Journal of Mathematical Sciences, Vol. 186, No. 4, October, 2012

WHEN ARE ALL GROUP CODES OF A NONCOMMUTATIVE GROUP ABELIAN (A COMPUTATIONAL APPROACH)?

C. García Pillado, S. González,
V. T. Markov, C. Martínez, and A. A. Nechaev

UDC 519.725+512.552.7

Abstract. Let G be a finite group and F be a field. Any linear code over F that is permutation equivalent to some code defined by an ideal of the group ring FG will be called a G-code. The theory of these "abstract" group codes was developed in 2009. A code is called Abelian if it is an A-code for some Abelian group A. Some conditions were given that all G-codes for some group G are Abelian but no examples of non-Abelian group codes were known at that time. We use a computer algebra system GAP to show that all G-codes over any field are Abelian if $|G| < 128$ and $|G| \notin \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, but for $F = \mathbb{F}_5$ and $G = \mathrm{S}_4$ there exist non-Abelian G-codes over F. It is also shown that the existence of left non-Abelian group codes for a given group depends in general on the field of coefficients, while for (two-sided) group codes the corresponding question remains open.

Introduction

Let F be a field. We consider the natural action of the symmetric group S_n on the n-dimensional space F^n defined as permutation of coordinates:

$$\sigma(a_1, \dots, a_n) = \big(a_{\sigma(1)}, \dots, a_{\sigma(n)}\big) \quad \text{for all} \quad (a_1, \dots, a_n) \in F^n.$$

We recall that two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq F^n$ are *permutation equivalent* if there exists a permutation $\sigma \in \mathrm{S}_n$ such that $\mathcal{C}_2 = \sigma(\mathcal{C}_1)$. For a given code $\mathcal{C} \subseteq F^n$, the group of all permutations $\sigma \in \mathrm{S}_n$ such that $\sigma(\mathcal{C}) = \mathcal{C}$ is denoted by $\mathrm{PAut}(\mathcal{C})$.

Let $G = \{g_0 = e, g_1, \dots, g_{n-1}\}$ be a finite group. Any (left) ideal L of the group ring FG defines a (left) group code $\mathcal{K}(L)$ of length n over F by the rule

$$(a_0, a_1, \dots, a_{n-1}) \in \mathcal{K}(L) \iff a_0 g_0 + a_1 g_1 + \dots + a_{n-1} g_{n-1} \in L.$$

Any code that is permutation equivalent to $\mathcal{K}(L)$ for some (left) ideal L of the ring FG is called a (*left*) *G-code.*

A code is called *Abelian* if it is an A-code for some Abelian group A. In [1], it was proved that there exist non-Abelian left group codes but no non-Abelian group codes were presented.

In this note, we show how to use the computer algebra system GAP [3] to describe some groups for which all group codes are Abelian as well as to give an example of a non-Abelian group code and to prove that all left group codes in $\mathbb{F}_2\mathrm{Q}_8$ are Abelian.

For any subsets A and B of a group G, we denote by AB the set of all products ab with $a \in A$ and $b \in B$. We say that a group G *has an Abelian decomposition* if there exist Abelian subgroups A, B in G such that $G = AB$. This condition was introduced in [1], where it was proved that if a group G has an Abelian decomposition then any G-code is an Abelian group code [1, Theorem 3.1]. We show that all groups G of orders less than 127, except those with $|G| \in \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, have an Abelian decompositions. Also we give the full list of groups of order $2^6 = 64$ having no Abelian decomposition. Some of these examples give also a negative answer to the following natural question: Does every group of exponent 4 and nilpotent length 2 have an Abelian decomposition? Then we show that there exist S_4-codes over $\mathbb{F}_5$ that are not Abelian codes. Finally, we show that all left ideals in the group ring $\mathbb{F}_2\mathrm{Q}_8$ are two-sided, so they are Abelian codes, while in [2] it was shown that there are left

Translated from Fundamentalnaya i Prikladnaya Matematika, Vol. 17, No. 2, pp. 75–85, 2011/12.

1072–3374/12/1864–0578

$[8,3,5]$-codes in $\mathbb{F}_4\mathrm{Q}_8$ but no left codes with the same parameters in any ring $\mathbb{F}_4A$, where A is an Abelian group of order 8 (it should be noted, to avoid confusion, that left group codes were called group codes in [2]).

1. Abelian Decompositions

The next lemma is an easy exercise in elementary group theory.

Lemma 1.1.

(1) *If A and B are two subgroups of a group G, then*

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}.$$

(2) *If $G = AB$ for some subgroups A and B, then for any subgroup A' conjugated to A there exists a subgroup B' conjugated to B such that $G = A'B'$.*

So one can use the following simple GAP function to decide whether a given group G has an Abelian decomposition.

```
HasAbelianDecomposition:=function(G)
local lat, A, x, xx, y, z, n, flag;
n:=Size(G);
lat:=LatticeSubgroups(G);
#GAP calculated the lattice of all subgroups
A:=Filtered(ConjugacyClassesSubgroups(lat),
x->IsAbelian(Representative(x)));
#A is the list of conjugacy classes of Abelian subgroups
flag:=0;
for xx in A do x:=Representative(xx);
#take any representative of a~given class
for y in A do for z in AsList(y) do
#test all Abelian subgroups in G
if Size(x)*Size(z)/Size(Intersection(x,z))=n
then return true; fi;
od; od;
od;
return false;
#function returns ’true’ if an Abelian decomposition was found
#and ’false’ otherwise
end;
```

The next code gives an example of the usage of this function.

```
for n in [2..127] do cnt:=0;
for G in AllSmallGroups(Size,n,IsAbelian,false) do
if not HasAbelianDecomposition(G) then cnt:=cnt+1; fi; od;
if cnt>1 then Print(n, " ", cnt, "\n"); fi;
od;
```

The output of this code is the following table.

```
24 2
48 6
54 1
60 1
64 19
```

```
72 7
96 26
108 4
120 6
```

There exist pure algebraic proofs that any group of order $p^i q^j$, where p, q are (not necessarily different) primes and $0 \leq i, j \leq 2$, has an Abelian decomposition, as well as any group of order $32 = 2^5$. These proofs will be published later. Also there is a construction of a group of order p^5 having no Abelian decomposition, where $p > 2$ is a prime. The output we have provided shows the sharpness of these results.

We see that there are two groups of order 24 that have no Abelian decomposition. We can identify one of them as follows.

Proposition 1.2. *The symmetric group* S_4 *has no Abelian decomposition.*

Proof. Execution of the following line in GAP

```
HasAbelianDecomposition(SymmetricGroup(4));
```

produces the result `false`. □

Note also that there are sufficiently many groups of order 64 having no Abelian decomposition. Table 1 contains the GAP library number, exponent, and nilpotent length for each of these groups.

Table 1. Groups of order 64 having no Abelian decomposition.

GAP number	Exponent	Nilpotent length
[64, 73]	4	2
[64, 74]	4	2
[64, 75]	4	2
[64, 76]	4	2
[64, 77]	4	2
[64, 78]	4	2
[64, 79]	4	2
[64, 80]	4	2
[64, 81]	4	2
[64, 82]	4	2
[64, 149]	8	3
[64, 150]	8	3
[64, 151]	8	3
[64, 170]	8	3
[64, 171]	8	3
[64, 172]	8	3
[64, 177]	8	3
[64, 178]	8	3
[64, 182]	8	3

We can give a nice presentation of these groups. For example, the first one, that with GAP index $[64, 73]$, can be constructed as follows. Consider an elementary Abelian 2-group N with three generators

z_1, z_2, and z_3 and also an elementary Abelian group H with three generators $\bar{x}_1$, $\bar{x}_2$, and $\bar{x}_3$. It is easy to prove, using Schreier's theorem [4, Theorem 15.1.1], that there exists an extension G with $N = Z(G)G$ and $G/N \cong H$ such that for some preimages x_1, x_2, and x_3 of $\bar{x}_1$, $\bar{x}_2$, and $\bar{x}_3$ the following relations are satisfied:

$$x_i^2 = z_i^2 = e, \quad i = 1, 2, 3; \quad [x_i, z_j] = [z_i, z_j] = e, \quad i, j = 1, 2, 3;$$
$$[x_i, x_j] = z_{i+j-2}, \quad i, j = 1, 2, 3, \quad i < j.$$

The required automorphisms $a \mapsto a^h$ of the group N are identity maps, and the factor system should be defined as follows:

$$(\bar{x}_1^{k_1} \bar{x}_2^{k_2} \bar{x}_3^{k_3}, \bar{x}_1^{r_1} \bar{x}_2^{r_2} \bar{x}_3^{r_3}) = z_1^{r_1 k_2} z_2^{r_1 k_3} z_3^{r_2 k_3} \quad \text{for all} \quad k_i, r_j \in \mathbb{F}_2, \quad i, j = 1, 2, 3.$$

2. Non-Abelian Group Codes in $\mathbb{F}_5\mathrm{S}_4$

Of course, it does not follow from Proposition 1.2 that there exist non-Abelian S_4-codes over some fields. Nevertheless, we provide such examples below. To the end of this section we fix $F = \mathbb{F}_5$ and $G = \mathrm{S}_4$ realized as the group of permutations of the set $\{0, 1, 2, 3\}$.

Our study of ideals in the group algebra FG is based on application of the GAP function `DirectSumDecomposition(A)`, which gives the decomposition of a semisimple finite dimensional ring A into a sum of minimal ideals. In our case, R is semisimple by the classical Maschke theorem, whence the following GAP code gives five minimal ideals in R.

```
G:=SymmetricGroup(4);
F:=GF(5);
R:=GroupRing(F,G);
D:=DirectSumDecomposition(R);;
List(D,Dimension);
```

The output of this fragment is `[ 9, 9, 4, 1, 1 ]`, i.e., there are two ideals of dimension 1, two ideals of dimension 9, and one ideal of dimension 4.

Theorem 2.1. *Codes corresponding to* 9*-dimensional minimal ideals of the ring* R *are non-Abelian.*

Proof. Direct calculation of the permutation automorphism group for the codes in question would take too much time; so we used the following "flanking manoeuvre."

First, we calculated the weight distributions for these two ideals using the following GAP function.

```
WeightDistribution:=function(I,R)
local wlist, k, j, d, x, V, B, mf;
mf:=Size(LeftActingDomain(R))-1;
wlist:=List([0..Dimension(R)],x->0);
wlist[1]:=1;
d:=Dimension(I);
B:=BasisVectors(Basis(I));
for j in [1..d] do
V:=SubspaceNC(R,B{[(j+1)..d]});
for x in V do
k:=Size(CoefficientsAndMagmaElements(B[j]+x))/2+1;
wlist[k]:=wlist[k]+mf;
od;
od;
return wlist;
end;
```

This function was used as follows:

```
WD1:=WeightDistribution:=function(D[1],R);
WD2:=WeightDistribution:=function(D[2],R);
```

The two weight distributions turned out to be identical, and they are described by the following table.

Weight d	Number of words of weight d	Weight d	Number of words of weight d
0	1	17	190080
8	324	18	320640
10	144	19	365184
12	5520	20	437952
13	2304	21	245760
14	23808	22	158400
15	23328	23	47232
16	111840	24	20608

Then we tested all Abelian codes of length 24 over $\mathbb{F}_5$. This part of the computation turned out to be the most time consuming; so we have applied the following simple observations:

(1) the action of a group automorphisms on any group can be extended to the group ring, and this extension is a weight-preserving automorphism of the group ring;

(2) during the computation of a weight distribution of some ideal, it happens that for some weight w the number of already found words with weight w exceeds the number of such words in the already known weight distribution WD1; then this weight distribution for this ideal cannot be identical to WD1, so the calculation for this ideal should stop at this moment.

So we used the following GAP functions.

(1) A technical function transforming automorphisms of a group to automorphisms of the group ring.

```
StandardIsomorphismsOfAGroupRing:=function(R,HH)
local H, h, f, x, y, B1, B2, C, n;
H:=[];
B1:=BasisVectors(Basis(R));
n:=Size(B1);
C:=List(B1, x->(CoefficientsAndMagmaElements(x)[1]));
for h in HH do
B2:=List([1..n], x->B1[Position(C,Image(h,C[x]))]);
#Print(B2, "\n");
Add(H, AlgebraHomomorphismByImagesNC( R, R, B1, B2 ));
od;
return H;
end;
```

(2) A function producing a list of ideals of given dimension k. Each of these ideals is defined as a sum of minimal ideals whose dimensions are enumerated in the list l.

```
CombinationsOfGivenSum:=function(l,k)
local AllCombList, n, s; n:=Size(l);
AllCombList:=Combinations([1..n]);
return Filtered(AllCombList, x->(Sum(List(x, i->l[i]))=k));
end;
```

(3) A function enumerating the permutations of the set of minimal ideals induced by the set H of group automorphisms.

```
PermutationsOfComponents:=function(R,H,DSD)
local x, y, h, HH, PL, l, B, I, II, pl;
l:=Size(DSD);
PL:=[[1..l]]; #identity permutation must present
HH:=StandardIsomorphismsOfAGroupRing(R,H);
for h in HH do
pl:=[];
for I in DSD do
B:=BasisVectors(Basis(I));
II:=Ideal(R,List(B,y->Image(h,y)));
Add(pl,Position(DSD,II));
od;
if not pl in PL then Add(PL,pl); fi;
od;
return PL;
end;
```

(4) A function checking if some permutation of minimal ideals contained in the permutation list PL transforms the set of minimal ideals into some set that is lexicographically less than the given one. While searching for an ideal with identical weight distribution it is sufficient to consider only those that correspond to lexicographically minimal sets of minimal ideals.

```
IsMinimalCombination:=function(L, PL)
local x, i;
for x in PL do
for i in L do
if x[i]>i then break; else if x[i]<i then return false; fi; fi;
od;
od;
return true;
end;
```

(5) A function comparing the weight distribution of an ideal to the given weight distribution.

```
EqualWeightDistribution:=function(I,R, WD)
local wlist, k, j, d, x, V, B, mf;
mf:=Size(LeftActingDomain(R))-1;
wlist:=List([0..Dimension(R)],x->0);
wlist[1]:=1;
d:=Dimension(I);
B:=BasisVectors(Basis(I));
for j in [1..d] do
V:=SubspaceNC(R,B{[(j+1)..d]});
for x in V do
k:=Size(CoefficientsAndMagmaElements(B[j]+x))/2+1;
wlist[k]:=wlist[k]+mf;
if wlist[k]>WD[k] then return false; fi;
od;
od;
```

```
return true;
end;
```

Now we present the main code that checks the statement of the theorem.

```
G:=SymmetricGroup(4);
F:=GF(5);
R:=GroupRing(F,G);
D:=DirectSumDecomposition(R);;
WD1:=WeightDistribution(D[1],R);
allab:=AllSmallGroups(Size,24,IsAbelian,true);;
for A in allab do
R:=GroupRing(F,A);;
dsd:=DirectSumDecomposition(R);;
dsddim:=List(dsd,Dimension);;
CL:=CombinationsOfGivenSum(dsddim,9);;
H:=AutomorphismGroup(G);;
dsdperm:=PermutationsOfComponents(R,H,dsd);;
RCL:=Filtered(CL, x->IsMinimalCombination(x,dsdperm));;
for C in RCL do I:=Sum(List(C, x->dsd[x]));;
if EqualWeightDistribution(I,R, WD1) then
Print("Equal weight distribution found\n");; break;
fi;
od;
od;
```

The execution of this code took several hours and no Abelian codes with weight distribution stored in `WD1` were found. □

Remark 2.2. In a subsequent paper, we give a pure algebraic proof that the ideals `D[3]`, `D[4]`, and `D[5]` define Abelian codes. However, no pure algebraic proof has been found for Theorem 2.1.

3. Base Field Change

It is unknown, in general, if for a given group G the existence of non-Abelian codes in FG depends on the coefficient field F. In a subsequent paper, we will prove the following two statements.

Proposition 3.1. *Let F be a subfield of a field E and G be a group. If all G-codes over E are Abelian, then all G-codes over F are Abelian.*

Proposition 3.2. *Let F be a subfield of a field E and G be a group. Suppose, in addition, that* $\operatorname{char} F \nmid |G|$ *and F is a splitting field for G, i.e.,*

$$FG \cong \bigoplus_{i=1}^{k} \mathrm{M}_{d_i}(F)$$

(*the group algebra is a direct sum of matrix algebras over F*). *Under these conditions, if all G-codes over F are Abelian, then all G-codes over E are Abelian.*

Here we emphasize the difference between the cases of group codes and left group codes: there is a rather simple example showing that the similar property of left group codes cannot be lifted to a field extensions in general.

Theorem 3.3. *Let $F = \mathbb{F}_2$, $E = \mathbb{F}_4$ be its extension, and G be the quaternion group Q_8. Then all left G-codes over F are Abelian but there exist left G-codes over E that are not.*

Proof. The second part of the statement follows from the already mentioned result of [2, Table 6]: there exist left $[8, 3, 5]$-codes in $\mathbb{F}_4\mathrm{Q}_8$ but no left A-codes over $\mathbb{F}_4$ have the same parameters for any Abelian group A of order 8.

To prove the first part of the statement, it is enough to check that any left ideal in FG is a two-sided ideal. Indeed, any Q_8-code over any field is Abelian by [1, Theorem 3.1] and the results of Sec. 1.

We again present here a GAP program checking this statement although a pure algebraic proof is known and will be published elsewhere.

Of course one can consider only principal left ideals since any left ideal is a sum of principal ones. The code below is not optimized for execution speed but seems to be the most simple one.

```
List(AllSmallGroups(Size,8), StructureDescription);
[ "C8", "C4 x C2", "D8", "Q8", "C2 x C2 x C2" ]
Q:=AllSmallGroups(Size,8)[4];;
F:=GF(2);;
R:=GroupRing(F,Q);;
for x in R do I:=LeftIdeal(R,[x]);
for y in R do
if not (x*y in I) then
Print(x,"*",y," not in Rx\n"); break;
fi;
od;
od
```

We have included the output for the first line since it seems to be the simplest way to define the quaternion group in a GAP session. The execution this code takes several seconds. It produced no output so the statement is valid. □

Acknowledgments. The authors wish to express their gratitude to A. V. Mikhalev for constant attention to their work.

REFERENCES

1. J. J. Bernal, Á. del Río, and J. J. Simón, "An intrinsical description of group codes," *Designs, Codes and Cryptography*, **51**, No. 3, 289–300 (2009).
2. E. Couselo, S. González, V. Markov, and A. Nechaev, "Loop codes," *Discrete Math. Appl.*, **14**, No. 2, 163–172 (2004).
3. http://www.gap-system.org/.
4. M. Hall, *The Theory of Groups*, Harper and Row, New York (1968).

Cristina García Pillado
University of Oviedo, Oviedo, Spain

Santos González
University of Oviedo, Oviedo, Spain

Victor Markov
Moscow State University, Moscow, Russia

Consuelo Martínez
University of Oviedo, Oviedo, Spain

Alexandr Nechaev
Moscow State University, Moscow, Russia
E-mail: alexnechaev@inbox.ru