RT-MAT 2004-31

IDEMPOTENTS IN GROUP ALGEBRAS
AND MINIMAL ABELIAN CODES

R. A. FERRAZ
and
C. P. MILIES

Dezembro 2004

IDEMPOTENTS IN GROUP ALGEBRAS AND MINIMAL ABELIAN CODES

RAUL ANTONIO FERRAZ AND CÉSAR POLCINO MILIES

ABSTRACT. We compute the number of simple components of a semisimple finite abelian group algebra and determine all cases where this number is minimal. This result is used to compute idempotent generators of minimal abelian codes, extending results of Arora and Pruthi [1], [11]. We also show how to compute the dimension and minimum distance of these codes in a simple way.

1. INTRODUCTION

Let $F = GF(q)$ be a field of prime power order q and let m be a positive integer which is relatively prime to q. The cyclic codes of length m over F can be viewed as ideals in either $F[X]/\langle X^m - 1\rangle$ or in the group algebra FC_m, where C_m denotes a cyclic group of order m. Taking the first viewpoint, Arora and Pruthi [11] computed the idempotent generators of minimal cyclic codes of length p^m in the case when either $p^m = 2$ or 4 or p is odd and the multiplicative order of q, modulo p^m, is $\varphi(p^m)$. In a subsequent paper [1] they studied the case when the length is $2p^m$.

By considering codes as ideals in the group algebra FC_{p^m} we are able to obtain these result in a much shorter way and to show that these are actually the only cases where the computation is possible along these lines (i.e., directly from the lattice of subgroups, without the need of roots of unity or even cyclotomic classes as in [1]).

In the next section, we give similar constructions for minimal abelian codes under the same conditions. In this way, we also extend the results of Berman [2, p.22], as far as possible.

In order to do this, in the first section of the paper we compute the number of simple components of a finite abelian group algebra FA and determine conditions for this number to be minimal. Such a computation can be obtained from the Theorem of Berman-Witt (see [4, Theorems 21.5 and 21.25] or [5, Theorem 47.2]) and from a result of Khülshammer [8], using character theory. Simplifying the methods of Ferraz [6] to the abelian case, we are able to evaluate this number in an elementary manner, using only the structure of FA.

Research supported by FAPESP, Procs. 02/02933-0 and 00/07291-0 and CNPq Proc. 300243/79-0 (RN).

2. The number of simple components

Let F be a finite field, with $|F| = q$ elements, and let A be a finite abelian group such that $(q, |A|) = 1$. Then FA is semisimple and, if $\{e_1, \dots, e_r\}$ is the set of primitive idempotents of FA, we have that

$$FA = \oplus_{i=1}^{r}(FA)e_i \simeq \oplus_{i=1}^{r} F_i,$$

where $F_i \simeq (FA)e_i$, $1 \leq i \leq r$ are fields which are finite extensions of F.

In [6], Ferraz gave a general method to compute the number r of simple components of a semisimple group algebra. In our present case of finite group algebras of abelian groups, we can give a simpler way to determine such a number. Set

$$\mathcal{A} = \oplus_{i=1}^{r} Fe_i.$$

Notice that $Fe_i \simeq F$ as fields in a natural way and that the number r of simple components is also the dimension of $\mathcal{A}$ as a vector space over F.

Lemma 2.1. *Let α be an element of FA. Then $\alpha \in \mathcal{A}$ if and only if $\alpha^q = \alpha$*

PROOF. Given $\alpha \in FA$, we write $\alpha = \sum_{i=1}^{r} \alpha_i$, with $\alpha_i = \alpha e_i \in F_i$, $1 \leq i \leq r$. Now α is an element of $\mathcal{A}$ if and only if each element α_i is in Fe_i for every index i. As $Fe_i \simeq F$, this happens if and only if $\alpha_i^q = \alpha_i$ for all i; hence, if and only if $\alpha^q = \alpha$. □

Let g be an element of the finite abelian group A. We recall that the *q-cyclotomic class of g* is the set

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\},$$

where t_g is the smallest positive integer, such that

$$q^{t_g} \equiv 1(\bmod o(g)),$$

and $o(g)$ denotes the order of g. Since $(q, o(g)) = 1$, there will always exist such a number t_g. It follows easily that if $S_g \neq S_h$, then $S_g \cap S_h = \emptyset$. Let $T = \{g_1, g_2, \dots, g_s\}$ denote a set of representatives of the q-cyclotomic classes.

Theorem 2.2. *Let F be a finite field, with $|F| = q$, and let A be a finite abelian group. such that $(q, |A|) = 1$. Then, the number of simple components of FA is equal to the number of q-cyclotomic classes of A.*

PROOF. As noted above, the number of simple components of FA is equal to the dimension of $\mathcal{A}$ over F. We shall exhibit a basis of this subalgebra with s elements.

Given a q-cyclotomic class S_g we define $\eta_g = \sum_{h \in S_g} h \in FA$. We claim that $\mathcal{B} = \{\eta_{g_i} | 1 \leq i \leq s\}$ is a F-basis $\mathcal{A}$. Clearly $\mathcal{B}$ is a linearly independent set so we only need to show that it also generates $\mathcal{A}$. We remark first that, since $\eta_{g_i}^q = \eta_{g_i}$, $1 \leq i \leq s$, it is clear that $\mathcal{B} \subset \mathcal{A}$.

Let $\alpha \in \mathcal{A} = \bigoplus_{i=1}^{r} Fe_i$. It follows from Lemma 2.1 that $\alpha = \alpha^q$. Hence if $\alpha = \sum\limits_{g\in A} \alpha_g g$, we have

$$\alpha = \sum_{g\in A} \alpha_g g = (\sum_{g\in A} \alpha_g g)^q = \sum_{g\in A} \alpha_g^q g^q.$$

Since $\alpha_g \in F$, we have that $\alpha_g^q = \alpha_g$ and thus

$$\sum_{g\in A} \alpha_g g = \sum_{g\in A} \alpha_g g^q.$$

So, for each $g \in A$, we have that $\alpha_g = \alpha_{g^q} = \cdots = \alpha_{g^{q^{t_g-1}}}$ and, consequently,

$$\alpha = \sum_{g\in T} \alpha_g \eta_g.$$

as claimed. □

A well-known theorem, due to Perlis and Walker [9], (see [10, Corollary 3.5.5]) shows that the number of simple components of the rational group algebra of a finite abelian group A is equal to both the number of cyclic subgroups of A and the number of its cyclic factors.

Notice that, if $h \in S_g$, then $h = g^{q^j}$ for some j. As $(q, o(g)) = 1$, it follows that $\langle g\rangle = \langle h\rangle$. So each q-cyclotomic class S_g is a subset of the set $\mathcal{G}_g$ of all generators of the cyclic group $\langle g\rangle$. So, it is clear that the number cyclic subgroups of A is a lower bound for the number of simple components and that this bound is attained if and only if $S_g = \mathcal{G}_g$, for all $g \in A$.

For positive integers r and m, we shall denote by $\bar{r} \in \mathbf{Z}_m$ the image of r in the ring of integer modulo m. Then,

$$\mathcal{G}_g = \{g^r \mid (r, o(g)) = 1\} = \{g^r \mid \bar{r} \in U(\mathbf{Z}_{o(g)}\}$$

and we have the following.

Theorem 2.3. *Let F be a finite field with $|F| = q$, and let A be a finite abelian group, of exponent e, such that $(q, |A|) = 1$. Then $S_g = \mathcal{G}_g$, for all $g \in A$ if and only if $U(\mathbf{Z}_e)$ is a cyclic group generated by $\bar{q} \in \mathbf{Z}_e$.*

PROOF. Assume first that $U(\mathbf{Z}_e)$ is cyclic generated by $\bar{q}$. For an element $g \in G$, we have that $o(g)|e$ and thus $\overline{(q)} \in \mathbf{Z}_{o(g)}$ is a generator of $U(\mathbf{Z}_{o(g)})$.

For every element h of $\mathcal{G}_g$ we have that $h = g^r$ for some positive integer r such that $\bar{r} \in U(\mathbf{Z}_t)$, so $\bar{r} = \bar{q}^j$ for some positive integer j and $h = g^{q^j} \in S_g$. This shows that $\mathcal{G}_g = S_g$.

Conversely, suppose that $\mathcal{G}_g = S_g$ for all $g \in G$. We recall that if A is a finite abelian group of exponent e then, there exists an element $g_0 \in A$ of order e and, in particular, $\mathcal{G}_{g_0} = S_{g_0}$. Hence, for each integer r such that $\bar{r} \in U(\mathbf{Z}_e)$, we have that $g_0^r \in S_{g_0}$ and there exists some integer j such that $\bar{r} = \bar{q}^j$. Thus, $\bar{q}$ generates $U(\mathbf{Z}_e)$, as claimed. □

It is well-known that $U(\mathbf{Z}_e)$ is cyclic if and only if $e = 2, 4, p^n$, or $2p^n$, where p is a odd prime integer, and n is a positive integer. Notice that, if q is odd then $\bar{q}$ is a generator of $U(\mathbf{Z}_2)$; it is a generator for $e = 4$ if $q \equiv 3 \ (mod\ 4)$ and is a generator of $U(\mathbf{Z}_e)$ for $e = p^n$, or $2p^n$, if and only if $o(q) = \Phi(p^n)$ in $U(\mathbf{Z}_{p^n})$ or $U(\mathbf{Z}_{2p^n})$.

Hence we have the following.

Corollary 2.4. *Let F be a finite field with $|F| = q$, and let A be a finite abelian group, of exponent e. Then $\mathcal{G}_g = S_g$ for all $g \in G$ if and only if one of the following holds:*

(i) *$e = 2$ and q is odd.*
(ii) *$e = 4$ and $q \equiv 3 \ (mod\ 4\ )$.*
(iii) *$e = p^n$ and $o(q) = \Phi(p^n)$ in $U(\mathbf{Z}_{p^n})$.*
(iv) *$e = 2p^n$ and $o(q) = \Phi(p^n)$ in $U(\mathbf{Z}_{2p^n})$.*

3. Minimal cyclic codes

Let H be a finite subgroup of a group G. We set

$$\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g.$$

Since $|H|$ divides $|A|$ and $(q, |A|) = 1$, it follows that $\widehat{H}$ is well defined and it clearly is an idempotent of FG.

Lemma 3.1. *Let p be a rational prime and let $A = \langle a \rangle$ be a cyclic group of order p^n, $n \leq 1$. Let*

$$A \ = \ A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A. Then the elements

$$e_0 = \widehat{A} \quad and \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \ 1 \leq i \leq n,$$

form a set of orthogonal idempotents such that $e_0 + e_1 + \cdots + e_n = 1$.

The proof is straightforward as in [7, Lemma VII.1.2]. It is noted in [7, Remark VII.1.3] that this method yields the set of primitive idempotents of $\mathbf{Q}A$ but that this is not so, in general, over finite fields. However, since these idempotents are $n+1$ in number it will be the set of primitive idempotents whenever FA has precisely $n+1$ components. Since the exponent of A is p^n, in view of the results of the previous section, we have that this happens if and only if q and n are related as described in Corollary 2.4. Hence, we have the following.

Corollary 3.2. *Let F be a finite field with $|F| = q$, and let A be a cyclic group of order p^n. Then, the set of idempotentes given in Lemma 3.1 is the set of primitive idempotents of A if and only if one of the following holds:*

(i) *$p = 2$, and either $n = 1$ and q is odd or $n = 2$ and $q \equiv 3 \ (mod\ 4\ )$.*

(ii) *p is an odd prime and $o(q) = \Phi(p^n)$ in $U(\mathbb{Z}_{p^n})$.*

As an immediate consequence, we obtain the following result of Pruthi and Arora.

Theorem 3.3. ([11, Theorem 3.5]) *Let F be a field with q elements and A a cyclic group of order p^n such that $o(q) = \Phi(p^n)$ in $U(\mathbb{Z}_{p^n})$. Let*

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

be the descending chain of all subgroups of A. Then, the set of primitive idempotents of FA is given by

$$e_0 = \frac{1}{p^n}\left(\sum_{a\in A} a\right)$$

and

$$e_i = \widehat{A_i} - \widehat{A_{i-1}},\ 1 \leq i \leq n.$$

A straightforward computation shows that these are the same idempotents given in [11, Theorem 3.5], though there they are expressed in terms of cyclotomic classes.

The idempotent generators of minimal ideals in the case of cyclic groups of order $2p^n$ now follow easily from the previous results.

Theorem 3.4. (Arora and Pruthi [1, Theorem 2.6]) *Let F be a field with q elements and G a cyclic group of order $2p^n$, p an odd prime, such that $o(q) = \Phi(p^n)$ in $U(\mathbb{Z}_{2p^n})$. Write $G = C \times A$ where A is the p- Sylow subgroup A of G and $C = \{1, t\}$ is its 2-Sylow subgroup. If e_i, $0 \leq i \leq n$ denote the primitive idempotents of FA then, the primitive idempotents of FG are*

$$\frac{(1+t)}{2}\cdot e_i \quad \textit{and} \quad \frac{(1-t)}{2}\cdot e_i \quad 0 \leq i \leq n.$$

PROOF. Notice that

$$FG \cong F(C \times A) \cong (FC)A \cong (F \oplus F)A.$$

Since the idempotents of FC are $(1+t)/2$ and $(1-t)/2$ and the idempotents of FA were computed in Theorem 3.3 above, the claim follows immediately. □

The dimension and minimum length of the minimal ideals $I_i = (FA)(\widehat{A_i} - \widehat{A_{i-1}})$ can be computed directly in a simple way, which will be given in the last section in the more general context of abelian codes.

The generating polynomials are not really necessary in this approach but will be given for the sake of completeness. They can be easily computed as follows. If $e_i(X) \in F[X]$ is any polynomial such that $e_i(a) = e_i$, then it is well-known that the generating polynomial of I_i is given by:

$$g_i(X) = gcd(e_i(X),\ X^{p^n} - 1), \quad 0 \leq i \leq n.$$

We compute:

$$\begin{aligned}
e_i(X) &= \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \frac{1}{p^{n-i-1}} \sum_{i=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \\
&= \frac{1}{p^{n-i-1}} \left[p \sum_{j=0}^{p^{n-i}-1} X^{jp^i} - \frac{1}{p^{n-i-1}} \sum_{i=0}^{p^{n-i+1}-1} X^{jp^{i-1}} \right] \\
&= \frac{1}{p^{n-i-1}} \left[(p-1) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right) - \left(\sum_{j=1}^{p^{n-i}-1} X^{jp^i} \right) \right] \\
&= \frac{1}{p^{n-i-1}} \left(p - \sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right)
\end{aligned}$$

Also:

$$\begin{aligned}
X^{p^n} - 1 &= (X^{p^i} - 1) \sum_{j=0}^{p^{n-i}-1} X^{jp^i} \\
&= (X^{p^{i-1}} - 1) \left(\sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}} \right) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right)
\end{aligned}$$

Since every root of $(X^{p^{i-1}} - 1)$ in an algebraic closure of F is also a root of $p - \sum_{j=0}^{(p-1)p^{i-1}} X^{jp^{i-1}}$, it follows that

$$g_i(X) = (X^{p^{i-1}} - 1) \left(\sum_{j=0}^{p^{n-i}-1} X^{jp^i} \right).$$

Since $deg(g_i(X)) = p^n - p^i + p^{i-1}$ we obtain (as we shall also see, in a different way, in section §5) that:

$$dim(I_i) = p^n - deg(g_i(X)) = p^i - p^{i-1} = \varphi(p^i).$$

4. Minimal abelian codes

We wish to extend this result to finite abelian groups. We shall first consider the case of p-groups.

Let A be an abelian p-group. For each subgroup H of A such that $A/H \neq \{1\}$ is cyclic we shall construct an idempotent of FA. We remark that, since A/H is a cyclic group of pth-power order, there exists only one subgroup H^* of A containing H, such that $|H^*/H| = p$. We define $e_H = \widehat{H} - \widehat{H^*}$. Clearly $e_H \neq 0$ and we have the following.

Lemma 4.1. *The elements e_H, defined as above together with $e_A = \widehat{A}$ form a set of pairwise orthogonal idempotents of FA whose sum is equal to* 1.

PROOF. The fact that these elements are idempotents is straightforward. Let H and K be different subgroups of A such that both A/H and A/K are cyclic, not equal to $\{1\}$, and let H^* and K^* be subgroups containing H and K respectivelly, such that H^*/H and K^*/K are cyclic of order p. We shall consider first the case when $H \subset K$. In this case, clearly $H^* \subseteq K$ and thus

$$e_h e_k \;=\; (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) \;=\; \widehat{K} - \widehat{K^*} - \widehat{K} + \widehat{K^*} \;=\; 0.$$

If neither of these subgroups is contained in the other then both H and K are properly contained in HK so also H^* and K^* are contained in HK hence $H^*K^* \subset HK$ and clearly $HK \subset H^*K^*$ therefore $HK = H^*K^*$. Now, since $HK \subset HK^* \subset H^*K^*$ it follows that also $HK^* = HK$ and, in a similar way, we have $H^*K = HK$. Thus:

$$e_h e_k \;=\; (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) \;=\; 0.$$

Also, if one of the idempotents is equal to e_A a similar result follows easily.

Finally, we wish to show that the sum of these idempotents is equal to 1. For each cyclic subgroup C of A we denote by $\mathcal{G}(C)$ the set of all elements of C that generate this subgroup; i.e.

$$\mathcal{G}(C) \;=\; \{c \in C \mid (o(c), |C|) = 1\}.$$

If $\mathcal{C}$ denotes the family of all cyclic subgroups of A then, clearly, $|A| = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)|$ and, since A is a p-group, $|\mathcal{G}(C)| = |C| - |C|/p$.

Let $\mathcal{S}$ denote the set of all subgroups H of A such that the quotient A/H is cyclic and denote $e = \sum_{H \in \mathcal{S}} e_h$. We claim that $e = 1$. To prove this fact, it is enough to show that $(FA)e = FA$. As we have shown that these idempotents are pairwise orthogonal, we have that

$$(FA)e \;=\; \oplus_{H \in \mathcal{S}} (FA)e_H$$

so

$$dim_F((FA)e) \;=\; \sum_{H \in \mathcal{S}} dim_F((FA)e_H).$$

Notice that $\widehat{H} = \widehat{H^*} - e_H$ and that $\widehat{H^*}e_H = 0$ thus

$$(FA)\widehat{H} = (FA)\widehat{H^*} \oplus (FA)e_H.$$

Hence

$$dim_F((FA)e_H) = dim_F(FA)\widehat{H} - dim_F(FA)\widehat{H^*}.$$

It follows from [10, Proposition 2.3.6] that

$$(1) \qquad dim_F((FA)e_H) = dim_F F[A/H] - dim_F F[A/H^*]$$

and, clearly,

$$dim_F F[A/H] = |A/H| \text{ and } dim_F F[A/H^*] = |A/H^*|.$$

It is well-known that there exists a bijection $\Phi : \mathcal{C} \to \mathcal{S}$ such that $|X| = |A/\Phi(X)|$ for all $X \in \mathcal{C}$. This is a consequence of character theory for finite abelian groups (see [12, Chapter 10]). If we denote by $C \in \mathcal{C}$ the subgroup such that $\Phi(C) = H$ we have

$$\begin{aligned} dim_F F[A/H] &= |C| \\ dim_F F[A/H^*] &= |A/H^*| = |A/H|/|H^*/H| = |C|/p \end{aligned}$$

so

$$dim_F((FA)e_H) = |C| - |C|/p = |\mathcal{G}(C)|$$

and thus

$$\sum_{H \in \mathcal{S}} dim_F((FA)e_H) = \sum_{C \in \mathcal{C}} |\mathcal{G}(C)| = |A|.$$

The result follows. □

The following is an immediate consequence of the lemma above and Corollary 2.4.

Theorem 4.2. *Let p be an odd prime and let A be an abelian p-group of exponent p^r. Then, the set of idempotents above is the set of primitive idempotents of FA if and only if one of the following holds:*

(i) *$p^r = 2$, and q is odd.*
(ii) *$p^r = 4$ and $q \equiv 3 \pmod{4}$.*
(iii) *p is an odd prime and $o(q) = \Phi(p^n)$ in $U(\mathbb{Z}_{p^n})$.*

Also, we have the following.

Theorem 4.3. *Let p be an odd prime and let A be an abelian p-group of exponent $2p^r$. Write $A = E \times B$, where E is an elementary abelian 2-group and B a p-group. Then the primitive idempotents of FA are products of the form $e.f$, where e is a primitive idempotent of FE and f a primitive idempotent of FB.*

Notice that the primitive idempotents of FB are given by Theorem 4.2 above and, writing $E = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$, a product of cyclic groups of order 2, then the primitive idempotents of FE are all products of the form $e = e_1 e_2 \cdots e_n$, where

$$e_i = \frac{1 + a_i}{2} \text{ or } e_i = \frac{1 - a_i}{2}, \quad 1 \leq i \leq n.$$

It should be noted that, in view of Corollary 2.4, these are the only cases where primitive idempotents of finite abelian group algebras can be computed in this way.

5. Dimension and minimum distance

Assume that $|A| = 2^m p^n$, where p denotes an odd prime and $m \geq 0$. As before, we write $A = E \times B$, where E is an elementary abelian 2-group of order 2^m (eventually trivial) and B a p-group.

As noticed right after Theorem 4.3, the primitive idempotents of FE are all products of the form $e_E = e_1 e_2 \cdots e_n$, where

$$e_i = \frac{1+a_i}{2} \quad \text{or} \quad e_i = \frac{1-a_i}{2}, \quad 1 \leq i \leq n.$$

and the primitive idempotents of FA are products of the form $e_E.e_B$, where e_E is a primitive idempotent of FE and e_B a primitive idempotent of FB.

Notice that for fixed idempotent e_E of FE and an element $y \in E$, we can write $y = a_1^{\varepsilon_1} \cdots a_m^{\varepsilon_m}$ where $\varepsilon_i = 0$ or 1, $1 \leq i \leq m$. Hence

$$(2) \qquad y e_E = a_1^{\varepsilon_1}\left(\frac{1 \pm a_1}{2}\right) \cdots a_m^{\varepsilon_m}\left(\frac{1 \pm a_m}{2}\right) = \pm e_E = (-1)^{\varepsilon_y} e_E.$$

where $\varepsilon_y = 0$ or 1.

Consider first primitive idempotents of the form $e_E\widehat{B}$. An element of $(FA)\cdot e_E\widehat{B}$ is of the form $\gamma \cdot e_E\widehat{B}$ where we can write $\gamma = \sum_{\substack{y\in E\\ b\in B}} x_{yb}\, yb$, so we have that

$$\gamma \cdot e_E\widehat{B} = \sum_{\substack{y\in E\\ b\in B}} x_{yb}\; y e_E.b\widehat{B} = \left(\sum_{\substack{y\in E\\ b\in B}} x_{yb}(-1)^{\varepsilon_y}\right) e_E\widehat{B}.$$

This computation shows both that the dimension of the ideal $I = (FA)\cdot e_E\widehat{B}$ is 1 and that its minimum length is $l(I) = |A|$.

Now, we consider idempotents of the form $e = e_E.e_H$ with with $e_E \in FE$, as above and $e_H = \widehat{H} - \widehat{H^*}$, where H is a subgroup of B such that B/H is cyclic of order p^i, say, and H^* is the unique subgroup of B containing H such that $[H^* : H] = p$. Set $I_e = (FA)e$.

Let $b \in B$ be an element such that $B = \langle b, H\rangle$. Then we also have that $H^* = \langle b^{p^{i-1}}, H\rangle$. Notice that

$$(1 - b^{p^{i-1}})e_E\widehat{H} = (1 - b^{p^{i-1}})e_E(\widehat{H^*} + e_H) = (1 - b^{p^{i-1}})e_E e_H \in I_e.$$

Since $b^{p^{i-1}} \notin H$ it is clear that $\mathrm{supp}((1 - b^{p^{i-1}})\widehat{H})$ is the disjoint union $H \cup b^{p^{i-1}}H$ and the weight of this element is $w((1 - b^{p^{i-1}})e_E\widehat{H}) = 2|E||H|$, so that if we denote by $l(I_e)$ the minimum distance of I_e, we have that

$l(I_e) \leq 2^{m+1}|H|$.

Since B is the disjoint union $B = H \cup bH \cup \cdots \cup b^{p^i-1}H$ we also have that $A = E \times B$ is the disjoint union $A = E \times H \cup b(E \times H) \cup \cdots \cup b^{p^i-1}(E \times H)$ so an arbitrary element of FA can be written in the form $\alpha = \sum_{j=0}^{p^i-1} \alpha_j b^j$, with $\alpha_j \in F[E \times H]$.

Notice that, taking into account formula 2 and the fact that $h\widehat{H} = \widehat{H}$ for all $h \in H$, we have that each product $\alpha_j e_E e_H$ is of the form $\alpha_j e_E e_H = k_j e_E e_H$, where $k_j \in F$, $0 \leq j \leq p^i - 1$.

Since $(FA) \cdot e_E e_H \subset (FA) \cdot e_E \widehat{H}$, an element $0 \neq \gamma \in (FA) \cdot e_E e_H = I_e$ can be written in the form

$$\begin{aligned} \gamma &= \alpha e_E \widehat{H} \\ &= \left(k_0 + k_1 b + \cdots + k_{p^i-1} b^{p^i-1}\right) e_E \widehat{H}. \end{aligned}$$

Since $\gamma \neq 0$, we have that at least one coefficient $k_j \neq 0$. If $\gamma = k_j b^j e_E \widehat{H}$ we would have that $e_E \widehat{H} \in (FA) \cdot e_E e_H$, a contradiction. So. at least two different coefficients $k_j, k_{j'}$ must be nonzero for every $\gamma \in I_e$ and thus $l(I_e) \geq 2^{m+1}|H|$. Hence

$$l(I_e) = 2^{m+1}|H|.$$

Finally, we shall compute the dimension of minimal ideals. Let $e = e_E e_H$ be a primitive idempotent. We have that:

$$FA \cdot e_E e_H = F[E \times B] \cdot e_E e_H = ((FE)B) \cdot e_E e_B = (FE \cdot e_E)B \cdot e_H.$$

As $(FE) \cdot e_E \cong F$ for all primitive idempotents of FE, we see that

$$FA \cdot e_E e_H \cong FB \cdot e_H,$$

so formula 1 gives that

$$dim[FA \cdot e_E e_H] = \varphi(p^i).$$

A similar argument shows that

$$dim[FA \cdot e_E \widehat{B}] = dim[FB \cdot \widehat{B}] = 1.$$

References

[1] S.K. Arora and M, Pruthi, *Minimal cyclic codes of length* $2p^n$, Finite Field and Appl., 5 (1999), 177-187.

[2] S.D. Berman, *Semisimple cyclic and abelian code II*, Cybernetics, 3, 3 (1967), 17-23.

[3] I.F. Blake and R.C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.

[4] C.W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol I, Wiley Interscience, New York, 1981.

[5] L. Dornhoff, *Group Representation Theory*, Part B, Marcel Dekker Inc., New York, 1971.

[6] R. Ferraz, Simple components and central units in group algebras, *J. Algebra*, **279** (2004), 191-203.

[7] E.G. Goodaire, E. Jespers and C. Polcino Milies, *Alternative Loop Rings*, North Holland Math. Studies N. 184, Elsevier, Amsterdam, 1996.

[8] B. Khülshammer, *Bemerkugen über die Gruppenalgebra als symmetrische Algebra III*, J. of Algebra, **88** (1984), 279-291.

[9] S. Perlis and G. Walker, Abelian group algebras, *Trans. amer. Math. Soc.*, **68** (1950), 420-426.

[10] C. Polcino Milies and S.K. Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002.

[11] M. Pruthi and S.K. Arora, *Minimal codes of prime power length*, Finite Field and Appl., **3** (1997), 99-113.

[12] J.J. Rotman,*An introduction to the theory of groups*, fourth ed., Graduate texts in Math., vol 148, Springer-Verlag, New York, 1995.

Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281, Cep-05311-970, São Paulo, Brazil.
E-mail address: raul@ime.usp.br

Instituto de Matemática e Estatística, Universidade de São Paulo, Caixa Postal 66281, Cep-05311-970, São Paulo, Brazil.
E-mail address: polcino@ime.usp.br

TRABALHOS DO DEPARTAMENTO DE MATEMÁTICA

TÍTULOS PUBLICADOS

2003-01 COELHO, F.U. and LANZILOTTA, M.A. Weakly shod algebras. 28p.

2003-02 GREEN, E.L., MARCOS, E. and ZHANG, P. Koszul modules and modules with linear presentations. 26p.

2003-03 KOSZMIDER, P. Banach spaces of continuous functions with few operators. 31p.

2003-04 GORODSKI, C. Polar actions on compact symmetric spaces which admit a totally geodesic principal orbit. 11p.

2003-05 PEREIRA, A.L. Generic Hyperbolicity for the equilibria of the one-dimensional parabolic equation $u_t = (a(x)u_x)_x + f(u)$. 19p.

2003-06 COELHO, F.U. and PLATZECK, M.I. On the representation dimension of some classes of algebras. 16p.

2003-07 CHERNOUSOVA, Zh. T., DOKUCHAEV, M.A., KHIBINA, M.A., KIRICHENKO, V.V., MIROSHNICHENKO, S.G., ZHURAVLEV, V.N. Tiled orders over discrete valuation rings, finite Markov chains and partially ordered sets. II. 43p.

2003-08 ARAGONA, J., FERNANDEZ, R. and JURIAANS, S.O. A Discontinuous Colombeau Differential Calculus. 20p.

2003-09 OLIVEIRA, L.A.F., PEREIRA, A.L. and PEREIRA, M.C. Continuity of attractors for a reaction-diffusion problem with respect to variation of the domain. 22p.

2003-10 CHALOM, G., MARCOS, E., OLIVEIRA, P. Gröbner basis in algebras extended by loops. 10p.

2003-11 ASSEM, I., CASTONGUAY, D., MARCOS, E.N. and TREPODE, S. Quotients of incidence algebras and the Euler characteristic. 19p.

2003-12 KOSZMIDER, P. A space C(K) where all non-trivial complemented subspaces have big densities. 17p.

2003-13 ZAVARNITSINE, A.V. Weights of the irreducible $SL_3(q)$-modules in defining characteristic. 12p.

2003-14 MARCOS, E. N. and MARTÍNEZ-VILLA, R. The odd part of a N-Koszul algebra. 7p.

2003-15 FERREIRA, V.O., MURAKAMI, L.S.I. and PAQUES, A. A Hopf-Galois correspondence for free algebras. 12p.

2003-16 KOSZMIDER, P. On decompositions of Banach spaces of continuous functions on Mrówka's spaces. 10p.

2003-17 GREEN, E.L., MARCOS, E.N., MARTÍNEZ-VILLA, R. and ZHANG, P. D-Koszul Algebras. 26p.

2003-18 TAPIA, G. A. and BARBANTI, L. Um esquema de aproximação para equações de evolução. 20p.

2003-19 ASPERTI, A. C. and VILHENA, J. A. Björling problem for maximal surfaces in the Lorentz-Minkowski 4-dimensional space. 18p.

2003-20 GOODAIRE, E. G. and MILIES, C. P. Symmetric units in alternative loop rings. 9p.

2003-21 ALVARES, E. R. and COELHO, F. U. On translation quivers with weak sections. 10p.

2003-22 ALVARES, E.R. and COELHO, F.U. Embeddings of non-semiregular translation quivers in quivers of type $Z\Delta$. 23p.

2003-23 BALCERZAK, M., BARTOSZEWICZ, A. and KOSZMIDER, P. On Marczewski-Burstin representable algebras. 6p.

2003-24 DOKUCHAEV, M. and ZHUKAVETS, N. On finite degree partial representations of groups. 24p.

2003-25 GORODSKI, C. and PODESTÀ, F. Homogeneity rank of real representations of compact Lie groups. 13p.

2003-26 CASTONGUAY, D. Derived-tame blowing-up of tree algebras. 20p.

2003-27 GOODAIRE, E.G. and MILIES, C. P. When is a unit loop *f*-unitary? 18p.

2003-28 MARCOS, E.N., MARTÍNEZ-VILLA, R. and MARTINS, M.I.R. Hochschild Cohomology of skew group rings and invariants. 16p.

2003-29 CIBILS, C. and MARCOS, E.N. Skew category, Galois covering and smash product of a category over a ring. 21p.

2004-01 ASSEM, I., COELHO. F.U., LANZILOTTA, M., SMITH, D.and TREPODE, SONIA Algebras determined by their left and right parts. 34p.

2004-02 FUTORNY, V., MOLEV, A. and OVSIENKO, S. Harish-Chandra Modules for Yangians. 29p.

2004-03 COX, B. L. and FUTORNY, V. Intermediate Wakimoto modules for affine $sl(n+1, C)$. 35p.

2004-04 GRISHKOV, A. N. and ZAVARNITSINE, A. V. Maximal subloops of simple Moufang loops. 43p.

2004-05 GREEN, E.L. and MARCOS, E. δ-Koszul Algebras. 15p.

2004-06 GORODSKI, C. Taut Representantions of compact simple lie groups. 16p.

2004-07 ASPERTI, A.C. and VALÉRIO, B.C. Ruled helicoidal surfaces in a 3-dimensional space form. 9p.

2004-08 ASSEM, I., CASTONGUAY, D., MARCOS, E.N. and TREPODE, S. Strongly simply connected schurian algebras and multiplicative bases. 26p.

2004-09 RODRIGUES, A.A.M., MIRANDA FILHO, R.C. and SOUZA, E.G. Definability and Invariance in First Order Structures. 15p.

2004-10 GIAMBRUNO, A. and MILIES, C. P. Free groups and involutions in the unit group of a group algebra. 5p.

2004-11 RAO, S. ESWARA and FUTORNY, V. Classification of integrable modules for affine lie superalgebras. 20p.

2004-12 GRISHKOV, A. N. and ZAVARNITSINE, A. V. Groups with triality. 22p.

2004-13 BUSTAMANTE, J. C. and CASTONGUAY, D. Fundamental groups and presentations of algebras. 10p.

2004-14 FERNANDES, S.M. and MARCOS, E.N. On the Fundamental Derivation of a Finite Dimensional Algebra. 15p.

2004-15 CARRIÓN, H.; GALINDO, P. and LOURENÇO, M.L. Banach spaces whose bounded sets are bounding in the bidual. 10p.

2004-16 KOSZMIDER, P. Projections in weakly compactly generated Banach spaces and Chang′s conjecture. 15p.

2004-17 KOSZMIDER, P. On a problem of Rolewicz about Banach spaces that admit support sets. 19p.

2004-18 GOODAIRE, E.G., MILIES, C.P. and PARMENTER, M.M. Central units in alternative loop rings. 8p.

2004-19 GIAMBRUNO, A. and MILIES, C. P. Free groups and involutions in the unit group of a group algebra. 5p.

2004-20 CARRIÓN, H. Entire Functions on l_1. 16p.

2004-21 SHESTAKOV, I. and ZHUKAVETS, N. Universal multiplicative envelope of free Malcev superalgebra on one odd generator. 28p.

2004-22 ASSEM, I., BUSTAMANTE, J.C., CASTONGUAY, D. and NOVOA, C. A note on the fundamental group of a one-point extension. 6p.

2004-23 BAHTURIN, Y. A., SHESTAKOV, I. P. and ZAICEV, M . V. Gradings on Simple Jordan and Lie Algebras. 25p.

2004-24 DOKUCHAEV. M., KIRICHENKO. V. and MILIES, C. P. Engel subgroups of triangular matrices over local rings. 16p.

2004-25 ADVÍNCULA, F. H. and MARCOS, E. N., Stratifications of algebras with radical square zero. 7p.

2004-26 ADVÍNCULA, F. H. and MARCOS, E. N., Algebras which are standardly stratified in all orders. 8p.

2004-27 DOKUCHAEV, M. A., KIRICHENKO, V. V., ZELENSKY, A. V. and ZHURAVLEV, V. N. Gorenstein matrices. 22p.

2004-28 PEREIRA, A. L. and PEREIRA, M. C. An extension of the method of rapidly oscillating solutions. 15p.

2004-29 DOKUCHAEV, M. and EXEL, R. Associativity of crossed products by partial actions, enveloping actions and partial representations. 24p.

2004-30 FUTORNY, V. and USTIMENKO, V. Small world semiplanes with generalised Schubert cells. 10p.

2004-31 FERRAZ, R. A. and MILIES, C. P. Idempotents in group algebras and minimal abelian codes. 11p.

Nota: Os títulos publicados nos Relatórios Técnicos dos anos de 1980 a 2002 estão à disposição no Departamento de Matemática do IME-USP.
Cidade Universitária "Armando de Salles Oliveira"
Rua do Matão, 1010 - Cidade Universitária
Caixa Postal 66281 - CEP 05315-970