Bull. Korean Math. Soc. **51** (2014), No. 6, pp. 1605–1614
http://dx.doi.org/10.4134/BKMS.2014.51.6.1605

STRUCTURE OF SOME CLASSES OF SEMISIMPLE GROUP ALGEBRAS OVER FINITE FIELDS

Neha Makhijani, Rajendra Kumar Sharma, and J. B. Srivastava

Abstract. In continuation to the investigation initiated by Ferraz, Goodaire and Milies in [4], we provide an explicit description for the Wedderburn decomposition of finite semisimple group algebras of the class of finite groups G, such that $G/\mathcal{Z}(G) \cong C_2 \times C_2$, where $\mathcal{Z}(G)$ denotes the center of G.

1. Introduction

In this paper, $\mathbb{F}_q$ denotes a finite field with $q = p^n$ elements and G is a finite group such that $\mathbb{F}_q[G]$ is semisimple. The group algebra $\mathbb{F}_q[G]$ and its Wedderburn decomposition are not only of interest in pure algebra, they also have applications in coding theory. Cyclic codes can be realized as ideals of group algebras over cyclic groups [8] and many other important codes appear as ideals of noncyclic group algebras [2, 8, 9]. With the concrete realization of the Wedderburn decomposition of $\mathbb{F}_q[G]$, it is straightforward to produce all the ideals of $\mathbb{F}_q[G]$.

It is known from [6, Theorem 1.2] that any group G, such that $G/\mathcal{Z}(G) \cong C_2 \times C_2$, is a direct product of an indecomposable group (with this property) and an abelian group. Since the structure of a semisimple abelian group algebra follows from the well known theorem due to Perlis and Walker [7, Theorem 3.5.4], we focus on the computation of Wedderburn decomposition of finite semisimple group algebras of indecomposable groups with this property. In fact there are five isomorphism classes of such groups [5, Section 3] and Table 1 gives their presentation. In [4], the structure of semi simple group algebras of these groups was determined over rationals and over those finite fields for which their Wedderburn decomposition has the least number of components. In [1], Bakshi-Gupta-Passi studied the problem of computing the primitive central idempotents and the Wedderburn decomposition of finite semisimple group algebras of metabelian groups using the concept of strong Shoda pairs and consequently obtained an explicit description of the primitive central idempotents

Received August 10, 2013; Revised May 18, 2014.
2010 *Mathematics Subject Classification.* 16S34, 20C05, 11Z05.
Key words and phrases. group algebra, Wedderburn decomposition.

and the Wedderburn decomposition of finite semisimple group algebra of the groups G_1 and G_2.

By applying the theory of Ferraz, developed in [3], we obtain a general expression for the decomposition of finite semisimple group algebras of groups in Table 1.

We start by establishing the basic notation. The ring of integers modulo u is denoted by $\mathbb{Z}_u$, the multiplicative order of $v \in \mathcal{U}(\mathbb{Z}_u)$ is denoted by $\mathrm{ord}_u(v)$ and for any positive integer l, (l, u) denotes the g.c.d. of l and u. If G is any finite group, then the order of $g \in G$ is denoted by $o(g)$, $[g]$ denotes the conjugacy class of g in G and γ_g denotes the class sum of g. The following notation is also used:

C_n	cyclic group of order n
R^m	external direct sum of m copies of the ring R
$M(n, K)$	algebra of all $n \times n$ matrices over the field K

TABLE 1. Finite indecomposable groups G with $\frac{G}{Z(G)} \cong C_2 \times C_2$

G	Presentation
G_1	$\langle\ x,\ y,\ t \mid x^2,\ y^2,\ t^{2^m},\ t \text{ central },\ x^{-1}y^{-1}xy = t^{2^{m-1}}\ \rangle$
G_2	$\langle\ x,\ y,\ t \mid x^2 =\ y^2 = t,\ t^{2^m},\ t \text{ central },\ x^{-1}y^{-1}xy = t^{2^{m-1}}\ \rangle$
G_3	$\langle\ x,\ y,\ t_1,\ t_2 \mid x^2,\ y^2 = t_2,\ t_1^{2^{m_1}},\ t_2^{2^{m_2}},$ $t_1,\ t_2 \text{ central },\ x^{-1}y^{-1}xy = t_1^{2^{m_1-1}}\ \rangle$
G_4	$\langle\ x,\ y,\ t_1,\ t_2 \mid x^2 = t_1,\ y^2 = t_2,\ t_1^{2^{m_1}},\ t_2^{2^{m_2}},$ $t_1,\ t_2 \text{ central },\ x^{-1}y^{-1}xy = t_1^{2^{m_1-1}}\ \rangle$
G_5	$\langle\ x,\ y,\ t_1,\ t_2,\ t_3 \mid x^2 = t_2,\ y^2 = t_3,\ t_1^{2^{m_1}},\ t_2^{2^{m_2}},\ t_3^{2^{m_3}},$ $t_1,\ t_2,\ t_3 \text{ central },\ x^{-1}y^{-1}xy = t_1^{2^{m_1-1}}\ \rangle$

2. Preliminaries

Let K be a field of characteristic $p \geq 0$ and G be a finite group.

Definition 2.1. An element $g \in G$ is said to be p-regular if $p = 0$ or $p > 0$ and $(p, o(g)) = 1$.

Let s be the L.C.M. of the orders of the p-regular elements of G, ξ be a primitive s^{th} root of unity over K and $T_{G,K}$ denote the multiplicative group consisting of those integers t, taken modulo s, for which $\xi \mapsto \xi^t$ defines an automorphism of $K(\xi)$ over K.

Observation 2.2. $T_{G,\mathbb{F}_q} = \{1, q, \ldots, q^{c-1}\} \bmod s$, where $c = \mathrm{ord}_s(q)$.

Definition 2.3. The cyclotomic K-class of γ_g is defined to be the set

$$S(\gamma_g) = \{\gamma_{g^t} \mid t \in T_{G,K}\}.$$

Proposition 2.4 ([3, Proposition 1.2]). *The number of simple components of $K[G]/J(K[G])$ is equal to the number of cyclotomic K-classes in G.*

Theorem 2.5 ([3, Theorem 1.3]). *Suppose that $Gal(K(\xi):K)$ is cyclic. Let t' be the number of cyclotomic K-classes in G. If $K_1,\dots,K_{t'}$ are the simple components of $\mathcal{Z}(K[G]/J(K[G]))$ and $S_1,\dots,S_{t'}$ are the cyclotomic K-classes of G, then with a suitable re-ordering of indices, $|S_i| = [K_i : K]$.*

If F is a finite field, $Gal(F(\xi):F)$ is cyclic showing that Theorem 2.5 is applicable to the group algebra $F[G]$.

In what follows, $q = p^n$, $p > 2$.

3. Wedderburn decomposition of $\mathbb{F}_q[G_1]$ and $\mathbb{F}_q[G_2]$

Consider the presentation of G_1 as discussed in Table 1:

$$\langle x,\ y,\ t \mid x^2,\ y^2,\ t^{2^m},\ t \text{ central},\ x^{-1}y^{-1}xy = t^{2^{m-1}}\rangle.$$

The elements of G_1 can be written uniquely as

$$t^i x^j y^k,\ 1 \le i \le 2^m,\ 0 \le j \le 1,\ 0 \le k \le 1.$$

It is important to note that any group G in this paper has a two-element commutator subgroup G' generated by a central element h of order 2 and so conjugacy classes of a noncentral element w is of the form $\{w, hw\}$.

The following are the distinct conjugacy classes of G_1:

(1) $[t^i] = \{t^i\},\ 1 \le i \le 2^m$,
(2) $[t^i x] = \{t^i x,\ t^{2^{m-1}+i}x\},\ 1 \le i \le 2^{m-1}$,
(3) $[t^i y] = \{t^i y,\ t^{2^{m-1}+i}y\},\ 1 \le i \le 2^{m-1}$,
(4) $[t^i xy] = \{t^i xy,\ t^{2^{m-1}+i}xy\},\ 1 \le i \le 2^{m-1}$.

Theorem 3.1. *If $m \ge 2$, then*

$$\mathbb{F}_q[G_1] \cong \mathbb{F}_q^4 \ \oplus \ \bigoplus_{k=1}^{m-1} \mathbb{F}_{q^{d_k}}^{2^{k+1}/d_k} \ \oplus \ M\left(2, \mathbb{F}_{q^d}\right)^{2^{m-1}/d},$$

where $d_k = \mathrm{ord}_{2^k}(q)$ and $d = d_m$.

Proof. Since $G_1' = \langle t^{2^{m-1}}\rangle$,

$$\begin{aligned} G_1/G_1' &\cong \langle x,\ y,\ t \mid x^2,\ y^2,\ t^{2^{m-1}},\ t \text{ central},\ x^{-1}y^{-1}xy = t^{2^{m-1}}\rangle \\ &\cong \langle x,\ y,\ t \mid x^2,\ y^2,\ t^{2^{m-1}},\ t \text{ central},\ xy = yx\rangle \\ &\cong C_{2^{m-1}} \times C_2 \times C_2. \end{aligned}$$

Thus

$$\begin{aligned} \mathbb{F}_q[G_1] &\cong \mathbb{F}_q[G_1/G_1'] \ \oplus \ \Delta(G_1, G_1') \\ &\cong \mathbb{F}_q[C_{2^{m-1}} \times C_2 \times C_2] \ \oplus \ \left(\bigoplus_{i=1}^{e_m^q} M\left(n_i, F_i\right)\right) \end{aligned}$$

$$\cong \mathbb{F}_q[C_{2^{m-1}}]^4 \ \oplus \ \left(\bigoplus_{i=1}^{e_m^q} M\left(n_i, F_i\right)\right)$$

$$\cong \mathbb{F}_q^4 \ \oplus \ \left(\bigoplus_{i=1}^{m-1} \mathbb{F}_{q^{d_i}}^{2^{i+1}/d_i}\right) \ \oplus \ \left(\bigoplus_{i=1}^{e_m^q} M\left(n_i, F_i\right)\right) \tag{3.1}$$

for some finite field extensions F_i of $\mathbb{F}_q$, $n_i \geq 2$ and $e_m^q \geq 1$.

It is easy to see that $\mathbb{F}_{q^d}$ is a splitting field of G_1. That is

$$\mathbb{F}_{q^d}[G_1] \cong \mathbb{F}_{q^d}^{2^{m+1}} \ \oplus \ \left(\bigoplus_{j=1}^{2^{m-1}} M\left(m_j, \mathbb{F}_{q^d}\right)\right)$$

for some $m_j \geq 2$.

But $2^{m+1} + 4 \times 2^{m-1} = 2^{m+2}$. As a result $m_j = 2 \ \forall \ j$.

Notice that $\mathbb{F}_{q^d}[G_1] \cong \mathbb{F}_{q^d} \otimes_{\mathbb{F}_q} \mathbb{F}_q[G_1]$. Therefore by the uniqueness of Wedderburn decomposition, $n_i = 2 \ \forall \ i$.

For each k, $1 \leq k \leq m-1$, let

$$A_{m-1}^k = \{i \mid 1 \leq i \leq 2^{m-1}, \ (i, 2^{m-1}) = 2^{m-k-1}\}.$$

If $i \in A_{m-1}^k$ and $s_1, \ s_2 \in T_{G,\mathbb{F}_q}$, then

$$\begin{aligned} & [(t^i xy)^{s_1}] = [(t^i xy)^{s_2}] \\ \Leftrightarrow \quad & is_1 \equiv is_2 \text{ or } is_2 + 2^{m-1} \bmod 2^m \\ \Leftrightarrow \quad & is_1 \equiv is_2 \bmod 2^{m-1} \\ \Leftrightarrow \quad & s_1 \equiv s_2 \bmod 2^k \end{aligned}$$

showing that there are $2^{k-1}/d_k$ distinct cyclotomic $\mathbb{F}_q$ classes of the form $S(\gamma_{t^i xy}), \ i \in A_{m-1}^k$ in G_1, each of size d_k.

Proceeding in a similar way, the remaining cyclotomic $\mathbb{F}_q$-classes can be determined. Therefore Proposition 2.4 and Theorem 2.5 yield

$$\mathcal{Z}(\mathbb{F}_q[G_1]) \cong \left(\mathbb{F}_q \ \oplus \ \bigoplus_{k=1}^{m} \mathbb{F}_{q^{d_k}}^{\varphi(2^k)/d_k}\right) \ \oplus \ \left(\mathbb{F}_q \oplus \bigoplus_{k=1}^{m-1} \mathbb{F}_{q^{d_k}}^{\varphi(2^k)/d_k}\right)^3$$

$$\cong \mathbb{F}_q^4 \ \oplus \ \bigoplus_{k=1}^{m-1} \mathbb{F}_{q^{d_k}}^{2^{k+1}/d_k} \ \oplus \ \mathbb{F}_{q^d}^{2^{m-1}/d} \tag{3.2}$$

and using equations (3.1) and (3.2), we obtain

$$\mathbb{F}_q[G_1] \cong \mathbb{F}_q^4 \ \oplus \ \bigoplus_{k=1}^{m-1} \mathbb{F}_{q^{d_k}}^{2^{k+1}/d_k} \ \oplus \ M\left(2, \mathbb{F}_{q^d}\right)^{2^{m-1}/d}. \qquad \square$$

Observe that

$$\begin{aligned} G_2 &= \langle x, \ y, \ t \mid x^2 = \ y^2 = t, \ t^{2^m}, \ t \text{ central}, \ x^{-1}y^{-1}xy = t^{2^{m-1}} \rangle \\ &\cong \langle x, \ y \mid x^2 = y^2, \ y^{2^{m+1}}, \ x^{-1}y^{-1}xy = y^{2^m} \rangle. \end{aligned}$$

With this presentation in hand, we observe that the following are the distinct conjugacy classes of G_2:

$\{y^i, \ y^{2^m+i}\} \ \forall \ i, \ 1 \leq i < 2^m, \ (i,2) = 1;$

$\{y^{2i}\} \ \forall \ i, \ 1 \leq i \leq 2^m;$

$\{xy^i,\ xy^{2^m+i}\}\ \forall\ i,\ 1 \le i \le 2^m$;

Theorem 3.2. *If $m \ge 2$, then*

$$\mathbb{F}_q[G_2] \cong \mathbb{F}_q^2\ \oplus\ \left(\oplus_{i=1}^{m}\ \mathbb{F}_{q^{d_i}}^{2^i/d_i}\right)\ \oplus\ M(2,\mathbb{F}_{q^d})^{2^{m-1}/d},$$

where $d_k = \mathrm{ord}_{2^k}(q)$ and $d = d_m$.

Proof. Let d' be the multiplicative order of q modulo 2^{m+1} and $s_1,\ s_2$ be distinct elements in $T = T_{G_2,\mathbb{F}_q} = \{1, q, \ldots, q^{d'-1}\} \bmod 2^{m+1}$.

If $i \in \mathcal{B} = \{j \mid 1 \le j < 2^m,\ (j,2) = 1\}$, then

$$\begin{aligned} & [y^{is_1}] = [y^{is_2}] \\ \Leftrightarrow\ & is_1 \equiv 2^m + is_2 \bmod 2^{m+1} \\ \Leftrightarrow\ & s_1 \equiv 2^m + s_2 \bmod 2^{m+1} \\ \Leftrightarrow\ & s_1 \equiv s_2 \bmod 2^m. \end{aligned}$$

Thus there are $2^{m-1}/d$ distinct cyclotomic $\mathbb{F}_q$ classes in G_2 of the type $S(\gamma_{y^i})$, when $i \in \mathcal{B}$, each of size d.

We shall now use the following presentation of the cyclic group C_{2^m} to explore the remaining cyclotomic $\mathbb{F}_q$ classes in G_2

$$\langle z \mid z^{2^m}\rangle.$$

For any $i \in \mathcal{B}_1 = \{j \mid 1 \le j \le 2^m\}$,

$$\begin{aligned} & [y^{2is_1}] = [y^{2is_2}] \\ \Leftrightarrow\ & 2is_1 \equiv 2is_2 \bmod 2^{m+1} \\ \Leftrightarrow\ & is_1 \equiv is_2 \bmod 2^m \\ \Leftrightarrow\ & [z^{is_1}] \equiv [z^{is_2}]. \end{aligned}$$

Thus

(1) $|S(\gamma_{y^{2i}})| = |S(\gamma_{z^i}) \mid \forall\ i \in \mathcal{B}_1$,
(2) $|\{S(\gamma_{y^{2i}}) | i \in \mathcal{B}_1\}| = |\{S(\gamma_{z^i}) \mid i \in \mathcal{B}_1\}|$.

We prove an analogous behavior for the cyclotomic $\mathbb{F}_q$ classes of the type $S(\gamma_{xy^i}),\ i \in \mathcal{B}_1$.

Notice that $(xy)^2 = x(yx)y = y^{2^m+4}$.

If $s \in T$, then $s = 2l+1$ for some $l \ge 0$ and

$$\begin{aligned} (xy)^s &= (xy)^{2l+1} \\ &= ((xy)^2)^l(xy) \\ &= (y^{2^m+4})^l xy \\ &= xy^{2^m l+4l+1} \\ &= xy^{(2^{m-1}+2)s-2^{m-1}-1}. \end{aligned}$$

Hence

$$(xy^i)^s = \begin{cases} xy^{(2^{m-1}+i+1)s-2^{m-1}-1} & \text{if } i \text{ is odd} \\ xy^{(i+1)s-1} & \text{if } i \text{ is even} \end{cases}$$

and

$$[(xy^i)^s] = \begin{cases} \{\ xy^{(2^{m-1}+i+1)s-2^{m-1}-1},\ xy^{(2^{m-1}+i+1)s+2^{m-1}-1}\} & \text{if } i \text{ is odd} \\ \{\ xy^{(i+1)s-1},\ xy^{2^m+(i+1)s-1}\} & \text{if } i \text{ is even.} \end{cases}$$

Then

$$\begin{aligned} & [(xy^i)^{s_1}] = [(xy^i)^{s_2}] \\ \Leftrightarrow \quad & (i+1)s_1 \equiv (i+1)s_2 \bmod 2^m \end{aligned}$$

and by a suitable reordering, we observe that the number (and size) of distinct cyclotomic $\mathbb{F}_q$ classes of the type $S(\gamma_{xy^i})$, $i \in \mathcal{B}_1$ in G_2 is same as the number (and size) of distinct cyclotomic $\mathbb{F}_q$ classes in C_{2^m}.

Since $\mathbb{F}_q[G/G'] \cong \mathbb{F}_q[C_{2^m}]^2$, therefore working parallel to the proof of Theorem 3.1, the result follows. □

4. The group algebras $\mathbb{F}_q[G_3]$ and $\mathbb{F}_q[G_4]$

The group G_3 can also be presented by

$$\langle x,\ y,\ t \mid x^2,\ t^{2^{m_1}},\ y^{2^{m_2+1}},\ t \text{ central},\ x^{-1}y^{-1}xy = t^{2^{m_1-1}}\rangle.$$

We trifurcate the distinct conjugacy classes of G_3 obtained with respect to this presentation as follows:

$\{t^j y^i,\ t^{2^{m_1-1}+j}y^i\ \},\ 1 \le i \le 2^{m_2+1},\ (i,2) = 1$ and $\ 1 \le j \le 2^{m_1-1}$;

$\{t^j y^i x,\ t^{2^{m_1-1}+j}y^i x\ \},\ 1 \le i \le 2^{m_2+1},\ 1 \le j \le 2^{m_1-1}$;

$\{t^j y^{2i}\ \};\ 1 \le i \le 2^{m_2},\ 1 \le j \le 2^{m_1}$;

We now obtain an expression for decomposition of the semisimple algebra $\mathbb{F}_q[C_{2^a} \times C_{2^b}]$.

Lemma 4.1. *Let $G = C_{2^a} \times C_{2^b}$. Then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \ \oplus \bigoplus_{m=0}^{a} \bigoplus_{\substack{n=0 \\ m+n>0}}^{b} \mathbb{F}_{q^{d(m,n)}}^{e(m,n)},$$

where $d(m,n) = \operatorname{ord}_{2^{\max(m,n)}}(q)$ and $e(m,n) = \frac{\varphi(2^m)\ \varphi(2^n)}{d(m,n)}$.

Proof. Let $C_{2^a} = \langle c\rangle$ and $C_{2^b} = \langle d\rangle$ and for any $m, n;\ 0 \le m \le a,\ 0 \le n \le b$,

$$A_m = \{c^i \mid (i, 2^a) = 2^{a-m}\},$$
$$B_n = \{d^i \mid (i, 2^b) = 2^{b-n}\}.$$

Suppose that $m + n > 0$.

If $(a_m, b_n) \in A_m \times B_n$ and $s_1,\ s_2 \in T_{G,\mathbb{F}_q}$, then

$$(a_m, b_n)^{s_1} = (a_m, b_n)^{s_2}$$

$$\Leftrightarrow \quad s_1 \equiv s_2 \bmod 2^{\max(m,n)}.$$

Thus there are $e(m,n)$ distinct $\mathbb{F}_q$-cyclotomic classes of the type $S(\gamma_{(a_m,b_n)})$ in G each of size $d(m,n)$; $(a_m,b_n) \in A_m \times B_n$.

Evidently $S(\gamma_{(1,1)}) = \{\gamma_{(1,1)}\}$. Therefore

$$\mathbb{F}_q[C_{2^a} \times C_{2^b}] \cong \mathbb{F}_q \ \oplus \ \overset{a}{\underset{m=0}{\oplus}} \ \overset{b}{\underset{\substack{n=0 \\ m+n>0}}{\oplus}} \ \mathbb{F}_{q^{d(m,n)}}^{e(m,n)}.$$

□

Theorem 4.2. *For any* $m_1,\ m_2 \geq 3$

$$\mathcal{Z}(\mathbb{F}_q[G_3]) \cong \overset{m_2}{\underset{n=0}{\oplus}} \ \mathbb{F}_{q^{d(m_1,n)}}^{e(m_1,n)} \ \oplus \ \mathbb{F}_q[C_2 \times C_{2^{m_1-1}} \times C_{2^{m_2+1}}],$$

where $d(l,k) = \operatorname{ord}_{2^{\max(l,k)}}(q)$ *and* $e(l,k) = \frac{\varphi(2^l)\varphi(2^k)}{d(l,k)}$. *Moreover*

$$\mathbb{F}_q[G_3] \cong \mathbb{F}_q^2 \ \oplus \ \overset{m_1-1}{\underset{m=0}{\oplus}} \ \overset{m_2+1}{\underset{\substack{n=0 \\ m+n>0}}{\oplus}} \ \mathbb{F}_{q^{d(m,n)}}^{2e(m,n)} \ \oplus \ \overset{m_2}{\underset{n=0}{\oplus}} \ M(2, \mathbb{F}_{q^{d(m_1,n)}})^{\,e(m_1,n)}.$$

Proof. Once the number of distinct cyclotomic $\mathbb{F}_q$ classes in G_3 and their cardinalities are known, the proof follows from Theorem 2.5. Therefore we aim at finding the same.

As seen earlier, $T_{G_3,\mathbb{F}_q} = \{1, q, \ldots, q^{d-1}\} \bmod 2^{\max(m_1,m_2+1)}$, where $d = d(m_1, m_2+1)$.

For any $m,\ n;\ 0 \leq m \leq m_1 - 1,\ 0 \leq n \leq m_2 + 1$, let

$$A'_m = \{j \mid 1 \leq j \leq 2^{m_1-1},\ (j, 2^{m_1-1}) = 2^{m_1-m-1}\},$$
$$B'_n = \{i \mid 1 \leq i \leq 2^{m_2+1},\ (i, 2^{m_2+1}) = 2^{m_2-n+1}\}.$$

Let s_1, s_2 be two distinct elements of $T_{G_3,\mathbb{F}_q}$. Consider the following:

(1) For any $j \in A'_m$ and $i \in B'_{m_2+1}$,

$$\begin{aligned} & [(t^j y^i)^{s_1}] = [(t^j y^i)^{s_2}] \\ \Leftrightarrow \quad & is_1 \equiv is_2 \bmod 2^{m_2+1} \text{ and } \begin{pmatrix} js_1 \equiv js_2 \bmod 2^{m_1} \text{ or} \\ js_1 \equiv 2^{m_1-1} + js_2 \bmod 2^{m_1} \end{pmatrix} \\ \Leftrightarrow \quad & s_1 \equiv s_2 \bmod 2^{\max(m,m_2+1)}. \end{aligned}$$

That is, there are $e(m, m_2+1)$ cyclotomic $\mathbb{F}_q$ classes of the form $S(\gamma_{t^j y^i})$ and cardinality $d(m, m_2+1)$, $j \in A'_m$ and $i \in B'_{m_2+1}$.

(2) Note that

$$\begin{aligned} (yx)^{2k+1} &= [(yx)^2]^k yx \\ &= (y^2 t^{2^{m_1-1}})^k yx \\ &= y^{2k+1} t^{2^{m_1-1}k} x \end{aligned}$$

so that if i is odd and $s \in T_{G_3,\mathbb{F}_q}$, then $(y^i x)^s = t^{2^{m_1-2}(s-1)} y^{is} x$.

The following is now obvious:

$$[(t^j y^i x)^s] = \begin{cases} \{\ t^{js} y^{is} x,\ t^{js+2^{m_1-1}} y^{is} x\ \} & \text{if } i \text{ is even} \\ \{\ t^{js+2^{m_1-2}(s-1)} y^{is} x,\ t^{js+2^{m_1-2}(s+1)} y^{is} x\ \} & \text{if } i \text{ is odd.} \end{cases}$$

For any $j \in A'_m, i \in B'_n$ and $m+n>0$,

$$\begin{aligned} & [(t^j y^i x)^{s_1}] = [(t^j y^i x)^{s_2}] \\ \Leftrightarrow\ & js_1 \equiv js_2 \bmod 2^{m_1-1} \text{ and } is_1 \equiv is_2 \bmod 2^{m_2+1} \\ \Leftrightarrow\ & s_1 \equiv s_2 \bmod 2^{\max(m,n)} \end{aligned}$$

and thus there are $e(m,n)$ cyclotomic $\mathbb{F}_q$ classes of the form $S(\gamma_{t^j y^i x})$ and size $d(m,n)$, $j \in A'_m,\ i \in B'_n$ and $m+n>0$.

(3) For any $m,\ n;\ 0 \le m \le m_1,\ 0 \le n \le m_2$, if

$$\begin{aligned} A''_m &= \{j \mid 1 \le j \le 2^{m_1},\ (\ j, 2^{m_1}) = 2^{m_1-m}\} \text{ and} \\ B''_n &= \{i \mid 1 \le i \le 2^{m_2},\ (\ i, 2^{m_2}) = 2^{m_2-n}\}, \end{aligned}$$

then proceeding in a similar way, we find that there are $e(m,n)$ cyclotomic $\mathbb{F}_q$ classes of the form $S(\gamma_{t^j y^{2i}})$, $j \in A''_m,\ i \in B''_n$ and $m+n>0$, each of them having $d(m,n)$ elements.

Thus using Theorem 2.5 and Lemma 4.1, we conclude that

$$\begin{aligned} \mathcal{Z}(\mathbb{F}_q[G_3]) &\cong \bigoplus_{m=0}^{m_1-1} \mathbb{F}_{q^{d(m,m_2+1)}}^{e(m,m_2+1)} \ \oplus\ \mathbb{F}_q \ \oplus \bigoplus_{m=0}^{m_1-1} \bigoplus_{\substack{n=0 \\ m+n>0}}^{m_2+1} \mathbb{F}_{q^{d(m,n)}}^{e(m,n)} \\ &\quad \oplus\ \mathbb{F}_q \ \oplus \bigoplus_{m=0}^{m_1} \bigoplus_{\substack{n=0 \\ m+n>0}}^{m_2} \mathbb{F}_{q^{d(m,n)}}^{e(m,n)} \\ &\cong \bigoplus_{n=0}^{m_2} \mathbb{F}_{q^{d(m_1,n)}}^{e(m_1,n)} \ \oplus\ \mathbb{F}_q[C_2 \times C_{2^{m_1-1}} \times C_{2^{m_2+1}}] \end{aligned}$$

and the rest follows. □

The following is an alternate presentation of G_4:

$$\langle x,\ y \mid x^{2^{m_1+1}},\ y^{2^{m_2+1}},\ x^{-1}y^{-1}xy = x^{2^{m_1}} \rangle.$$

The analysis in G_4 is similar to that in G_3. So we state the decomposition of $\mathbb{F}_q[G_4]$ without proof:

Theorem 4.3. *For any $m_1,\ m_2 \ge 3$*

$$\mathbb{F}_q[G_4] \cong \mathbb{F}_q \ \oplus \bigoplus_{m=0}^{m_1} \bigoplus_{\substack{n=0 \\ m+n>0}}^{m_2+1} \mathbb{F}_{q^{d(m,n)}}^{e(m,n)} \ \oplus \bigoplus_{n=0}^{m_2} M(2, \mathbb{F}_{q^{d(m_1,n)}})^{\ e(m_1,n)},$$

where $d(l,k) = \operatorname{ord}_{2^{\max(l,k)}}(q)$ and $e(l,k) = \frac{\varphi(2^l)\varphi(2^k)}{d(l,k)}$.

5. The group algebra $\mathbb{F}_q[G_5]$

As previously, we begin with a lemma that enables us to determine the decomposition of $\mathbb{F}_q[G_5]$ that is much in spirit of Theorem 4.2.

Lemma 5.1. *Let $G = C_{2^a} \times C_{2^b} \times C_{2^c}$. Then*

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \bigoplus_{m=0}^{a} \bigoplus_{n=0}^{b} \bigoplus_{\substack{l=0 \\ m+n+l>0}}^{c} \mathbb{F}_{q^{d(m,n,l)}}^{e(m,n,l)},$$

where $d(m,n,l) = \operatorname{ord}_{2^{\max(m,n,l)}}(q)$ and $e(m,n,l) = \frac{\varphi(2^m)\ \varphi(2^n)\ \varphi(2^l)}{d(m,n,l)}$.

Observe that the following is a presentation of G_5:

$$\langle x, y, t \mid t^{2^{m_1}},\ x^{2^{m_2+1}},\ y^{2^{m_3}+1},\ t \text{ central},\ x^{-1}y^{-1}xy = t^{2^{m_1-1}} \rangle.$$

Theorem 5.2. *For any $m_1, m_2, m_3 \geq 3$,*

$$\mathbb{F}_q[G_5] \cong \mathbb{F}_q \ \oplus \bigoplus_{m=0}^{m_1-1} \bigoplus_{n=0}^{m_2+1} \bigoplus_{\substack{l=0 \\ m+n+l>0}}^{m_3+1} \mathbb{F}_{q^{d(m,n,l)}}^{e(m,n,l)} \ \oplus \bigoplus_{n=0}^{m_2} \bigoplus_{l=0}^{m_3} M\left(2, \mathbb{F}_{q^{d(m_1,n,l)}}\right)^{e(m_1,n,l)},$$

where $d(m,n,l) = \operatorname{ord}_{2^{\max(m,n,l)}}(q)$ and $e(m,n,l) = \frac{\varphi(2^m)\ \varphi(2^n)\ \varphi(2^l)}{d(m,n,l)}$.

6. Validation of results in [4]

It is known that $\mathcal{U}(\mathbb{Z}_{2^n}) \cong C_2 \times C_{2^{n-2}}$. However the multiplicative order of an arbitrary element $q \in \mathcal{U}(\mathbb{Z}_{2^n})$ is not known.

Theorem 6.1. *Let $q \in \mathbb{Z}$ such that*

$$q \equiv 1 \bmod 2^m \text{ and } q \not\equiv 1 \bmod 2^{m+1}$$

for some $m \geq 3$.

Then

$$q^{2^r} \equiv 1 \bmod 2^{m+r} \text{ and } q^{2^r} \not\equiv 1 \bmod 2^{m+r+1}\ \forall\ r \geq 0.$$

That is, $\operatorname{ord}_{2^{m+r}}(q) = 2^r\ \forall\ r \geq 0$.

Theorem 6.2. *Let $q \in \mathcal{U}(\mathbb{Z}_{2^n})$, $n \geq 3$. If $d = \operatorname{ord}_{2^n}(q)$ and $d_2 = \operatorname{ord}_{2^n}(q^2)$, then*

$$d_2 = \begin{cases} d & \text{if } d = 1 \\ d/2 & \text{if } d > 1. \end{cases}$$

Moreover,

(1) *If $q \equiv 1 \bmod 8$, then*

$$d = \begin{cases} 1 & \text{if } n \leq m \\ 2^{n-m} & \text{if } n > m \end{cases}$$

m being the largest integer such that $q \equiv 1 \bmod 2^m$.

(2) *If $q \equiv 3$ or $5 \bmod 8$, then $d = 2^{n-2}$.*

(3) *If $q \equiv 7 \bmod 8$, then $d = 2^{n-m+1}$, $m \leq n$ being the largest integer such that $q^2 \equiv 1 \bmod 2^m$.*

For any group G in Table 1, let $C(q, G)$ and $N(q, G)$ be the number of commutative and non-commutative components in the Wedderburn decomposition of $\mathbb{F}_q[G]$ respectively. A lower bound for $C(q, G)$ and $N(q, G)$ has been obtained in [4] and it is proved that the minimal number is achieved when $q \equiv 3 \mod 8$. The same can be derived using Theorem 6.2 and the decompositions obtained in Sections 3 through 5.

References

[1] G. K. Bakshi, S. Gupta, and I. B. S. Passi, *The algebraic structure of finite metabelian group algebras*, arXiv:1311.1296 [math.RT], to appear in Comm. Algebra.

[2] P. Charpin, *The Reed-Solomon code as ideals of a modular algebra*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 17, 597–600.

[3] R. A. Ferraz, *Simple components of the center of $FG/J(FG)$*, Comm. Algebra **36** (2008), no. 9, 3191–3199.

[4] R. A. Ferraz, E. G. Goodaire, and C. P. Milies, *Some classes of semisimple group (and loop) algebras over finite fields*, J. Algebra **324** (2010), no. 12, 3457–3469.

[5] E. Jespers, G. Leal, and C. P. Milies, *Classifying indecomposable R.A. loops*, J. Algebra **176** (1995), no. 2, 569–584.

[6] G. Leal and C. P. Milies, *Isomorphic group (and loop) algebras*, J. Algebra **155** (1993), no. 1. 195–210.

[7] C. P. Milies and S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002.

[8] V. S. Pless and W. C. Huffman, *Handbook of Coding Theory*, Elsevier, New York, 1998.

[9] R. E. Sabin and S. J. Lomonaco, *Metacyclic error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), no. 3, 191–210.

Neha Makhijani
Department of Mathematics
Indian Institute of Technology
New Delhi, India
E-mail address: nehamakhijani@gmail.com

Rajendra Kumar Sharma
Department of Mathematics
Indian Institute of Technology
New Delhi, India
E-mail address: rksharmaiitd@gmail.com

J. B. Srivastava
Department of Mathematics
Indian Institute of Technology
New Delhi, India
E-mail address: jbsrivas@gmail.com