics, Oviedo University, Spain
santos@uniovi.es; cmartinez@uniovi.es
[2] Department of Mechanics and Mathematics, Moscow State University, Russia
ov_markova@mail.ru

Abstract. Mathematical objects in this paper are group codes. In the first part of the paper we present a survey with some of the main results about group codes, mainly the existence of group codes that are not abelian group codes, the minimal length and the minimal dimension of such codes and the existence of a non-abelian group code that has better parameters than any abelian group code. In particular, in a previous paper [1], we have shown that the minimal dimension of a group code that is not abelian group code is 4. However, all known examples of group codes of dimension 4 that are non-abelian group codes are constructed using groups that are not p-groups.
We do not know if such codes exist for the case of p-groups, but in the second part of this paper we prove that, under some restrictions on the base field, all four-dimensional G-codes for an arbitrary finite p-group G are abelian.

Keywords: Group Codes · Length · Dimension · Groups · Non-abelian Groups · Abelian Groups

Introduction

Error correcting codes play a key role to guarantee the reliability of (digital) information that is sent through a channel with noise. During the transmission process some errors may appear and it is essential for the recipient to be able to detect that some errors have indeed been produced and, eventually, to correct them. This process of detection and correction of errors can take place thanks to error correcting codes *with good properties*.

Usually linear codes are the most widely used, since Linear Algebra provide some powerful tools to deal with them. For general information about Coding Theory we refer readers to [2] and [3]. So all codes considered here are, in particular, vector subspaces of dimension k of an F-vector space of dimension n. We will refer to n as the length of the code and k is its dimension.

It is worth to mention that there are some important and useful non-linear codes, for instance, binary Hamming codes. However, Hamming codes can be

* granted by MTM2017-83506-C2-2-P, FD-GRUPIN-IDI/2018/000193 and RFBR grant 17-01-00895 A.

seen as linear codes over the ring $\mathbb{Z}_4$ as proved by A. Nechaev in 1989 (see [4]) and Hammons et al. in 1994 (see [5]).

At present, many algebraic structures (groups, rings, modules, ...) are used in Coding Theory.

All groups and fields considered in what follows are supposed to be finite and p denotes a prime.

Cyclic codes have nice properties and efficient decodifying algorithms have been developed for them. A code $\mathcal{C}$ is cyclic if it satisfies that a word $\mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ if and only if $(c_2, \ldots, c_n, c_1) \in \mathcal{C}$.

A cyclic code can be seen as an ideal in the quotient ring $F[x]/(x^n - 1)$ and it is generated by a (unique) monic polynomial $g(x)$ satisfying $g(x)|x^n - 1$.

The notion of group code extends in a natural way the one of cyclic code. A cyclic code is a group code when the associated group is cyclic.

In this paper we will survey on group codes constructed using non-abelian groups. It is clear that work with non-abelian groups is sensibly more complicated than work with abelian groups. So the aim of that survey is to prove that the use of non-abelian groups has interest and opens new possibilities. We will include also some new results about group codes of dimension 4.

1 Group Codes

From now on F will denote a finite field and $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$ will denote a finite group of order n. The set of all formal linear combinations of elements of G,

$$FG = \left\{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in F \right\}$$

has a well known structure of algebra over F and is called the group algebra (or group ring) of G over F.

Following [6] we say that a linear code $\mathcal{C}$ over F is a (left) G-code if its length is equal to $n = |G|$ and there exists a one-to-one mapping $\nu : \{1, \ldots, n\} \to G$ such that

$$\left\{ \sum_{i=1}^{n} a_i \nu(i) : (a_1, \ldots, a_n) \in \mathcal{C} \right\}$$

is a (left) ideal in FG. We will also say that this (left) ideal is permutation equivalent to the code $\mathcal{C}$.

A code $\mathcal{C}$ is called an (abelian) group code if there exists an (abelian) group A such that $\mathcal{C}$ is an A-code.

So a cyclic code is a G-code, where G is a cyclic group.

The question of how to distinguish group codes among linear codes was addressed in [6] using the *automorphism permutation group* of the code. Given a code $\mathcal{C}$ and a permutation $\sigma \in S_n$, for $\mathbf{c} = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathcal{C}$, we denote $\sigma(\mathbf{c}) = (\alpha_{\sigma(0)}, \alpha_{\sigma(1)}, \ldots \alpha_{\sigma(n-1)})$. The automorphism permutation group of the

code $\mathcal{C}$, $\mathrm{PAut}(\mathcal{C})$, is the subgroup of S_n that consists of all permutations $\sigma \in S_n$ satisfying that $\sigma(\mathcal{C}) = \mathcal{C}$.

In [6] authors prove that a code $\mathcal{C}$ of length n is a left group code (resp. a group code) if and only if $\mathrm{PAut}(\mathcal{C})$ contains H (resp. $H \cup C_{S_n}(H)$), where H is a transitive subgroup of order n. The code $\mathcal{C}$ is an abelian group code if and only if $\mathrm{PAut}(\mathcal{C})$ contains a regular abelian subgroup $A \leq S_n$.

These characterizations, important from a theoretical point of view, are not very helpful in applications. For instance, they could not help to address the question about the existence of group codes that cannot be realized as abelian group codes (we will call those codes *non-abelian group codes*, for short). Let us emphasise that a given code $\mathcal{C}$ can be seen as group code over two different groups. It is possible also that one of them is abelian and the other is not. So, in order to justify the study of non-abelian group codes, the first question that was needed to answer was: Do they exist?

We started studying this question in [7], where we proved that if G is a non-abelian group and there is a G-code that is a non-abelian group code, then $|G| \geq 24$. Then we found the first examples of non-abelian group codes using the group S_4. We started with the semisimple case, constructing for $G = S_4$ and $F = \mathbb{Z}_5$ a G-code whose weight distribution does not coincide with the weight distribution of any abelian group code of length 24. To check the weight distributions of all those codes we needed the help of a computer. The result turned out to be the same in the non-semisimple case and we could prove the existence of G-codes over $\mathbb{Z}_2$ and $\mathbb{Z}_3$ that are non-abelian group codes. It is worth to mention that case $F = \mathbb{Z}_3$ follows the same lines of case $F = \mathbb{Z}_5$. However, when $F = \mathbb{Z}_2$ some interesting differences appear, since the considered code has the same parameters and the same weight distribution of some abelian code of length 24.

However those codes constructed using the group $G = S_4$ have worse parameters than abelian group codes of the same length. So, in that point it was still unclear that the study of non-abelian group codes is worth. But finally we were able to construct some non-abelian group codes that achieve better properties than abelian group codes of the same length.

Using the group $G = \mathrm{SL}(2, \mathbb{Z}_3)$ we could construct a binary code having dimension 6 and minimal weight 10. So such code is, in some sense, optimal.

Indeed, in [8] we prove that a binary code of length 24 and dimension 6 has minimal distance ≤ 10. Furthermore, the distance 10 can not be reached using an abelian group code. And, what is also important, in this construction we did not have to use computers. All results were proved in a pure algebraic way and they allow to say that the study of non-abelian group codes is worth.

Still we can ask if the existence of non-abelian group codes is some exceptional fact and appears only in some cases or, by the contrary, it happens in all characteristics.

V. Markov checked the existence of non-abelian group codes for every prime field $\mathbb{Z}_p$, $p < 100$ and conjectured that there are non-abelian group codes of length 24 over every finite field.

In [9] we proved that for every $p \geq 3$ there are G-codes over $\mathbb{Z}_p$ of dimension 9, where $G = S_4$, that are not abelian. In a similar way, we could prove that there are G-codes over $\mathbb{Z}_p$ that are not abelian and have dimension 4, with $G = \mathrm{GL}(2, \mathbb{Z}_3)$.

Now we can give a positive answer to Markov's conjecture using a previous result in [7]:

Theorem 1. *If E/F is an extension of fields, G is a finite group and every G-code over E is abelian, then every G-code over F is abelian.*

Nothing is known about the converse of the assertion in the above mentioned theorem.

2 Dimension of Non-abelian Group Codes

In the results mentioned until now we have paid attention specially to the length of the group code. So we know that 24 is the minimal length of a non-abelian group code and this length is achieved, that is, there are G-codes over any finite field with length 24 and that are non-abelian group codes.

In this section we will pay attention to the dimension of those codes. What is the minimal dimension of a non-abelian group code?

It was shown in [6] that any one-dimensional group code over a field F is an abelian group code (moreover it is a C-code for a cyclic group C). And as we have mentioned in the previous section there are non-abelian group codes of dimension 4. What about codes of dimensions 2 and 3?

This question was addressed in [1] were we proved the following main result:

Theorem 2. *Let $\mathcal{C}$ be a G-code over a finite field F, where G is a finite group. If $\dim_F \mathcal{C} \leq 3$, then $\mathcal{C}$ is an abelian group code*

So now we can say that the minimal length of a non-abelian group code is 24 and the minimal dimension is 4 and there are non-abelian group codes of dimension 4 and length 24. However, in none of the known examples there is a non-abelian group code linked to a p-group. We can not claim that if G is a p-group then every G-code is an abelian group code, but we can prove that, with some additional restrictions on the base field, this is the case.

Theorem 3. *Let p be a prime, and let G be a finite p-group. If F is a field with $|F| < p^3$ then any G-code $\mathcal{C}$ over F with $\dim_F \mathcal{C} = 4$ is an abelian group code.*

In what follows we will prove this result, considering before the semisimple case and then the modular case in a separate way.

3 Semisimple case

Given a field F, we denote its multiplicative group by F^*. Let $M_k(F)$ be the algebra of all $k \times k$-matrices over F. For any integer $n \geq 1$ we use the notation $\mathrm{GL}_n(F)$, $\mathrm{T}_n(F)$ and $\mathrm{UT}_n(F)$ respectively for the group of all invertible $n \times n$-matrices, the group of all invertible upper triangular $n \times n$-matrices and the group of all upper unitriangular $n \times n$-matrices, i.e. upper triangular matrices with diagonal elements equal to 1, over the field F.

As usual write $A \leq B$ to express that A is a subgroup of the group B, while $A \lhd B$ means that A is a normal subgroup in B. $Z(G)$ and $Z(R)$ will denote the center of the group G and of the ring R, respectively.

Let's remember a useful sufficient condition for all G-codes to be abelian.

Theorem 4 ([6, 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.*

We say that a group G *has an abelian decomposition* if it satisfies the condition of this theorem.

For any finite group G and any subgroup $N \leq G$ we consider an element $N_\Sigma = \sum_{u \in N} u \in FG$. We will use the following properties of N_Σ: $N_\Sigma = uN_\Sigma = N_\Sigma u$ for every $u \in N_\Sigma$, and $N_\Sigma \in Z(FG)$ iff $N \lhd G$.

Given two finite groups G, H of the same order n and a one-to-one mapping $\varphi : G \to H$ we define its natural extension $\tilde{\varphi} : FG \to FH$ by the rule

$$\tilde{\varphi}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \varphi(g).$$

If I, J are left (right, two-sided) ideals in the group rings FG and FH, respectively, and there exists a one-to-one mapping $\varphi : G \to H$ such that $\tilde{\varphi}(I) = J$, we say that I and J are *permutation equivalent*.

We say that a subgroup $U \leq G$ acts trivially (from the left) on some set $X \subseteq FG$ if $ux = x$ for every $u \in U$ and $x \in X$. Our proofs are based on Theorem 4 and on the following simple observation.

Lemma 1 ([1, Lemma 1.3]). *Let F be a field and let G, H be two groups of the same order $n < \infty$. Suppose that there exist two normal subgroups $N \lhd G$ and $K \lhd H$ such that $G/N \cong H/K$, and that N acts trivially on some (left, right, two-sided) ideal $I \in FG$. Then I is permutation equivalent to some (left, right, two-sided) ideal of the ring FH.*

Evidently Lemma 1 remains valid is we consider the right action instead of the left action.

We add here the following remark which we will use in what follows.

Lemma 2. *Let e be a central idempotent of a group ring $R = FG$. Then the mapping $f : g \mapsto ge$ for any $g \in G$ is a group homomorphism from G to the group of invertible elements of the ring Re and its kernel acts trivially on $I = Re$ from the left and from the right.*

Proof. Straightforward.

In this section we assume that F is a finite field such that $|F| = q < p^3$ with $(p, q) = 1$ and that G is a finite p-group.

By Maschke's theorem the ring $R = FG$ decomposes into the direct sum of matrix rings over some extensions of the base field F. It follows that any ideal I of the ring R has the form $I = Re$ for some central idempotent $e \in R$. Suppose that $I = Re$ is an ideal in R such that $\dim_F I = 4$. Then either I is commutative or I is isomorphic to the ring $M_2(F)$. If I is commutative then G' acts trivially on I and one can take $H = G/G' \times A$ in Lemma 1 where A is an arbitrary abelian group with $|A| = |G'|$ to show that I defines an abelian group code.

Now consider the case $I \cong M_2(F)$. Let $f : G \to \mathrm{GL}_2(F)$ be the homomorphism defined in Lemma 2 and let K be its kernel. Then $|G/K| = p^r$ for some integer $r > 0$ (otherwise G acts trivially on I hence any subspace of I is an ideal which is impossible since I is a simple ring) and p^r divides $|\mathrm{GL}_2(F)| = (q^2 - 1)(q^2 - q) = q(q - 1)^2(q + 1)$.

Next we prove that $r \leq 4$ for $p > 2$ and $r \leq 5$ for $p = 2$.

If $p = 2$ then only the values $q = 3, 5, 7$ are possible since $q < p^3 = 8$ and $(q, p) = 1$. In these cases $|\mathrm{GL}_2(\mathbb{Z}_3)| = 48 = 16 \cdot 3$, $|\mathrm{GL}_2(\mathbb{Z}_5)| = 480 = 32 \cdot 15$, $|\mathrm{GL}_2(\mathbb{Z}_7)| = 2016 = 32 \cdot 63$, correspondingly, thus $r \leq 5$.

Suppose now that $p > 2$. Then either $p^r | (q + 1)$ or $p^r | (q - 1)^2$. If $p^r | (q - 1)^2$ then $r = 2k$ where $p^k | (q - 1)$. Since $q < p^3$ then $k \leq 2$ thus $r \leq 4$. At last consider the case $p^r | (q + 1)$. By condition we have $q + 1 \leq p^3$, hence $r \leq 3$.

Propositions [7, 3.1] and [7, 4.2] imply that if $|G/K| = p^r$ where $r \leq 4$ or $|G/K| = 2^r$ where $r \leq 5$ then the group G/K has an abelian decomposition. Application of Lemmas 1, 2 and Theorem 4 finishes the proof of Theorem 3 in the semisimple case.

4 Modular Case

In this section we assume that F is a finite field with $\mathrm{char} F = p$ and $|F| = q = p^s$ with $s \leq 2$. Let G be a finite p-group.

Let I be an ideal in FG with $\dim I = 4$. Arguing as in [1], we consider the left and right action of G on I. We fix two group homomorphisms $\varphi, \psi : G \to \mathrm{GL}(I) = \mathrm{GL}_4(F)$ defined as follows:

$$\forall g \in G,\ v \in I, \varphi(g)(v) = gv,\ \psi(g)(v) = vg^{-1}.$$

Let $K = \varphi(G)$ and $L = \psi(G)$. Then $K, L \leq \mathrm{GL}_4(F)$ $AB = BA$ for any $A \in K$ and $B \in L$ by associativity. Our aim is to prove that at least one of these groups has an abelian decomposition and then to apply 1 and Theorem 4 which would imply that I defines an abelian group code.

In what follows we will denote the elements of a matrix by the same letter as the matrix itself but in the lower case, for example, $A = (a_{i,j})$.

As in [1] we can assume that the subgroup K has no abelian decomposition and is contained in $\mathrm{UT}_4(F)$ since $\mathrm{UT}_4(F)$ is a Sylow p-subgroup in $\mathrm{GL}_4(F)$.

First note that the group $\mathrm{UT}_4(F)$ has the following abelian decomposition:

$$\mathrm{UT}_4(F) = \left\{ \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \beta \\ 0 & 0 & 0 & 1 \end{pmatrix} : \alpha, \beta \in F \right\} \left\{ \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, b, c, d \in F \right\}.$$

So $K \neq \mathrm{UT}_4(F)$.

4.1 Case $|F| = p = \mathrm{char} F$

If $p = 2$ and K is a proper subgroup of $\mathrm{UT}_4(F)$ then either $|K| = 32$ and K has an abelian decomposition by [7, Proposition 4.2] or $|K| \in \{1, 2, 4, 8, 16\}$ and K has an abelian decomposition by [7, Proposition 3.1]. A contradiction shows that the statement is valid for $p = 2$. Suppose now that p is odd. Then the only possible value of $|K|$ is p^5. Consider the natural homomorphism $\xi : UT_4(F) \to F^3$ defined as follows:

$$\xi : \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & f \\ 0 & 0 & 1 & g \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto (a, d, g)$$

for all $a, b, c, d, f, g \in F$, and let $N = \ker \xi \cap K$, $V = \xi(K)$. Since $|\ker \xi| = p^3$, $|V| \geq p^2$. But if $|V| = p^3$ then K contains a generating system of the group $\mathrm{UT}_4(F)$ modulo its Frattini subgroup $\ker \xi = UT_4(F)'$ (cf. [10, Corollary 10.4.3]) so $K = \mathrm{UT}_4(F)$, a contradiction. If $|V| = p^2$ then $|N| = p^3 = |\ker \xi|$. An easy calculation shows that the centralizer of $\ker \xi$ is contained in the commutative group

$$\left\{ \begin{pmatrix} 1 & 0 & b & c \\ 0 & 1 & d & f \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : b, c, d, f \in F \right\}.$$

This implies commutativity of the group L and the theorem in this case is valid.

4.2 Case $|F| = p^2$

Now we assume that $|F| = p^2$. Let F_0 be the subfield in F containing p elements. Then F is a two-dimensional space over F_0 with a basis $1, \theta$.

Lemma 3. *By some choice of basis in I we can assume that the groups K and L are contained in the group H of block upper-triangular matrices of the form*

$$\left(\begin{array}{c|c} 1 & \overline{v} \\ \hline 0 & \\ 0 & A \\ 0 & \end{array} \right), \tag{1}$$

where $A \in \mathrm{GL}_3(F)$ and $\overline{v} \in F^3$.

Proof. Let $\Delta = \omega G = \left\{ \sum\limits_{g\in G} a_g g \mid \sum\limits_{g\in G} a_g = 0 \right\}$ be the augmentation ideal of the group ring FG. It is well known (see e.g. [11, Lemma 3.1.6]) that this ideal is nilpotent and that its left annihilator coincides with its right annihilator and is the one-dimensional ideal $V = F(\sum\limits_{g\in G} g)$. It follows that any non-zero left (right, two-sided) ideal in FG contains V. Taking a basis of I with the first vector in V we see that any operator of left (right) action of an element $g \in G$ has a matrix of the form (1) with respect to this basis.

As in the previous proof we can assume that the subgroup K is contained in $\mathrm{UT}_4(F)$ since $\mathrm{UT}_4(F)$ is a Sylow p-subgroup in the group of matrices having the form (1).

We need some auxiliary results.

Lemma 4. *If M, N are two groups, M is commutative and every subgroup of N has an abelian decomposition then every subgroup of the group $M \times N$ has an abelian decomposition.*

Proof. Consider the natural projection $\pi : M \times N \to N$. For any $S \leq M \times N$ let $\pi(S) = AB$, where A, B are abelian subgroups in $\pi(S)$. If $\tilde{A} = \pi^{-1}(A) \cap S$ then $\tilde{A}$ is commutative since $\tilde{A} \subseteq M \times A$ and the same is true for $\tilde{B} = \pi^{-1}(B) \cap S$. Note now that $S = \tilde{A}\tilde{B}$: if $x \in S$ then $\pi(x) = ab$ with $a \in A$ and $b \in B$, so $x = \tilde{a}\tilde{b}c$ for some $\tilde{a} \in \tilde{A}$, $\tilde{b} \in \tilde{B}$ and $c \in \ker \pi = M$. Then $\tilde{b}c \in \tilde{B}$ since $c \in M \cap S$.

Lemma 5. *Let $W = F^2$ be a two-dimensional space over F and let V be any F_0-subspace of W with $\dim_{F_0} V = 3$. Then there exist two linearly independent (over F_0) elements $v_1, v_2 \in V$ such that $v_2 = \theta v_1$.*

Proof. Since $|V| = p^3 > |F|$, it follows that $\dim_F FV \geq 2$ and there exist two vectors $e_1, e_2 \in V$ linearly independent over F and a vector $e_3 \in V$, such that e_1, e_2, e_3 is a basis for V over F_0. As a vector of W

$$e_3 = (\alpha_1 1 + \beta_1 \theta)e_1 + (\alpha_2 1 + \beta_2 \theta)e_2$$

for some $\alpha_i, \beta_i \in F_0$, $i = 1, 2$. Then define

$$v_1 = \beta_1 e_1 + \beta_2 e_2 \neq 0,\ v_2 = e_3 - \alpha_1 e_1 - \alpha_2 e_2 = \theta(\beta_1 e_1 + \beta_2 e_2) \neq 0,$$

since e_1, e_2, e_3 are linearly independent over F_0. By definition $v_2 = \theta v_1$.

Lemma 6. *Let $W = F^2$ be a two-dimensional space over F. Then there exists a basis of W over F_0 of the form $v_1, \theta v_1, v_2, \theta v_2$.*

Proof. Take a basis v_1, v_2 of W over F and note that $v_1, \theta v_1, v_2, \theta v_2$ are linearly independent over F_0. Hence they generate a 4-dimensional space over F_0, which necessary coincides with W.

Lemma 7. *If $|F| = p^2$ with a prime p then every subgroup in $\mathrm{UT}_3(F)$ has an abelian decomposition.*

Proof. Let S be a subgroup in $G = \mathrm{UT}_3(F)$. First note that $\mathrm{UT}_3(F) = AB$ where

$$A = \left\{ \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : \alpha, \beta \in F \right\}, \qquad B = \left\{ \begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix} : \alpha, \beta \in F \right\}.$$

So we have to prove that S has an abelian decomposition only for $S \neq G$. Then $|S| \in \{p^i : 0 \leq i \leq 5\}$. If $p = 2$ then the result follows from [7, Proposition 4.2]. Assume that $p > 2$ and that $|S| = p^5$.

Now consider a group homomorphism $\xi : \mathrm{UT}_3(F) \to (F^2, +)$ defined as follows:

$$\xi : \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} \mapsto (\alpha, \beta) \quad \forall \alpha, \beta, \gamma \in F.$$

Clearly $\ker \xi = G' = Z(G)$. If $\dim_{F_0} \xi(S) < 3$ then $|S| = |\xi(S)| \cdot |S \cap \ker \xi| \leq p^2 \cdot p^2 = p^4$ which contradicts the assumption $|S| = p^5$. If $\dim_{F_0} \xi(S) = 4$ then $SG' = G$ and $S = G$ by virtue of [10, Corollary 10.3.3], which also leads to a contradiction. So we must have $\dim_{F_0} \xi(S) = 3$, so $|S/(S \cap G')| = p^3$, hence $|S \cap G'| = p^2$ and $S \supset G'$. By Lemma 5 there exist two linearly independent (over F_0) vectors $v_1 = (\alpha_1, \beta_1)$ and $v_2 = (\alpha_2, \beta_2)$ in $\xi(S)$ such that $(\alpha_1, \beta_1) = \lambda(\alpha_2, \beta_2)$ for some $\lambda \in F$. There exist matrices $x, y \in S$ such that

$$x = \begin{pmatrix} 1 & \alpha_1 & \gamma_1 \\ 0 & 1 & \beta_1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & \alpha_2 & \gamma_2 \\ 0 & 1 & \beta_2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{for some } \gamma_1, \gamma_2 \in F.$$

Direct calculation shows that $[x, y] = 1$, so x, y and $G' = Z(G)$ generate an abelian subgroup A of the group S. Since $|A| = p^4$, we obtain $S = A\langle z \rangle$ for any element $z \notin A$.

Now we proceed with the proof of Theorem 3. First note that if $a_{1,2} = a_{3,4} = 0$ for any matrix $A = (a_{i,j}) \in K$, then K is abelian, which contradicts our assumption.

Case 1. Suppose that $a_{2,3} = a_{3,4} = 0$ for any matrix $A = (a_{i,j}) \in K$. Then there exists an inclusion $\xi : K \to \mathrm{UT}_2(F) \times \mathrm{UT}_3(F)$ given by the rule

$$\xi(A) = \left(\begin{pmatrix} 1 & a_{1,3} \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a_{1,2} & a_{1,4} \\ 0 & 1 & a_{2,4} \\ 0 & 0 & 1 \end{pmatrix} \right).$$

Lemmas 4 and 7 imply that K has an abelian decomposition, a contradiction.

Case 2. If $a_{2,3} = a_{1,2} = 0$ for any matrix $A \in K$, then K is anti-isomorphic to a group from the previous case with the anti-isomorphism given by the rule $A \to P^{-1}A^TP$, where P is the backward identity matrix and A^T is the transposed matrix A.

Case 3. Suppose that $a_{3,4} = 0$ for any matrix $A \in K$, but there exist matrices $A^{(1)}, A^{(2)} \in K$ with $a^{(1)}_{1,2} \neq 0$ and $a^{(2)}_{2,3} \neq 0$.

Consider a matrix $X \in H$ (see Lemma 3). Let $C = [A^{(2)}, X] = A^{(2)}X - XA^{(2)}$, then $c_{3,3} = -a^{(2)}_{2,3}x_{3,2}$ and $c_{4,3} = -a^{(2)}_{2,3}x_{4,2}$. Suppose now that $X \in L$. Then $C = 0$, thus $x_{3,2} = x_{4,2} = 0$ and $x_{2,2} = 1$ since L is a p-group. Therefore matrices $\left\{ \begin{pmatrix} x_{3,3} & x_{3,4} \\ x_{4,3} & x_{4,4} \end{pmatrix} | X \in L \right\}$ form a p-subgroup L_2 of $\mathrm{GL}_2(F)$ and there exists a matrix $T \in \mathrm{GL}_2(F)$ such that $TL_2T^{-1} \leq \mathrm{UT}_2(F)$. If we take $U = \begin{pmatrix} E & 0 \\ 0 & T \end{pmatrix} \in \mathrm{GL}_4(F)$ with E standing for the identity matrix in $M_2(F)$, then $ULU^{-1} \leq \mathrm{UT}_4(F)$. Note that $UKU^{-1} \leq \mathrm{UT}_4(F)$ and $b_{3,4} = 0$ for any matrix $B \in UKU^{-1}$. If $b_{2,3} = 0$ for every matrix $B \in UKU^{-1}$ then we can apply the argument of case 1. Therefore without loss of generality we assume further that $K, L \leq \mathrm{UT}_4(F)$ and that there exists a matrix $B \in K$ such that $b_{2,3} \neq 0$. In this case the relation $[B, X] = 0$ implies that $x_{3,4} = 0$ for any $X \in L$. Since K is not abelian, there exist $A', A'' \in K$ with $[A', A''] \neq 0$, which is equivalent to $a'_{1,2}a''_{2,3} - a''_{1,2}a'_{2,3} \neq 0 \vee a'_{1,2}a''_{2,4} - a''_{1,2}a'_{2,4} \neq 0$. Then

$$\begin{cases} [A', X] = 0 \\ [A'', X] = 0 \end{cases}$$

is equivalent to

$$\begin{cases} a'_{1,2}x_{2,3} - a'_{2,3}x_{1,2} = 0 \\ a'_{1,2}x_{2,4} - a'_{2,4}x_{1,2} = 0 \\ a''_{1,2}x_{2,3} - a''_{2,3}x_{1,2} = 0 \\ a''_{1,2}x_{2,4} - a''_{2,4}x_{1,2} = 0 \end{cases} . \tag{2}$$

Consider the case when $a'_{1,2}a''_{2,3} - a''_{1,2}a'_{2,3} \neq 0$. Then the first and the third equations of (2) imply that $x_{1,2} = x_{2,3} = 0$. Since $a'_{1,2} \neq 0$ or $a''_{1,2} \neq 0$, the second or the forth equation show that $x_{2,4} = 0$, thus L is commutative. The case when $a'_{1,2}a''_{2,4} - a''_{1,2}a'_{2,4} \neq 0$ is analogous.

The anti-isomorphism from case 2 can be applied to reduce the case when $a_{1,2} = 0$ for any matrix $A \in K$ to the considered case.

Case 4. Suppose that $a_{2,3} = 0$ for any matrix $A \in K$, but there exist matrices $A^{(1)}, A^{(2)} \in K$ with $a^{(1)}_{1,2} \neq 0$ and $a^{(2)}_{3,4} \neq 0$. Consider a matrix $X \in H$. Let again $C = [A^{(2)}, X]$, then $c_{3,2} = a^{(2)}_{3,4}x_{4,2}$ and $c_{3,3} = a^{(2)}_{3,4}x_{4,3}$. Suppose now that $X \in L$. Then $C = 0$, thus $x_{4,2} = x_{4,3} = 0$ and $x_{4,4} = 1$ since L is a p-group. Therefore matrices $\left\{ \begin{pmatrix} x_{2,2} & x_{2,3} \\ x_{3,2} & x_{3,3} \end{pmatrix} | X \in L \right\}$ form a p-subgroup in $\mathrm{GL}_2(F)$. Arguing as in case 3, we can assume that $K, L \leq UT_4(F)$. In this case the relation $[A^{(2)}, X] = 0$ implies that $x_{2,3} = 0$. For a matrix $X \in L$ having the aforementioned structure the system of equations $[A, X] = 0 \ \forall A \in K$ is equivalent to the system of linear equations

$$a_{1,2}x_{2,4} + a_{1,3}x_{3,4} - a_{2,4}x_{1,2} - a_{3,4}x_{1,3} = 0 \ \forall A \in K. \tag{3}$$

Since K is not abelian, the rank over F of the coefficient matrix in (3) is at least 2. If this rank is at least 3, then the space of its solutions over F is at most 1-dimensional.

It is easy to check that L is abelian.

Consider the case when the system (3) has rank 2. Then the set of vectors $V = \{(a_{1,2}, a_{1,3}, a_{2,4}, a_{3,4}) |\ A \in K\}$ form a linear space over F_0 of dimension 2, 3 or 4. If $\dim_{F_0} V = 2$, then $|K| \leq p^4$ (since we have no restrictions on matrix elements in the position $(1,4)$), therefore K has an abelian decomposition by [7, Proposition 3.1], a contradiction. If $\dim_{F_0} V = 3$, by Lemma 5 we have a basis over F_0 for V of the form $v_1, v_2 = \theta v_1, v_3$. Consider matrices $A_1, A_2, A_3 \in K$ corresponding to the vectors v_1, v_2, v_3 and subgroups $K_1 = \langle A_1, A_2 \rangle$ and $K_2 = \langle A_3 \rangle$ in K. Since v_1 and v_2 generate a 1-dimensional linear space over F, thus K_1 is abelian and $K = (K_1 Z(K))(K_2 Z(K))$, a contradiction.

If $\dim_{F_0} V = 4$, similarly by Lemma 6 we have a basis over F_0 for V of the form $v_1, v_2 = \theta v_1, v_3, v_4 = \theta v_3$. Again we have matrices $A_1, A_2, A_3, A_4 \in K$ corresponding to these vectors and subgroups $K_1 = \langle A_1, A_2 \rangle$ and $K_2 = \langle A_3, A_4 \rangle$ in K. Both K_1 and K_2 are abelian and $K = (K_1 Z(K))(K_2 Z(K))$, a contradiction.

Case 5. Suppose that there exist matrices $A^{(1)}, A^{(2)}, A^{(3)} \in K$ with $a^{(1)}_{1,2} \neq 0$, $a^{(2)}_{2,3} \neq 0$ and $a^{(3)}_{3,4} \neq 0$.

A subgroup of K generated by $A^{(1)}, A^{(2)}, A^{(3)}$ contains a matrix A with nonzero entries $a_{1,2}, a_{2,3}$ (A may be taken equal to $A^{(1)}$, or $A^{(2)}$ or $A^{(1)}A^{(2)}$) and a matrix A' with nonzero entries $a'_{2,3}, a'_{2,4}$. If it is possible to choose $A = A'$, i.e. $a_{1,2} \neq 0, a_{2,3} \neq 0$ and $a_{3,4} \neq 0$, then A is a non-derogatory matrix, that is its characteristic polynomial coincides with its minimal polynomial. It follows from [12, Theorem 1.3.5] that all matrices commuting with A form a commutative F-algebra. In particular, $C(A) = C_{\mathrm{GL}_4(F)}(A)$ is commutative, hence is $L \subset C(A)$. Assume next $a_{3,4} = a'_{1,2} = 0$. Consider a matrix $X \in L$ and the relations $[A, X] = [A', X] = 0$. As in case 3, the relation $[A, X] = 0$ implies $x_{3,2} = x_{4,2} = 0$, $[A', X] = 0$ implies $x_{4,3} = 0$. Thus X is an upper-triangular matrix, consequently, $X \in \mathrm{UT}_4(F)$ since L is a p-group. Then $[A, X] = [A', X] = 0$ imply $x_{1,2} = x_{3,4} = 0$, that is, L is abelian.

This finishes the proof of Theorem 3.

There exists an alternative proof of Theorem 3 for the case $|F| = p$, namely, it can be deduced from the case $|F| = p^2$ using a slightly modified Theorem 5.1 [7].

Proposition 1. *Let F be a subfield of a field E and G be a group. If all G-codes over E of given dimension k are abelian then all G-codes over F of given dimension k are abelian.*

Proof. For any ideal $I \lhd FG$, $\dim_E(EI) = \dim_F(I)$ and $\mathrm{PAut}(I) = \mathrm{PAut}(EI)$ by [7, Lemma 5.1], so the proof of [7, Theorem 5.1] remains valid.

5 An example

Here we show that the method used in the proof of Theorem 3 does not work if $|F| \geq p^3$. First we prove

Lemma 8. *For any prime p and any field F such that* $\mathrm{char}F = p$ *and* $|F| > p^2$ *the group* $\mathrm{UT}_3(F)$ *contains a subgroup S that does not have an abelian decomposition.*

Proof. It is easy to see that there exists an element $t \in$ such that $1, t, t^2$ are linearly independent over the subfield F_0 of the field F with $|F_0| = p$ (for instance it is true if t generates F^*). Indeed, if F_0 is a finite field then one can take as t any generating element of F over F_0, otherwise the set of all roots in F of all non-zero polynomials over the field F_0 of degree ≤ 2 is finite, and it is sufficient to take t outside of this set. Consider the following three matrices:

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & t & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad z = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & t^2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let S be the subgroup generated by z, y, z. It is clear that $(\mathrm{UT}_3(F))' = Z(\mathrm{UT}_3(F))$, so $S' \subseteq Z(S)$ and the group S' is generated by $[x, y]$,$[y, x]$ and $[x, z]$. By direct calculation we obtain

$$[x, y] = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad [x, z] = \begin{pmatrix} 1 & 0 & \beta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad [y, z] = \begin{pmatrix} 1 & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $\alpha = 1 - t$, $\beta = t^2 - 1$, $\gamma = t^3 - 1$. α, β, γ are linearly independent over F_0 (otherwise the elements 1, $t + 1$ and $t^2 + t + 1$ would be linearly dependent over F_0) so α, β, γ generate a subgroup of order p^3 of the additive group $(F, +)$, and $|S'| = p^3$. Since the vectors $(1, 1)$, $(t, 1)$ and $(1, t^2)$ are linearly independent over F_0, we get $|S/S'| = p^3$ so $|S| = p^6$.

Let us prove that the centralizer of each non-central element $g \in S$ in the group S is a commutative group of order p^4. To do this, fix an element $a = x^k y^l z^m c$ with $(k, l, m) \in \mathbb{Z}_0 \setminus \{(0, 0, 0)\}$ and $c \in Z(S)$ and consider an arbitrary element $x^u y^v z^w d \in S$ where $(u, v, w) \in \mathbb{Z}_0^3$ and $d \in Z(S)$. Computing the commutator $[a, b]$ we see that $ab = ba$ if and only if $(k + lt + m)(u + v + wt^2) = (k + l + mt^2)(u + vt + w)$ (here we identify the elements of $\mathbb{Z}_p$ with the correspondent elements of F_0). In matrix form we obtain

$$\begin{pmatrix} k & l & m \end{pmatrix} \begin{pmatrix} 0 & 1 - t & t^2 - 1 \\ t - 1 & 0 & t^3 - 1 \\ 1 - t^2 & 1 - t^3 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = 0.$$

Dividing by $t - 1 \neq 0$ we get

$$\begin{pmatrix} k & l & m \end{pmatrix} \begin{pmatrix} 0 & -1 & t + 1 \\ 1 & 0 & t^2 + t + 1 \\ -t - 1 & -t^2 - t - 1 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = 0.$$

Computing coefficients with respect to the basis $\{1, t, t^2\}$ of F over F_0 we obtain the following system of equations:

$$\begin{pmatrix} l-m & -k-m & k+l \\ -m & -m & k+l \\ 0 & -m & l \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Subtracting the second equation from the first one and the third equation from the second one gives an equivalent system

$$\begin{pmatrix} l & -k & 0 \\ -m & 0 & k \\ 0 & -m & l \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Note that the matrix of the last system contains 2×2 submatrices with determinants $-k^2$, m^2 and l^2, hence for any $(k, l, m) \neq (0, 0, 0)$ the rank of this matrix equals 2. It follows that the last system of equations has $|F_0| = p$ solutions, so the centralizer of a in S is $\langle a \rangle S'$ thus it is a commutative group of p^4 elements. Then it is a maximal abelian subgroup in S since any abelian subgroup containing a must be contained in $C_S(a)$. So if $S = AB$ for some abelian subgroups A and B then without loss of generality we can assume that A and B contain $Z(S)$ and that $A = C_S(a)$ and $B = C_S(b)$ for any elements $a \in A \setminus Z(S)$ and $b \in B \setminus Z(S)$. But then $|S| = |A||B|/|A \cap B| \leq p^4 p^4 / p^3 = p^5 < p^6 = |S|$. The contradiction proves our claim.

Proposition 2. *If F is a field with* $\mathrm{char} F = p$ *and $|F| > p^2$ then there exist two subgroups $K, L \subseteq \mathrm{UT}_4(F)$ such that $AB = BA$ for any $A \in K$, $B \in L$, but neither K nor L has an abelian decomposition.*

Proof. Consider the groups

$$K_1 = \left\{ \begin{pmatrix} 1 & a & 0 & c \\ 0 & 1 & 0 & g \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, c, g \in F \right\}$$

and

$$L_1 = \left\{ \begin{pmatrix} 1 & 0 & b & c' \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & h \\ 0 & 0 & 0 & 1 \end{pmatrix} : b, c', h \in F \right\}.$$

It is easy to check that elements of K_1 commute with those of L_1, and that there exist isomorphisms

$$\begin{pmatrix} 1 & a & 0 & c \\ 0 & 1 & 0 & g \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & a & c \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & b & c' \\ 0 & 1 & 0 & 0 \\ 0 & 1 & h & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & b & c' \\ 0 & 1 & h \\ 0 & 0 & 1 \end{pmatrix}$$

between K_1, L_1 and $\mathrm{UT}_3(F)$. The inverse images $K \subseteq K_1$ and $L \subseteq L_1$ of the group S from Lemma 8 under these isomorphisms have the desired properties.

It follows only that the technique used in Section 3 cannot be applied to the case when $|F| > p^2$. Of course this does not answer in negative the question of existence for the non-abelian codes of dimension 4 in the case of p-groups.

Acknowledgements

Authors want specially remember Victor Markov and acknowledge his valuable contribution to this paper before he passed away in July 2019.

References

1. García Pillado, C., González, S., Markov, V., Markova, O. and Martínez, C.: Group codes of dimension 2 and 3 are abelian. Finite Fields and their Applications. **55**, 167–176 (2019)
2. Macwilliams, F.J., Sloane, N.J.A.: The theory of Error-Correcting Codes, North-Holland, Amsterdam-London-New York-Tokyo (1977)
3. Pless, V.S., Huffman, W.C., Editors: Handbook of Coding Theory I, II. Elsevier (1998)
4. Nechaev, A.A.: Kerdock code in a cyclic form, Diskret. Mat. **1**(4), 123–139 (1989) (in Russian); English transl. in: Discrete Math. Appl. **2**(6), 659-683 (1992)
5. Hammons Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., and Solé,P.: The Z_4-linearity of Kerdock, Preparata, Goetals and related codes, IEEE Trans. Inform. Theory **40**, 301–319 (1994)
6. Bernal, J.J., del Río, Á., and Simón, J.J.: An intrinsical description of group codes. Designs, Codes and Cryptography, **51**(3), 289–300 (2009)
7. García Pillado, C., González, S., Markov, V., Martínez, C., and Nechaev, A.A.: Group codes over non-abelian groups. J. Algebra Appl., **12**, 1350037-1–1350037-20 (2013)
8. García Pillado, C., González, S., Markov, V., Martínez, C., and Nechaev, A.A.: New examples of non-abelian group codes, Adv. Math. Commun. **10**(1), 1–10 (2016)
9. García Pillado, C., González, S., Markov, V., Martínez, C.: Non-abelian group codes over an arbitrary finite field. Fundementalnaya i prikladnaya matematika, **20**(1), 17–22 (2015) (*in Russian*).
10. Hall, M.: The Theory of Groups. Harper and Row, NY (1968)
11. Passman, D.S.: The algebraic structure of group rings, John Wiley & Sons, New York, London, Sydney, Toronto (1977)
12. Suprunenko, D.A., Tyshkevich, R.I.: Commutative matrices, Academic Pr., New York, NY (1968)