Algebra and Discrete Mathematics RESEARCH ARTICLE
Number ?. **(????).** pp. 1–6

A nilpotent non abelian group code

Gabriele Nebe, Artur Schäfer

Communicated by Communicated person

19.11.2012

Abstract. The paper reports an example for a nilpotent group code which is not monomially equivalent to some abelian group code.

Introduction

A linear code is a subspace of the row space F^n for some field F. The most important linear codes for practical applications are cyclic codes. A cyclic code can be considered as an ideal of the ring $F[x]/(x^n - 1)$. This structure gives rise to fast decoding algorithms [5, Chapter 3]. F.J. MacWilliams [6] gave an interpretation of cyclic codes as ideals of the group ring $FC_n \cong F[x]/(x^n - 1)$ and generalised this to the concept of group ring codes. A G-code is a two-sided ideal C in the group ring FG. The code C is called **abelian** (**cyclic**, **nilpotent**) if the group G is abelian (resp. cyclic or nilpotent).

If the group G can be written as $G = AB$ for two abelian subgroups $A, B \leq G$, for short G has an **abelian decomposition**, then by [3, Theorem 3.1] every G-code is an abelian group code. However it is not true in general that any group ring code is abelian: In [4] a group ring code in $\mathbb{F}_5 S_4$ is given that is not abelian; note that S_4 is the smallest group that does not have an abelian decomposition, and 5 is the smallest prime not dividing the order of S_4. Ángel del Río (personal communication) asked whether all nilpotent group ring codes are abelian. His question was the motivation for this short note. Using experiments in Magma we

2010 Mathematics Subject Classification: *05E20, 94B05, 94B15.*

Key words and phrases: *group ring codes, monomial equivalence, nilpotent groups.*

find a metabelian group G of order 2^6 and an ideal $C \trianglelefteq \mathbb{F}_3G$ that is not an abelian group code. Again all smaller p-groups G admit an abelian decomposition, so this is the smallest possible example for non abelian nilpotent group ring code. Generalising the criterion of [3, Theorem 1.2] to monomial equivalences we show that this code C is not monomially equivalent to an abelian group code.

1. Monomial group codes

Let F be some field and F^n the space of rows of length n. The standard basis of F^n will always be denoted by $(e_1, \ldots, e_n)$. A **linear code** of length n over F is a subspace $C \leq F^n$. The symmetric group S_n acts by coordinate permutations on F^n. We call two linear codes **permutation equivalent** if they are in the same orbit under this action and denote by $\mathrm{Perm}(C) := \{\sigma \in S_n \mid C\sigma = C\}$ the stabiliser of C in S_n. There is a coarser notion of **monomially equivalence** defined by the natural action of the full monomial group $\mathrm{Mon}_n(F) := F^* \wr S_n$, the stabiliser of C is the **monomial automorphism group** $\mathrm{Mon}(C) := \mathrm{Stab}_{\mathrm{Mon}_n(F)}(C)$. Since $S_n \leq \mathrm{Mon}_n(F)$ we have $\mathrm{Perm}(C) \leq \mathrm{Mon}(C)$. As $\mathrm{Mon}_n(F)$ is a semidirect product, there is a split short exact sequence

$$1 \to (\mathbb{F}^*)^n \to \mathrm{Mon}_n(F) \xrightarrow{\phi} S_n \to 1.$$

Then $\mathrm{Perm}(C) = \phi(\mathrm{Perm}(C))$ is a subgroup of $\phi(\mathrm{Mon}(C))$.

Definition 1. *Let $G = \{g_1, \ldots, g_n\}$ be a finite group and let F be a field. Any ideal $I \trianglelefteq FG$ defines a linear code $C(I) \leq F^n$ by*

$$(a_1, a_2, ..., a_n) \in C(I) \Leftrightarrow a_1g_1 + a_2g_2 + \cdots + a_ng_n \in I.$$

*Any code which is permutation equivalent to $C(I)$ for some ideal I of FG is called a G-**code**. Similarly, any code which is monomial equivalent to $C(I)$ for some ideal I of FG is called a G-**mcode**.*

Clearly every G-code is also a G-mcode.
The code $C = \langle(1, 0, 2, 0), (0, 1, 0, 3)\rangle \leq \mathbb{F}_5^4$ is a C_4-mcode but not a C_4-code.

The next remark is well known, see for instance [3, Lemma 1.1].

Remark 1. Let $H = \{1 = h_1, \ldots, h_n\}$ be a regular subgroup of S_n such that $1h_j = j$ for all $1 \leq j \leq n$. For $1 \leq k \leq n$ define $\pi_k \in S_n$ by $j\pi_k = kh_j$. Then the centralizer $C_{S_n}(H) = \{1 = \pi_1, \ldots, \pi_n\} =: \rho(H)$ is a regular subgroup of S_n which is anti-isomorphic to H.

Proof. We have $j\pi_k h_\ell = kh_j h_\ell$ and $jh_\ell \pi_k = 1(h_j h_\ell)\pi_k = kh_j h_\ell$. So $\rho(H)$ and H commute. Let $\pi \in C_{S_n}(H)$ and $k := 1\pi$. Then $\sigma := \pi\pi_k^{-1} \in C_{S_n}(H)$ stabilises 1, and so $k\sigma = 1h_k\sigma = 1\sigma h_k = 1h_k = k$ which shows that $\sigma = 1$. Moreover $h_k \mapsto \pi_k$ is the required anti-isomorphism. □

Lemma 1. *Let $H \leq \mathrm{Mon}_n(F)$ such that $H \cong \phi(H)$. Assume that $\phi(H)$ is a regular subgroup of S_n. Then there is an element $\lambda \in (F^*)^n$ such that $\tilde{H} := \lambda H \lambda^{-1} \leq S_n$. Moreover the centralizer*

$$\lambda C_{\mathrm{Mon}_n(F)}(H)\lambda^{-1} = F^* \times C_{S_n}(\tilde{H}) = F^* \times \rho(\tilde{H}).$$

Proof. Let $(e_1, \ldots, e_n)$ denote the standard basis of F^n. Since $\phi(H)$ acts regularly on $\{1, \ldots, n\}$ we can enumerate $H = \{1 = h_1, h_2, ..., h_n\}$ such that $e_1 h_i = \lambda_i e_i$ for some $\lambda_i \in F^*$, $i = 1, 2, ..., n$. Set $\lambda = \mathrm{diag}(1, \lambda_2, ..., \lambda_n) \in (F^*)^n$. Then

$$e_i(\lambda h_j \lambda^{-1}) = \lambda_i e_i h_j \lambda^{-1} = e_1 h_i h_j \lambda^{-1} = e_1 h_k \lambda^{-1} = e_k \qquad (1)$$

for all $1 \leq i, j \leq n$, where h_k is uniquely determined by $h_i h_j = h_k$. So $\tilde{H} := \lambda H \lambda^{-1} \leq S_n$.
To obtain the centralizer of H in the monomial group let $X := \langle F^*, C_{S_n}(\tilde{H})\rangle$. Then clearly $X \leq C_{\mathrm{Mon}_n(F)}(\tilde{H})$. Conversely, take an element $c \in C_{Mon_n(F)}(\tilde{H})$. Multiplying c by some suitable element of X we may assume that $e_1 c = e_1$. Then

$$e_k c = e_1 \tilde{h}_k c = e_1 c \tilde{h}_k = e_1 \tilde{h}_k = e_k \text{ for all } 1 \leq k \leq n$$

so $c = 1$. □

Theorem 1. *Let C be a linear code of length n over a field F and let G be a finite group of order n.*

1. *C is a right G-mcode (i.e. monomially equivalent to some right ideal in FG) if and only if G is isomorphic to a subgroup $H \leq \mathrm{Mon}(C)$ such that $\phi(H)$ is a regular subgroup of S_n.*

2. *C is a G-mcode if and only if G is isomorphic to a subgroup $H \leq \mathrm{Mon}(C)$ such that $\phi(H)$ and $\phi(C_{\mathrm{Mon}(C)}(H))$ are regular subgroups of S_n.*

Proof. **1.** Suppose C is a right G-mcode. Since the statement is invariant under monomial equivalence, we may assume that $C = C(I)$ for some right ideal I of FG. Then $\phi(G) = G \leq \mathrm{Perm}(C)$ is a regular subgroup of S_n. Conversely, suppose $G \leq \mathrm{Mon}(C)$ for a code $C \leq F^n$ such that $\phi(G) \leq S_n$ is regular. By Lemma 1 the group G is conjugate to some subgroup of $S_n \leq \mathrm{Mon}_n(F)$, so replacing C by some monomial equivalent code, we may assume that $G \leq \mathrm{Perm}(C)$. Then the statement follows from [3, Theorem 1.2]

2. Again the statement is invariant under monomial equivalence, so by Lemma 1 we may again assume that $G \leq \mathrm{Perm}(C)$. Since the centralizer of G in the full monomial group is generated by the center $F^* = Z(\mathrm{Mon}_n(F))$ and the centralizer of G in S_n, the condition of the theorem implies that $C_{\mathrm{Mon}(C)}(G) = C_{\mathrm{Mon}_n(F)}(G) = F^* \times \rho(G)$. Again we may use [3, Theorem 1.2] to get the claim. □

2. A 2-group code that is not abelian

In this section we will show that not all nilpotent group codes are abelian. To this aim we want to find an ideal I in some group ring FG of a p-group G for which $\phi(\mathrm{Mon}(C(I)))$ does not contain an abelian regular subgroup. We use the small groups library in GAP and Magma. The smallest p-group G that does not have an abelian decomposition has order 2^6. We choose $F = \mathbb{F}_3$ the smallest field of characteristic $\neq 2$ and some central idempotent e of FG so that $\mathrm{Mon}(C(eFG))$ is not too large. With Magma we check that $\phi(\mathrm{Mon}(C(eFG)))$ does not contain a regular abelian subgroup.

Theorem 2 (Counterexample)**.** *Let G be the group of order 64 with presentation*

$$\begin{aligned} \langle x_1, ..., x_6 \quad | \quad & x_1^2 = \cdots = x_6^2 = 1, \\ & [x_4, x_1] = [x_5, x_1] = [x_6, x_1] = 1, \\ & [x_4, x_2] = [x_5, x_2] = [x_6, x_2] = 1, \\ & [x_4, x_3] = [x_5, x_3] = [x_6, x_3] = 1, \\ & [x_5, x_4] = [x_6, x_4] = [x_5, x_6] = 1, \\ & [x_2, x_1] = x_4, [x_3, x_1] = x_5, [x_3, x_2] = x_6 \rangle \end{aligned}$$

(G=SmallGroup(64,73) in the GAP/Magma ([1]/[2]) library). Then $G' = Z(G)$ and G/G' are elementary abelian of order 8, in particular G is metabelian. Furthermore, let $\chi_1, .., \chi_{22}$ be the irreducible complex characters of G in the ordering given in GAP/Magma and $\epsilon_1, ..., \epsilon_{22} \in \mathbb{C}G$ be the corresponding central primitive idempotents. Set $\epsilon = \epsilon_2 + \epsilon_5 + \epsilon_7 + \epsilon_9 + \epsilon_{11} + \epsilon_{13} + \epsilon_{15} + \epsilon_{17} + \epsilon_{19} \in \mathbb{Z}[\frac{1}{2}]G$ and see this as a central idempotent in $\mathbb{F}_3G$. Then the code $C(\epsilon\mathbb{F}_3G)$ is not monomial equivalent to an abelian code. In particular it is not permutation equivalent to an abelian code.

Proof. For the proof we give the Magma program to construct this code and check that it is not monomially equivalent to some abelian group ring code using the criterion of Theorem 1.

```
g:=SmallGroup(64,73);
A:=GroupAlgebra(CyclotomicField(#g),g);
d:=ClassFunctionSpace(g);b:=Basis(d);
// all complex characters
e:=[];
// the central primitive idempotents
for i in [1..#b] do
a:=0;
for j in g do
s:=b[i](j^-1)*A!j;
a:=a+s;
end for;
e[i]:=b[i](Id(g))/(#g)*a;
end for;
E:=e[2]+e[5]+e[7]+e[9]+e[11]+e[13]+e[15]+e[17]+e[19];
// all coefficients of E are rational numbers
I:=ideal⟨A | E⟩;
// the ideal I has dimension 27
m:=ZeroMatrix(GF(3),Dimension(I),#g);
// Generator matrix of the code
bb:=Basis(I);
for ii in [1..Dimension(I)] do
for jj in [1..#g] do
m[ii][jj]:=Coefficients(bb[ii])[jj];
end for;
end for;
C:=LinearCode(m);
M:=MonomialGroup(C);
phiofM:=Image(BlocksAction(M,1,2));
// Computes the monomial group M of the code and the image under phi
Subgroups(phiofM:IsAbelian:=true,IsTransitive:=true);
// Returns all subgroups of phiofM which are abelian and transitive.
```

The order of M is $2 \cdot 2^{11}$, the order of $\phi(M)$ is 2^{11}. The group $\phi(M)$ does not contain any abelian regular subgroup, So this code is not monomial equivalent to an abelian code by Theorem 1. □

References

[1] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.6; 2012. (http://www.gap-system.org)

[2] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997) 235-265. (http://magma.maths.usyd.edu.au/magma/)

[3] J.J. Bernal, Á. del Río, J.J. Simón, An intrinsical description of group codes, Designs, Codes and Cryptography, 51 (2009) 289-300.

[4] C. García Pillado, S. González, V. T. Markov, C. Martínez, A. A. Nechaev, When are all group codes of a noncommutative group Abelian (a computational approach)? Journal of Mathematical Sciences **186** (2012) 578-585.

[5] W. Lütkebohmert, Codierungstheorie, Vieweg (2003).

[6] F. J. MacWilliams, Codes and ideals in group algebras. 1969 Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967) pp. 317-328 Univ. North Carolina Press, Chapel Hill, N.C.

Contact information

G. Nebe
Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
E-Mail: nebe@math.rwth-aachen.de
URL: www.math.rwth-aachen.de/∼nebe/

A. Schäfer
Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
E-Mail: artur.schaefer@rwth-aachen.de
URL: