Abstract

If $\mathbb{F}_q$ is a finite field, $C$ is a vector subspace of $\mathbb{F}_q^n$ (linear code), and $G$ is a subgroup of the group of linear automorphisms of $\mathbb{F}_q^n$, $C$ is said to be $G$-invariant if $g(C) = C$ for all $g \in G$. A solution to the problem of computing all the $G$-invariant linear codes $C$ of $\mathbb{F}_q^n$ is offered. This will be referred as the invariance problem. When $n = |G|t$, we determine conditions for the existence of an isomorphism of $\mathbb{F}_q[G]$-modules between $\mathbb{F}_q^n$ and $\mathbb{F}_q[G] \times \cdots \times \mathbb{F}_q[G]$ ($t$-times), that preserves the Hamming weight. This reduces the invariance problem to the determination of the $\mathbb{F}_q[G]$-submodules of $\mathbb{F}_q[G] \times \cdots \times \mathbb{F}_q[G]$ ($t$-times). The concept of Gaussian binomial coefficient for semisimple $\mathbb{F}_q[G]$-modules, which is useful for counting $G$-invariant codes, is introduced. Finally, a systematic way to compute all the $G$-invariant linear codes $C \subseteq \mathbb{F}_q^n$ is provided when $(|G|, q) = 1$.

Keywords. $G$-invariant codes, semisimple group algebras, Gaussian binomial coefficient, semisimple $\mathbb{F}_q[G]$-modules, primitive idempotents.

1 Introduction

Throughout this work $\mathbb{F}_q$ denotes a finite field with $q$ elements. A code $C$ is a vector subspace of $\mathbb{F}_q^n$. The Hamming distance $d(x, y)$ between two vectors $x, y \in \mathbb{F}_q^n$ is defined to be the number of coordinates in which $x$
and $y$ differ. The Hamming weight $wt(x)$ of a vector $x \in F_q^n$ is the number of nonzero coordinates in $x$. If $C$ is a code, its minimum weight is $wt(C) := \min\{wt(c) \mid c \in C\}$. The group of linear automorphisms of $C$ is denoted by $Aut_{F_q}(C)$, and the monomial automorphism group of $C$ is denoted by $MAut(C)$. Given a code, to make emphasis on its dimension $k$ and the length $n$ of its vectors (codewords), it usually is referred as an $[n,k]$-code. Given an $[n,k]$-code, to make emphasis on its minimum weight $\delta$, it usually is referred as an $[n,k,\delta]$-code.

The group algebra $F_q[G]$ of a finite group $G$ over $F_q$, is the set of the formal linear combinations of elements in $G$ with coefficients in $F_q$, i.e., $F_q[G] := \{\sum_{g \in G} a_g g \mid a_g \in F_q\}$, this set is a ring with the following sum and multiplication:

$$\left(\sum_{g \in G} a_g g\right) + \left(\sum_{g \in G} b_g g\right) := \sum_{g \in G} (a_g + b_g)g,$$

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{h \in G} b_h h\right) := \sum_{g \in G} \sum_{h \in G} (a_g b_h)gh.$$  

The identity of this ring is usually denoted by 1, but strictly speaking it is the identity element of $G$ times the unity of $F_q$. The Hamming weight $wt_G(x)$ of an element $x \in F_q[G]$ is the cardinality of its support respect to the basis $G$.

One of the most well-known class of linear codes is the one of cyclic codes, these are precisely the invariant codes under the automorphism $\sigma$ of $F_q^n$ given by $\sigma(a_0, a_1, ..., a_{n-1}) := (a_{n-1}, a_0, ..., a_{n-2})$ (ch4, [9]). Cyclic codes and some of their generalizations, such as consta-cyclic codes and quasi-cyclic codes, respond to the question of finding the invariant codes under some automorphisms of $F_q^n$. For instance, cyclic codes are the invariant codes under the cyclic shift $\sigma$; quasi-cyclic codes are the invariant codes under $\sigma^k$, where $k$ is a divisor of $n$; and consta-cyclic codes are those which are invariant under the mapping $\rho(a_0, a_1, ..., a_{n-1}) := (ca_{n-1}, a_0, ..., a_{n-2})$ with $c \in F_q^*$ [17]. All of these families of codes have in common that they are invariant under the groups $\langle \sigma \rangle$, $\langle \sigma^k \rangle$ and $\langle \rho \rangle$, respectively.

In general, given $G \leq Aut_{F_q}(F_q^n)$, one might ask which are the codes $C \subset F_q^n$ such that $g(C) = C$ for all $g \in G$? Offering an answer to this question is the first aim of this work; the second aim is to develop a formula to count $G$-invariant codes. when $G \leq Aut_{F_q}(F_q^n)$, $F_q^n$ can be endowed with a structure of left $F_q[G]$-module where $(\sum_{g \in G} \lambda_g g) \cdot v := \sum_{g \in G} \lambda_g g(v)$ for all $v \in F_q^n$, so
the $G$-invariant codes of $\mathbb{F}_q^n$ are precisely its $\mathbb{F}_q[G]$-submodules. From now on, every module will be assumed to be a left module.

If $C \subset \mathbb{F}_q^n$ is a $G$-invariant code for some subgroup $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n)$, then $\{g \mid c \in C, g \in G\} \leq \text{Aut}_{\mathbb{F}_q}(C)$, so the invariance problem is related to the problem of finding codes which have a non-trivial permutation (monomial) automorphism group. Some authors have addressed this last problem. For example, in [5] B. K. Dey and B. Sundar Rajan investigated the algebraic structure of a class of codes that they called $G$-invariant codes. In their work, a $G$-invariant code over $\mathbb{F}_q$ is a code that is closed under an arbitrary abelian group of permutations with exponent relatively prime to $q$. They characterized the dual codes and the self-duality of these $G$-invariant codes. Furthermore, they offered a minimum weight bound for a $G$-invariant code, and extended Karlin’s decoding algorithm [10] from systematic quasi-cyclic codes to systematic quasi-abelian codes. In [11] W. Knapp and P. Schmid, consider $[n, k]$-codes $C \subset \mathbb{F}_q^n$ such that "the permutation part of their monomial automorphisms" given by $\text{MAut}_{\text{Pr}}(C) := \{f \in S_n \mid df \in \text{MAut}(C)\}$ (where $d$ is represented by a diagonal invertible matrix on the canonical basis) contains $A_n$, $S_n$, or the Mathieu group. They proved that if $n > 6$ and $A_n \subset \text{MAut}_{\text{Pr}}(C)$, then $C$ should be equivalent to the zero code, $\mathbb{F}_q^n$, the repetition code or its dual. Moreover, they classified (up to equivalence) the few exceptions that occurred when $n \leq 6$ and studied the case in which $\text{MAut}_{\text{Pr}}(C)$ contains the Mathieu group (but not $A_n$), obtaining codes related to Golay codes.

To obtain the main results of this work, the $G$-invariant codes are considered as semisimple $\mathbb{F}_q[G]$-modules (see this definition in section 2). Taking advantage of the property of semisimplicity, a method to compute them and a formula to count them is developed. Our results apply for arbitrary finite groups, these might be permutation groups or not.  

This work addressed different questions related to the invariance problem. It is organized as follows: In Section 2, some preliminaries about semisimple modules and some results that will be used later are presented. Then, in Section 3 we address the question of determining when $\mathbb{F}_q^n$, with a structure of $\mathbb{F}_q[G]$-module as above, is isomorphic, with an isomorphism that preserves the Hamming weight, to a direct sum of copies of $\mathbb{F}_q[G]$. A clear particular answer to this, but not unique, occurs when $G$ is the group generated by the cyclic shift of $\mathbb{F}_q^n$. Throughout Sections 4 and 5 we introduce

---

1 Actually these groups might have elements that do not preserve the Hamming weight, but for some applications of the results to coding theory, these can be regarded as groups of permutations or monomial transformations.
and study the concept of Gaussian binomial coefficient for finite semisimple \( \mathbb{F}_q[G] \)-modules, and develop an algorithm to efficiently compute all the possible sums of a collection of simple isomorphic \( \mathbb{F}_q[G] \)-submodules of a given finite \( \mathbb{F}_q[G] \)-module. This algorithm is used later in Section 6 to provide a method to determine all the \( G \)-invariant codes of \( \mathbb{F}_n^q \) when \((|G|, q) = 1\). Finally, in Sections 7 and 8, we propose a theoretically possible solution to solve the invariance problem when our method could not be applied, and give some examples illustrating the most important results, respectively.

2 Preliminaries

As it was mentioned above, the \( G \)-invariant codes in \( \mathbb{F}_n^q \) are precisely its \( \mathbb{F}_q[G] \)-submodules. We use this module structure they possess to compute them and to count them. For that, these modules are required to be semisimple modules. In this section we present the concept of semisimple module among some other important definitions and results that will be used in the upcoming sessions. For reviewing properties about semisimple modules and rings see [4] section 3B and [3] section 25.

Let \( A \) be a ring, \( M \) and \( S \) be \( A \)-modules. \( S \) is a \textbf{simple module} if \( S \) does not have proper submodules different from \( 0 \). \( S \) is an \textbf{inescindible module} if \( S \) cannot be expressed as a direct sum of non-trivial submodules. \( M \) is a \textbf{semisimple module} if it can be expressed as a direct sum of simple submodules; or equivalently, if for any \( A \)-submodule \( N \) of \( M \) there exists a submodule \( U \) of \( M \) such that \( M = N \oplus U \). \( A \) is a \textbf{semisimple ring} if every non-zero \( A \)-module is semisimple.

Two elements \( x, y \in A \) are called \textbf{orthogonal} if \( xy = yx = 0 \). An element \( e \in A \) is called \textbf{idempotent} if \( e^2 = e \); and it is \textbf{primitive} if \( e = f + g \) where \( f, g \in A \) are orthogonal idempotents, implies \( f = 0 \) or \( g = 0 \).

Let \( M \) and \( N \) be \( A \)-modules. If there exists an \( A \)-module \( U \) such that \( M \cong N \oplus U \), it is said that \( N \) \textbf{divides} \( M \), and denoted by \( N \mid M \). If \( M \) is a semisimple finitely generated \( A \)-module and \( S \) is a simple \( A \)-module such that \( S \mid M \), the \textbf{multiplicity} \( n \) of \( S \) in \( M \) is defined as the greatest natural number such that \( nS \mid M \) with \( nS = S \oplus \cdots \oplus S \) (\( n \)-times). Let \( I \subset A \) be an ideal. \( I \) is \textbf{minimal ideal} if \( I \) is a simple \( A \)-submodule. Let \( M \) be a finitely generated \( A \)-module over a semisimple ring. If \( \{Af_1, ..., Af_r \} \) is a collection of minimal ideals of \( A \) such that \( Af_j \mid M \) for all \( j \in \{1, ..., r \} \), and for any simple \( A \)-submodule \( N \) of \( M \) there exists a unique \( j \in \{1, ..., r \} \) such that \( N \cong Af_j \), then \( \{Af_1, ..., Af_r \} \) will be said to be is a \textbf{basic set of ideals} for \( M \). A collection of idempotents \( \{e_1, ..., e_r \} \subset A \) such that \( Ae_1, ..., Ae_r \) is a
basic set of ideals for $M$ will be called a **basic set of idempotents** for $M$. If $e \in A$ is a primitive idempotent such that $Ae \mid M$, then the **homogenous component associated to $e$** $(Ae)$ will be the $A$-submodule of $M$ defined by $\sum_{U \subseteq M \wedge U \simeq Ae} U$. Schur’s lemma ([16], Lemma 2.6.14), Maschke’s theorem ([16], Theorem 3.4.7), and Krull-Schmidt theorem (presented in [18], page 538) are well-known results that could be found in many books of Algebra. However, these are usually presented in different contexts and ways, for this reason, and to make easier to read this work, we present them below in a context that is necessary for our applications.

**Lemma 2.1 (Schur’s lemma)** Let $M$ and $N$ be simple $\mathbb{F}_q[G]$-modules. Let $f : M \to N$ be a non-zero morphism. Then $f$ is an isomorphism.

**Theorem 2.2 (Maschke’s theorem)** Let $G$ be a finite group. Then the group algebra $\mathbb{F}_q[G]$ is semisimple if and only if $|G|$ is invertible in $\mathbb{F}_q$.

**Theorem 2.3 (Krull-Schmidt theorem)** Let $M$ be a finite $\mathbb{F}_q[G]$-module. Then there exists a collection $\{A_i \mid i = 1, \ldots, n\}$ of indecomposables $\mathbb{F}_q[G]$-modules such that $M = A_1 \oplus \cdots \oplus A_n$. Furthermore, this decomposition is unique up to isomorphism and permutation of the summands.

Lemma 2.2 and [3] Theorem 25.10 imply the following result: If $G$ is a finite group such that $(|G|, q) = 1$, and $M$ is a finite $\mathbb{F}_q[G]$-module. Then there exists a collection $\{I_j \mid j \geq 1\}$ of minimal ideals of $\mathbb{F}_q[G]$ such that $M \cong \oplus_{j=1}^{n} I_j$. This result gives some light on how to compute the $G$-invariant codes in $\mathbb{F}_q$. First, all the $\mathbb{F}_q[G]$-submodules (G-invariant codes) of $\mathbb{F}_q^n$ isomorphic to minimal ideals (i.e., simple $\mathbb{F}_q[G]$-modules) should be computed (a solution to this is presented in Section 6.2). Then, all the possible direct sums of these modules should be determined (a solution to this is presented in Section 5). The following lemma is just a slight modification of [12], Theorem 4.3 (part 1), in the context of $\mathbb{F}_q[G]$-modules.

**Lemma 2.4** Let $A = \mathbb{F}_q[G]$, $e \in A$ be a primitive idempotent, $I = Ae$, and $M$ an $A$-module. If $\eta_e : \text{Hom}_A(Ae, M) \to eM$ is given by $\varphi \mapsto \varphi(e)$, then $\eta_e$ is an isomorphism of $\mathbb{F}_q$-vector spaces.

**Proof.** It is clear that $\eta_e$ is linear and injective. If $x \in eM$, $f_x : Ae \to M$ given by $ae \mapsto (ae)x$ defines a morphism of $A$-modules such that $\eta_e(f_x) = ex = x$, so $\eta$ is surjective.

2Similarly, it will be said that $e(Ae)$ is associated to $H$.  

5
Note that a basic set of idempotents is a collection of primitive orthogonal idempotents. Its elements are primitive because they generate minimal ideals and are orthogonal by Lemma 2.4 and Lemma 2.1.

In the following example we compute the decomposition of \( \mathbb{F}_5[S_3] \) into its homogeneous components. This will be used later again in Example 8.2.

**Example 2.5** Let \( S_3 = \langle a, b \mid a^3 = b^2 = 1, bab^{-1} = a^2 \rangle = \{1, a, a^2, b, ba, ba^2 \} \) and \( A = \mathbb{F}_5[S_3] \). Then \( \{c_1 = 1+a+a^2+b+ba+ba^2, e_2 = 1+a^2+4b+4ba+4ba^2, e_3 = 2+3a+2b+3ba^2, e_4 = 2+3a+3b+2ba^2 \} \) is a set of primitive orthogonal idempotents of \( A \) such that \( 1 = \sum_{i=1}^{4} e_i \). In addition, by Lemma 2.4 and Lemma 2.7, \( Ae_1 \not\cong Ae_2 \) because \( e_1Ae_2 = e_1\mathbb{F}_5e_2 = \mathbb{F}_5e_1e_2 = 0 \), and \( Ae_3 \cong Ae_4 \) because \( y = 1+2a+b \) is a unity in \( A \) (with inverse \( 2+4a+4b+2ba+2ba^2 \)) such that \( ye_3y^{-1} = e_4 \). Therefore, \( H_1 = Ae_1 \), \( H_2 = Ae_2 \) and \( H_3 = Ae_3 \oplus Ae_4 \) are the homogeneous components of \( A \).

**Lemma 2.6** Let \( A = \mathbb{F}_q[G] \) be semisimple, \( I \leq A \) be a minimal ideal such that \( I \) has multiplicity 1 in \( A \), and \( n \in \mathbb{Z}^+ \). If \( N \neq 0 \) is a cyclic \( A \)-submodule of \( nI \), then \( N \) is simple and \( N \cong I \).

**Proof.** Let \( N \neq 0 \) be a cyclic \( A \)-submodule of \( nI \). Then there exists \( 0 \neq x \in nI \) such that \( N = Ax \), thus \( N \) is isomorphic to \( A/\text{ann}(x) \) (where \( \text{ann}(x) \) is the annihilator of \( x \)), and this is isomorphic to a direct complement \( S \) of \( \text{ann}(x) \) in \( A \), which there exists because \( A \) is semisimple, so \( N \cong S \). On the other hand, the unique simple \( A \)-submodule (up to isomorphism) that divides \( nI \) is \( I \), thus the unique simple \( A \)-submodule (up to isomorphism) that divides \( N \) is \( I \). Consequently, there exists \( k \in \mathbb{Z}^+ \) with \( k \leq n \) such that \( kI \cong N \cong S \leq A \) and as the multiplicity of \( I \) in \( A \) is 1, then \( k = 1 \), so \( I \cong N \).

## 3 \isomorphism{F_q^n} with \( \mathbb{F}_q[G] \times \cdots \times \mathbb{F}_q[G] \)

Let \( C_n \) denote the cyclic group of order \( n \) generated by the cyclic shift \( \sigma \). This group acts by evaluation on \( \mathbb{F}_q^n \) endowing it with a structure of \( \mathbb{F}_q[C_n] \)-module. Another natural \( \mathbb{F}_q[C_n] \)-module is \( \mathbb{F}_q[C_n] \) itself. A classic way of determining the cyclic linear codes of \( \mathbb{F}_q^n \) is by using the isomorphism of \( \mathbb{F}_q[C_n] \)-modules, \( \phi: \mathbb{F}_q^n \to \mathbb{F}_q[C_n] \) given by, \( (a_0, a_1, ..., a_{n-1}) \mapsto a_0 + a_1\sigma + ... + a_{n-1}\sigma^{n-1} \), this provides a bijection between the ideals of the group algebra \( \mathbb{F}_q[C_n] \) and the invariant codes of \( \mathbb{F}_q^n \) under the cyclic shift.

---

3 This idempotents were computed using [7] Theorem 3.3 and doing some computations in Sage.
Next, it is shown that $f \vdash \rho \vdash \Omega \vdash \Sigma$. Furthermore, this $\phi$ preserves the Hamming weight, i.e., for all $v \in \mathbb{F}_q^n$, $wt(v) = wt_{\mathbb{C}^n}(\phi(v))$. Let us take that situation to a more general context. If $G \leq Aut_{\mathbb{F}_q}(\mathbb{F}_q^n)$ and $n = t|G|$ one may ask, whether there exists an isomorphism of $\mathbb{F}_q[G]$-modules between $\mathbb{F}_q^n$ and $\bigoplus_{i=1}^t \mathbb{F}_q[G]$ preserving Hamming weight. The following result will help to answer that question.

Let $G$ be a finite group. If $M$ is an $\mathbb{F}_q[G]$-module, the representation induced by left multiplication by elements of $G$ in $M$ is $\rho : G \to Aut_{\mathbb{F}_q}(M)$ given by $g \mapsto \rho(g)$, where $\rho(g)(v) = gv$ for all $v \in M$. If $R = \bigoplus_{i=1}^t \mathbb{F}_q[G] = \mathbb{F}_q[G] \times \cdots \times \mathbb{F}_q[G]$ (t-times) is an external direct sum of $\mathbb{F}_q[G]$ (i.e. with pointwise addition and pointwise left multiplication by elements of $\mathbb{F}_q[G]$), the Hamming weight is defined on $R$ as $wt'((i_1, \ldots, i_t)) = \sum_{j=1}^t wt_G(i_j)$ for all $(i_1, \ldots, i_t) \in R$.

**Theorem 3.1** Let $G \leq Aut_{\mathbb{F}_q}(\mathbb{F}_q^n)$ with $n = |G| \cdot t$. Let $\pi_j : R \to \mathbb{F}_q[G]$ be given by $(i_1, \ldots, i_t) \mapsto i_j$ for all $j = 1, \ldots, t$, where $R = \mathbb{F}_q[G] \times \cdots \times \mathbb{F}_q[G]$ (t-times); $\mu$ be the canonical basis of $\mathbb{F}_q^n$, and $\eta = \bigcup_{j=1}^t \mathbb{G}_j$ where $G_j = \{v \in R \mid \pi_j(v) \in G and \pi_i(v) = 0, for i \neq j\}$. Let $\rho : G \to Aut_{\mathbb{F}_q}(\mathbb{F}_q^n)$, $\rho' : G \to Aut_{\mathbb{F}_q}(R)$ be the representations induced by the $\mathbb{F}_q[G]$-modules structure of $\mathbb{F}_q^n$ (given by evaluation) and $R$ (given by left multiplication), respectively. Let $g \in G$, $[\rho(g)]_\mu$ be the matrix of $\rho(g)$ with respect to the basis $\mu$, and $[\rho'(g)]_\eta$ the matrix of $\rho'(g)$ with respect to the basis $\eta$. Let $S = \{s_1, \ldots, s_k\}$ be a generating set for $G$, and $M \leq GL(n, q)$ the group of monomial matrices. Then, there is a bijection $\phi$ from $H := \{A \in M \mid [\rho(s_i)]_\mu A^{-1} = [\rho'(s_i)]_\eta A, i = 1, \ldots, k\}$ to the set $L$ of the $\mathbb{F}_q[G]$-isomorphisms from $\mathbb{F}_q^n$ to $R$ that preserve the Hamming weight, given by, $A \mapsto f_A$ with $[f_A(v)]_\eta := A[v]_\mu$ for all $v \in \mathbb{F}_q^n$.

**Proof.** Let $wt$ and $wt'$ denote the Hamming weight on $\mathbb{F}_q^n$ and $R$, respectively. By definition $wt'(r) := \sum_{j=1}^t wt_G(\pi_j(r))$. Let $h : L \to H$ be given by $f \mapsto \eta[f]_\mu$, for all $f \in L$.

First, we show that $\phi$ has, in fact, $L$ as its codomain. Let $A \in H$, then $A[\rho(s_i)]_\mu = [\rho'(s_i)]_\eta A$ for all $i = 1, \ldots, k$. Let $f : \mathbb{F}_q^n \to R$ be the linear transformation given by $[f(v)]_\eta := A[v]_\mu$, then $\eta[f]_\mu = A$, so $f(\rho(s_i)) = \rho'(s_i)(f)$ for all $i = 1, \ldots, k$, and $\phi(A) = f$ is an isomorphism of $\mathbb{F}_q[G]$-modules. Now we observe that $f$ preserves the Hamming weight. For $v \in \mathbb{F}_q^n$, $[f(v)]_\eta = A[v]_\mu$, thus $wt(v) = wt(A[v]_\mu)$ because $A$ is a monomial matrix, but $wt([f(v)]_\eta) = \sum_{j=1}^t wt(\pi_j(f(v))) = \sum_{j=1}^t wt_G(\pi_j(f(v))) = wt'(f(v))$ by definition of $wt'$, thus $wt(v) = wt'(f(v))$.

Next, it is shown that $H$ is, in fact, the codomain of $h$. If $f \in L$ and $g \in G$, then $f(\rho(g)) = \rho'(g)(f)$, thus $\eta[f \circ \rho(g)]_\mu = \eta[\rho'(g) \circ f]_\mu$. Let
and only if \( f \) serves the Hamming weight. Consequently, \( C \) is isomorphic to \( N \) in \( R \) given by \( \eta = i \) and \( \phi = e \). As it is clear that \( \phi \) and \( h \) are mutually inverse, the proof is complete.

**Example 3.2** Let \( \alpha \) be the automorphism of \( \mathbb{F}_3^4 \) given by \( \alpha(a_0, a_1, a_2, a_3) = (a_1, a_0, a_3, a_2) \), and \( G := \langle \alpha \rangle = \{1, \alpha\} \). \( G \) has order 2, thus one may ask if \( \mathbb{F}_3^4 \) and \( \mathbb{F}_3[G] \times \mathbb{F}_3[G] \) are isomorphic as \( \mathbb{F}_3[G] \)-modules with an isomorphism that preserves Hamming weight. Let \( \rho : G \to \text{Aut}_{\mathbb{F}_3}(\mathbb{F}_3^4) \) be the inclusion and \( \rho' : G \to \text{Aut}_{\mathbb{F}_3}(R) \) be given by \( \alpha \mapsto \iota_0 \) where \( \iota_0 \) is the left multiplication by \( \alpha \). Let \( \mu \) denote the canonical basis of \( \mathbb{F}_3^4 \) and \( \eta = \{(1,0), (\alpha,0), (0,1), (0,\alpha)\} \). If we consider the monomial matrix

\[
M := \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0
\end{bmatrix}
\]

then \( M[\rho(\alpha)]_\mu = [\rho'(\alpha)]_\eta M \). Hence, according to Theorem 3.1, \( f : \mathbb{F}_3^4 \to R \) given by \( [f(v)]_\eta := M[v]_\mu \) is an isomorphism of \( \mathbb{F}_3[G] \)-modules that preserves the Hamming weight. Consequently, \( C \subseteq \mathbb{F}_3^4 \) is a \( G \)-invariant code if and only if \( f(C) \) is a \( \mathbb{F}_3[G] \)-submodule (2-quasi-cyclic code) of \( R \) which is isomorphic to \( C \) as \( \mathbb{F}_3[G] \)-module and as metric space, i.e., the \( G \)-invariant codes in \( \mathbb{F}_3^4 \) are equivalent to the 2-quasi-cyclic codes.

## 4 The Gaussian binomial coefficient for semisimple \( \mathbb{F}_q[G] \)-modules

In this section a Gaussian binomial coefficient for semisimple \( \mathbb{F}_q[G] \)-modules is introduced and some of its properties are studied. This coefficient will be useful for counting \( G \)-invariant codes.

**Definition 4.1 (Gaussian binomial Coefficient)** Let \( N \) and \( M \) be finite semisimple \( \mathbb{F}_q[G] \)-modules. The Gaussian binomial coefficient of \( M \) in \( N \) is defined as

\[
\binom{M}{N}_q := |\{U \leq M \mid U \cong N\}|.
\]
Lemma 4.2 Let $A = \mathbb{F}_q[G]$ be semisimple, $M$, $N$ and $T$ be finite $A$-modules, and $I \leq A$ be a minimal ideal such that $I \mid M$. Then the following statements hold:

1. $(\frac{M}{N})_q \neq 0$ if and only if $N \mid M$.

2. If $N \mid M$, then $(\frac{N}{I})_q \leq (\frac{M}{I})_q$.

3. If $U$ is an $A$-module such that $(\frac{kI}{I})_q \leq (\frac{U}{I})_q$, then $kI \mid U$.

4. If $\text{Hom}_A(T, N) = 0$, then $(\frac{M \oplus N}{T})_q = (\frac{M}{T})_q$.

5. If $\text{Hom}_A(T, N) = 0$, then $(\frac{M}{T \oplus N})_q = (\frac{M}{T})_q(\frac{M}{N})_q$.

Proof.

1. $N \mid M$ if and only if $N$ is embedded in $M$, if and only if $(\frac{M}{N})_q \neq 0$.

2. It is clear.

3. If $X$ is a set of simple $A$-submodules of $U$ isomorphic to $I$ such that $(\frac{kI}{I})_q \leq |X|$, then $\sum_{x \in X} x \cong rI$ for some $r \in \mathbb{Z}^+$, thus $(\frac{kI}{I})_q \leq |X| \leq (\frac{rI}{I})_q$, implying that $k \leq r$, so $kI \mid rI \mid U$.

4. $\text{Hom}_A(T, N) = 0$ if and only if $T$ and $N$ have no simple common divisors. Let $M' \cong M$ and $N' \cong N$ such that the internal direct sum $M' \oplus N' = M \oplus N$. As $M \mid M \oplus N$ then $(\frac{M}{T})_q = (\frac{M'}{T})_q \leq (\frac{M \oplus N}{T})_q = (\frac{M' \oplus N'}{T})_q$. If the equality does not hold, there would exists $L \leq M' \oplus N'$, with $L \cong T$ and $L \not\cong M'$, thus there exists a simple $A$-module $S \leq L$ such that $S \cap M' = 0$. Hence $S \mid N$, but $S \mid T$, which contradicts $\text{Hom}_A(T, N) = 0$.

5. Consider the function $f : \{L \leq M \mid L \cong T \oplus N\} \rightarrow \{U \leq M \mid U \cong T\} \times \{Z \leq M \mid Z \cong N\}$ given by $f(L) = (L_1, L_2)$ where $L = L_1 \oplus L_2$, $L_1 \cong T$, and $L_2 \cong N$. $f$ is well defined. Otherwise, there exists $L$ in its domain such that $L = L_1 \oplus L_2 = X_1 \oplus X_2$ where $L_1 \cong X_1 \cong T$, $L_2 \cong X_2 \cong N$, and $L_1 \neq X_1$ or $L_2 \neq X_2$. Without loss of generality, $L_1 \neq X_1$ and there exists a simple $A$-submodule $S$ of $L_1$ that is not contained in $X_1$, then its multiplicity in $S \oplus X_1 \leq L$ is greater than its multiplicity in $T$. However, this contradicts $\text{Hom}_A(T, N) = 0$. If $\text{Hom}_A(T, N) = 0$, then $f$ is invertible with inverse $f^{-1}(A, B) = A \oplus B$, therefore $(\frac{M}{T \oplus N})_q = (\frac{M}{T})_q(\frac{M}{N})_q$. 

9
Corollary 4.3 Let $A = \mathbb{F}_q[G]$ be semisimple. Let $M \cong \bigoplus_{j=1}^t n_j I_j$ be an $A$-module, where $I_j \leq A$ is a minimal ideal and $n_j$ its multiplicity in $M$ for all $j = 1, \ldots, t$. Let $N \leq M$, if $N \cong \bigoplus_{l \in J} k_l I_l$ where $J \subseteq \{1, \ldots, t\}$, then

$$
\binom{M}{N}_q = \prod_{l \in J} \left( k_l I_l \right)_{q}.
$$

Proof. Let $J \subseteq \{1, \ldots, t\}$ be such that $N \cong \bigoplus_{l \in J} k_l I_l$. As $N \leq M$, $k_l \leq n_l$ for all $l \in J$, thus

$$
\binom{M}{N}_q = \left( \bigoplus_{j=1}^t n_j I_j \right)_{q}
= \prod_{l \in J} \left( \bigoplus_{j=1}^t n_j I_j \right)_{q} \quad \text{by Lemma 4.2 part 5}
= \prod_{l \in J} \binom{n_l I_l}{k_l I_l}_q \quad \text{by Lemma 4.2 part 4}.
$$

Definition 4.4 Let $A$ be an arbitrary ring, $M$ a finitely generated semisimple $A$-module and let $SS(M)$ be defined as the collection of all simple $A$-submodules of $M$.

If $X \subseteq SS(M)$ is such that $\sum_{x \in X} x = M$, then it will be said that $X$ generates $M$, or $X$ is a generating set by simple $A$-submodules of $M$.

If $Y \subseteq SS(M)$ is such that $\sum_{y \in Y} y = \bigoplus_{y \in Y} y$, then it will be said that $Y$ is independent, or $Y$ is an independent set of simple $A$-submodules of $M$.

If $X \subseteq SS(M)$ is independent and generates $M$, it will be said that $X$ is a basis for $M$, or $X$ is a basis by simple $A$-submodules of $M$.

Lemma 4.5 Let $A$ be an arbitrary ring, and $M$ be finitely generated semisimple $A$-module.

1. If $X \subseteq SS(M)$ and $X$ generates $M$, then $X$ contains a basis.

2. If $X \subseteq SS(M)$, $X$ is independent and $X$ has the cardinality of a basis for $M$, then $X$ is a basis.

Proof.

1. Let $X \subseteq SS(M)$ be such that $\sum_{x \in X} x = M$. If $\sum_{x \in X} x \neq \bigoplus_{x \in X} x$ (i.e. $X$ is not independent), there exists $x_0 \in X$ such that $x_0 \subseteq$
\[ \sum_{x \in X - \{x_0\}} x = M. \] If \( X_0 = X - \{x_0\} \) is independent, the proof concludes. Otherwise, the same reasoning can be applied to \( X_0 \) and this process can be repeated until obtaining a subset of \( X \) that is independent and generates \( M \).

2. Let \( X, Y \subseteq SS(M) \) be such that \( \sum_{x \in X} x = \bigoplus_{x \in X} x, M = \bigoplus_{y \in Y} y \) and \( |X| = |Y| \). As \( \bigoplus_{x \in X} x \subset M = \bigoplus_{y \in Y} y \), \( \bigoplus_{x \in X} x \cong \bigoplus_{y \in J} y \) with \( J \subseteq Y \), so by Theorem 2.3 \( |J| = |X| = |Y| \), implying that \( \bigoplus_{x \in X} x = \bigoplus_{y \in Y} y = M \).

**Lemma 4.6** Let \( A = F_q[G] \) be semisimple. If \( I \subseteq A \) is a minimal ideal, and \( k, n \in \mathbb{Z}^+ \) with \( 2 \leq k \leq n \), then
\[
\binom{nI}{kI_q} = \frac{(nI)_q}{(kI)_q} \frac{(nI)_q - (2I)_q}{(kI)_q - (2I)_q} \ldots \frac{(nI)_q - (k-1)I)_q}{(kI)_q - (k-1)I}_q.
\]

**Proof.** Let \( X = \{ N \leq nI \mid N \cong kI \} \), and \( Y = \{ A \subseteq SS(nI) \mid |A| = k \wedge A \text{ is independent} \} \) the collection of basis by simple \( A \)-submodules of the elements of \( X \) (by Lemma 4.5 part 2). If \( R \) is the relation on \( Y \) given by \( aRb \) if and only if \( a \) generates the same \( A \)-module as \( b \), for all \( a, b \in Y \), then \( R \) is an equivalence relation. If \( Y/R \) is the quotient set determined by \( R \), then the function \( f : Y/R \rightarrow X \) given by \( [x] \mapsto \sum_{m \leq [x]} m \) is a bijection, so \( |Y/R| = |X| = \binom{nI}{kI_q} \). On the other hand, every equivalence class on \( Y/R \) has the same cardinality which is the number of basis by simple \( A \)-submodules of \( kI \). Thus \( |Y/R| = \frac{|Y|}{|[x_0]|} \) for some \( x_0 \in Y \), hence
\[
\frac{nI}{kI_q} = \frac{\# \text{ of l. i. sets of simple } A \text{-submodules of } nI \text{ having cardinality } k}{\# \text{ of basis by simple } A \text{-submodules of } kI}.
\]

For building a independent set of simple \( A \)-submodules of \( nI \) having cardinality \( k \) (i.e. an element of \( Y \)), we should start by taking a simple \( A \)-module \( S_1 \), and for that, we have \( \binom{nI}{I_q} \) possible choices. For taking another simple \( A \)-module \( S_2 \) such that the collection \( \{S_1, S_2\} \) remains independent, we have \( \binom{(nI)_q - (2I)_q}{I_q} \) possible choices. To take a simple \( A \)-module \( S_3 \) such that the collection \( \{S_1, S_2, S_3\} \) remains independent, we have \( \binom{(nI)_q - (k-1)I}_q \) possible elections. In general, to chose a simple \( A \)-module \( S_k \) such that the collection \( L = \{S_1, S_2, S_3, \ldots, S_{k-1}, S_k\} \) remains independent, we have \( \binom{(nI)_q - (k-1)I}_q \) possibilities. Therefore, at the end of this process, we will construct a independent set of simple \( A \)-submodules of \( nI \) having size \( k \). We did the choices of the \( A \)-modules \( S_i \) without worrying about the
order, and depending on that, the same set $L$ can be obtained, so we have that $|Y| = \frac{(nI)_{q}^{(nI)_{q} - (lI)_{q}} \cdots (lI)_{q} - ((k-1)I)_{q}}{k!}$, where $(lI)_{q} = 1$.

To build a basis by simple $A$-submodules of $kI$ we could apply the same reasoning used before. For that it should be taken into account that an independent set of simple $A$-submodules of $kI$ that has cardinality $k$ is in fact a basis for $kI$ (by Lemma 4.5, part 2), hence

$$|x_0| = \frac{(kI)_{q}^{(kI)_{q} - (lI)_{q}} \cdots (lI)_{q} - ((k-1)I)_{q}}{k!}.$$  

**Lemma 4.7** Let $A = \mathbb{F}_q[G]$ be semisimple, $I \leq A$ be a minimal ideal with multiplicity 1 in $A$, and $n \in \mathbb{Z}^+$. If $U^* := U - \{0\}$ for all $U \leq nI$, then $X := \{U^* \mid U \leq nI \land U \cong I\}$ is a partition of $(nI)^*$.

**Proof.** If $n = 1$, the assertion is true. Otherwise, if $V, W \in X$ and $W \neq V$, then there exist $U$ and $T$ distinct simple $A$-submodules of $nI$ such that $V = U^*$ and $W = T^*$, as $U \cap T = \{0\}$, $\emptyset = U^* \cap T^* = V \cap W$. If $x \in (nI)^*$, $Ax \subseteq nI$, so $Ax \cong I$ (by Lemma 2.6), and $x \in Ax - \{0\} \in X$.

**Corollary 4.8** Let $A$, $I$, and $n$ be as in Lemma 4.7. If $\dim_{q}(I) = k$, then $\frac{(nI)_{q}^{(nI)_{q} - (lI)_{q}} \cdots (lI)_{q} - ((k-1)I)_{q}}{k!}$.

**Proof.** Let $X$ be as in Lemma 4.7, then $(nI)^* = \sqcup_{V \in X} V$, so $|(nI)^*| = |X| \cdot |I^*|$, hence

$$\binom{nI}{I}_{q} = |X| = \frac{|(nI)^*|}{|I^*|} = \frac{|nI| - 1}{|I| - 1} = \frac{q^{nk} - 1}{q^k - 1}.$$  

Observe that Corollary 4.8 presents the Gaussian binomial coefficient as a product of simpler Gaussian binomial coefficients, which in turn are later expressed in simpler terms in Lemma 4.6. This last terms are finally calculated, when the minimal ideals that appear in them have multiplicity 1 in their group algebra, in Corollary 4.8. As every minimal ideal $I$ of a semisimple commutative group algebra $\mathbb{F}_q[G]$ has multiplicity 1 in $\mathbb{F}_q[G]$, now we can compute any Gaussian binomial coefficient when $G$ is abelian.

### 4.1 Counting all the $G$-invariant codes

The following result plays an important role in the solution of the invariance problem.
Lemma 4.9 Let $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n)$ such that $A = \mathbb{F}_q[G]$ is semisimple. Let \[ \{I_j \mid j = 1, \ldots, r\} \] be a basic set of ideals for $\mathbb{F}_q^n$, and $H_j \cong n_jI_j$ be the homogeneous component of $\mathbb{F}_q^n$ associated to $I_j$ for all $j = 1, \ldots, r$. Let \[ S(M) := \{C \subseteq M \mid C \text{ is a } G \text{-invariant code}\} \] for all $G$-invariant code $M \leq \mathbb{F}_q^n$, and $Z := \{\oplus_{i=1}^r M_i \mid M_i \text{ is a } A \text{-submodule of } H_i, \text{ for all } i = 1, \ldots, r\}$. Let \[ D(B) := \prod_{j \in B} \{1, \ldots, n_j\} \text{ for all } B \in T := 2^{\{1, \ldots, r\}} - \emptyset \}. \] Then,

1. $S(\mathbb{F}_q^n) = Z$, and $|S(\mathbb{F}_q^n)| = \prod_{j=1}^r |S(H_j)|$.

2. $|S(\mathbb{F}_q^n)| = \left[\sum_{B \in T} \sum_{\{t_j\}_{j \in D(B)}} \left(\prod_{j \in B} \binom{n_j}{t_j} \right)q^n\right] + 1$ and \[ \prod_{j=1}^r \left(\sum_{t_j=1}^{n_j} \binom{n_j}{t_j}q^n + 1\right). \]

Proof.

1. It is clear that $S(\mathbb{F}_q^n) = Z$. Let $f : S(\mathbb{F}_q^n) \rightarrow \prod_{j=1}^r S(H_j)$ be given by $N \mapsto (N_j)_{j=1}^r$, where $N_j$ is the homogeneous component of $N$ associated to $I_j$ if $I_j | N$ and $N_j = 0$ otherwise for all $j = 1, \ldots, r$. Then $f$ is invertible with inverse $g$ given by $(A_j)_{j=1}^r \mapsto \oplus_{j=1}^r A_j$.

2. Observe that

\[ S(\mathbb{F}_q^n) = \left[\bigcup_{B \in T} \bigcup_{\{t_j\}_{j \in D(B)}} \{C \leq \mathbb{F}_q^n \mid C \cong \oplus_{j \in B} t_jI_j\}\right] \bigcup \{0\}, \]

thus $|S(\mathbb{F}_q^n)| = \left[\sum_{B \in T} \sum_{\{t_j\}_{j \in D(B)}} \left(\prod_{j \in B} \binom{n_j}{t_j} q^n\right)\right] + 1$ (by Corollary 4.3).

Note that $|S(H_j)| = 1 + \binom{n_j}{t_j} + \binom{n_j}{2t_j} + \cdots + \binom{n_j}{t_j} + \cdots + \binom{n_j}{n_j} + 1 = \sum_{t_j=1}^{n_j} \binom{n_j}{t_j} q^n + 1$ for all $j = 1, \ldots, r$, thus \[ \prod_{j=1}^r |S(H_j)| = \prod_{j=1}^r \left(\sum_{t_j=1}^{n_j} \binom{n_j}{t_j} q^n + 1\right). \]

4.2 Counting 1-generator $G$-invariant codes

Let $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n)$. If $\mathbf{0} \neq C \subseteq \mathbb{F}_q^n$ is a cyclic $\mathbb{F}_q[G]$-submodule, it will be said that $C$ is a 1-generator $G$-invariant code. Now we use the Gaussian binomial coefficient to count 1-generator $G$-invariant codes in $\mathbb{F}_q^n$. In [19] Séguin discussed the enumeration of 1-generator quasi-cyclic codes in the special case when the prime factorization of $x^m - 1$ is the same in $\mathbb{F}_q[x]$ as in $\mathbb{F}_q[x]$; later in [13], J. Pei and X. Zhang offered a more general approach.
to the same question. As 1-generator quasi-cyclic codes are a particular case of 1-generator $G$-invariant codes, a more general approach to that question is offered here.

**Lemma 4.10** Let $G \leq \text{Aut}_q(\mathbb{F}_q^n)$ such that $A = \mathbb{F}_q[G]$ is semisimple. Let $\{I_j \mid j = 1, \ldots, r\}$ be a basic set of ideals for $\mathbb{F}_q^n$. Let $n_j$ and $k_j$ be the multiplicity of $I_j$ in $\mathbb{F}_q^n$ and $A$, respectively, for all $j = 1, \ldots, r$. Let $l_j = \min\{n_j, k_j\}$ and $h_j = \dim_{\mathbb{F}_q}(I_j)$ for all $j = 1, \ldots, r$, $Y = \bigoplus_{j=1}^r l_j I_j$, $X = \{C \subseteq \mathbb{F}_q^n \mid C$ is a 1-generator $G$-invariant code$\}$, and $D(B) = \prod_{j \in B}\{1, \ldots, l_j\}$ for all $B \in T := 2^{\{1, \ldots, r\}} - \{\emptyset\}$. Then,

1. $C \in X$ if and only if $C \nmid Y$ and $C \neq 0$.

2. $|X| = \sum_{B \in T} \sum_{(t_j) \in D(B)} \left( \prod_{j \in B} \binom{n_j l_j}{l_j} \right) = \left[ \prod_{j=1}^r \left( \sum_{t_j=1}^{l_j} \binom{n_j l_j}{t_j} + 1 \right) \right] - 1$.

3. If $l_j = 1$ for all $j = 1, \ldots, r$, then $|X| = \sum_{B \in T} \left( \prod_{j \in B} \binom{n_j l_j}{l_j} \right) = \left[ \prod_{j=1}^r \left( \binom{n_j l_j}{l_j} + 1 \right) \right] - 1$. Moreover, if $k_j = 1$ for all $j = 1, \ldots, r$, then $|X| = \sum_{B \in T} \left( \prod_{j \in B} \frac{q^{n_j l_j} - 1}{q - 1} \right) = \left[ \prod_{j=1}^r \left( \frac{q^{n_j l_j} - 1}{q - 1} + 1 \right) \right] - 1$.

**Proof.**

1. $C \in X$ if and only if $C$ is a cyclic $A$-module and $C \neq 0$, if and only if $0 \neq C \mid A$ (because $A$ is semisimple), if and only if $C \nmid Y$ and $C \neq 0$.

2. By part 1, $X = \bigcup_{B \in T} \bigcup_{(t_j) \in D(B)} \{C \subseteq \mathbb{F}_q^n \mid C \cong \oplus_{j \in B} t_j I_j\}$, thus

$$|X| = \sum_{B \in T} \sum_{(t_j) \in D(B)} |\{C \subseteq \mathbb{F}_q^n \mid C \cong \oplus_{j \in B} t_j I_j\}|$$

$$= \sum_{B \in T} \sum_{(t_j) \in D(B)} \left( \binom{\mathbb{F}_q^n}{\oplus_{j \in B} t_j I_j} \right)$$

$$= \sum_{B \in T} \sum_{(t_j) \in D(B)} \prod_{j \in B} \binom{n_j I_j}{l_j I_j}$$

where the last equality is by Corollary 4.3. On the other hand, by part 1, $X = \{\oplus_{j=1}^r U_j \mid U_j \subseteq \mathbb{F}_q^n \land U_j \mid l_j I_j\} - \{0\}$. Let $f : X \rightarrow$
\[
\prod_{j=1}^{r} \{ Z \leq F^n \mid l_j I_j \} - \{ \emptyset \}
\]
be given by 
\[
f(L) = (L_j)_{j=1}^{r}
\]
where 
\[
L_j
\]
is the homogeneous component of 
\[L\]
associated to 
\[I_j\]
, if 
\[I_j \mid L\]
and 0 otherwise. It is easy to see that 
\[f\]
is a bijection, so 
\[
|X| = \prod_{j=1}^{r} |\{ Z \leq F^n \mid l_j I_j \} - \{ \emptyset \}|
\]

3. If 
\[l_j = 1\]
for all 
\[j = 1, ..., r\], then 
\[D(B) = \{(1, ..., 1)\}\]
for all 
\[B \in T\].
Hence by part 2,
\[
|X| = \sum_{B \in T} \left( \prod_{j \in B} \left( \frac{n_j I_j}{I_j} \right)_q \right)
\]
\[
= \left[ \prod_{j=1}^{r} \left( \sum_{t_j=1}^{l_j} \left( \frac{(l_j I_j)}{I_j} \right)_q + 1 \right) \right] - 1.
\]
Moreover, if 
\[k_j = 1\]
for all 
\[j = 1, ..., r\], then 
\[l_j = 1\]
for all 
\[j = 1, ..., r\].
So by part 2,
\[
|X| = \sum_{B \in T} \left( \prod_{j \in B} \frac{q^{n_j h_j} - 1}{q^{h_j} - 1} \right)
\]
\[
= \left[ \prod_{j=1}^{r} \left( \frac{q^{n_j h_j} - 1}{q^{h_j} - 1} + 1 \right) \right] - 1,
\]
where the last equality is by Corollary 4.8.

5 Computing sum of 
\[\mathbb{F}_q[G]\]-submodules

Let 
\[A = \mathbb{F}_q[G]\]
be semisimple, and 
\[M\]
be a finite 
\[A\]-module. As the submodules of 
\[M\]
must be direct sum of simple submodules, these can be computed by taking all the possible sums of simple submodules of 
\[M\]. However, if the sums of these simple submodules is not carefully done, the amount of work could increase considerably because every submodule of 
\[M\]
may be expressed in many different ways as a direct sum of simple submodules of 
\[M\]. The following result provides a partial solution to that problem.
Lemma 5.1 Let $A = \mathbb{F}_q[G]$ be semisimple, $I \leq A$ be a minimal ideal. Let $M$ be a finite $A$-module, such that $I \mid M$. Let $H$ be the homogenous component of $M$ associated to $I$, and $n$ be the multiplicity of $I$ in $M$. Let $\{N_i\}_{i \in J}$ with $J = \{1, \ldots, r\}$ be the collection of all $A$-submodules of $M$ isomorphic to $I$, and $\binom{J}{k}$ the collection of subsets of $J$ with $k$ elements.

Let $(F, Z, X)$ be given as output of Algorithm 1. Then the following statements hold:

1. $F$ contains all $A$-submodules of $H$.
2. If $y_0, y_1 \in Z$, then $\sum_{j \in y_0} N_j \neq \sum_{j \in y_1} N_j$.
3. For all $y \in Z$, $\sum_{j \in y} N_j = \oplus_{j \in y} N_j$.

Proof. Let $E := \bigcup_{t=1}^n \binom{J}{t}$. Observe that $E = X \cup Z$.

1. Proceeding by induction on the multiplicity $l$ of $I$ in the $A$-submodules of $H$, it is easy to see that for $l = 2$, the statement holds, i.e., $F$ contains all $A$-submodules of $H$ that are the sum of two simple $A$-modules. Suppose that the same is true for $l \leq k$ with $k$ a positive integer, i.e., $F$ contains all $A$-submodules of $H$ that are the direct sum of $l$ simple $A$-modules with $l \leq k$. Let $y \in E$ with $|y| = k$. If $y \in Z$, it is clear that $\sum_{j \in y} N_j \in F$. Otherwise, if $y \in X$, there exists $z \in Z$ with $|z| \leq k$ such that $\sum_{j \in y} N_j \subseteq \sum_{i \in z} N_i \in F$ (by construction of $X$, Algorithm 1 lines 22, 23, and 24). If $\sum_{j \in y} N_j = \sum_{i \in z} N_i$, the proof ends. On the other hand, if $\sum_{j \in y} N_j \subseteq \sum_{i \in z} N_i$, the multiplicity of $I$ in $\sum_{j \in y} N_j$ must be less than the multiplicity of $I$ in $\sum_{i \in z} N_i$, which is at most $|z| \leq k$, and by inductive hypothesis, $\sum_{j \in y} N_j$ belongs to $F$.

2. Suppose that there exist $y, y' \in Z$ with $y \neq y'$ and $\sum_{i \in y} N_i = \sum_{i \in y'} N_{i}$. Without loss of generality, $y$ was added before than $y'$ to $Z$ in line 9 of Algorithm 1. Then $\sum_{i \in y} N_i = \sum_{i \in y'} N_{i}$ implies $N_{j} \subseteq \sum_{i \in y} N_{i}$ for all $j \in y'$. Let $R_{y} := \{ j \in J - y \mid N_{j} \subseteq \oplus_{i \in y} N_{i} \}$ (the obtained set after executing the loop in line 12 of Algorithm 1), then $y' \subseteq R_{y} \cup y$. In addition, $|y'| \in [|y|, \min\{|R_{y} \cup y|, n\}]$, but in the step in which $y$ was added to $Z$, $y'$ did not belong to $Z$ (because $y$ was added before than $y'$ to $Z$), thus $y'$ was added to $X$ (by construction of $X$, Algorithm 1 lines 22, 23, and 24) which contradicts that $y' \in Z$. 

16
Algorithm 1 Sum of simple $A$-modules

1: function Subadd($\{N_1, ..., N_r\}, n$)
2:     $X = \emptyset$; $J = \{1, ..., r\}$  ▷ Where $\emptyset$ is the empty set.
3:     $Z = \{\{1\}, \{2\}, ..., \{r\}\}$
4:     $F = \{N_1, ..., N_r, 0\}$
5:     for $k = 2$ to $n$ do
6:         for $y \in \binom{J}{k}$ do
7:             $R_y = \emptyset$
8:             if not $y \in X$ then
9:                 add $y$ to $Z$
10:                add $\sum_{j \in y} N_j$ to $F$
11:               $count = 0$
12:              for $t \in J - y$ do
13:                  if $count < \left( \frac{k!}{t!} \right) q - |y|$ then ▷ this conditional could be omitted, but that would make the algorithm to execute slower, so for the proof of Lemma 5.1 it can be ignored.
14:                      if $N_t \subset \sum_{j \in y} N_j$ then
15:                          add $t$ to $R_y$
16:                      $count = count + 1$
17:                     end if
18:                   else
19:                      break
20:                   end if
21:               end for
22:             end if
23:             for $j = k$ to $\min\{|R_y \cup y|, n\}$ do
24:                 for $u \in \binom{R_y \cup y}{j}$ do
25:                     add $u$ to $X$
26:                 end for
27:             end for
28:         end for
29:     end function
30: return $(F, Z, X)$
31: end function
3. Suppose that there exists $y \in Z$ such that $\sum_{i \in y} N_i$ is not a direct sum, then there exists $l \in E$ with $|l| \leq |y|$ and $\oplus_{j \in l} N_j = \sum_{i \in y} N_i$. If $l \in Z$, then $l$ was added first than $y$ to $Z$ in line 9 of Algorithm 1 (because $|l| \leq |y|$). Let $R_l := \{ i \in J - l \mid N_i \subset \oplus_{j \in l} N_j \}$ (the obtained set after executing the loop in line 12 of Algorithm 1), then $y \subseteq R_l \cup l$. In addition, $|y| \in [ |l|, \min\{|R_l \cup l|, n\}]$, but in the step in which $l$ was added to $Z$, $y$ did not belong to $Z$ (because $|l| \leq |y|$), thus $y$ was added to $Z$ (by construction of $Z$, Algorithm 1, lines 22, 23, and 24) which contradicts that $y \in Z$. If $l \in X$, there exists $y' \in Z$ with $|y'| \leq |l|$ such that $\oplus_{j \in l} N_j \subseteq \sum_{j \in y'} N_j$ (by construction of $X$, Algorithm 1 lines 22, 23 and 24), so $\sum_{i \in y} N_i = \oplus_{j \in l} N_j = \oplus_{j \in y'} N_j$, but $y \neq y'$ (because $|y'| \leq |l| \leq |y|$) and $y, y' \in Z$ which contradicts part 2).

6 Computing the $G$-invariant codes of $\mathbb{F}_q^n$

In this section we provide a method to compute all the $\mathbb{F}_q[G]$-submodules ($G$-invariant codes) of $\mathbb{F}_q^n$ for a given $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n)$, when $|G|$ and $q$ are relative primes. In this case Theorem 2.2 guaranties that the $\mathbb{F}_q[G]$-submodules of $\mathbb{F}_q^n$ are direct sums of simple $\mathbb{F}_q[G]$-submodules. As the simple submodules of $\mathbb{F}_q^n$ are contained in its homogeneous components, we will start by giving a way of computing these last.

6.1 Additional results for the solution of the invariance problem

In this subsection different results that help to determine the $G$-invariant codes of $\mathbb{F}_q^n$ are presented, starting with Theorem 6.1 which is a particular case of [3] Theorem 54.12.

**Theorem 6.1 (Minimal divisor)** Let $A = \mathbb{F}_q[G]$ be a finite semisimple group algebra, $e \in A$ be a primitive idempotent, $I = Ae$ be the minimal ideal generated by $e$, and $M$ be a finite $A$-module. Then

$$I \mid M \text{ if and only if } eM \neq 0.$$ 

**Lemma 6.2** Let $A = \mathbb{F}_q[G]$ be semisimple. Let $X$ be a basic set of idempotents for a finite $A$-module $M$. Let $e \in X$ be a primitive idempotent, such that $I = Ae \mid M$, and $H$ be the homogeneous component associated to $I$. If $n$ is the multiplicity of $I$ in $H$, then the following statements hold:

1. $H \cong n(Ae)$ as $A$-modules.
2. \( eM \cong n(eAe) \) as \( \mathbb{F}_q \)-spaces.

3. If \( e \) is central, then \( eM = H \).

**Proof.**

1. It is clear.

2. Note that \( eM \cong \text{Hom}_A(Ae, M) \cong n\text{Hom}_A(Ae, Ae) = n(eAe) \) as \( \mathbb{F}_q \)-vector spaces, where the first and last isomorphisms are by Lemma 2.1 and the second isomorphism is due to additivity of \( \text{Hom}_A(Ae, \cdot) \) respect to direct sums and Lemma 2.1. Therefore \( eM \cong n(eAe) \) as \( \mathbb{F}_q \)-vector spaces.

3. If \( e \) is central, \( eM \) is clearly an \( A \)-submodule of \( M \) such that for all \( f \in X - \{e\} \), \( f(eM) = 0 \), because the idempotents in \( X \) are orthogonal. This imply that the unique (up to isomorphism) simple divisor of \( eM \) is \( I \) (by Theorem 6.1), thus \( eM \leq H \). On the other hand, by Lemma 2.1 \( eM \cong \text{Hom}_A(Ae, M) \cong n(eAe) = nI \cong H \) as \( \mathbb{F}_q \)-vector spaces, where the last isomorphism is by part 1, hence \( eM = H \).

**Corollary 6.3** If \( A \), \( M \), \( H \), \( e \), and \( n \) are as in Lemma 6.2, then \( n = \dim_{\mathbb{F}_q}(H)/\dim_{\mathbb{F}_q}(eAe) = \dim_{\mathbb{F}_q}(eM)/\dim_{\mathbb{F}_q}(eAe) \).

There are situations in which one have a generator element of a minimal ideal that is not an idempotent, and want to determine if the ideal generated by this element divides a given module. We present a solution this problem in Corollary 6.4.

**Corollary 6.4** Let \( A = \mathbb{F}_q[G] \) be semisimple, \( e \in A \) be a primitive idempotent, \( M \) be a finite \( A \)-module, and \( 0 \neq f \in I = Ae \) be such that \( I \mid M \). Then

1. \( eM \neq 0 \) if and only if \( fM \neq 0 \)

2. If \( e \) and \( f \) are central, \( fM \) is the homogeneous component of \( M \) associated to \( I \), and the multiplicity of \( I \) in \( M \) is \( e = \dim_{\mathbb{F}_q}(fM)/\dim_{\mathbb{F}_q}(Af) \).

**Proof.**

1. If \( eM = 0 \), then there exists \( b \in A \) such that \( fM = (be)M = b(eM) = 0 \). Similarly, if \( fM = 0 \), then \( eM = 0 \).
2. Let $e$ and $f$ be central, then $eM = fM$ and $eAe = fAf = Af$, so by Corollary 6.3, $n = \dim_{F_q}(eM)/\dim_{F_q}(eAe) = \dim_{F_q}(fM)/\dim_{F_q}(Af)$ is the multiplicity of $I$ in $M$. Besides, if $H$ is the homogeneous component associated to $I$, $H = eM = fM$ by Lemma 6.2 part 3.

**Lemma 6.5** Let $A = F_q[G]$, $M$ an $A$-module, and $m \in M$. Then $A \cdot m = \langle O(m) \rangle_{F_q}$ where $O(m)$ is the orbit of $m$ under the multiplication by elements of $G$.

Lemma 6.2 (part 3), offers an easy way to compute the homogeneous component associated to a minimal ideal generated by a central primitive idempotent, so it is natural to ask over what happens when this idempotent is not central. Theorem 6.6 englobes both situations. However, in practice, it is recommended to use Corollary 6.2 instead of this theorem, when possible, because it is easier to be applied.

**Theorem 6.6** Let $A = F_q[G]$ be semisimple, $M$ be a finite $A$-module. Let $e \in A$ be a primitive idempotent such that $I = Ae | M$, $H$ be the homogeneous component of $M$ associated to $I$, and $n$ be the multiplicity of $I$ in $M$. If $\beta = \{\beta_1, \beta_2, \ldots, \beta_r\}$ is a generating set of $M$ as $F_q$-vector space, then $\sum_{j=1}^r A(e\beta_j) = H$.

**Proof.** Let $O(x)$ denote the orbit of $x$ under the left action of $G$ in $M$ for all $x \in M$. From Lemma 6.2, $eM \cong n(eAe) \leq nI$ (as $F_q$-vector spaces). Let $y_i \in n(eAe)$ such that its $i$-th entry is $e$ and $0$ otherwise, for all $i = 1, \ldots, n$. Then $Y := \{y_i \mid i = 1, \ldots, n\} \subset n(eAe)$ is such that $nI = \bigoplus_{i=1}^n A y_i$. For any $\phi \in Isom_H(nI)$, its restriction $\eta$ to $eM \subset H$ belongs to $Isom_q(eM, n(eAe))$ and is such that $\eta^{-1}(Y) = \{z_i := \eta^{-1}(y_i) \mid i = 1, \ldots, n\}$ is a subset of $eM$ such that $H = \bigoplus_{i=1}^n A z_i$ (because $Y$ generates $nAe$). On the other hand, $X := \{e\beta_1, e\beta_2, \ldots, e\beta_r\}$ generates $eM$ as vector space, hence $z_1 = \sum_{j=1}^r c_{ij} e\beta_j$ for all $i = 1, \ldots, n$, then $g z_1 = \sum_{j=1}^r c_{ij} g(e\beta_j)$ for all $i = 1, \ldots, n$ and $g \in G$, so $O(z_1) \subset \bigcup_{j=1}^r O(e\beta_j)_{F_q} = \sum_{j=1}^r O(e\beta_j)_{F_q} = \sum_{j=1}^r A(e\beta_j) \subseteq H$ for all $i = 1, \ldots, n$, where the last of the equalities follows from Lemma 6.5. Then $O(z_1)_{F_q} = A z_1 \subset \sum_{j=1}^r A(e\beta_j)$ (by Lemma 6.5), and $\bigoplus_{j=1}^r A z_i = H \subseteq \sum_{j=1}^r (A e\beta_j)$.

**Lemma 6.7** Let $G = \{g_i \mid i = 1, \ldots, k\} \leq Aut_{F_q}(F^n_q)$ such that $A = F_q[G]$ is semisimple. Let $O(x)$ denote the orbit of $x$ under the action by evaluation of $G$, for all $x \in F^n_q$. Let $I = Ae \leq A$ with $e$ a primitive idempotent. Let $M = Am$ and $N = An$ be cyclic $A$-submodules of $F^n_q$. Let $B$ be the matrix
whose i-th row is given by \( g_i(m) \), and \( C \) be the matrix obtained by extending \( B \) adding it \( n \) as a row. Then the following statements hold:

1. \( M \cong I \) if and only if \( \dim_{q'}(I) = \text{rank}(B) \) and \( e \cdot O(m) \neq \{0\} \). Moreover, if \( e \) is central, the condition \( e \cdot O(m) \neq \{0\} \) could be replaced by \( e \cdot m \neq 0 \).

2. \( N \leq M \) if and only if \( \text{rank}(C) = \text{rank}(B) \). Moreover, If \( N, M \) are simple \( A \)-modules, \( N = M \) if and only if \( \text{rank}(C) = \text{rank}(B) \).

**Proof.**

1. If \( M \cong I \), then \( I \mid M \) and by Theorem 6.1 \( e \cdot M \neq 0 \), so that \( e \cdot O(m) \neq \{0\} \) (because \( M = \langle O(m) \rangle_{q'} \), by Lemma 5.5), thus \( e \cdot O(m) \neq \{0\} \) and \( \dim_{q'}(I) = \dim_{q'}(M) = \text{rank}(B) \) (by Lemma 5.5). Conversely, if \( \{0\} \neq e \cdot O(m) \subseteq e \cdot M \), Theorem 6.1 implies that \( I \mid M \), but \( \dim_{q'}(I) = \text{rank}(B) = \dim_{q'}(M) \) (by Lemma 5.5), therefore \( I \cong M \) as \( A \)-modules. If \( e \) is central, \( e(O(m)) = 0 \) if and only if \( e(m) = 0 \).

2. If \( N \leq M \), then \( n \in M = \langle O(m) \rangle_{q'} \), thus \( \text{rank}(C) = \text{rank}(B) \). Conversely, if \( \text{rank}(C) = \text{rank}(B) \), then \( n \in M = \langle O(m) \rangle_{q'} \), so \( g(n) \in M \) for all \( g \in G \), thus \( O(n) \subseteq M \), and by Lemma 6.5 \( N = A n = \langle O(n) \rangle_{q'} \leq M \). Moreover, if \( N \) and \( M \) are simple \( A \)-modules, then \( N \leq M \) if and only if \( N = M \), if and only if \( \text{rank}(C) = \text{rank}(B) \).

### 6.2 A method to compute \( G \)-invariant codes

In [19] Séguin describes an algorithm to obtain a unique generator for each \( q \)-ary 1-generator quasi-cyclic code, later in [15] J. Pei and X. Zhang offer a more general approach to the same question. In this section we present a method to find a unique generating set for every \( G \)-invariant code of \( \mathbb{F}_q^n \) respect to some subgroup \( G \) of \( \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n) \). As quasi-cyclic codes are a particular case of \( G \)-invariant codes, ours solution is more general than the presented by Séguin, J. Pei and X. Zhang.

Let \( G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_q^n) \) such that \( A = \mathbb{F}_q[G] \) is semisimple, \( X \) be a basic set of idempotents for \( \mathbb{F}_q^n \), and \( H_e \) the homogeneous component associated to \( Ae \) for all \( e \in X \). By doing what is indicated in the Steps 1 – 3 (presented below) for all \( e \in X \) we can obtain all simple \( A \)-submodules of \( \mathbb{F}_q^n \). Then, by doing what is indicated in Step 4 all \( A \)-submodules (\( G \)-invariant codes) of \( \mathbb{F}_q^n \) are obtained.
Step 1: (Computation of homogeneous components). Determine the homogeneous component $H_e$ of $\mathbb{F}_q^n$, which can be done by using Lemma 6.2 (part 3), or Corollary 6.3 (part 2) if $e$ is central. Otherwise, by using Theorem 6.6.

Step 2: (Computation of quotient sets). Once $H_e$ is determined, considering that all cyclic $A$-modules, and therefore all simple $A$-modules, are generated as $\mathbb{F}_q$-spaces by the orbit of one generating element (by Lemma 6.5), the quotient set $H_e/G = \{O(m) \mid m \in H_e\}$ of the orbits under the action by evaluation of $G$ on $H_e$ is determined.

Step 3: (Determine a unique generating orbit for every simple $A$-module). Determine those orbits on $H_e/G$ that generate simple $A$-modules and obtain a unique generating orbit for every simple $A$-submodule contained in $H_e$. All the orbits in $H_e/G$ generate $A$-modules which have $I$ (up to isomorphisms) as a unique simple divisor (by [4] Proposition 3.20, part 2), so by Lemma 6.7 (part 1) and Theorem 6.1, we just need to check whether an orbit generates a space with the right dimension $i = \dim_{\mathbb{F}_q}(I)$ and obtain a unique generating orbit for every simple $A$-submodule. A way to do this is as follows: First, if $A$ is non-commutative, compute all the orbits $O$ of $L := \{o \in H_e/G \mid |o| = \min\{|u| \mid u \in I/G - \{\{0\}\}\}\}$ such that $\dim_{\mathbb{F}_q}(<O>) = i$. When $A$ is commutative, it is not necessary to compute $L$, because in this case every orbit different from the orbit of the zero vector will generate a simple $A$-module (by Lemma 2.6). Second, identify when two of orbits in $L$ (when $A$ is non-commutative) or $H_e/G$ (when $A$ is commutative) generate the same simple $A$-module by using Lemma 6.7 (part 2) to obtain only one generating orbit for every simple $A$-submodule contained in $H_e$.

Step 4: (Computing direct sums). Once we have all the simple $A$-modules contained in $\mathbb{F}_q^n$ and the multiplicity of $Ae$ in $H_e$ (this last can be obtained by using Corollary 6.3), every $A$-submodule of each homogeneous component can be computed, in an efficient way, by using Algorithm 1. After that, the $A$-submodules of $\mathbb{F}_q^n$ can be determined by taking all possible direct sums of these submodules, this time without any worry of wasting resources, i.e., with no risks of getting repetitions. Otherwise, the function presented in the proof of Lemma 4.9 (part 1) would not be a bijection.

Let us make some remarks on how to get a generating set for every $G$-invariant code. If we provide a (indexed) list of all the simple modules contained in an homogeneous component of $\mathbb{F}_q^n$, Algorithm 1 gives a colle-
tion $Z$ of subsets of the set of indices, such that every $A$-submodule of the homogeneous component can be seen as a sum, indexed by a unique element of $Z$, of some of these simple modules. Thus we could obtain a unique generating set for every $A$-submodule of an homogeneous component of $F^n_q$ that has been calculated by the Algorithm [1]. A generating set for one of the modules calculated by Algorithm [1] can be obtained just by taking a non-zero element in each of the simple $A$-modules that appears in its decomposition. In general, for the $A$-submodules of $F^n_q$ ($G$-invariant codes), as they are direct sum of $A$-submodules of the homogeneous components of $F^n_q$, we just need to take the unions of the generating sets of these summands. We have just determined how to compute generating sets for $G$-invariant codes. Nonetheless, when working with a code, it is important to know a basis of it. The obvious way to obtain a basis for a $G$-invariant code is by computing it from a generating set. The following results will show another way to do so.

**Theorem 6.8** Let $A = F_q[G]$ be semisimple, $e$ be a primitive idempotent, $Ax$ a cyclic $A$-module isomorphic to $Ae$. Let $B := \{b_1, b_2, \ldots, b_k\}$ a $F_q$-basis for $Ae$.

1. There exists $g \in G$ such that $e(gx) \neq 0$.
2. If $ex \neq 0$, then $B' := \{b_1x, b_2x, \ldots, b_kx\}$ is $F_q$-basis for $Ax$.
3. There exist a generator $z$ of $Ax$ such that $B' := \{b_1z, b_2z, \ldots, b_kz\}$ is $F_q$-basis for $Ax$.

**Proof.**

1. As $Ax \cong Ae$, $eAx \neq 0$ (by Theorem [6.1]), so there exists $g \in G$ such that $e(gx) \neq 0$ (by Lemma [6.5]).
2. If $f : Ae \rightarrow Ax$ is given by $f(ey) = (ey)x$, then $f$ is a morphism of $A$-modules, which is non-zero (because $ex \neq 0$), and so it is an $A$-isomorphism (by Lemma [2.1]). Therefore, $f(B) = B'$ is a $F_q$-basis for $Ax$.
3. if follows from parts 1 and 2.

If $A = F_q[G]$ is semisimple, and $M$ is a finite (not necessarily simple) $A$-module, then Theorem [6.8] can be applied to compute a $F_q$-basis $M$. If the decomposition of $M$ into simple submodules is $M = \bigoplus_{i=1}^t Am_i$, we just
need to know a basic set of idempotents for $M$, and which of ideal generated by these idempotent is isomorphic to $A m_i$ for all $i = 1, \ldots, t$. By doing so, we can determine a $\mathbb{F}_q$-basis for every summand $A m_i$, and so we can compute a basis for $M$ just by taking the union of these $\mathbb{F}_q$-basis.

7 What to do when a basic set of idempotents is not known

Observe that the previous ideas work if a basic set of idempotents for $\mathbb{F}_n^a$ is known. In the following lines an alternative solution is discussed. Let $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_n^a)$ such that $\mathbb{F}_q[G]$ be semisimple. To find a basic set of primitive idempotents for $\mathbb{F}_q[G]$ the results presented in [8], [2], [1], or [6] might be useful. After having determined a basic set of idempotents for $\mathbb{F}_q[G]$, by using Lemma 6.1, a basic set of idempotents for $\mathbb{F}_n^a$ can be computed. Otherwise, considering that, in theory, the use of primitive idempotents of $\mathbb{F}_q[G]$ to solve the invariance problem is not strictly necessary, we could work using the following reasoning instead.

Lemma 7.1 Let $G \leq \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_n^a)$, $S = \{s_1, \ldots, s_r\}$ be a generating set for $G$, $\langle s_i \rangle$ be the cyclic group generated by $s_i$ for all $i = 1, \ldots, r$, and $C \subseteq \mathbb{F}_q^n$ be a code. The following conditions are equivalent:

1. $C$ is a $G$-invariant code
2. $C \in \bigcap_{i=1}^{r} \{ D \subseteq \mathbb{F}_q^n \mid D \text{ is } \mathbb{F}_q[\langle s_i \rangle] \text{-submodule of } \mathbb{F}_q^n \}$

Proof. $C$ is $G$-invariant if and only if $g(C) = C$ for all $g \in G$, if and only if $s_i(C) = C$ for all $i = 1, \ldots, r$, if and only if $C$ is $\mathbb{F}_q[\langle s_i \rangle]$-submodule of $\mathbb{F}_q^n$ for all $i = 1, \ldots, r$, if and only if $C \in \bigcap_{i=1}^{r} \{ D \subseteq \mathbb{F}_q^n \mid D \text{ is } \mathbb{F}_q[\langle s_i \rangle] \text{-submodule of } \mathbb{F}_q^n \}$.

So one can solve the problem of determining the $G$-invariant codes by finding the $\langle s_i \rangle$-invariant codes, where $S = \{s_1, \ldots, s_r\}$ is a generating set of $G$. This theoretic result is unpractical thought, but if we combine what we know up to now with Lemma 7.1, we could be able to lower the computations. For example, If we want to compute the $G$-invariant codes of $\mathbb{F}_n^a$, we could find first the $N$-invariant codes for certain subgroup $N$ of $G$, such that the idempotents of $\mathbb{F}_q[N]$ are easier to compute, and then see which of these codes are invariant under the elements of $T = \{t_i \mid i = 1, \ldots, u\}$, where $T$ is a set of representatives of $G/N$. With that reasoning, the invariance problem could be solved with a more reasonable effort when we do not know a basic set of idempotents for $\mathbb{F}_n^a$. 

24
8 Examples of computations of $G$-invariant codes

In this section some examples that illustrate the process of solving the invariance problem will be presented. For that aim, we will use all the steps 1–4 presented in section 6.2.

Example 8.1 Consider $\gamma \in \text{Aut}_{F_2}(F_9^2)$ given by $\gamma = \sigma^3$, where $\sigma$ is the cyclic shift, then $\langle \gamma \rangle \cong C_3 = \{1, x, x^2\}$ and $F_9^2$ is an $F_2[C_3]$-module. Let $A = F_2[C_3]$. As $(|C_3|, 2) = 1$, $A$ is semisimple (by Lemma 2.2). Using Corollary 6.4 (part 1) is easy to see that the minimal ideals $I_0 := A(x - 1)$ and $I_1 := A(x^2 + x + 1)$ of $A$ divide $F_9^2$, so its simple $A$-submodules ($C_3$-invariant codes) are isomorphic to $I_0$ and $I_1$. As these ideals are not isomorphic, $\{I_0, I_1\}$ is a basic set of ideals for $F_9^2$.

Computing the $A$-submodules of the homogeneous components $H_0$ and $H_1$ of $F_9^2$ associated to $I_0$ and $I_1$, respectively.

Step 1: (Computation of homogeneous components). As both $I_0$ and $I_1$ divide $F_9^2$, and $A$ is commutative ring, by Corollary 6.4 (part 2), $H_0 := (\gamma + id)(F_9^2)$ is the homogeneous component of $F_9^2$ associated to $I_0$, and $H_1 := (\gamma^2 + \gamma + id)(F_9^2)$ is the homogeneous component associated to $I_1$. Let $\beta$ be the canonical basis of $F_9^2$, then

$$(\gamma + id)(\beta) = \{100100000, 010010000, 001001000, 000100100, 000010010, 000001001, 100000100, 010000010, 001000010, 001000010\}$$

and $$(\gamma + \gamma^2 + id)(\beta) = \{100100100, 010010010, 001001001\}$$ generate $H_0$ and $H_1$ as $F_2$-vector space, respectively.

Steps 2: (Computation of quotient sets). Let $H_0/\langle \gamma \rangle$ and $H_1/\langle \gamma \rangle$ be the quotient sets determined by the action by evaluation of $\langle \gamma \rangle$ on $H_0$ and $H_1$, respectively, and $O(v)$ the orbit of $v$ for all $v \in F_9^2$. Then

$H_0/\langle \gamma \rangle - \{O(000000000)\}$ is given by

$$\{O(100100000), O(010010000), O(110110000), O(001001000), O(101101000), O(010110100), O(110010100), O(011001010), O(101001100), O(001101100), O(111011100), O(011111100), O(101111100), O(011011110), O(101011110), O(001111110)\}.$$
and $H_1/\langle \gamma \rangle - \{O(000000000)\}$ is given by

$$\{O(111111111), \ O(100100000), \ O(010010010), \ O(110101110), \ O(001001001), \ O(101101101), \ O(011011011)\}.$$  

Steps 3: (Determining a unique generating orbit for every simple $A$-module). As $A$ is commutative, every orbit different from the orbit of the zero vector in $H_0/\langle \gamma \rangle$ and $H_1/\langle \gamma \rangle$, generates a simple $A$-module (by Lemma 2.6). Moreover, as every orbit in $H_0/\langle \gamma \rangle$ has size 3 and $|I_0| = 4$, every simple $A$-module in $H_0$ has a unique generating orbit. Similarly, as every orbit in $H_1/\langle \gamma \rangle$ has size 1 and $|I_1| = 2$, every simple $A$-module in $H_1$ has a unique generating orbit.

If we determine a unique generating vector for every simple $\mathbb{F}_2[C_3]$-submodule of $\mathbb{F}_2^9$ that is isomorphic to $I_0$, we get

$$n_0=100100000, \ n_1=010010000, \ n_2=110110000, $$
$$n_3=001001000, \ n_4=101101000, \ n_5=011011000, $$
$$n_6=111111000, \ n_7=110010100, \ n_8=010110100, $$
$$n_9=101001100, \ n_{10}=001101100, \ n_{11}=111011100, $$
$$n_{12}=011111100, \ n_{13}=011001010, \ n_{14}=111101010, $$
$$n_{15}=001011010, \ n_{16}=101111010, \ n_{17}=111001110, $$
$$n_{18}=011101110, \ n_{19}=101011110, \ n_{20}=001111110.$$  

If we determine a unique generating vector for every simple $\mathbb{F}_2[C_3]$-submodule of $\mathbb{F}_2^9$ that is isomorphic to $I_1$, we get

$$m_0=100100100, \ m_1=010010010, \ m_2=110110110, $$
$$m_3=001001001, \ m_4=101101101, \ m_5=011011011, $$
$$m_6=111111111.$$  

Let $N_i := A \gamma_i$ for all $i = 0, \ldots, 20$, and $M_j := A \beta_j$ for all $j = 0, \ldots, 6$.

Note that $h_0 := \dim_{\mathbb{F}_2}(H_0) = \dim_{\mathbb{F}_2}((\langle \gamma \rangle + \langle \id \rangle(\beta))) = 6$ and $h_1 := \dim_{\mathbb{F}_2}(H_1) = \dim_{\mathbb{F}_2}((\langle \gamma \rangle + \langle \gamma^2 \rangle + \langle \id \rangle(\beta))) = 3$, so the multiplicities of $I_0$ and $I_1$ in $H_0$ and $H_1$, respectively, are in both cases equal to 3 (by Corollary 6.3), thus $H_0 \cong I_0 \oplus I_0 \oplus I_0$ and $H_1 \cong I_1 \oplus I_1 \oplus I_1$, hence $(I_0 \oplus I_0 \oplus I_0) = \frac{2^{3x3} - 1}{2 - 1} = 21$, $(I_1 \oplus I_1 \oplus I_1) = \frac{2^{3x3} - 1}{2 - 1} = 7$ (by Corollary 4.8), which coincides with the computations we have just made.

Steps 4: (Computing direct sums). By using Algorithm 4 all the non-simple $A$-submodules of $H_0$ and $H_1$ can be computed. Let $(F_0, Z_0, X_0)$, and $(F_1, Z_1, X_1)$ be the outputs given by Algorithm 4 for the inputs $\{N_i \mid i =$
0, ..., 20}, 3) and \( \{M_i \mid i = 0, ..., 6, 3\} \), respectively.

Then the \( A \)-submodules of \( H_0 \) isomorphic to \( I_0 \oplus I_0 \) are of the form \( \oplus_{j \in \mathbb{Z}_3} N_j \) with \( l \in (\mathbb{Z}_3^2, 2) \), and

\[
(\mathbb{Z}_3^2) = \{(0, 1), (0, 3), (0, 5), (0, 13), (0, 15), (1, 3), (1, 9), (1, 10), (2, 3), (2, 4), (9, 2), (2, 10), (3, 7), (8, 3), (4, 7), (8, 4), (5, 7), (8, 5), (6, 7), (1, 4), (8, 6)\}
\]

The \( A \)-submodules of \( H_1 \) isomorphic to \( I_1 \oplus I_1 \) are of the form \( \oplus_{j \in \mathbb{Z}_3} M_j \) with \( l \in (\mathbb{Z}_3^2, 2) \), and

\[
(\mathbb{Z}_3^2) = \{(0, 1), (0, 3), (0, 5), (1, 3), (1, 4), (2, 3), (2, 4)\}.
\]

There is only one \( A \)-submodule of \( H_0 \) (\( H_1 \)) isomorphic to \( I_0 \oplus I_0 \oplus I_0 \) (\( I_1 \oplus I_1 \oplus I_1 \)) which is the homogeneous component \( H_0 \) (\( H_1 \)) itself, and this can be considered as \( \oplus_{j \in \mathbb{Z}_3} (\oplus_{j \in \mathbb{Z}_3} M_j) \) with \( l \in (\mathbb{Z}_3^2, 2) = \{(0, 1, 3)\} \).

By Lemma 4.9 (part 1) the collection \( W := \{U \oplus V \mid U \in F_0, V \in F_1\} \), is precisely the collection of all the \( C_3 \)-invariant codes of \( F_0^9 \). If we take two different elements \((W_0, W_1), (T_0, T_1) \in F_0 \times F_1\), then \( W_0 \oplus W_1 \neq T_0 \oplus T_1 \).

Otherwise, the function given in the proof of lemma 4.9 (part 1) would not be a bijection. Thus, we can be sure that when calculating \( W \) no element will be computed more than once.

Note that \( (\mathbb{Z}_3^2, 2) = 2^{2 \times 2} - 1 = 5 \) and \( (\mathbb{Z}_3^2, 2) = 2^{2 \times 2} - 1 = 3 \), hence, by Lemma

\[
(\mathbb{Z}_3^2, 2) \quad (\mathbb{Z}_3^2, 2) \quad (\mathbb{Z}_3^2, 2) = \frac{(3I_0)}{2} \quad \frac{(3I_0)}{2} \quad \frac{(2I_0)}{2} = \frac{21 \times 20}{6 \times 2} = 21 = |(\mathbb{Z}_3^2)|, \quad (\mathbb{Z}_3^2, 2) \quad (\mathbb{Z}_3^2, 2) = \frac{(3I_1)}{2} \quad \frac{(3I_1)}{2} \quad \frac{(2I_1)}{2} = \frac{7 \times 6}{5 \times 2} = 7 = |(\mathbb{Z}_3^2)|, \quad \text{which is consistent with our computations}.
\]

Now we count the total of \( C_3 \)-invariant codes and 1-generator \( C_3 \)-invariant codes. Let \( S(M) := \{C \subseteq M \mid C \text{ is a } C_3 - \text{invariant code}\} \) for all \( C_3 \)-invariant code \( M \subseteq F_0^9 \). Then, by Lemma 4.9 (part 2),

\[
\prod_{j=0}^{1} |S(H_j)| = \prod_{j=0}^{1} \left[ \sum_{t_j \in \{1, ..., n_j\}} \left( \frac{n_j I_j}{t_j I_j} \right) + 1 \right] = \left[ \sum_{t_0=1}^{3} \left( \frac{3I_0}{t_0 I_0} \right) + 1 \right] \times \left[ \sum_{t_1=1}^{3} \left( \frac{3I_1}{t_1 I_1} \right) + 1 \right] = ([21 + 21 + 1] + 1) \times ([7 + 7 + 1] + 1) = 704
\]

27
and as \( W = S(\mathbb{F}_2^9) \), \( |W| = |S(\mathbb{F}_2^9)| = \prod_{j=0}^{1} |S(H_j)| = 704. \) Let \( X = \{ C \subseteq \mathbb{F}_2^9 \mid C \) is a 1-generator \( C_3 \) - invariant code\}, then by Lemma 4.10 (part 3)

\[
|X| = \left[ \prod_{j=0}^{1} \left( \frac{q^{n_i h_j} - 1}{q^{h_j} - 1} + 1 \right) \right] - 1
= \left[ \left( \frac{2^{3 \times 2} - 1}{2^3 - 1} + 1 \right) \times \left( \frac{2^3 \times 1 - 1}{2^3 - 1} + 1 \right) \right] - 1
= \left[ (21 + 1) \times (7 + 1) \right] - 1 = 175.
\]

**Example 8.2** Let \( A = F_5[S_3] \). As \(|S_3|, 5) = 1, A is semisimple. Let \( \beta \) be the canonical basis of \( F_5[S_3] \), and \( x, y \in \text{Aut}_{F_5}(F_5) \) be such that

\[
[x]_\beta = \begin{bmatrix}
0 & 3 & 4 & 4 & 0 & 3 & 3 & 2 & 1 \\
4 & 1 & 0 & 2 & 0 & 3 & 1 & 3 & 2 \\
0 & 1 & 2 & 4 & 4 & 2 & 1 & 2 & 2 \\
3 & 0 & 2 & 3 & 3 & 0 & 2 & 2 & 3 \\
2 & 0 & 3 & 3 & 4 & 3 & 3 & 2 & 0 \\
2 & 0 & 1 & 4 & 4 & 0 & 1 & 4 & 0 \\
0 & 4 & 4 & 4 & 3 & 2 & 1 & 1 & 0 \\
2 & 1 & 1 & 4 & 1 & 3 & 3 & 2 & 3 \\
1 & 1 & 2 & 4 & 1 & 1 & 0 & 2 & 2
\end{bmatrix}
\]

and

\[
[y]_\beta = \begin{bmatrix}
0 & 2 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\
4 & 2 & 0 & 0 & 4 & 3 & 0 & 0 & 0 \\
2 & 3 & 4 & 1 & 0 & 4 & 1 & 1 & 1 \\
1 & 1 & 0 & 2 & 2 & 3 & 0 & 3 & 4 \\
4 & 3 & 0 & 1 & 1 & 4 & 0 & 3 & 4 \\
2 & 4 & 0 & 2 & 3 & 0 & 0 & 1 & 3 \\
1 & 3 & 0 & 3 & 4 & 4 & 1 & 3 & 0 \\
0 & 1 & 0 & 3 & 2 & 0 & 0 & 4 & 0 \\
0 & 2 & 0 & 0 & 1 & 4 & 0 & 2 & 0
\end{bmatrix}
\]

Let \( G = \langle x, y \rangle \). Then \( f : G \rightarrow S_3 = \langle a, b \mid a^3 = b^2 = 1, bab = a^2 \rangle = \{1, a, a^2, b, ba, ba^2\} \) given by \( x \mapsto a \) and \( y \mapsto b \) is an isomorphism. By Example 8.2, \( e_0 = 1 + a + a^2 + b + ba + ba^2, e_1 = 1 + a + a^2 + 4b + 4ba + 4ba^2, e_2 = 2 + 3a^2 + 2b + 3ba^2 \) are a basic set of idempotents for \( F_5[S_3] \). Using Theorem 6.7 is easy to see that the minimal ideal \( I_j := Ae_j \) divides \( F_5^9 \) for all
\( j = 0, 1, 2, \) thus \( \{ I_0, I_1, I_2 \} \) is a basic set of ideals for \( \mathbb{F}_5^9 \). Furthermore, using Corollary \( 6.3 \) is easy to see that the multiplicity of \( I_j \) is \( j + 1 \) for all \( j = 0, 1, 2 \).

**Step 1:** (Computation of homogeneous components). As \( e_0, e_1 \) are central elements of \( A \) and both \( I_0 \) and \( I_1 \) divide \( \mathbb{F}_5^9 \), then by Lemma \( 6.2 \)

\[ H_0 := e_0 \mathbb{F}_5^9 = (id + x + x^2 + y + yx + yx^2)(\mathbb{F}_5^9) = (140442324) \mathbb{F}_5 \]

is the homogeneous component associated to \( I_0 \), and \( H_1 := e_1 \mathbb{F}_5^9 = (id + x + x^2 + 4y + 4yx + 4yx^2)(\mathbb{F}_5^9) = \langle \{10020401, 001112001\} \rangle \mathbb{F}_5 \) is the homogeneous component associated to \( I_1 \). On the other hand, by Theorem \( 6.6 \), the set \( \{ e_2 v \mid v \in \beta \} = \{140111222, 142330020, 322033442, 414332434, 322021431, 323102302, 232403203, 231322332, 411020204 \} \) generates the homogenous component \( H_2 \) associated to \( I_2 \), as \( A \)-module.

**Steps 2:** (Computation of quotient sets). Let \( H_i/G \) be the quotient set determined by the action by evaluation of \( G \) on \( H_i \) for all \( i = 0, 1, 2 \), and \( O(v) \) be the orbit of \( v \) for all \( v \in \mathbb{F}_5^9 \). Then \( H_0/G - \{ O(000000000) \} \) is given by

\[ \{ O(410113231), O(140442324), O(230334143), O(320221412) \} \]

and \( H_1/G - \{ O(000000000) \} \) is given by

\[ \{ O(442204101), O(110020401), O(220040302), O(001112001), O(111132402), O(221102303), O(331122204), O(441142100), O(002224002), O(112244403), O(222214304), O(332234200) \} \]

As \( |H_2/G| = 2667 \), we prefer not to write it explicitly. Contrary to the previous example, not all the orbits in \( H_2/G \) generate simple \( A \)-submodules.

**Steps 3:** (Determining unique generating orbit for every simple \( A \)-module). As the multiplicity of \( I_0 \) and \( I_1 \) in \( A \) is 1, every orbit in \( H_0/G \) and \( H_1/G \) generates a simple \( A \)-module (by Lemma \( 2.6 \)), but in none of the cases there exists a simple \( A \)-module with a unique generating orbit. On the other hand, in \( H_2/G \) there are orbits that do not generate simple \( A \)-modules, these are precisely those that generate \( A \)-modules isomorphic to \( 2I_2 \). For example, \( O(100000032) = \{100000032, 130021232, 320034341, 042311021, 012314343, 001430241 \} \). We use the instructions given in Step 3 (Section \( 6.4 \)) to get a unique generating orbit of \( H_i/G \) for each simple \( A \)-submodule of \( H_i \) for all
i = 0, 1, 2. When determining a unique generating vector for the simple $A$-submodules of $\mathbb{F}_5^0$ isomorphic to $I_0$, we get the vector $l_0 = 140442324$. When doing the same for the simple $A$-submodules of $\mathbb{F}_5^0$ isomorphic to $I_1$, we get

$$m_0 = 110020401, \quad m_1 = 001112001, \quad m_2 = 111132402, \quad m_3 = 221102303, \quad m_4 = 331122204, \quad m_5 = 441142100,$$

and when doing it for the simple $A$-submodules of $\mathbb{F}_5^0$ isomorphic to $I_2$, we get

$$n_0 = 221100102, \quad n_1 = 103100210, \quad n_2 = 001331412, \quad n_3 = 233311232, \quad n_4 = 234001133, \quad n_5 = 131401423, \quad n_6 = 221014101, \quad n_7 = 342101443, \quad n_8 = 413201013, \quad n_9 = 213021224, \quad n_{10} = 412101120, \quad n_{11} = 144011334, \quad n_{12} = 411001232, \quad n_{13} = 430201003, \quad n_{14} = 234301142, \quad n_{15} = 042010323, \quad n_{16} = 234141023, \quad n_{17} = 234110040, \quad n_{18} = 414301401, \quad n_{19} = 140111222, \quad n_{20} = 044411334, \quad n_{21} = 001100443, \quad n_{22} = 320321100, \quad n_{23} = 310110242, \quad n_{24} = 400401244, \quad n_{25} = 013201040, \quad n_{26} = 324111111, \quad n_{27} = 121001341, \quad n_{28} = 033301213, \quad n_{29} = 020311031, \quad n_{30} = 322021431.$$

Let $L_0 := A_{l_0}$, $M_i := A_{l_i}$ for all $i = 0, ..., 5$, and $N_j := A_{l_j}$ for all $j = 0, ..., 30$.

As $I_j$ has multiplicity $j + 1$ in $\mathbb{F}_5^n$ for $j = 0, 1, 2$, respectively. For that reason, $H_0 \cong I_0$ and $H_1 \cong I_1 \oplus I_1$ and $H_2 \cong I_2 \oplus I_2 \oplus I_2$. As the multiplicity of $I_1$ in $A$ is 1 by Corollary 4.8, $\left(\frac{I_1 \oplus I_1}{I_1}\right)_5 = \frac{5! \times 2}{5! - 1} = 6$. Observe that, up to now, we do not have a formula to calculate $\left(\frac{I_2 \oplus I_2 \oplus I_2}{I_2}\right)_5 = 31$.

Steps 4: (Computing direct sums). By using Algorithm 1, we can compute all the non-simple $A$-submodules of $H_2$ ($H_1$ only has one non-simple $A$-submodule which is $I_1$ itself, and $H_0$ does not have non-simple $A$-submodules, because $H_0$ is simple). Let $\langle F_2, Z_2, X_2 \rangle$ be the output given by Algorithm 1 for the input $(\{N_i \mid i = 0, ..., 30\}, 3)$.

The $A$-submodules of $H_1$ isomorphic to $I_2 \oplus I_2$ are of the form $\oplus_{j \in I} N_j$ with $l \in \left(\frac{L_2}{L_2}\right)$, and

$$\left(\frac{L_2}{L_2}\right) = \{0, 1\}, \{0, 6\}, \{0, 8\}, \{0, 10\}, \{0, 11\}, \{0, 14\}, \{1, 6\}, \{1, 7\}, \{8, 1\}, \{1, 11\}, \{1, 15\}, \{2, 6\}, \{2, 7\}, \{9, 2\}, \{2, 13\}, \{2, 15\}, \{3, 6\}, \{3, 7\}, \{9, 3\}, \{10, 3\}, \{11, 3\}, \{4, 6\}, \{4, 7\}, \{8, 4\}, \{9, 4\}, \{12, 4\}, \{5, 6\}, \{5, 7\}, \{8, 5\}, \{9, 5\}, \{12, 5\}$$. 
There is only one $A$-submodule of $H_2$ isomorphic to $I_2 \oplus I_2 \oplus I_2$, which is $H_2$ itself.

By Lemma 4.9 the collection $W := \{L_0 \oplus U \oplus V \mid U \in F_1 \land V \in F_2\}$, is the collection of all the $S_3$-invariant codes of $\mathbb{F}_5^9$.

By doing some computations in Sage we got that that $N_0, N_1, N_2, N_3, N_4, N_5$ are all the simple $A$-submodules contained in $N_0 \oplus N_1 \cong 2I_2$, so $(I_2 \oplus I_2)^5 = 6$, hence $(I_2 \oplus I_2 \oplus I_2)^5 = \frac{(3I_2)^5 \cdot (3I_2)^5 - 1}{(I_2 \oplus I_2)^5} = \frac{31 \times 30}{6 \times 5} = 31 = |(Z_2)|$, which is consistent with our computations.

To finish we offer an example over how to compute a basis for a given $G$-invariant code using Theorem 6.8 (part 2). Observe that $\{e_2, ae_2\}, \{e_0\}, \{e_1\}$ are basis for $I_2, I_0, I_1$, respectively. Consider the $A$-submodule $C := (N_0 \oplus N_1) \oplus M_0 \oplus L_0 \cong 2I_2 \oplus I_1 \oplus I_0$. As $e_2(n_0)$, $e_2(xn_1)$, $e_1(m_0)$, and $e_0(l_0)$ are non-zero, by Theorem 6.8 (part 2),

$$\gamma := (\{e_2 \cdot n_0, ae_2 \cdot n_0\} \cup \{e_2 \cdot x(n_1), ae_2 \cdot x(n_1)\}) \cup \{e_1 \cdot m_0\} \cup \{e_0 \cdot l_0\}$$

$$= (\{144030301, 33400403\} \cup \{414320423, 043130422\}) \cup \{110020401\} \cup \{140442324\}$$

is a basis for $C$.

References

[1] G. K. Bakshi, S. Gupta, I. S. Passi, Semisimple metacyclic group algebras, Proc. Indian Acad. Sci. (Math. Sci.) 121 (4)(2011), 379–396.

[2] G. K. Bakshi, S. Gupta, I. S. Passi, The structure of finite semisimple metacyclic group algebras, J. Ramanujan Math. Soc. 28 (2)(2013), 141–158.

[3] C. Curtis, I. Reiner. Representation Theory of Finite Groups and Associative Algebras. John Wiley and sons, 1962.

[4] C. Curtis, I. Reiner. Methods of representation theory with applications to finite groups and orders. vol. 1, John Wiley and sons, 1981.

[5] B. K. Dey, B. Sundar Rajan, Codes closed under arbitrary abelian group of permutatations. J. Disc. Math. 18 (1)(2004), 1-18.
[6] C. Ding, D. R. Kohel, S. Ling, Split group codes. IEEE Transactions on Information Theory 46 (2)(2000), 485-495.

[7] F. S. Dutra, R. A. Ferraz and C. Polcino Milies, Semisimple group codes and dihedral codes, Algebra and Disc. Math.3 (2009), 28-48.

[8] I. V. Gelder, G. Olteanu, Finite group algebras of nilpotent groups: A complete set of orthogonal primitive idempotents, Finite Fields and Their Applications 17 (2011), 157–165.

[9] W. C. Huffman, V. Pless, Fundamentals of error correcting codes. Cambridge University Press, 2003.

[10] M. Karlin, Decoding of circulant codes. IEEE Transactions on Information Theory 16 (1970), 797-802.

[11] W. Knapp, P. Schmid, Codes with prescribed permutation group, J. Algebra 67 (1980), 415-435.

[12] H. Nagao, Y. Tsushima. Representations of finite groups. Academic Press Inc., 1989.

[13] F. J. MacWilliams, “Combinatorial problems of elementary abelian groups,” Ph.D. Thesis, Harvard University, 1962.

[14] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. New York: Elsevier/North Holland, 1977.

[15] J. Pei, X. Zhang, 1-generator quasi-cyclic codes, Journal of Systems Science and Complexity 20 (2007), 554-561.

[16] C. Polcino Milies and S. K. Sehgal, An Introduction to Group Rings, Kluwer academic publishers, 2002.

[17] D. Radkova, A.J. Van Zanten, Constacyclic codes as invariant subspaces. Linear Algebra and its Applications 430 (2009), 855-864.

[18] J. Rotman, Advanced modern algebra. Prentice Hall, 2003.

[19] G. E. Seguin, A class of 1-generator quasi-cyclic codes, IEEE Transactions on Information Theory 50 (2004),1745-1753.