21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

Ideal Group codes and their Syndrome Decoding

Michele Elia[1] and Cristina García Pillado[2]

Abstract— **Ideal group codes are defined as principal ideals in the group algebra of a finite group G over a finite field $\mathbb{F}$. An overview of their properties along with their encoding and syndrome decoding are presented. The correction of a single error, using syndromes, is described in detail.**

I. INTRODUCTION

Ideal group codes are a natural generalization of cyclic codes, which can be described as ideals in the group algebra of a cyclic group over a finite field [6], [1], [3].
Let G be a finite group, and $\mathbb{F}$ a finite field. The group algebra $\mathbb{F}G$ consists of the expressions

$$a = \sum_{i=1}^{|G|} f_i g_i \qquad f_i \in \mathbb{F}, \quad g_i \in G, \tag{1}$$

where the sum is defined componentwise, that is, the coefficients of the same g_i are added following field addition. The product is computed by applying the distributive law: the product of the group elements is performed first, and the coefficients of the same group element are then added [2], [9], [10], [11].
The group algebra $\mathbb{F}G$ is a vector space of dimension $|G|$ over the field $\mathbb{F}$, and has the structure of an associative ring, which is commutative if and only if the group G is abelian. If the characteristic p of the field $\mathbb{F}$ is relatively prime to the group order $|G|$, the group algebra is semisimple [2], [4]. Let $\mathfrak{g}$ be a zero divisor in $\mathbb{F}G$. A left ideal $\mathfrak{G}$ in $\mathbb{F}G$ is the set

$$\mathfrak{G} = \{a = x\mathfrak{g} : x \in \mathbb{F}G\} =< \mathfrak{g} > .$$

Definition 1: A group code $K(\mathbb{F}G)$ is a left ideal $\mathfrak{G}$, and the element $\mathfrak{g}$ is called the code generator. The size $n = |G|$ of G is the code length, and the dimension k of $\mathfrak{G}$, as a module over $\mathbb{F}$, is the code dimension.

Note that results and conclusions are the same using right ideals.

Definition 2: A basis $\mathfrak{B}$ for the group code $K(\mathbb{F}G)$ is a basis as a subalgebra of the group algebra $\mathbb{F}G$. The basis $\mathfrak{B}$ is a set of k elements $\{\omega_1, \omega_2, \ldots, \omega_k\}$ of $K(\mathbb{F}G)$ that are linearly independent over $\mathbb{F}$.

It will be assumed throughout that the characteristic of the field $\mathbb{F}$ does not divide the order of the group G. Thus the group ring satisfies the minimal conditions [4, Theorem 24.2, p.160], and the ideal $\mathfrak{G}$ contains an idempotent element $\mathfrak{e}$ which may be taken as the code generator.
When the characteristic of $\mathbb{F}$ is a divisor of the order of the group, there may exist non-principal ideals. In this case, it is pointed out that many of the properties of $\mathfrak{G}$ that will be proved, still hold. However, no further comment will be made.
As an immediate consequence of their definition, group codes are characterized by the following property.

Proposition 1: Let $\mathfrak{e}$ be the idempotent element that generates the group code $K(\mathbb{F}G)$. Then there exist k elements $u_1, u_2, \ldots, u_k$ which are linearly independent in $\mathbb{F}G$, and such that the k elements $u_1\mathfrak{e}, u_2\mathfrak{e}, \ldots, u_k\mathfrak{e}$ form an $\mathbb{F}$-basis for $K(\mathbb{F}G)$.

A. Group code generator and generator matrix

A question that may arise, given the generator $\mathfrak{g}$ of a group code, is how to find the dimension of the code. This computational problem is easily tackled by using the representations of group algebra $\mathbb{F}G$. Every representation $D^{(n_o)} : G \longrightarrow GL_{n_o}(\mathbb{L})$ of G, where $\mathbb{L}$ is possibly an extension field of $\mathbb{F}$, induces a representation of the group algebra $\mathbb{F}G$

$$D^{(n_o)}(a) = \sum_{i=1}^{|G|} f_i D^{(n_o)}(g_i) \qquad f_i \in \mathbb{F}, \quad g_i \in G. \tag{2}$$

A representation of $\mathbb{F}G$ is reducible or irreducible as is the representation of G. It is recalled that, in the closure $\bar{\mathbb{F}}$ of $\mathbb{F}$, the representations of $\mathbb{F}G$ are fully reducible into a direct sum of (absolutely) irreducible representations. The number of distinct (inequivalent) irreducible representations is equal to the number s of equivalence classes $\mathfrak{C}_h$ of G.
The following theorem is a direct corollary of [5, Theorem 1], which is reported in Appendix for reference.

Theorem 1: The dimension of the ideal group code generated by $\mathfrak{g}$ is equal to the rank of the matrix $R(\mathfrak{g})$ in the group algebra representation induced by a right regular representation of G.

Since the characteristic $p \nmid |G|$, the group algebra $\mathbb{F}G$ is semisimple and the number of minimal central ideals (simple subalgebras) is equal to the number s of classes of G [2], [7]. Let χ_j be an irreducible $\mathbb{F}$-character of G, i.e., the character of an irreducible representation of $\mathbb{F}G$ in the algebraic closure of $\mathbb{F}$. The element

$$\mathfrak{e}_j = \frac{\chi_j(1)}{n} \sum_{g \in G} \chi_j(g^{-1}) g \tag{3}$$

*This work was partially supported by BES-2008-004410[2] (research fellowship associated to project MTM2007-67884-C04-01)

[1]Michele Elia is with the Politecnico di Torino, 10129 Torino, Italy michele.elia7@gmail.com

[2]Cristina García Pillado is with the University of Oviedo, Spain cpillado@orion.ciencias.uniovi.es

is a central idempotent generating a minimal central ideal, as shown, for instance, in [7, p. 274]. Let g_1 denote the identity of G; from the properties of characters [4] it follows that

$$\sum_{j=1}^{s} \mathfrak{e}_j = g_1,$$

and also the 'orthogonality' relations $\mathfrak{e}_j\mathfrak{e}_h = 0$ if $j \neq h$. The group algebra $\mathbb{F}G$ and the ideal $\mathfrak{O} = \{0\}$ are said to be trivial ideals. An ideal $\mathfrak{J}$ is irreducible if it cannot be written as the (direct) sum of two non-trivial ideals $\mathfrak{J}_1$ and $\mathfrak{J}_2$ such that $\mathfrak{J}_1\mathfrak{J}_2 = 0$. Irreducible ideals are characterized by the following lemma, quoted, without proof, from [2] and [4].

Lemma 1: A minimal central ideal $\mathfrak{J}^{(j)}$ of dimension 1 is irreducible. If the dimension is greater than 1, then it is the square of $n_j = \chi_j(1)$, and $\mathfrak{J}^{(j)}$ can be decomposed as a module into a direct sum of n_j modules $\mathfrak{J}_h^{(j)}$, $h = 1, \ldots, n_j$, which are non-central irreducible ideals of dimension n_j. The decomposition may take place in an extension field of $\mathbb{F}$.

A consequence of this Lemma is that the number N_{ir} of irreducible ideals is

$$N_{ir} = \sum_{i=1}^{s} \chi_i(1).$$

The s minimal central ideals are given by (3) and each irreducible ideal emerges from the decomposition of a minimal central ideal. Thus, every irreducible ideal is known, a fact that will be exploited in describing of a syndrome decoding algorithm. Each ideal is obtained from the decomposition of some minimal central ideal, and it may be supposed that a whole set $\{\mathfrak{f}_j\}_{j=1}^{N_{ir}}$ of idempotent generators of the irreducible (left) ideals is known. Let $\mathfrak{X} = \mathbb{F}G\mathfrak{x}$ be an ideal generated by $\mathfrak{x} \in \mathbb{F}G$; to find the irreducible ideal components of $\mathfrak{X}$ it is sufficient to compute $X_j = \mathfrak{x}\mathfrak{f}_j$, for $j = 1, \ldots, N_{ir}$: whenever $X_j = 0$, the ideal generated by $\mathfrak{f}_j$ is not a component of the ideal generated by $\mathfrak{x}$.

Generator matrix. Given the basis $\{u_1\mathfrak{e}, u_2\mathfrak{e}, \ldots, u_k\mathfrak{e}\}$ of the code, we obtain the generator matrix $\mathbf{G}$ as an $n \times k$ matrix over $\mathbb{F}$, where the coefficients of $u_j\mathfrak{e}$ are the entries of column $j, j = 1, \ldots, k$. Componentwise, the encoding is performed as

$$\mathbf{c} = \mathbf{G}\mathbf{x}, \tag{4}$$

where $\mathbf{x}$ and $\mathbf{c}$ are column vectors of dimensions k and n respectively over $\mathbb{F}$. The rank of the generator matrix $\mathbf{G}$ is k. Further, after reordering its rows, i.e., reordering if necessary the group elements, the first k rows of $\mathbf{G}$ are linearly independent, and form a non-singular square matrix $\mathbf{B}$. It follows that $\tilde{\mathbf{G}} = \mathbf{G}\mathbf{B}^{-1}$ is an echelon matrix of the form $(\mathbf{I}_k|\mathbf{A})^T$. The group code with generator matrix $\tilde{\mathbf{G}}$ is systematic; this implies the existence of k linearly independent elements $\{w_1, w_2, \ldots, w_k\}$ in $\mathbb{F}G$ such that $\{w_1\mathfrak{e}, w_2\mathfrak{e}, \ldots, w_k\mathfrak{e}\}$ is an $\mathbb{F}$-basis of the ideal $\mathbb{F}G\mathfrak{e}$.

B. Parity-check ideal and parity-check matrix

Since the group code $K(\mathbb{F}G)$ is a left zero divisor in the group algebra, there is a right zero divisor $\mathfrak{H}$, of maximum dimension, such that $\mathfrak{G}\mathfrak{H} = 0$. The annihilator $\mathfrak{H}$ of $\mathfrak{G}$ is a direct sum of irreducible right ideals generated by a set of idempotents $\{\mathfrak{e}_{i_1}, \mathfrak{e}_{i_2}, \ldots, \mathfrak{e}_{i_t}\}$. The dimension of the ideal $\mathfrak{H}$ is

$$\sum_{j=1}^{s} \ell_j \chi_j(1), \tag{5}$$

where $0 \leq \ell_j \leq \chi_j(1)$ is the number of irreducible ideals associated with an irreducible character χ_j. Each irreducible ideal $\mathfrak{J}_h^{(j)}$, of dimension n_j, corresponds to an irreducible representation $D_{h_j}^{(j)}(g)$ of G of $n_j \times n_j$ matrices. Therefore, every irreducible ideal $\mathfrak{J}_h^{(j)}$ is characterized by a set of parity equations of the form

$$\sum_{g} D_{\ell_i}^{(i)}(g)c(g) = O_i \quad \forall \ell_i \neq h, \quad \forall i. \tag{6}$$

Parity-check matrix. A parity-check matrix can be obtained from the generator matrix of equation (4) by exploiting the property $\mathbf{H}\mathbf{G} = O$ [8], i.e., $\mathbf{H}$ is an $(n-k) \times n$ matrix of maximum rank $n-k$. Using $\mathbf{H}$, the parity-check equation takes the form

$$\mathbf{H}\mathbf{c} = \mathbf{0}. \tag{7}$$

The rank of $\mathbf{H}$ can also be computed as the sum of the dimensions of the irreducible ideals that do not belong to the code, that is

$$n - k = \sum_{h=1}^{s-t} \ell_{i_h} n_{i_h}.$$

The matrix $\mathbf{H}$, in echelon form, is easily obtained from the echelon form of the generator matrix $\tilde{\mathbf{G}} = (\mathbf{I}_k|\mathbf{A})^T$ as $\tilde{\mathbf{H}} = (-\mathbf{A}|\mathbf{I}_{n-k})$.

a) Minimum distance: The Hamming weight $w_H(\mathbf{c})$ of a codeword $\mathbf{c}$ is defined as the number of non-zero coefficients in the representation (1) of $\mathbf{c}$. The Hamming distance between two codewords $\mathbf{b}$ and $\mathbf{c}$, $d_H(\mathbf{b}, \mathbf{c})$, is the Hamming weight of their difference, i.e. $d_H(\mathbf{b}, \mathbf{c}) = w_H(\mathbf{c} - \mathbf{b})$.

Definition 3: The minimum distance d of a group code $K(\mathbb{F}G)$ is the minimum distance between any pair of distinct codewords

$$d = \min_{\substack{\mathbf{u},\mathbf{v} \in K(\mathbb{F}G) \\ \mathbf{u} \neq \mathbf{v}}} d_H(\mathbf{u}, \mathbf{v}).$$

The next property follows immediately from this definition, and from the standard properties of linear codes.

Proposition 2: The minimum distance d of a group code $K(\mathbb{F}G)$ is equal to the minimum weight of the non-zero codewords. Further, d may be computed as the minimum number of linearly dependent columns in the parity-check matrix $\mathbf{H}$.

b) Singleton Bound: Exploiting the definition for a set of parity-check equations (6), the minimum distance of an ideal group code may be upper bounded as

$$d \leq 1 + \sum_{h} n_{i_h}, \tag{8}$$

since, in the set (6) of linear equations, any block of n_{i_h} columns is linearly independent, for every ideal in the code definition. This bound is referred to as the Singleton Bound for group codes.

II. DECODING

Given a group code $K(\mathbb{F}G)$ of length n, dimension k and minimum distance d, let $\mathbf{c} \in K(\mathbb{F}G)$ be a transmitted codeword. Let $\mathbf{r} \in \mathbb{F}G$ be the received word, which is the codeword $\mathbf{c}$ affected by an error pattern $\mathbf{e}$ of weight less than $\lfloor \frac{d-1}{2} \rfloor$, (i.e., the number of errors falls within the code error correcting capability), that is

$$\mathbf{r} = \mathbf{c} + \mathbf{e}.$$

A minimum distance decoding algorithm looks for a codeword $\hat{\mathbf{c}} \in K(\mathbb{F}G)$ that is at minimum distance from $\mathbf{r}$:

$$\hat{\mathbf{c}} = \arg \min_{\mathbf{u} \in K(\mathbb{F}G)} d_H(\mathbf{r}, \mathbf{u}),$$

where 'arg' means the argument of the function 'min', that is, an element $\mathbf{u} \in K(\mathbb{F}G)$ yielding the minimum value of the Hamming distance, i.e. $d_H(\mathbf{r}, \mathbf{u}) \leq d_H(\mathbf{r}, \mathbf{c})$ for every non-zero $\mathbf{c} \in K(\mathbb{F}G)$. Note that $\mathbf{u}$ may not be unique.

A. Syndrome decoding

In general, dealing with minimum distance decoding, the direct computation of the codeword at minimum distance from the received word may be very expensive, even when the number of correctable errors is small. An approach that is a sort of syndrome decoding may lead to algorithms of more manageable complexities.

Let $\mathcal{T} = \{\mathfrak{f}_1, \ldots, \mathfrak{f}_{N_{ir}}\}$ be the set of all generators of irreducible ideals in $\mathbb{F}G$. Its cardinal (i.e., the number of irreducible ideals), which may be expressed in terms of the dimensions of the irreducible representations of G, is $N_{ir} = \sum_{i=1}^{s} n_i$. Further, it is not restrictive to suppose that all generators are idempotent, a condition that always holds in semisimple rings [7].

Let $\mathfrak{g}$ be a generator of the group code $K(\mathbb{F}G)$, which is a sum of m generators of irreducible ideals $\mathfrak{f}_{j_1}, \ldots, \mathfrak{f}_{j_m}$, since

$$(\mathbb{F}G)\mathfrak{g} = \bigoplus_{i=1}^{m} (\mathbb{F}G)\mathfrak{f}_{j_i}$$

and the irreducible ideals $(\mathbb{F}G)\mathfrak{f}_{j_i}$ are submodules of the ideal generated by $\mathfrak{g}$ whose pairwise intersections are the null-ideal.
A codeword of $K(\mathbb{F}G)$ has the form $\mathfrak{c} = \mathfrak{x}\mathfrak{g}$, and the parity-check conditions are of the form

$$\mathfrak{c}\mathfrak{t} = 0 \quad \forall \mathfrak{t} \in \mathcal{T} \backslash \{\mathfrak{f}_{j_1}, \ldots, \mathfrak{f}_{j_m}\},$$

since every element in $\mathcal{T} \backslash \{\mathfrak{f}_{j_1}, \ldots, \mathfrak{f}_{j_m}\}$ is an annihilator of $\mathfrak{g}$. Therefore, the set of $N_{ir} - m$ syndromes may be defined:

$$S_{\mathfrak{t}} = \mathfrak{r}\mathfrak{t} = (\mathfrak{c} + \mathfrak{e})\mathfrak{t} = \mathfrak{c}\mathfrak{t} + \mathfrak{e}\mathfrak{t} = \mathfrak{e}\mathfrak{t} \quad \forall \mathfrak{t} \in \mathcal{T} \backslash \{\mathfrak{f}_{j_1}, \ldots, \mathfrak{f}_{j_m}\}.$$

Decoding at minimum distance is equivalent to searching for a solution of minimum Hamming weight of the set of key-equations

$$\hat{\mathfrak{e}}\mathfrak{h} = S_{\mathfrak{t}} \quad \forall \mathfrak{t} \in \mathcal{T} \backslash \{\mathfrak{f}_{j_1}, \ldots, \mathfrak{f}_{j_m}\}.$$

If the number of errors is not greater than $\lfloor \frac{d-1}{2} \rfloor$, the solution of minimum weight is unique. The problem is to find an algorithm that exploits syndrome knowledge to efficiently decode every group code. The case of correcting a single error is not entirely trivial, and is considered in detail.

B. Syndrome correction of a single error

Let G be a non-abelian group and $\mathbb{F}$ be a finite field whose characteristic is not a divisor of the group order $|G|$. Let $\mathfrak{e}_1 = \sum_{g \in G} g$ be the generator of the minimal central ideal associated with the identity character of G.
Let $K(\mathbb{F}G)$ be a group code of length n, dimension k, and minimum distance $d \geq 3$, whose generator $\mathfrak{f}$ does not contain $\mathfrak{e}_1$. Consequently $\mathfrak{e}_1\mathfrak{f} = \mathfrak{f}\mathfrak{e}_1 = 0$. Since the minimum distance is greater than 3, the code must have further annihilator irreducible ideals with generators $\mathfrak{h}_2, \mathfrak{h}_3, \ldots, \mathfrak{h}_t$.
If $\mathfrak{c} = \mathfrak{m}\mathfrak{f}$ is the transmitted codeword, assuming a single error, the error pattern is $e = Eg_j$ and the received word is $\mathfrak{r} = \mathfrak{c} + \mathfrak{e}$.
We may compute t ($t \geq 2$) syndromes

$$S_1 = r\mathfrak{e}_1, \qquad S_i = \mathfrak{r}\mathfrak{b}_i, \quad i = 2, \ldots, t,$$

where $\mathfrak{b}_i$ are generators of irreducible ideals. The following theorem concerns group codes that may be seen as a generalization of Hamming codes. Further, it may be useful to speed up the search for the error position in decoding single error correcting codes.

Theorem 2: Let G be a non-abelian group, and suppose that the characteristic p of $\mathbb{F}$ does not divide $|G|$, the group order. The minimum distance of any irreducible group code $K(\mathbb{F}G)$ of dimension k greater than 1 is at least 3.

Proof: Preliminarily, observe that the code generated by $\mathfrak{e}_1$ has minimum distance $d = |G|$, thus irreducible codes of dimension 1 may have minimum distance far greater than 3.
Now, assume the code is generated by $\mathfrak{g}$ and of dimension greater than 1. If the minimum distance is 2, then a codeword of the form $\mathfrak{c} = x_1 g_{j_1} + x_2 g_{j_2}$ certainly exists with $g_{j_1} \neq g_{j_2}$ (note that codewords of weight 1, i.e., of the form $x_1 g_j$ do not exist). Therefore, there is an element x of $\mathbb{F}G$ such that

$$x\mathfrak{g} = x_1 g_{j_1} + x_2 g_{j_2},$$

and by item 4) of Lemma 2 in the Appendix, we have

$$0 = x\mathfrak{g}\mathfrak{e}_1 = (x_1 g_{j_1} + x_2 g_{j_2})\mathfrak{e}_1 = (x_1 + x_2)\mathfrak{e}_1,$$

from which it follows that $x_1 + x_2 = 0$. Consequently, the word of weight 2 has the form $x_1(g_{j_1} - g_{j_2})$. Consider a

faithful irreducible representation D_ℓ such that $D_\ell(\mathfrak{g}) = O$, which certainly exists by Corollary (9.7) [7, p.147]. Then $D_\ell(g_{j_1} - g_{j_2}) = O$, which implies $g_{j_1} = g_{j_2}$ since the representation is faithful. The contradiction concludes the proof. ∎

Theorem 3: Assuming that a code $K(\mathbb{F}G)$ is an irreducible ideal of dimension greater than 1, and using the above notations,

1) The error magnitude is obtained from the syndrome $S_1 = E\mathfrak{e}_1$.
2) The error is located by an algorithm mimicking Chien's search, utilising the other syndromes:
   a) Find the values i such that $Eg_i\mathfrak{b}_2 - S_2$ is zero.
   b) Use the remaining syndromes to single out the unique position j.

Proof: Item 1) is trivially true since we have $g_i\mathfrak{e}_1 = \mathfrak{e}_1$. To find j, consider all indexes i_h such that $Eg_{i_h}\mathfrak{b}_2 - S_2 = 0$. Subtracting two expressions with different indexes i_1 and i_2, it is seen that $[g_{i_1} - g_{i_2}]\mathfrak{b}_2 = 0$, i.e., the annihilator of b_2 has the form $[g_{i_1} - g_{i_2}]$. Therefore, using the remaining syndromes, the ambiguity is resolved. ∎

III. A NUMERICAL EXAMPLE

Let S_3 be the symmetric group on 3 elements. The group elements g_i have a standard representation as permutations

$$g_1 = (1), g_2 = (123), g_3 = (132),$$
$$g_4 = (12), g_5 = (23), g_6 = (13),$$

and are partitioned into three conjugacy classes

$$\begin{array}{lcll} \mathcal{C}_0 & = & \{g_1\}; & \text{order } 1 \\ \mathcal{C}_1 & = & \{g_2, g_3\}; & \text{order } 3 \\ \mathcal{C}_2 & = & \{g_4, g_5, g_6\}; & \text{order } 2 \end{array},$$

where elements in the same class have the same order. Thus, in the group algebra $\mathcal{A} = \mathbb{F}_5[S_3]$ we have 3 central minimal ideals $\mathfrak{I}_1$, $\mathfrak{I}_2$, and $\mathfrak{I}_3$ that correspond to the group irreducible characters shown in the table

	g_1	g_2	g_3	g_4	g_5	g_6
χ_1	1	1	1	1	1	1
χ_2	1	1	1	−1	−1	−1
χ_3	2	−1	−1	0	0	0

These ideals are generated by idempotents that are central elements defined by:

$$\mathfrak{e}_1 = g_1 + g_2 + g_3 + g_4 + g_5 + g_6$$
$$\mathfrak{e}_2 = g_1 + g_2 + g_3 - g_4 - g_5 - g_6$$
$$\mathfrak{e}_3 = 4g_1 - 2g_2 - 2g_3$$

Note that $e_1 + e_2 + e_3 = g_1$ (the group identity) and $e_1e_2 = e_1e_3 = e_2e_3 = 0$.
Further, we have two irreducible ideals, which are non-central, generated by

$$\mathfrak{f}_1 = 2g_1 + 3g_3 + 2g_4 + 3g_6$$
$$\mathfrak{f}_2 = 2g_1 + 3g_2 + 3g_4 + 2g_6$$

Therefore, we have 4 codes which are irreducible ideals, namely the codes generated by $\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{f}_1, \mathfrak{f}_2$, plus one code which is a minimal central ideal, i.e. the code generated by $\mathfrak{e}_3$, which is reducible. In the following table, these codes are summarized, along with their generators and Hamming weight distributions.

generator	(n, k, d)	$w_H(x)$
e_1	$(6, 1, 6)$	$1 + 4x^6$
e_2	$(6, 1, 6)$	$1 + 4x^6$
e_3	$(6, 4, 2)$	$1 + 24x^2 + 24x^3 + 144x^4 + 288x^5 + 144x^6$
f_1	$(6, 2, 4)$	$1 + 12x^4 + 12x^6$
f_2	$(6, 2, 4)$	$1 + 12x^4 + 12x^6$
$e_1 + e_2$	$(6, 2, 3)$	$1 + 8x^3 + 16x^6$

A code with a composite ideal generator $(\mathfrak{e}_1 + \mathfrak{e}_2)$ has been included for comparison: the minimum distance is smaller than the irreducible ideals of the same dimension.

c) Encoding and Decoding: Consider the code generated by f_1. It has parameters $(6, 2, 4)$, hence it can correct one error. Since it is a linear code, parity-check and generator matrices are

$$\mathbf{H} = \begin{bmatrix} 4 & 4 & 4 & 0 & 0 & 0 \\ 1 & 1 & 0 & 4 & 0 & 0 \\ 0 & 4 & 0 & 0 & 4 & 0 \\ 4 & 0 & 0 & 0 & 0 & 4 \end{bmatrix} \quad \mathbf{G} = \begin{bmatrix} 2 & 3 \\ 0 & 2 \\ 3 & 0 \\ 2 & 0 \\ 0 & 3 \\ 3 & 2 \end{bmatrix}.$$

Using $\mathbf{G}$ and $\mathbf{H}$, the code can be treated with the standard algebraic methods of linear codes; however, the example will be developed in the group algebra framework, because this exploits features of the algebra of ideals, otherwise invisible. Let $m = g_2 + g_3$ be a message which is encoded as $\mathfrak{c} = m\,\mathfrak{f}_1 = 3g_1 + 2g_3 + 3g_4 + 2g_6$. Let $\mathfrak{r} = 3g_1 + 2g_3 + 4g_4 + 2g_6$ be the received word. Three syndromes, corresponding to the irreducible ideals with generators $\mathfrak{e}_1$, $\mathfrak{e}_2$, and $\mathfrak{f}_2$, are then computed:

$$S_1 = \mathfrak{r}\mathfrak{e}_1 = \mathfrak{e}_1, \qquad S_2 = \mathfrak{r}\mathfrak{e}_2 = 4\mathfrak{e}_2$$

$$S_3 = \mathfrak{r}\mathfrak{f}_2 = 3g_1 + 2g_3 + 2g_4 + 3g_5.$$

Since the syndromes are not zero, then some error occurred, and correction is tried assuming that only a single error Eg_i occurred. If the procedure fails, then the errors are more than one, but cannot be corrected. The syndrome S_1 tells us that the error magnitude is $E = 1$. The error location is given by a 'Chien search', i.e.

$$\begin{array}{lcl} \Delta & = & Eg_i\mathfrak{f}_2 - S_3 = g_i(2g_1 + 3g_2 + 3g_4 + 2g_6) \\ & & \quad - (3g_1 + 2g_3 + 2g_4 + 3g_5) \end{array}$$

is computed for all $i \in \{1, 2, 3, 4, 5, 6\}$. The values of i such that $\Delta = 0$ give the potential error positions. Explicitly, we have:

i	Δ
1	$4g_1 + 3g_2 + 3g_3 + g_4 + 2g_5 + 2g_6$
2	$2g_1 + 2g_2 + g_3 + 3g_4 + 4g_5 + 3g_6$
3	0
4	0
5	$2g_1 + 2g_2 + g_3 + 3g_4 + 4g_5 + 3g_6$
6	$4g_1 + 3g_2 + 3g_3 + g_4 + 2g_5 + 2g_6$

It is deduced from this table that the error is in position 3 or 4. The ambiguity is resolved using the syndrome S_2 and computing $g_3\mathfrak{e}_2 - S_2$ and $g_4\mathfrak{e}_2 - S_2$, obtaining

$$g_3\mathfrak{e}_2 - S_2 = 2g_1 + 2g_2 + 2g_3 + 3g_4 + 3g_5 + 3g_6$$
$$g_4\mathfrak{e}_2 - S_2 = 0$$

Therefore, an error of magnitude 1 is located in position 4.

IV. CONCLUSIONS

Ideal group codes over group algebras are an extension of the principle underlying cyclic codes over finite fields. A generator matrix of an ideal group code has been introduced, from which efficient encoding methods can be devised. A syndrome decoding method has also been outlined, since it could be useful in practical applications. The method is fully developed, and illustrated by an example, for single error correction. The extension to correct more than one error is a challenging open problem.

APPENDIX

A regular representation of G induces a representation of $\mathbb{F}G$ over the field $\mathbb{F}$.

Theorem 4: Let $\mathfrak{I}$ be a left (right) ideal of $A = \mathbb{F}G$ with generators $\mathfrak{f}_1, \ldots, \mathfrak{f}_t$. Let $M_1, \ldots, M_t$ be the matrices corresponding to $\mathfrak{f}_1, \ldots, \mathfrak{f}_t$ in a regular left (right) representation of the group algebra induced by a left (right) regular representation of the group G. Let M be the block matrix

$$M = \begin{bmatrix} M_1 \\ \vdots \\ M_t \end{bmatrix}.$$

Then the dimension of $\mathfrak{I}$ as an $\mathbb{F}$-vector space equals the rank of M.

Proof: Let $G = \{g_1, \ldots, g_n\}$. For each element $\mathfrak{f} \in A$, the corresponding matrix, in a left regular representation of the group algebra induced by a left regular representation of the group G, has entries m_{ij}, where

$$g_i\mathfrak{f} = m_{i1}g_1 + \cdots + m_{in}g_n.$$

In other words, the entries in the i-th row of M_k are the coefficients of the element $g_i\mathfrak{f}_k$ in the $\mathbb{F}$-basis $\{g_1, \ldots, g_n\}$. The elements $g_i\mathfrak{f}_k$, for $i = 1, \ldots, n$ and $k = 1, \ldots, t$, form a system of generators for the left ideal $\mathfrak{I} = A\mathfrak{f}_1 + \ldots + A\mathfrak{f}_t$ as an $\mathbb{F}$-vector space. The rank of M gives the dimension of their $\mathbb{F}$-span and hence the dimension of $\mathfrak{I}$ as an $\mathbb{F}$-vector space.

Similarly, for any right ideal $\mathfrak{I} = \mathfrak{f}_1 A + \cdots + \mathfrak{f}_t A$ we consider a regular right representation of G. The entries in the i-th row of M_k are the coefficients of the element $\mathfrak{f}_k g_i$ in the $\mathbb{F}$-basis $\{g_1, \ldots, g_n\}$. Again, the rank of M gives the dimension of $\mathfrak{I}$ as an $\mathbb{F}$-vector space. ∎

The following Lemma may also be useful to check whether an element of $\mathbb{F}G$ is a zero divisor. Recall that $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.

Lemma 2: Let $\mathbb{F}G$ be a semisimple group algebra, and let $\{D_j\}_{j=1}^{N_{ir}}$ be the set of its irreducible $\bar{\mathbb{F}}$-representations. Then,

1) If the sum of the coefficients of an element $z = \sum_{g\in G} c(g)g$ is zero, then z is a zero divisor.
2) If $\zeta = \sum_{g\in G} b(g)g$ is an annihilator of a zero divisor z, then, certainly one of the sums $\sum_{g\in G} c(g)$ or $\sum_{g\in G} b(g)$ is 0.
3) The sum of the coefficients of any central ideal, with the exclusion of $\mathfrak{e}_1$, is 0.
4) The sum of the coefficients of any $\bar{\mathbb{F}}_q$-irreducible ideal, with the exclusion of $\mathfrak{e}_1$, is 0.

Proof: Let D_1 denote the one-dimensional identity representation, i.e., $D_1(g) = 1$ for every $g \in G$. Point 1) assumes that $\sum_{g\in G} c(g) = 0$, so

$$D_1(z) = \sum_{g\in G} c(g)D_1(g) = \sum_{g\in G} c(g) = 0.$$

It follows that z belongs to the kernel of D_1; hence z is a zero-divisor.

Point 2) is proved by applying D_1 to the product $zh = 0$. We have

$$D_1(zh) = D_1(z)D_1(h) = \sum_{g\in G} c(g) \sum_{g\in G} b(g) = 0,$$

which implies that one of the two factors is necessarily equal to 0.

Proof of Point 3). Let $z = \sum_{g\in G} c(g)g$ be a zero divisor. It is not therefore invertible in the algebra.

Observe that the sum of the coefficients of $\mathfrak{e}_1$, which is $|G|$, is different from 0 because $p \nmid |G|$ by hypothesis. Thus, point 3) is a consequence of equation (3) and the orthogonality relations of the irreducible characters [7].

Point 4) is proved similarly: since irreducible ideals satisfy the condition $\mathfrak{f}_j \cdot \mathfrak{e}_1 = 0$, then $D_1(\mathfrak{f}_j) \cdot D_1(\mathfrak{e}_1) = 0$ [7, p. 146-147], and the conclusion follows from point 2) since $D_1(\mathfrak{e}_1) \neq 0$. ∎

REFERENCES

[1] J.J. Bernal, Á del Río, J.J. Simón, An intrinsical description of group codes, *Designs, Codes and Cryptography*, 51, no. 3 (2009), 289–300.
[2] M. Burrow, Representation Theory of Finite Groups, *Academic press,* New York (1965).
[3] E. Couselo, S. González, V. Markov, A. Nechaev, Loop codes, *Discr. Math. and Appl.*, v.14, no. 2 (2004), 163–172.
[4] R. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, *John Wiley & Sons,* London (1962).
[5] M. Elia, E. Gorla, On the computation of Ideal dimensions in Group Algebras, arXiv:1403.7920.
[6] C. García Pillado, S. González, V. Markov, C. Martínez, A. Nechaev, Group codes over non-abelian groups, *Journal of Algebra and its Applications*, v.12, no.7 (2013).
[7] M. I. Isaacs, Character theory of finite groups, Dover (1994).
[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North Holland Mathematical Library, Vol. 16, *Elsevier Science Publishers,* B.V. (1988).

[9] R.S. Pierce, Associative algebras, *Springer*, New York (1982).
[10] C. Polcino Milies, S. K. Sehgal, An Introduction to Group Rings, *Kluwer*, Dordrecht (2002).
[11] B.L.Van der Warden, Modern Algebra, New York: Frederick Ungar Pub., 1966.