Efficient Description of some Classes of Codes using Group Algebras

Chimal-Dzul, Henry ; Gassner, Niklas ; Rosenthal, Joachim ; Schnyder, Reto

DOI: https://doi.org/10.1016/j.ifacol.2022.11.020

Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 55-30 (2022) 7–12

Efficient Description of some Classes of Codes using Group Algebras

Henry Chimal-Dzul, Niklas Gassner, Joachim Rosenthal and Reto Schnyder

Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich
(e-mail: {henry.chimal-dzul, niklas.gassner, rosenthal, reto.schnyder}@math.uzh.ch)

Abstract: Circulant matrices are an important tool widely used in coding theory and cryptography. A circulant matrix is a square matrix whose rows are the cyclic shifts of the first row. Such a matrix can be efficiently stored in memory because it is fully specified by its first row. The ring of $n \times n$ circulant matrices can be identified with the quotient ring $\mathbb{F}[x]/(x^n - 1)$. In consequence, the strong algebraic structure of the ring $\mathbb{F}[x]/(x^n - 1)$ can be used to study properties of the collection of all $n \times n$ circulant matrices. The ring $\mathbb{F}[x]/(x^n - 1)$ is a special case of a group algebra and elements of any finite dimensional group algebra can be represented with square matrices which are specified by a single column. In this paper we study this representation and prove that it is an injective Hamming weight preserving homomorphism of $\mathbb{F}$-algebras and classify it in the case where the underlying group is abelian.
Our work is motivated by the desire to generalize the BIKE cryptosystem (a contender in the NIST competition to get a new post-quantum standard for asymmetric cryptography). Group algebras can be used to design similar cryptosystems or, more generally, to construct low density or moderate density parity-check matrices for linear codes.

Keywords: Coding Theory, Linear Codes, MDPC codes, Circulant matrices, group algebras

1. INTRODUCTION

In coding theory and cryptography, one often works with large matrices. Large matrices require a considerable amount of storage, so it is natural to look for families of matrices which can be efficiently stored.

A very commonly used family of such matrices is the ring of circulant matrices. Since all rows of a circulant matrix are cyclic shifts of the first row, one only needs to store the first row instead of the whole matrix. This property makes them attractive for cryptographic applications (Baldi et al., 2007; Berger et al., 2009). For example, circulant matrices are used in the cryptosystems BIKE (Aragon et al., 2020) and HQC (Aguilar Melchor et al., 2020), which are two contenders for the fourth round of the NIST Post-Quantum Cryptography Standarization.

On a more algebraic side, circulant matrices over a field k form a k-algebra and can be described with the ring $k[x]/(x^n - 1)$. Indeed, by identifying an element $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in k[x]/(x^n - 1)$ with the $n \times n$ circulant matrix

$$C(f) = \begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix} \in \mathrm{Mat}_n(k),$$

we get a k-algebra isomorphism from $k[x]/(x^n-1)$ to the k-algebra of circulant matrices. Note also that $k[x]/(x^n - 1)$ is the group algebra $k[C_n]$ of the cyclic group C_n with n elements. More generally, (Santini et al., 2021) study matrices whose rows are related through an arbitrary family of permutations rather than just cyclic shifts.

Group algebras themselves have a history in coding theory. Their first general usage in coding theory was in (Berman, 1967) and independently by (MacWilliams, 1970). Both studied group codes as ideals in a group algebra. For a more recent treatment of group codes, we refer to (Huffman et al., 2021, Chapter 16). For a purely mathematical study of group algebras, we refer to (Jespers and del Río, 2015a,b) and (Milies and Sehgal, 2002).

The matrix $C(f)$ can be considered as the transformation matrix of the linear transformation $k[x]/(x^n - 1) \to k[x]/(x^n - 1)$ given by $h \mapsto fh$ with respect to the ordered basis $\mathcal{B} = \{1, x, x^2, \ldots, x^{n-1}\}$ of $k[x]/(x^n - 1)$. Elements of any finite-dimensional group algebra $k[G]$ can be represented with square matrices in a similar way.

The aim of this paper is to study a representation of a group algebra $k[G]$ obtained by mapping its elements to transformation matrices of linear maps from $k[G]$ to itself. We prove that this representation is a Hamming weight preserving monomorphism of k-algebras and show that an element of a finite-dimensional group algebra is invertible if and only if the corresponding square matrix is invertible. We will then classify matrix representations of $k[G]$ when G is a finite abelian group. Similarly to the paper by MacWilliams (1970), we will use the fact that a finite abelian group is the product of cyclic groups to do so.

⋆ Henry Chimal-Dzul acknowledges the support of Swiss Confederation under a Government Excellence Fellowship (ESKAS-Nr 2021.0139). The second and third author are supported by armasuisse Science and Technology (Project Nr.: CYD C-2020010). All authors were supported in part by the Swiss National Science Foundation grant 188430.

10.1016/j.ifacol.2022.11.020

This paper is organized as follows. Section 2 contains some basic definitions and notations concerning group algebras and a way to represent them with square matrices. In Section 3, we study basic properties of this representation, the most important result of this section is that this matrix representation is weight-preserving. Section 4 is the highlight of this paper, as we give a classification of matrices obtained from our method when working with abelian groups. Finally, in Section 5, we will discuss some possible applications in cryptography and coding theory. To the best of the authors' knowledge, Sections 4 and 5 are entirely new contributions.

2. GROUP ALGEBRAS AND THEIR MATRIX REPRESENTATIONS

Let k denote a field. A k-algebra (or algebra over k) is an associative ring $(A, +, \cdot)$ with multiplicative identity 1_A such that

(1) $(A, +)$ is a k-vector space;
(2) $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in k$ and $a, b \in A$.

Because an algebra over k is simultaneously a k-vector space and a ring, various results and notions of linear algebra and ring theory are inherited in this setting. In particular, a k-algebra A that is finite-dimensional as a vector space over k is called a finite-dimensional algebra, while A is said to be commutative provided that the ring A is commutative. Given two algebras A and B over k, an algebra homomorphism is a map $\phi : A \to B$ that satisfies $\phi(1_A) = 1_B$ and is a k-linear ring homomorphism.

One of the most important examples of k-algebras is the group algebra $k[G]$ formed from a field k and a group G (written multiplicatively). As a set, $k[G]$ is the collection of all finite formal sums [1]

$$\sum_{i=1}^{n} \lambda_i g_i = \lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_n g_n,$$

where $n \in \mathbb{N}$, $\lambda_i \in k$ and $g_i \in G$ for all $1 \leq i \leq n$. Addition [2] and multiplication, as well as multiplication by scalars $\mu \in k$, are defined in the obvious ways:

$$\sum_{i=1}^{n} \lambda_i g_i + \sum_{i=1}^{n} \mu_i g_i := \sum_{i=1}^{n} (\lambda_i + \mu_i) g_i,$$

$$\left(\sum_{i=1}^{n} \lambda_i g_i\right)\left(\sum_{j=1}^{m} \mu_j h_j\right) := \sum_{i=1}^{n}\sum_{j=1}^{m} (\lambda_i \mu_j) g_i h_j,$$

$$\mu \sum_{i=1}^{n} \lambda_i g_i := \sum_{i=1}^{n} \mu \lambda_i g_i, \mu \in k.$$

With these operations, it is easy to verify that $k[G]$ is indeed a k-algebra. The identity of the ring $k[G]$ is $1e_G$ and $k[G]$ is commutative if and only if G is an abelian group. We can identify the set G with the set $\{1g : g \in G\}$, so that G is a subset of $k[G]$. Thus, as a k-vector space, the set G is a basis of $k[G]$. As a result, $k[G]$ is a finite-dimensional k-algebra if and only if G is a finite group.

A classical result for group algebras is that every group homomorphism induces a k-algebra homomorphism between the respective group algebras. To be precise, we have the following result.

Proposition 1. (Milies and Sehgal, 2002, Corollary 3.2.8) Let k be a field and G and H groups. Then a group homomorphism $\psi : G \to H$ induces an algebra homomorphism $\tilde{\psi} : k[G] \to k[H]$ given by

$$\sum_{i=1}^{n} \lambda_i g_i \mapsto \sum_{i=1}^{n} \lambda_i \psi(g_i).$$

Moreover, $\tilde{\psi}$ is injective (respectively surjective) if and only if ψ is injective (respectively surjective).

2.1 A Matrix Representation of Finite-Dimensional Group Algebras

Recall that a matrix representation of degree m of a finite-dimensional algebra A over k is an algebra homomorphism from A into the k-algebra $\mathrm{Mat}_m(k)$. A matrix representation is said to be faithful if it is injective. In this section we will explicitly construct a faithful matrix representation of a finite-dimensional group algebra. To this aim and from now on, G denotes an arbitrary finite group of order n, denoted multiplicatively, and k a field.

Let $\mathrm{End}(k[G])$ denote the set of all algebra homomorphisms from $k[G]$ into itself. If we define addition of two algebra homomorphisms $\alpha, \beta \in \mathrm{End}(k[G])$ by the rule

$$(\alpha + \beta)(f) = \alpha(f) + \beta(f), \qquad f \in k[G],$$

then $\mathrm{End}(k[G])$ becomes an additive abelian group. This group becomes a ring with identity if we define multiplication of homomorphisms by composition. Moreover, $\mathrm{End}(k[G])$ is an algebra over k when multiplication by scalars $\lambda \in k$ is set to be

$$(\lambda\alpha)(f) = \lambda\alpha(f), \qquad f \in k[G].$$

On the other hand, every element in $\mathrm{End}(k[G])$ is in particular a k-linear transformation. Thus, given an ordered basis $\mathcal{B}$ of $k[G]$, from linear algebra we know that to every $\alpha \in \mathrm{End}(k[G])$ we can associate the transformation matrix $M_{\mathcal{B}}(\alpha) \in \mathrm{Mat}_n(k)$, so that the action of α is completely described by $M_{\mathcal{B}}(\alpha)$. This association satisfies the following properties for all $\lambda \in k$ and $\alpha, \beta \in \mathrm{End}(k[G])$ (Roman, 2007, Theorem 2.15):

(1) $M_{\mathcal{B}}(\lambda\alpha + \beta) = \lambda M_{\mathcal{B}}(\alpha) + M_{\mathcal{B}}(\beta)$;
(2) $M_{\mathcal{B}}(\alpha\beta) = M_{\mathcal{B}}(\alpha) M_{\mathcal{B}}(\beta)$;
(3) $M_{\mathcal{B}}(1) = I_n$.

In the language of algebras, the previous association defines an k-algebra homomorphism $\theta : \mathrm{End}(k[G]) \to \mathrm{Mat}_n(k)$ given by

$$\alpha \mapsto M_{\mathcal{B}}(\alpha). \tag{1}$$

Moreover, θ is an isomorphism of algebras and so $\alpha \in \mathrm{End}(k[G])$ is invertible if and only if $M_{\mathcal{B}}(\alpha)$ is an invertible matrix.

In light of the above, any k-algebra homormophism $\varphi : k[G] \to \mathrm{End}(k[G])$ would give a matrix representation of degree n through the following diagram:

$$\begin{array}{ccc} k[G] & \xrightarrow{\varphi} & \mathrm{End}(k[G]) \\ & \searrow & \downarrow \theta \\ & & \mathrm{Mat}_n(k) \end{array}$$

We now focus on defining an algebra homomorphism $\varphi : k[G] \to \mathrm{End}(k[G])$. To this end, we have the following lemma whose proof follows directly from the definitions.

[1] We allow the possibility that some of the λ_i are zero but no g_i may be repeated, so that an element of $k[G]$ may be written in formally different ways.
[2] We may assume that two formal sums involve the same group elements $g_1, \ldots, g_n$ by inserting zeros if necessary.

Lemma 2. Let $f \in k[G]$ and $\phi(f) : k[G] \to k[G]$ be the map given by the rule $h \mapsto fh$. Then $\phi(f) \in \mathrm{End}(k[G])$.

We call the map $\phi(f)$ in the previous lemma the *associated endomorphism to* f.

Proposition 3. Let $\varphi : k[G] \to \mathrm{End}(k[G])$ be the map defined as $f \mapsto \phi(f)$. Then φ is an injective algebra homomorphism.

Proof. The fact that φ is an algebra homomorphism follows immediately from the associativity and distributivity in $k[G]$. Since $k[G]$ has identity, $\phi(f)$ is the zero map if and only if $f = 0 \in K[G]$. Thus φ is injective.

In the following result we give a matrix representation of degree n of $k[G]$. Its proof follows from the properites of the k-algebra homomorphism θ defined in (1).

Theorem 4. Let $f \in k[G]$ and fix an order between the elements of G, say $\mathcal{B} = \{g_1, g_2, \ldots, g_n\}$. Then the map from $k[G]$ into $\mathrm{Mat}_n(k)$ given by $f \to M_{\mathcal{B}}(\phi(f))$ is a faithful matrix representation of degree n of $k[G]$.

From now on we will abbreviate $M_{\mathcal{B}}(\phi(f))$ as $M_{\mathcal{B}}(f)$. It is clear that $M_{\mathcal{B}}(f)$ depends on the chosen order of the elements of G. Changing the order of the elements of G will simply result in $M_{\mathcal{B}}(f)$ being conjugated with a permutation matrix P, i.e., we get a matrix of the form $P^{-1}M_{\mathcal{B}}(f)P$. Therefore, up to conjugation with permutation matrices, the matrix $M_{\mathcal{B}}(f)$ is unique. This motivates the following definition.

Definition 5. Let $f \in k[G]$ and fix an order between the elements of G, say $\mathcal{B} = \{g_1, g_2, \ldots, g_n\}$. The matrix $M_{\mathcal{B}}(f)$ is called the matrix representation of f with respect to $\mathcal{B}$.

We now give an example.

Example 6. Let k be an arbitrary field and D_4 the dihedral group of order 8, that is,

$$D_4 = \langle x^i y^j \mid x^4 = y^2 = (xy)^2 = 1 \rangle.$$

Thus D_4 consists of the elements

$$g_1 = 1, \;\; g_2 = x, \;\; g_3 = x^2, \;\; g_4 = x^3,$$
$$g_5 = y, \;\; g_6 = xy, \;\; g_7 = x^2y, \;\; g_8 = x^3y.$$

Considering the ordered basis $\mathcal{B} = \{g_1, \ldots, g_8\}$ of $k[D_4]$, an element $f \in k[D_4]$ can be written as $f = \big(a_1g_1 + a_2g_2 + a_3g_3 + a_4g_4\big) + \big(b_1g_1 + b_2g_2 + b_3g_3 + b_4g_4\big)g_5$. By doing so, the matrix representation of $f \in k[D_4]$ is

$$M_{\mathcal{B}}(f) = \begin{pmatrix} a_1 & a_4 & a_3 & a_2 & b_1 & b_2 & b_3 & b_4 \\ a_2 & a_1 & a_4 & a_3 & b_2 & b_3 & b_4 & b_1 \\ a_3 & a_2 & a_1 & a_4 & b_3 & b_4 & b_1 & b_2 \\ a_4 & a_3 & a_2 & a_1 & b_4 & b_1 & b_2 & b_3 \\ b_1 & b_2 & b_3 & b_4 & a_1 & a_4 & a_3 & a_2 \\ b_2 & b_3 & b_4 & b_1 & a_2 & a_1 & a_4 & a_3 \\ b_3 & b_4 & b_1 & b_2 & a_3 & a_2 & a_1 & a_4 \\ b_4 & b_1 & b_2 & b_3 & a_4 & a_3 & a_2 & a_1 \end{pmatrix} \in \mathrm{Mat}_8(k).$$

3. SOME PROPERTIES OF THE MATRIX REPRESENTATION

In this section, we will study some properties of the matrix representation of $k[G]$ given in Theorem 4. These properties concern invertibility and the Hamming weight of the rows and columns of $M_{\mathcal{B}}(f)$. Throughout this section we will continue using the notation introduced before and we consider the basis $\mathcal{B} = \{g_1, \ldots, g_n\}$, where $g_1, \ldots, g_n$ is a fixed order of the group G. Moreover, let $k[G]^*$ be the group of units of $k[G]$.

3.1 Weight preserving property

In this section we investigate the Hamming weight of the matrix representation of an element $f \in k[G]$. We show that the Hamming weight of any row and column of $M_{\mathcal{B}}(f)$ is the same.

We have a natural notion of weight in $k[G]$. For a vector $v = (v_1, v_2, \ldots, v_n) \in k^n$, we write $\mathrm{supp}(v)$ to denote the support of v, i.e.,

$$\mathrm{supp}(v) = \{i \mid v_i \neq 0\}.$$

Similarly, for $f = \sum_{i=1}^n \lambda_{g_i} g_i \in k[G]$, the support of f is

$$\mathrm{supp}(f) = \{i \mid \lambda_{g_i} \neq 0\}.$$

Definition 7. Let $v \in k^n$ be a vector. Then its (Hamming) weight is the number of non-zero entries of v, i.e.,

$$\mathrm{wt}(v) = |\mathrm{supp}(v)|.$$

Let $f \in k[G]$. Then its (Hamming) weight is defined as

$$\mathrm{wt}(f) = |\mathrm{supp}(f)|.$$

It turns out that the row- and column weight of the matrix representation of an element $f \in k[G]$ is exactly the weight of f.

Proposition 8. Let $f = \sum_{i=1}^n \lambda_{g_i} g_i \in k[G]$ be an element and $M_{\mathcal{B}}(f)$ its matrix representation with respect to $\mathcal{B}$. Let $c_1, c_2, \ldots, c_n$ be the columns of $M_{\mathcal{B}}(f)$ and $r_1, r_2, \ldots, r_n$ be the rows of $M_{\mathcal{B}}$. Then, for all $j \in \{1, \ldots, n\}$,

$$\mathrm{wt}(f) = \mathrm{wt}(c_j) = \mathrm{wt}(r_j).$$

Proof. Let $w = \mathrm{wt}(f)$ and let $\lambda_{\tilde{g}_1}, \lambda_{\tilde{g}_2}, \ldots, \lambda_{\tilde{g}_w}$ be the non-zero coefficients of f, i.e.

$$f = \sum_{i=1}^{w} \lambda_{\tilde{g}_i} \tilde{g}_i.$$

Note first that c_j is a vector representation of

$$\phi(f)(g_j) = \sum_{i=1}^{w} \lambda_{\tilde{g}_i} (\tilde{g}_i g_j),$$

hence $\mathrm{wt}(c_j) = \mathrm{wt}(f)$.

Now, consider the row r_j and let $k \in \{1, \ldots, n\}$. The k'th entry of r_j is the coefficient of g_j in

$$\sum_{i=1}^{w} \lambda_{\tilde{g}_i} (\tilde{g}_i g_k) = \sum_{i=1}^{n} \lambda_{g_i g_k^{-1}} g_i.$$

Thus, the k'th entry of r_j is non-zero if and only if $\lambda_{g_j g_k^{-1}} \neq 0$, which happens if and only if $\tilde{g}_m g_k = g_j$ for some $m \in \{1, \ldots, w\}$. We see that this happens if and only if $g_k \in \{\tilde{g}_1^{-1} g_j, \tilde{g}_2^{-1} g_j, \ldots, \tilde{g}_w^{-1} g_j\}$. Thus, we conclude that

$$\mathrm{wt}(r_j) = w = \mathrm{wt}(f).$$

3.2 Invertibility

Notice first that it follows immediately from Theorem 4 that if $f \in k[G]^*$, then $M_{\mathcal{B}}(f)$ is an invertible matrix. The converse also holds as it is shown in the next proposition.

Proposition 9. Let $f \in k[G]$. The matrix $M_{\mathcal{B}}(f)$ is invertible if and only if $f \in k[G]^*$.

Proof. Assume that $M_{\mathcal{B}}(f)$ is invertible. Without loss of generality, we may also assume that $g_1 = e_G$, the neutral element of G. Since $M_{\mathcal{B}}(f)$ is invertible, its columns $c_1, \ldots, c_n$ are linearly independent, implying that they span k^n as k-vector space. In particular, there exists $\mu_1, \mu_2, \ldots, \mu_n \in k$ such that

$$\sum_{i=1}^{n} \mu_i c_i = (1, 0, \ldots, 0)^T.$$

Now, for all $j \in \{1, \ldots, n\}$, $c_j = (c_{j,1}, c_{j,2}, \ldots, c_{j,n})^T$ is a vector representation of the element

$$\sum_{i=1}^{n} c_{j,i} g_i,$$

which, by definition of the matrix representation, equals fg_j. Thus, it follows that

$$1 = \sum_{i=1}^{n} \mu_i f g_i = f \cdot \sum_{i=1}^{n} \mu_i g_i.$$

Now, let $f^{-1} = \sum_{i=1}^{n} \mu_i g_i$. Since matrix inverses are always both sided, we get that

$$M_{\mathcal{B}}(f^{-1}) = M_{\mathcal{B}}(f)^{-1}.$$

In particular,

$$M_{\mathcal{B}}(f^{-1}) M_{\mathcal{B}}(f) = I_n.$$

Applying the argumentation from before to the columns of $M_{\mathcal{B}}(f^{-1})$, we get that $f^{-1}f = 1$.

Remark 10. Note that this result implies that one-sided units in $k[G]$ are both-sided and that an element f of $k[G]$ is either a unit or there exist $h, \tilde{h} \in k[G]$ such that $hf = 0 = f\tilde{h}$. That is, elements in $k[G]$ are either units or zero divisors.

Proposition 11. Let k be any field, G, H be groups, $\psi : G \to H$ be a group homomorphism and $\tilde{\psi} : k[G] \to k[H]$ be the induced homomorphism of k-algebras. Let $f \in k[G]$. If $f \in k[G]^*$, then $\tilde{\psi}(f) \in k[H]^*$. Moreover, if ψ is injective, the converse holds as well.

Proof. Assume first that $f \in k[G]^*$. Then

$$1_{k[H]} = \tilde{\psi}(1_{k[G]}) = \tilde{\psi}(ff^{-1}) = \tilde{\psi}(f)\tilde{\psi}(f^{-1}).$$

We show the converse by contraposition. Assume that ψ is injective, then so is $\tilde{\psi}$. Assume that $f \notin k[G]^*$. Then there exists no $g \in k[G]$ such that $fg = 1$, so the associated map $\phi(f)$ is not surjective. The map $\phi(f)$ is a linear endomorphism and $k[G]$ a finite-dimensional vector space, so $\phi(f)$ has non-trivial kernel. This implies that there exists a $h \in k[G] \setminus \{0\}$ such that $fh = 0$. Then

$$\tilde{\psi}(f)\tilde{\psi}(h) = \tilde{\psi}(fh) = \tilde{\psi}(0) = 0.$$

Since $\tilde{\psi}$ is injective, we get that $\tilde{\psi}(h) \neq 0$, implying that $\tilde{\psi}(f)$ is a zero-divisor and thus $\tilde{\psi}(f) \notin k[H]^*$.

4. CLASSIFICATION FOR ABELIAN GROUPS

In this section we present a classification of the matrix representation of elements of finite-dimensional commutative group algebras. We start by recalling some standard results concerning tensor products of group algebras.

First, observe that the tensor product $A \otimes_k B$ of two k-algebras A and B is itself a k-algebra with the multiplication induced by $(a \otimes b) \cdot (\tilde{a} \otimes \tilde{b}) = (a\tilde{a} \otimes b\tilde{b})$. Thus, given two groups G and H, $k[G] \otimes_k k[H]$ is a k-algebra. Furthermore, $k[G \times H] \cong k[G] \otimes_k k[H]$ as k-algebras, where the map is induced by mapping a pair $(g, h) \in G \times H$ to the tensor $g \otimes h$ (Milies and Sehgal, 2002). We will show in Proposition 12 below that the matrix representation of an element $g \otimes h$ is the Kronecker product of the matrix representations of g and h. Recall that the Kronecker product of an $m \times n$ matrix $A = (a_{ij})_{ij}$ over k and a $p \times q$ matrix B over k is the $mp \times nq$ block matrix $A \otimes B$ given by

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{21}B & \cdots & a_{n1}B \\ a_{21}B & a_{22}B & \cdots & a_{n2}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Notice that the Kronecker product is associative, i.e. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$, and that the application $\otimes$ is bilinear.

As before, let $g_1, \ldots, g_m$ be an ordering of the elements of G, $h_1, \ldots, h_n$ an ordering of the elements of H, $\mathcal{B}_G = \{g_1, \ldots g_m\}$ and $\mathcal{B}_H = \{h_1, \ldots h_n\}$ the corresponding k-bases of $k[G]$ and $k[H]$. We define the set

$$B_{G \otimes H} = \{g_1 \otimes h_1, \ldots, g_1 \otimes h_n, g_2 \otimes h_1, \ldots, g_m \otimes h_n\},$$

which is an ordered basis of $k[G] \otimes_k k[H]$.

Proposition 12. Let $a \in k[G]$, $b \in k[H]$, $M_{\mathcal{B}_G}(a)$ be the matrix representation of a with respect to $\mathcal{B}_G$ and $M_{\mathcal{B}_H}(b)$ be the matrix representation of b respect to $\mathcal{B}_H$. Then

$$M_{B_{G \otimes H}}(a \otimes b) = M_{\mathcal{B}_G}(a) \otimes M_{\mathcal{B}_H}(b).$$

Proof. Let $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ and assume that $\phi_a(g_i) = \sum_{s=1}^{m} \lambda_{g_s} g_s$ and $\phi_b(h_j) = \sum_{t=1}^{n} \mu_{h_t} h_t$. Then we see that

$$\phi_{a \otimes b}(g_i \otimes h_j) = a g_i \otimes b h_j = \left(\sum_{s=1}^{m} \lambda_{g_s} g_s \right) \otimes \left(\sum_{t=1}^{n} \mu_{h_t} h_t \right)$$
$$= \sum_{s=1}^{m} \sum_{t=1}^{n} \lambda_{g_s} \mu_{h_t} (g_s \otimes h_t).$$

It follows that the $((i-1)n+j)$'th column of $M_{B_{G \otimes H}}(a \otimes b)$ is

$$v = (\lambda_{g_1}\mu_{h_1}, \ldots, \lambda_{g_1}\mu_{h_n}, \lambda_{g_2}\mu_{h_1}, \ldots, \lambda_{g_m}\mu_{h_n})^T.$$

We have that the i'th column of M_a is given by $(\lambda_{g_1}, \lambda_{g_2}, \ldots, \lambda_{g_n})^T$ and the j'th column of M_b is given by $(\mu_{h_1}, \mu_{h_2}, \ldots, \mu_{h_n})^T$, so the $((i-1)n+j)$'th column of $M_a \otimes M_b$ is also given by v.

Let $\mathcal{B}_{G \times H} = \{(g_1, h_1), \ldots, (g_1, h_n), (g_2, h_1), \ldots, (g_m, h_n)\}$. It holds that $M_{\mathcal{B}_{G \times H}}(f) = M_{\mathcal{B}_{G \otimes H}}(\tilde{f})$, where $\tilde{f}$ is the image of f under the identification $k[G \times H] \cong k[G] \otimes_k k[H]$. For notational purposes, we will identify elements of the group algebra of the product of groups with their image in the tensor product of the group algebras.

We will classify the matrix representations of elements of finite-dimensional commutative group algebras. It is well-known that a finite abelian group is isomorphic to the product of cyclic groups (Roman, 2007, Theorem 6.16).

Given a finite multiplicative cyclic group $C_n = \langle x \rangle$ of order n, the matrix representation of an element $f = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \in k[C_n]$ with respect to the ordered basis $\{1, x, \ldots x^{n-1}\}$ is the circulant matrix

$$C(f) = \begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}.$$

We write $P_{n,i} = C(x^{i-1})$ for $i = 1, \ldots, n$ (the index n specifies the size of the matrix). We use the standard notation $a \mid b$ for "a divides b".

Theorem 13. Let G be an abelian, non-cyclic group. Then there exist $n \in \mathbb{N}$ and $a_1 \mid a_2 \mid \ldots \mid a_n$ such that $|G| = \prod_{i=1}^{n} a_i$, and an ordered basis $\mathcal{B}$ such that for every $f \in k[G]$, we have that

$$M_{\mathcal{B}}(f) = \sum_{i_2=1}^{a_2} \cdots \sum_{i_n=1}^{a_n} C(f_{i_2,\ldots,i_n}) \otimes P_{a_2,i_2} \otimes \cdots \otimes P_{a_n,i_n},$$

where all $C(f_{i_2,\ldots,i_n})$ are circulant matrices of size $a_1 \times a_1$, such that the summands $C(f_{i_2,\ldots,i_n}) \otimes P_{a_2,i_2} \otimes \cdots \otimes P_{a_n,i_n}$ have pairwise disjoint support.

Proof. From the classification of abelian groups, we know that there exist $a_1 \mid a_2 \mid \ldots \mid a_n$ such that

$$G \cong C_{a_1} \times \cdots \times C_{a_n},$$

so we show the statement for $k[C_{a_1} \times \cdots \times C_{a_n}]$. We let x_i be a generator of C_{a_i} and consider the basis $\mathcal{B}_i = \{1, x_i, \ldots, x_i^{a_i-1}\}$ of $k[C_i]$.

We will argue why the summands have disjoint support at the end and first show the rest of the statement by induction on n.

Consider $n = 2$ and let $f \in k[C_{a_1} \times C_{a_2}]$. Write

$$f = \sum_{i=1}^{a_1} \sum_{j=1}^{a_2} \lambda_{i,j} (x_1^{i-1} \otimes x_2^{j-1}).$$

We rewrite

$$f = \sum_{j=1}^{a_2} \left(\left(\sum_{i=1}^{a_1} \lambda_{i,j} x_1^{i-1} \right) \otimes x_2^{j-1} \right).$$

For all $j \in \{1, \ldots, n\}$, let $f_j = \sum_{i=1}^{a_1} \lambda_{i,j} x_1^{i-1} \in k[C_{a_1}]$. Using Proposition 12, we get that

$$\begin{aligned} M_{C_{a_1} \otimes C_{a_2}}(f_j \otimes x_2^{j-1}) &= M_{\mathcal{B}_1}(f_j) \otimes M_{\mathcal{B}_2}(x_2^{j-1}) \\ &= C(f_j) \otimes P_{a_2,j}, \end{aligned}$$

so it follows that

$$M_{C_{a_1} \otimes C_{a_2}}(f \otimes x_2^{j-1}) = \sum_{j=1}^{a_2} C(f_j) \otimes P_{a_2,j}.$$

For $n > 2$, let $f \in k[C_{a_1} \times \cdots \times C_{a_n}]$ and write

$$f = \sum_{i_1=1}^{a_1} \cdots \sum_{i_n=1}^{a_n} \lambda_{i_1,\ldots,i_n} (x_1^{i_1-1} \otimes \cdots \otimes x_n^{i_n-1}).$$

For all $i_n \in \{1, \ldots, a_n\}$, let

$$f_{i_n} = \sum_{i_1=1}^{a_1} \cdots \sum_{i_{n-1}=1}^{a_{n-1}} \lambda_{i_1,\ldots,i_n} (x_1^{i_1-1} \otimes \cdots \otimes x_{n-1}^{i_{n-1}-1}),$$

which lies in $k[C_{a_1}] \otimes_k \cdots \otimes_k k[C_{a_{n-1}}]$. We write f as

$$f = \sum_{i_n=1}^{a_n} f_{i_n} \otimes x_n^{i_n-1}.$$

Fix i_n. By induction hypothesis we can write the matrix $M_{C_{a_1} \otimes \cdots \otimes C_{a_{n-1}}}(f_{i_n})$ as

$$\sum_{i_2=1}^{a_2} \cdots \sum_{i_{n-1}=1}^{a_{n-1}} C(f_{i_2,\ldots,i_n}) \otimes P_{a_2,i_2} \otimes \cdots \otimes P_{a_{n-1},i_{n-1}},$$

where $f_{i_2,\ldots,i_n} = \sum_{i_1=1}^{a_1} \lambda_{i_1,\ldots,i_n} x_1^{i_1-1}$. Now, applying Proposition 12 and rearranging the order of the summation symbols, we get that $M_{C_{a_1} \otimes \cdots \otimes C_{a_n}}(f)$ is given by

$$\sum_{i_2=1}^{a_2} \cdots \sum_{i_n=1}^{a_n} C(f_{i_2,\ldots,i_n}) \otimes P_{a_2,i_2} \otimes \cdots \otimes P_{a_n,i_n}.$$

Now, we argue as to why the matrix summands have disjoint support. If any of the summands have shared support, one can construct an element $h \in k[C_{a_1}] \otimes_k \cdots \otimes_k k[C_{a_2}]$, such that the row weight of $M_{C_{a_1} \otimes \cdots \otimes C_{a_n}}(h)$ does not equal $\mathrm{wt}(h)$, which contradicts Proposition 8.

Example 14. Let k be an arbitrary field and identify $\mathbb{Z}_2 \times \mathbb{Z}_2$ with $\langle x, y \mid x^2 = 1, y^2 = 1, xy = yx \rangle$. Consider the ordered basis $\mathcal{B} = \{g_1, \ldots, g_4\}$, where

$$g_1 = 1, \;\; g_2 = y, \;\; g_3 = x, \;\; g_4 = xy.$$

Every element $f \in k[\mathbb{Z}_2 \times \mathbb{Z}_2]$ can be written as

$$f = \sum_{i=1}^{4} a_i g_i, \qquad a_i \in k. \tag{2}$$

For a fixed $f \in k[G]$ written as in (2), the matrix representation of f is

$$M_{\mathcal{B}}(f) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix} \in \mathrm{Mat}_4(k).$$

We may write the element f as $(a_1 + a_3 x) + (a_2 + a_4 x)y$, so we see that $M_{\mathcal{B}}(f)$ can be written as

$$\begin{pmatrix} a_1 & a_3 \\ a_3 & a_1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a_2 & a_4 \\ a_4 & a_2 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

5. POSSIBLE APPLICATIONS

5.1 An MDPC code-based cryptosystem

We will outline a possible MDPC code-based cryptosystem that is based on BIKE (Aragon et al., 2020).

Fix a group G of size n and let $w \approx \frac{\sqrt{2n}}{2}$ and $t \approx \sqrt{2n}$ be odd.

- **Private Key:** Pick $h_1, h_2 \in \mathbb{F}_2[G]^*$, both of weight w.
- **Public Key:** Let $h = h_1^{-1} h_2$. Publish (h, t).
- **Encryption:** Encode the message as $e_1, e_2 \in \mathbb{F}_2[G]^*$ such that $\mathrm{wt}(e_1) + \mathrm{wt}(e_2) = t$ and encrypt as $s = e_1 + he_2$.
- **Decryption:** Compute $h_1 s = h_1 e_1 + h_2 e_2$. Since h_1 and h_2 are of moderate density, e_1 and e_2 can be recovered, e.g. with a bit-flipping algorithm (Gallager, 1962).

Remark 15. The whole process can be reformulated with matrices by replacing the elements h_1, h_2 with their matrix representation $M_{\mathcal{B}}(h_i)$ with respect to the basis $\mathcal{B} = \{g_1, \ldots, g_n\}$, where $g_1, \ldots, g_n$ is an order of the group G, and e_1, e_2 with the first column of their matrix representation. By Proposition 8, the matrix $(M_{\mathcal{B}}(h_1) \mid M_{\mathcal{B}}(h_2))$ is a matrix of moderate density, allowing us to recover e_1 and e_2.

Remark 16. If we let n be a prime such that 2 is primitive modulo n and G be the cyclic group of order n, this cryptosystem is exactly BIKE.

Possible advantages of working with group algebras over BIKE could be, with suitable choices for G, the weakened algebraic structure. Also note that some group algebras contain elements which can be represented with very little data, which could be used for very small public keys. For example, Kronecker products of circulant matrices can be built from two, in comparison, short vectors. So some elements of group algebras of abelian groups can be represented by very little data (see Theorem 13).

Possible difficulties include efficient implementation of group multiplications and finding units in group algebras. Further, if the group G contains a non-trivial normal subgroup N, the map $\mathbb{F}_2[G] \to \mathbb{F}_2[G/N]$ might be usable for attacks.

5.2 Construction of LDPC and MDPC block codes

Several algebraic methods for constructing low density parity check (LPDC) and moderate density parity check (MDPC) codes have been investigated. Among these, perhaps one of the most relevant is the construction of the $[155, 64, 20]$ quasi-cyclic (QC) LDPC code designed by Tanner (Tanner et al., 2004). The key idea in his construction is the use of the structure of the multiplicative group of $\mathbb{F}_p$, where p is a prime, to place circulant matrices within a parity check matrix that defines the LDPC code. To be more specific, let a, b be two nonzero elements in $\mathbb{F}_p$ with orders $o(a) = k$ and $o(b) = j$. The LDPC code is specified by the parity-check matrix

$$H = \begin{pmatrix} \mathbb{I}_1 & \mathbb{I}_a & \mathbb{I}_{a^2} & \cdots & \mathbb{I}_{a^{k-1}} \\ \mathbb{I}_b & \mathbb{I}_{ab} & \mathbb{I}_{a^2b} & \cdots & \mathbb{I}_{a^{k-1}b} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbb{I}_{b^{j-1}} & \mathbb{I}_{ab^{j-1}} & \mathbb{I}_{a^2b^{j-1}} & \cdots & \mathbb{I}_{a^{k-1}b^{j-1}} \end{pmatrix},$$

where $\mathbb{I}_i$ is a $p \times p$ identity matrix with rows cyclically shifted to the left by i positions.

In the case of the $[155, 64, 20]$ QC-LDPC designed by Tanner, the values $p = 31$, $a = 2$ and $b = 5$ were chosen. Thus $o(a) = 5$, $o(b) = 3$ and the parity-check matrix is given by

$$H = \begin{pmatrix} \mathbb{I}_1 & \mathbb{I}_2 & \mathbb{I}_4 & \mathbb{I}_8 & \mathbb{I}_{16} \\ \mathbb{I}_5 & \mathbb{I}_{10} & \mathbb{I}_{20} & \mathbb{I}_9 & \mathbb{I}_{18} \\ \mathbb{I}_{25} & \mathbb{I}_{19} & \mathbb{I}_7 & \mathbb{I}_{14} & \mathbb{I}_{28} \end{pmatrix} \tag{3}$$

The matrices $\mathbb{I}_i$ appearing in the parity check matrix H in (3) are the 31×31 identity matrix with rows cyclically shifted to the left by i positions. Therefore, the matrices $\mathbb{I}_i$ in (3) are examples of circulant matrices, which we can identify with the group algebra $\mathbb{F}_2[C_{31}]$ where $C_{31} = \langle x \rangle$ is the cyclic multiplicative group of order $p = 31$. Under this representation, the matrix H may be written as follows:

$$H = \begin{pmatrix} x^1 & x^2 & x^4 & x^8 & x^{16} \\ x^5 & x^{10} & x^{20} & x^9 & x^{18} \\ x^{25} & x^{19} & x^7 & x^{14} & x^{28} \end{pmatrix}.$$

It is straightforward to verify that the matrix representation of $x^i \in \mathbb{F}_2[C_{31}]$ with respect to the ordered basis $\mathcal{B} = \{1, x, \ldots, x^{30}\}$ of $\mathbb{F}_2[C_{31}]$ is precisely $M_{\mathcal{B}}(x^i) = \mathbb{I}_i$. This remark brings to the light a natural generalization for the construction proposed by Tanner.

Let G be a finite group (not necessarily abelian) and k a finite field. Let $a, b \in k[G]$ be units having order $o(a) = k$ and $o(b) = j$, respectively. Then we construct a block linear code with parity check matrix

$$\begin{pmatrix} M_{\mathcal{B}}(a) & M_{\mathcal{B}}(a^2) & \cdots & M_{\mathcal{B}}(a^{k-1}) \\ M_{\mathcal{B}}(ab) & M_{\mathcal{B}}(a^2b) & \cdots & M_{\mathcal{B}}(a^{k-1}b) \\ \vdots & \vdots & \cdots & \vdots \\ M_{\mathcal{B}}(ab^{j-1}) & M_{\mathcal{B}}(a^2b^{j-1}) & \cdots & M_{\mathcal{B}}(a^{k-1}b^{j-1}) \end{pmatrix}.$$

Notice that the weight preserving property of the matrix representation allows us to determine the weight of the rows (and columns) of the matrices $M_{\mathcal{B}}(a^ib^j)$ from the weight of the elements $a^jb^j \in k[G]$. Thus, choosing elements of low weight will imply in the construction of a parity-check matrix of an LDPC code. Similarly, choosing elements of moderate weight could yield a parity-check matrix of an MDPC code.

This code construction is not limited to abelian groups, but when the group G is abelian, the representation of the matrices studied here may help to efficiently store H in memory.

REFERENCES

Aguilar Melchor, C., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Bos, J., Deneuville, J.C., Dion, A., Gaborit, P., Lacan, J., Persichetti, E., Robert, J.M., Véron, P., and Zémor, G. (2020). Hamming Quasi-Cyclic (HQC). *NIST PQC Call for Proposals*. Round 3 Submission.

Aragon, N., Barreto, P.S., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., Melchor, C.A., Misoczki, R., Persichetti, E., Sendrier, N., Tillich, J.P., Vasseur, V., and Zémor, G. (2020). BIKE: Bit Flipping Key Encapsulation. *NIST PQC Call for Proposals*. Round 3 Submission.

Baldi, M., Chiaraluce, F., Garello, R., and Mininni, F. (2007). Quasi-cyclic low-density parity-check codes in the mceliece cryptosystem. In *2007 IEEE International Conference on Communications*, 951–956. IEEE.

Berger, T.P., Cayrel, P.L., Gaborit, P., and Otmani, A. (2009). Reducing key length of the mceliece cryptosystem. In *International Conference on Cryptology in Africa*, 77–97. Springer.

Berman, S. (1967). On the theory of group codes. *Cybernetics*, 3(1), 25–31.

Gallager, R. (1962). Low-density parity-check codes. *IRE Transactions on information theory*, 8(1), 21–28.

Huffman, W., Kim, J., and Solé, P. (2021). *Concise Encyclopedia of Coding Theory*. CRC Press.

Jespers, E. and del Río, A. (2015a). *Group ring Groups*, volume 1. De Gruyter.

Jespers, E. and del Río, A. (2015b). *Group ring Groups*, volume 2. De Gruyter.

MacWilliams, F.J. (1970). Binary codes which are ideals in the group algebra of an abelian group. *The Bell System Technical Journal*, 49(6), 987–1011. doi:10.1002/j.1538-7305.1970.tb01812.x.

Milies, C. and Sehgal, S. (2002). *An Introduction to Group Rings*. Algebra and Applications. Springer Netherlands.

Roman, S. (2007). *Advanced Linear Algebra*. Graduate Texts in Mathematics. Springer, 3rd edition.

Santini, P., Persichetti, E., and Baldi, M. (2021). Reproducible families of codes and cryptographic applications. *Journal of Mathematical Cryptology*, 16(1), 20–48.

Tanner, R., Sridhara, D., Sridharan, A., Fuja, T., and Costello, D. (2004). Ldpc block and convolutional codes based on circulant matrices. *IEEE Transactions on Information Theory*, 50(12), 2966–2984.