Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

Helene Tuft Bjørshol

Codes in Algebras

Master's thesis in Mathematical Sciences
Supervisor: Øyvind Solberg
Co-supervisor: Aslak Bakke Buan
December 2023

NTNU
Norwegian University of
Science and Technology

Helene Tuft Bjørshol

Codes in Algebras

Master's thesis in Mathematical Sciences
Supervisor: Øyvind Solberg
Co-supervisor: Aslak Bakke Buan
December 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

NTNU
Norwegian University of
Science and Technology

Abstract

Using some theory about the automorphisms of extended quadratic residue codes, we show that the extended binary Golay code is an ideal in the group algebra of the symmetric group on 4 elements over $\mathbb{Z}_2$. We then take advantage of the additional structure found in a group algebra to get a deeper understanding of the properties of this code. Finally we use this insight to explore how new codes may be constructed.

Sammendrag

Vi viser, ved hjelp av teorien om automorfier til utvidede kvadratiske restkoder, at den utvidede binære Golay-koden er et ideal i gruppealgebraen til den symmetriske gruppen på 4 elementer over $\mathbb{Z}_2$. Vi utnytter deretter den ekstra strukturen som gruppealgebraer kommer med til å få en dypere forståelse av egenskapene til denne koden. Til slutt bruker vi denne innsikten til å utforske hvordan nye koder kan konstrueres.

Contents

1 Introduction

This thesis is about error correcting code theory. This theory is concerned with methods on how to secure that information is safely transferred from one place to another. More specifically, it focuses on detecting when information has been compromised and restoring it. A code is thus used to reshape (code) the information by applying to it a recognizable mathematical structure before transferring. We want codes that allow for as many errors as possible to be detected and corrected. This is different from cryptography, which is the theory concerned with ways of transferring information securely while keeping it secret from any third part. In error-correcting code theory one generally ignores this problem. In both fields however, there is the question of finding more efficient constructions that minimize the computational, and thereby also the economical and environmental cost. Thus error-correcting code theory is relevant to the United Nations 12th sustainable development goal about responsible consumption and production.

In this thesis we use one particular example of an error-correcting code, namely the *extended binary Golay code*, denoted $\mathcal{G}_{24}$. This code has many nice properties. There are therefore many equivalent ways of constructing this code, some examples are the Reed-Solomon code over the field of 8 elements, and more recent, as a zero divisor code in the group ring $\mathbb{Z}_2 D_{24}$ [11]. In this thesis we define it as the extended code of the binary Golay code $\mathcal{G}_{23}$, the latter we define both with respect to its properties as a cyclic and quadratic residue code. From there we show that $\mathcal{G}_{24}$ is an idempotent code in the group algebra of the symmetric group on 4 elements over $\mathbb{Z}_2$.

The background for this assignment is the scientific article "Extended Golay Codes as Ideals" by Bernhardt, Landrock and Manz [2]. It describes the constructions of the two *extended Golay codes*, which are the *extended binary Golay code* of length 24 and the *extended ternary Golay code* of length 12, as ideals in group algebras. These constructions are based on some results about the automorphism groups of extended quadratic residue codes.

The main and beginning part of this assignment focuses on the results that are presented in [2]. We first outline the background definitions and results that apply to the constructions given in the article. We then look specifically at the case involving $\mathcal{G}_{24}$, embedded in the group algebra $\mathbb{Z}_2 S_4$. The first part involves some general theory about quadratic residue codes and their automorphisms, as well as some results concerning the *decoding* of what is defined as *idempotent codes*. Our aim is to give a more thorough introduction to these concepts, in order for it to be accessible to a more inexperienced reader.

For the second part of this paper, we look at how the endomorphism ring of the group algebra $\mathbb{Z}_2 S_4$ as a $\mathbb{Z}_2 S_4$-module offers a decomposition of this algebra that allows us to say more about its structure and the embedding of the extended binary Golay code inside it. We then make an attempt at applying these results in the final part, where we see if there could be ways of finding new codes or new constructions of older codes by starting out with an algebra with some chosen structural properties. Although we find a way to construct

submodules of algebras from a subset of basis vectors, this does not offer an obvious way to find generators for those submodules as idempotent codes.

The motivation throughout this thesis is the general mathematical principle that the more structure we can apply, the more knowledge we have. This is a particular interest when it comes to finding good algorithms for decoding codes. We therefore try to outline different structures as detailed as possible, and we include those calculations we think have a possibility of offering some further insights. This approach has proven particularly useful, as it has led us to discover and correct a mistake in [2] about the element that is defined as a generator for $\mathcal{G}_{24}$ as an idempotent code.

The contents are divided into the following chapters. In Chapter 2 we define what is known as quadratic residue codes and present some results about the automorphisms of these codes. This is the theoretical background for the construction method that we later apply to $\mathcal{G}_{24}$. In Chapter 3 we show that there is a method of decoding that applies to all *idempotent codes*. Chapter 4 introduces the extended Golay code $\mathcal{G}_{24}$ as an extended code of the quadratic residue code of length 23. We thereby show that $\mathcal{G}_{24}$ can be embedded as an ideal in the group algebra that is a representation of the symmetric group S_4 over the field $\mathbb{Z}_2 = \mathbb{F}_2$, and that $\mathcal{G}_{24}$ then is an idempotent code. In Chapter 5 we look at the ring of endomorphisms of $\mathbb{Z}_2S_4$ as a module over itself and show that this offers more details about the structural properties of this group algebra. This again offers more details about the embedding of $\mathcal{G}_{24}$ in $\mathbb{Z}_2S_4$. Finally, in Chapter 6, we make an attempt at applying the results found in Chapter 5 in order to see if we can determine the existence on a code inside another algebra than $\mathbb{Z}_2S_4$, but with some of the similar properties for endomorphisms between submodules. For some of the details that are less relevant in their given context, but might be interesting all the same, we include an Appendix.

I would very much like to thank my supervisor, Professor Øyvind Solberg, for being very positive, thorough and easy to communicate with. In addition, I have to thank Eiolf Kaspersen for his wonderful help and support both in math and life. A little thank you also goes to Torus, who has, most literary, been by my side every day.

2 Quadratic Residue Codes and their Automorphisms

We begin with a general presentation of what is known as quadratic residue codes. In particular, we give some results about the groups formed by automorphisms of these codes, as this lays the foundation for a method of constructing a group algebra around such a code. As mentioned in the introduction, we later apply these results to the specific case of the extended binary Golay code. The results established in this chapter are, unless otherwise mentioned, based on those presented in [2, Chapter 1]. We do however try to give a more thorough presentation of the coding- and representation theory on which these results are based.

We start with the basic definition from which quadratic residue codes take their name.

Definition 2.1. Let r be an odd prime. For $a \in \mathbb{N}$ we say that a is a *quadratic residue* modulo r if a is a nonzero square modulo r and that a is a *quadratic nonresidue* if a is a nonsquare modulo r. We write

$$(a/r) \;=\; \begin{cases} 0 & \text{if } a \;\equiv\; 0 (\text{mod } r) \\ 1 & \text{if } a \text{ is a quadratic residue modulo } r \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } r \end{cases},$$

where (a/r) is called the *Legendre symbol*.

The sets of quadratic and nonzero non-quadratic residues modulo r are denoted as Q_r and N_r, respectively.

We now remind the reader of some of the basic notions related to cyclic codes. Let $\mathbb{F}_q$ be a field with q elements, that is $q = p^k$ for some prime p and positive integer k. Remember that the cyclic codes over $\mathbb{F}_q$ of length r are the ideals of $\mathbb{F}_q[x]/(x^r - 1)$. We first define the following.

Definition 2.2. [6, page 114] Let $0 \leq s \leq r$. The *q-cyclotomic coset of s modulo r* is given as

$$C_s \;=\; \{s, sp, \ldots, sp^{d-1}\} (\text{mod } r),$$

where d is the smallest positive integer for which $sp^d \equiv s (\text{mod } r)$.

For the following we refer to Theorem 3.7.6 and Theorem 4.1.1 in [6].

Lemma 2.3. *Let $0 \leq s \leq r$ where r is a prime. Suppose q is relatively prime to r and ξ is a primitive element in $\mathbb{F}_{q^{|C_s|}}$. Then the minimal polynomial of ξ^s over $\mathbb{F}_q$ is*

$$M_{\xi^s}(x) \;=\; \prod_{i \in C_s} (x - \xi^i).$$

The following proposition defines what is known as *quadratic residue codes*. In this case we have $q = p$.

Proposition 2.4. *Let p be a prime for which $p \in Q_r$. Let ξ be a primitive rth root of unity in $\mathbb{F}_{p^m}$ for some m. If*

$$q(x) \;=\; \prod_{i \in Q_r} (x - \xi^i) \quad \textit{and} \quad n(x) \;=\; \prod_{i \in N_r} (x - \xi^i),$$

then

$$x^r - 1 \;=\; (x-1)q(x)n(x) \;\in\; \mathbb{F}_{p^m}[x].$$

Moreover, $q(x)$ and $n(x)$ have coefficients in $\mathbb{F}_p$.

Proof. The factorization of $x^r - 1$ follows directly from the fact that

$$\mathbb{F}_r \;=\; Q_r \cup N_r \cup \{0\}.$$

As for the last part, let p be a prime with $p \in Q_r$. First note that since $p \in Q_r$, then Q_r contains

$$C_1 \;=\; \{1, p, p^i, \ldots, p^{d-1}\} (\text{mod } r),$$

where d is the smallest positive integer such that $p^d \equiv 1 (\text{mod } r)$. In general, for any primitive element σ in $\mathbb{F}_r$ (that is, σ is a generator for $\mathbb{F}_r^*$), if $\sigma \equiv x_\sigma \pmod r$ for some x_σ, we have

$$\sigma^{2k} \;\equiv\; (x_\sigma^k)^2 \pmod r \;\implies\; \sigma^{2k+1} \;\equiv\; (x_\sigma^k)^2 x_\sigma \pmod r,$$

hence $\sigma^{2k} \in Q_r$ and $\sigma^{2k+1} \in N_r$. Thus Q_r is a cyclic group with σ^2 as a generator. Moreover, since $p \in Q_r$. then Q_r is closed under multiplication by p since

$$\sigma^2 p^i \;\equiv\; x_\sigma^2 x_p^{2i} \;\equiv\; (x_\sigma x_p^i)^2 \pmod r.$$

In other words, $C_s \subseteq Q_r$ if and only if $s \in Q_r$, hence Q_r is a disjoint union of cyclotomic cosets, and so

$$q(x) \;=\; \prod_{i \in Q_r} (x - \xi^i) \;=\; \prod_{C_s \subseteq Q_r} \prod_{i \in C_s} (x - \xi^i),$$

where $\prod_{i \in C_s} (x - \xi^i)$ is the minimal polynomial of ξ^s over $\mathbb{F}_p$ by Lemma 2.3, i.e has coefficients in $\mathbb{F}_p$. Hence $q(x)$ has coefficients in $\mathbb{F}_p$. By the same logic this also holds for $n(x)$.

□

The ideals with minimal generator polynomial either $q(x)$ or $n(x)$ are called the *quadratic residue codes* of length r over $\mathbb{F}_p$. These are equivalent codes. Let $\mathcal{C}$ be a quadratic residue code with generating idempotent $e(x)$. If $q(x)$ is the minimal polynomial for $\mathcal{C}$ then

$$e(x) \;=\; a_0 + \sum_{i \in Q_r} x^i.$$

Otherwise, if $\mathcal{C}$ is generated by $n(x)$ then

$$e(x) \;=\; a_0 + \sum_{i \in N_r} x^i.$$

For the previous facts, see [6, Theorem 6.6.5]. Note that $\langle q(x) \rangle$ and $\langle n(x) \rangle$ are sometimes referred to as the *odd-like* quadratic residue codes, in which case we call $\langle (x-1)q(x) \rangle$ and $\langle (x-1)n(x) \rangle$ the *even-like* quadratic residue codes.

The *extended quadratic residue code* is constructed given the more general definition that follows.

Definition 2.5. If $\mathcal{C}$ is cyclic code, then the *extended code* or *extension*, of $\mathcal{C}$, denoted $\widehat{\mathcal{C}}$, is the code constructed by adding a parity check at a position labelled ∞.

Note that the extended code of a quadratic residue code is not cyclic but rather a submodule of $\mathrm{Span}_{\mathbb{F}_p}\langle x^0, \ldots, x^{r-1}, x^\infty \rangle$.

As mentioned earlier, the first part of this thesis is concerned with constructing a group ring in which an extended quadratic residue code can be embedded as an ideal. We choose this group basis using our knowledge about automorphism groups of quadratic residue codes.

2.1 Automorphism Groups of Extended Binary Quadratic Residue Codes

We identify the canonical basis vectors $x^0, \ldots x^{22}, x^\infty$ with the *projective line* given as $P(r) = \mathbb{F}_r \cup \{\infty\}$. The details of the following definition are later used in the proof of Lemma 4.4.

Definition 2.6. We define the *special linear group* and *projective special linear group* by

$$\begin{aligned} \mathrm{SL}_2(r) \;&=\; \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \; a,b,c,d \;\in\; \mathbb{F}_r \;\text{ and }\; ad - bc \;=\; 1 \right\}, \\ \mathrm{PSL}_2(r) \;&=\; \mathrm{SL}_2(r) / \langle -I \rangle \,. \end{aligned}$$

These groups come with some additional results, which we can explore after giving the following definition.

Definition 2.7. [5, Page 210] A group action by a group G on a set X is *transitive* if for all $x_1, x_2 \in X$ there exists some $g \in G$ such that $x_1 g = x_2$. The group action is called 2 - *transitive* if for all x_1, x_2, x_1', x_2' with $x_1 \neq x_1'$ and $x_2 \neq x_2'$ there exists some $g \in G$ such that $x_1 g = x_2$ and $x_1' g = x_2'$.

Note that while $r = 8m \pm 1$, then $\mathrm{PSL}_2(r)$ can also be realized as the group of all permutations of $P(r)$ of the form

$$i \;\mapsto\; \frac{a \cdot i + b}{c \cdot i + d},$$

where $a, b, c, d \in \mathbb{F}_r$ and $ad - bc = 1$ [10, Chapter 16.5]. This leads to the following proposition.

Proposition 2.8. *Let r be a prime of the form $r = 8m \pm 1$. Let σ a primitive element of $\mathbb{F}_r$ and for $i \in P(r)$ define*

$$\begin{aligned} s_r &: \ i \mapsto i + 1, \\ \mu &: \ i \mapsto i\sigma^2, \\ \alpha_{r+1} &: \ i \mapsto \begin{cases} j & \text{where } ij \equiv -1 (\text{mod } r) \text{ if } i \neq 0, \infty \\ \infty & \text{if } i = 0 \\ 0 & \text{if } i = \infty, \end{cases} \end{aligned}$$

as permutations of $P(r)$. Then

$$\mathrm{PSL}_2(r) \ \cong \ \langle s_r, \mu, \alpha_{r+1} \rangle,$$

where $\mathrm{PSL}_2(r)$ acts 2-transitively on $P(r)$.

For the proof, see [10, Theorem 9]. Note that the permutation given as α_{r+1} in the above proposition maps elements in Q_r to elements in N_r and vice versa.

Now, remember that a *monomial matrix* is a square matrix with exactly one nonzero coordinate in any row or column, and that a *permutation matrix* is a monomial matrix where all the nonzero coordinates are 1s. Based on these properties we define two automorphism subgroups of a code $\mathcal{C}$.

Definition 2.9. [6, page 22+26] The *permutation automorphism group* of a code $\mathcal{C}$, is the set of all permutations that maps $\mathcal{C}$ to itself, denoted $\mathrm{PAut}(\mathcal{C})$. Likewise the *monomial automorphism group* of $\mathcal{C}$ is the group formed by all monomial transformations being automorphisms of $\mathcal{C}$, denoted $\mathrm{MAut}(\mathcal{C})$.

Note that in general, since any permutation can be written in the form of a monomial matrix, then $\mathrm{PAut}(\mathcal{C}) \leq \mathrm{MAut}(\mathcal{C}) \leq \mathrm{Aut}(\mathcal{C})$, where the latter denotes the group all automorphisms of $\mathcal{C}$. Furthermore, if $\mathcal{C}$ is binary then any monomial transformation is a permutation matrix, and so the sets are identical. We now present a special case of what is known as the *Gleason-Prange theorem*, which can be found as [10, Theorem 10]. We also refer there for a proof.

Theorem 2.10. *Let $\mathcal{C}$ be an quadratic residue code of length $r = 8m \pm 1$ for $m \in \mathbb{N}$ over $\mathbb{Z}_2$. Let $\widehat{\mathcal{C}}$ be the extended code of $\widehat{\mathcal{C}}$. Then*

$$\mathrm{PSL}_2(r) \ \leq \ \mathrm{PAut}(\hat{\mathcal{C}}).$$

This concludes the general part about encoding of quadratic residue codes. For now, it might not be obvious to the reader how the results established so far directly adds algebraic structure to the vector space of a general (extended) quadratic residue code. Later when we look at the specific case of the extended binary Golay code, we see that the properties of this code in particular allow us to choose a specific subgroup of $\mathrm{PSL}_2(r)$ as a basis for the group algebra containing this code.

3 Decoding Idempotent Codes

The purpose of building more structure around an error-correcting code, is to introduce more efficient methods of *decoding* received codewords. In this chapter we show that there is a natural decoding method that applies to any code once we have shown that the code can be generated by a sum of idempotents. Unless otherwise stated, these definitions and results are found in [2, Section 4].

We let $\mathbb{F}$ be a field, G a finite group with identity 1. Let $A := \mathbb{F}G$; the vector space with basis G over $\mathbb{F}$. Then A is a *group algebra*. Note that multiplication in A is naturally defined from multiplication in $\mathbb{F}$ and the binary operation G. An element $a \in A$ is a vector that can be written as $a = \sum_{g\in G} a_g g$. The two maps given in the following definition will be applied repeatedly in the proofs in this section. The latter also turns out to be a useful tool in understanding the structures we later examine in the group algebra $\mathbb{Z}_2 S_4$.

Definition 3.1. For any $a \in A$, let $\tau\colon A \to A$ and $\lambda\colon A \to \mathbb{F}$ be the maps given as

$$\begin{aligned} \lambda(a) &= a_1, \\ \tau(a) &= \sum_{g\in G} a_g g^{-1}. \end{aligned}$$

The map τ is called the *antipode* of A.

We use the next definition to prove the subsequent lemma.

Definition 3.2. [3, page 192] A homomorphism $\phi : R \to S$ is an *antiisomorphism* if ϕ is a bijection and

$$\phi(r_1 +_R r_2) = \phi(r_1) +_S \phi(r_2) \text{ and } \phi(r_1 \cdot_R r_2) = \phi(r_2) \cdot_S \phi(r_1),$$

for all $r, s \in R$. In the case where $R = S$, we say that ϕ is an *antiautomorphism*.

Thus we have the following fact about the function we just defined as τ.

Lemma 3.3. *The mapping τ given in (3.1) is an antiautomorphism.*

Proof. It is straightforward to check that τ is a homomorphism of vector spaces. Now consider an arbitrary element $a = \sum_{g\in G} a_g g \in A$. Since g is the inverse of g^{-1} then $\tau(\tau(a)) = a$ and hence τ is an automorphism. In particular,

$$\begin{aligned} (\tau \cdot \tau)(a) = \tau(\tau(a)) &= \tau\left(\tau\left(\sum_{g\in G} a_g g\right)\right) \\ &= \tau\left(\sum_{g\in G} a_g g^{-1}\right) = \sum_{g\in G} a_g g = a, \end{aligned}$$

so $\tau = \tau^{-1}$. Now let $b = \sum_{g\in G} b_g g \in A$ as well. Then

$$\begin{aligned}\tau(a+b) \;&=\; \tau\left(\sum_{g\in G}(a_g+b_g)g\right) \;=\; \sum_{g\in G}(a_g+b_g)g^{-1}\\ &= \sum_{g\in G} a_g g^{-1} + \sum_{g\in G} b_g g^{-1} \;=\; \tau(a)+\tau(b).\end{aligned}$$

Moreover, we have

$$\begin{aligned}\tau(a\cdot b) \;&=\; \tau\left(\sum_{g,h\in G}(a_g b_h)gh\right) \;=\; \sum_{g,h\in G}(a_g b_h)(gh)^{-1}\\ &= \sum_{g,h\in G}(a_g b_h)h^{-1}g^{-1} \;=\; \tau(b)\tau(a).\end{aligned}$$

Hence τ is an antiautomorphism. □

Note also that, if $X, Y \subseteq A$, we have

$$\begin{aligned} a \in \tau(X)\cap\tau(Y) \;&\Longrightarrow\; a\in\tau(X) \text{ and } a\in\tau(Y)\\ &\Longrightarrow\; \tau(a)\in X \text{ and } \tau(a)\in Y\\ &\Longrightarrow\; \tau(a)\in X\cap Y\\ &\Longrightarrow\; a\in\tau(X\cap Y).\end{aligned}$$

For $a, b \in A$, let $\langle\cdot,\cdot\rangle$ denote the *standard inner product in* A, i.e $\langle a,b\rangle = \sum_{g\in G} a_g b_g$. In general, it will be useful to remind ourselves of some of the most basic definitions and results in vector space theory. The identity given in the following lemma will be a useful tool for the later proofs.

Lemma 3.4. *For any $a, b \in A$ we have*

$$\lambda(a\tau(b)) \;=\; \langle a,b\rangle.$$

Proof. Let $a = \sum_{g\in G} a_g g$ and $b = \sum_{h\in G} b_h h$ in A. Then

$$\begin{aligned} a\tau(b) \;&=\; \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h^{-1}\right)\\ &= \sum_{\substack{g,h\in G\\ g=h}} a_g b_h g h^{-1} + \sum_{\substack{g,h\in G\\ g\neq h}} a_g b_h g h^{-1} \;=\; \sum_{g\in G} a_g b_g + \sum_{\substack{g,h\in G\\ g\neq h}} a_g b_h g h^{-1}.\end{aligned}$$

Hence $\lambda(a\tau(b)) = \sum_{g\in G} a_g b_g = \langle a,b\rangle$. □

Note that it follows that $\lambda(\tau(a)b) = \lambda(\tau(a)\tau(\tau(b))) = \langle\tau(a),\tau(a)\rangle = \langle a,b\rangle$ as well. Likewise, we have

$$\lambda(ab) \;=\; \langle a,\tau(b)\rangle \;=\; \langle\tau(a),b\rangle \;=\lambda(\tau(a)\tau(b)).$$

We now list a few definitions that will be necessary for establishing the subsequent result. The following applies to any right or left module over a ring.

Definition 3.5. [3, Page 374] Let R be a ring and M a left R-module. The *left annihilator* of M is given as

$$\mathrm{Ann}_l(M) \;=\; \{l \in R \mid lm = 0 \text{ for all } m \in M\}\,.$$

Let N be a right R-module. The *right annihilator* of N is given as

$$\mathrm{Ann}_r(N) \;=\; \{r \in R \mid nr = 0 \text{ for all } n \in N\}\,.$$

If J is an ideal in R, we let $\mathrm{Ann}_{l,J}(M) = \mathrm{Ann}_l(M) \cap J$ and $\mathrm{Ann}_{r,J}(M) = \mathrm{Ann}_r(N) \cap J$. In particular, we can use the above definition for a code $\mathcal{C}$ in A.

The rest of this section applies to idempotent codes which we define next.

Definition 3.6. A code $\mathcal{C}$ is an *idempotent code* if $\mathcal{C} = \sum_{j=1}^{m} e_j A$, where $e_1, \ldots, e_m$ are idempotents in A.

We also use the following notion to build some additional structure around $\mathcal{C}$ inside the group algebra.

Definition 3.7. An idempotent $e \in A$ is a *central idempotent* if $ea = ae$ for all $a \in A$.

Note that the *dual* or *orthogonal* of $\mathcal{C}$ is the code defined as

$$\mathcal{C}^{\perp} = \{a \in A \mid a \cdot c = 0 \;\text{ for all } c \in \mathcal{C}\}$$

[6, page 6]. In the following two results let ε a central idempotent, let $B = \varepsilon A$, and let $\mathcal{C} = \sum_{j=1}^{m} e_j A$ be an idempotent code contained in B.

Lemma 3.8. *Assume $\tau(B) = B$ and $\mathcal{C}^{\perp} \cap B = \mathcal{C}$. Then*

$$\mathcal{C} \;=\; \bigcap_{i=1}^{m} (\varepsilon - \tau(e_i))A.$$

Proof. Assume that $\mathcal{C} = \mathcal{C}^{\perp} \cap B$ and $B = \tau(B)$. We first show that

$$\mathcal{C}^{\perp} \;=\; \tau(\mathrm{Ann}_l(\mathcal{C})). \tag{1}$$

For the inclusion from right to left we have

$$\begin{aligned} a \in \mathrm{Ann}_l(\mathcal{C}) \;&\Longrightarrow\; 0 = ac = \lambda(ac) = \langle a, \tau(c)\rangle = \langle \tau(a), c\rangle \;\text{ for all } c \in \mathcal{C} \\ &\Longrightarrow\; \tau(a) \in \mathcal{C}^{\perp}. \end{aligned}$$

Hence $\tau(\mathrm{Ann}_l(\mathcal{C})) \subseteq \mathcal{C}^{\perp}$. On the other hand,

$$\begin{aligned} a \in \mathcal{C}^{\perp} \;&\Longrightarrow\; 0 = \langle a, c\rangle = \langle \tau(a), \tau(c)\rangle = \lambda(\tau(a)c) \;\text{ for all } c \in \mathcal{C} \\ &\Longrightarrow\; \lambda(\tau(a)cg) = 0 \;\text{ for all } c \in \mathcal{C} \text{ and } g \in G \\ &\Longrightarrow\; \text{the coefficient of } g^{-1} \text{ in } \tau(a)c \text{ is } 0 \;\text{ for all } g \in G, c \in \mathcal{C} \\ &\Longrightarrow\; \tau(a)c = 0 \;\text{ for all } c \in \mathcal{C} \\ &\Longrightarrow\; \tau(a) \in \mathrm{Ann}_l(\mathcal{C}). \end{aligned}$$

Thus $\tau(\tau(a)) = a \in \tau(\mathrm{Ann}_l(\mathcal{C}))$. Hence $\mathcal{C}^\perp = \tau(\mathrm{Ann}_l(\mathcal{C}))$. We next show that

$$\mathrm{Ann}_{l,B}(\mathcal{C}) \;=\; \bigcap_{i=1}^{m} \mathrm{Ann}_{l,B}(e_i A). \tag{2}$$

Remember that $\mathcal{C} = \sum_{i=1}^{m} e_i A$, with $e_1, \ldots, e_m$ orthogonal. Then $e_j a \in \mathcal{C}$ for $1 \leq j \leq m$, since $e_j a \in A$ and thus $\sum_{i=1}^{m} e_i \cdot e_j a = e_j a \in \mathcal{C}$. The first identity holds since for $b \in B$ we have

$$\begin{aligned}
b \in \mathrm{Ann}_{l,B}(\mathcal{C}) &\iff b \cdot \sum_{i=1}^{m} e_i a_i = 0 \;\text{ for all } a_i \in A \\
&\iff be_i a = 0 \;\text{ for all } 1 \leq i \leq m,\; a \in A \\
&\iff b \in \mathrm{Ann}_{l,B}(e_i A) \;\text{ for all } 1 \leq i \leq m \\
&\iff b \in \bigcap_{i=1}^{m} \mathrm{Ann}_{l,B}(e_i A).
\end{aligned}$$

For the third part, we show that

$$\mathrm{Ann}_{l,B}(e_i A) \;=\; A(\varepsilon - e_i). \tag{3}$$

Since ε is a central idempotent then for any $b \in B = \varepsilon A$ we have $b = \varepsilon a = a\varepsilon$ for some $a \in A$. But then $\varepsilon b = \varepsilon^2 a = \varepsilon a = b = a\varepsilon = a\varepsilon^2 = b\varepsilon$. Thus $\varepsilon e_i = e_i = e_i \varepsilon$ since $e_i \in B$. We first show the right inclusion. We have

$$\begin{aligned}
A(\varepsilon - e_i)e_i A \;&=\; A(\varepsilon e_i - e_i^2)A \\
&=\; A(e_i - e_i)A \;=\; 0.
\end{aligned}$$

Hence $A(\varepsilon - e_i) \subseteq \mathrm{Ann}_{l,B}(e_i A)$. On the other hand, suppose $b \in \mathrm{Ann}_{l,B}(e_i A)$. Then for any e_i we have $be_i a = 0$ for all $a \in A$, so $be_i \cdot 1 = be_i = 0$. Thus

$$\begin{aligned}
b \;=\; b - be_i \;=\; b(\varepsilon - e_i) \;&=\; a\varepsilon(\varepsilon - e_i) \\
&=\; a(\varepsilon^2 - \varepsilon e_i) \\
&=\; a(\varepsilon - e_i) \quad \in\; A(\varepsilon - e_i).
\end{aligned}$$

and so $\mathrm{Ann}_{l,B}(e_i A) \subseteq A(\varepsilon - e_i)$. For the final part, we want to show that

$$\tau(A(\varepsilon - e_i)) \;=\; (\varepsilon - \tau(e_i))A. \tag{4}$$

We see directly that

$$\begin{aligned}
\tau(A(\varepsilon - e_i)) \;&=\; \tau(\varepsilon - e_i)\tau(A) \\
&=\; (\tau(\varepsilon) - \tau(e_i))\tau(A) \;=\; (\tau(\varepsilon) - \tau(e_i))A.
\end{aligned}$$

It remains to show that $\tau(\varepsilon) = \varepsilon$. We see that

$$\begin{aligned}
\tau(\varepsilon)A \;=\; \tau(\varepsilon)\tau(A) \;=\; \tau(A\varepsilon) \;&=\; \tau(B) \;=\; B \\
&=\; \tau(\varepsilon A) \;=\; \tau(A)\tau(\varepsilon) \;=\; A\tau(\varepsilon).
\end{aligned}$$

Hence $b = \tau(\varepsilon)a = a\tau(\varepsilon)$, since $\tau(\varepsilon)$ is a central element in A. But then

$$\begin{aligned} \tau(\varepsilon)b &= \tau(\varepsilon)^2 a = \tau(\varepsilon^2)a = \tau(\varepsilon)a, \\ b\tau(\varepsilon) &= a\tau(\varepsilon)^2 = a\tau(\varepsilon^2) = a\tau(\varepsilon), \end{aligned}$$

so we have $b = \tau(\varepsilon)b = b(\varepsilon)$. But then $\tau(\varepsilon)$ is the identity on B, which we already know that ε is. Hence $\tau(\varepsilon) = \varepsilon$ and so

$$(\tau(\varepsilon) - \tau(e_i))A = (\varepsilon - \tau(e_i))A.$$

Finally, by combining the initial assumptions with (1), (2), (3) and (4), we have

$$\begin{aligned} \mathcal{C} = \mathcal{C}^{\perp} \cap B &= \tau(\mathrm{Ann}_l(\mathcal{C})) \cap \tau(B) \\ &= \tau(\mathrm{Ann}_{l,B}(\mathcal{C})) \\ &= \tau\left(\bigcap_{i=1}^{m} \mathrm{Ann}_{l,B}(e_i A)\right) \\ &= \tau\left(\bigcap_{i=1}^{m} A(\varepsilon - e_i)\right) \\ &= \bigcap_{i=1}^{m} \tau(A(\varepsilon - e_i)) = \bigcap_{i=1}^{m} (\varepsilon - \tau(e_i))A, \end{aligned}$$

which concludes our proof. □

Our last lemma introduces a method for decoding $\mathcal{C}$.

Lemma 3.9. *Let $\mathfrak{B}$ be a basis for B. Suppose $\mathcal{C}$ is a d-error correcting code w.r.t $\mathfrak{B}$. Then every $b \in B$ of weight $\leq d$ is uniquely determined by $\tau(e_i)b$ for $i = 1, \ldots, m$.*

Proof. Let $b, b' \in B$ be vectors of weight at most d such that $\tau(e_i)b = \tau(e_i)b'$ for $1 \leq i \leq m$. We have

$$\begin{aligned} \tau(e_i)b - \tau(e_i)b' = 0 &\implies \tau(e_i)(b - b') = 0 \\ &\implies a\tau(e_i)(b - b') = 0 \text{ for all } a \in A,\ i = 1, \ldots, m \\ &\implies b - b' \in \mathrm{Ann}_{r,B}(A\tau(e_i)) \text{ for all } i = 1, \ldots, m \\ &\implies b - b' \in \bigcap_{i=1}^{m} \mathrm{Ann}_{r,B}(A\tau(e_i)). \end{aligned}$$

We next show that for any $i = 1, \ldots, m$ we have

$$\mathrm{Ann}_{r,B}(A\tau(e_i)) = (\varepsilon - \tau(e_i))A. \tag{5}$$

First, we see that

$$\begin{aligned} A\tau(e_i)(\varepsilon - \tau(e_i))A &= A(\tau(e_i)\varepsilon - \tau(e_i)^2)A \\ &= A(\tau(e_i)\varepsilon - \tau(e_i))A \quad \text{since } \tau(e_i)^2 = \tau(e_i^2) = \tau(e_i) \\ &= 0. \end{aligned}$$

Hence $(\varepsilon - \tau(e_i))A \subseteq \mathrm{Ann}_{r,B}(A\tau(e_i))$. To show the opposite inclusion, choose some $b'' \in \mathrm{Ann}_{r,B}(A\tau(e_i))$. Then $b'' = \varepsilon a$ for some $a \in A$ and $\tau(e_i)b'' = 0$. Hence we have

$$\begin{aligned} b'' \;=\; b'' - \tau(e_i)b'' \;&=\; \varepsilon a - \tau(e_i)\varepsilon a \\ &=\; \varepsilon a - \tau(e_i)a \\ &=\; (\varepsilon - \tau(e_i))a \;\in\; (\varepsilon - \tau(e_i))A, \end{aligned}$$

since $\tau(e_i)\varepsilon = \tau(e_i)\tau(\varepsilon) = \tau(\varepsilon e_i) = \tau(e_i)$. Hence (5) holds. But then

$$b - b' \;\in\; \bigcap_{i=1}^{m} (\varepsilon - \tau(e_i))A \;=\; \mathcal{C}. \qquad \text{(Lemma 3.8.)}$$

Since b and b' both have weight $\leq d$, then $b - b'$ has weight $\leq 2d$. But since $\mathcal{C}$ is d-error correcting, then the minimal weight of $\mathcal{C}$ is $2d+1$. Hence $b - b' \in \mathcal{C}$ can only be true if $b - b' = 0$, that is $b = b'$. $\square$

4 The extended binary Golay code $\mathcal{G}_{24}$ as an ideal in $\mathbb{Z}_2 S_4$

The remaining part of this thesis is based on our study of a particular quadratic residue code known as *the extended binary Golay code*, denoted by $\mathcal{G}_{24}$. As indicated by its name, this code was originally constructed as an extension of *the binary Golay code*, which corresponds to the quadratic residue code of length 23. The extended binary Golay has many particularly nice properties. It is self-dual (self-orthogonal). And it is doubly-even, meaning that the weights of all its codewords are divisible by 4. Moreover, there are many different constructions that yield an ideal which is equivalent to this code.

In this chapter we describe the construction introduced in [2], showing that $\mathcal{G}_{24}$, as the extended quadratic residue code of length 24, can be embedded as an ideal in the group algebra $\mathbb{Z}_2 S_4$, where S_4 is the symmetric group of 4 digits. Unless otherwise stated, these definitions and results are found in [2, Section 2].

We introduce $\mathcal{G}_{24}$ as the extension of the binary quadratic residue code of length 23. Using the notation from Chapter 2, we have $q = p = 2$ and $r = 23$. The sets of quadratic and non-quadratic residues modulo 23 in this case are

$$\begin{aligned} Q_{23} &= \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}, \\ N_{23} &= \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}. \end{aligned}$$

Moreover, over $\mathbb{Z}_2$ we have $x^{23} - 1 = (x+1)q_{23}(x)n_{23}(x)$, where

$$\begin{aligned} q_{23}(x) &= 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}, \\ n_{23}(x) &= 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}. \end{aligned}$$

Hence $\langle q_{23}(x) \rangle$ and $\langle n_{23}(x) \rangle$ are QR-codes. Their *generating idempotents* are

$$\sum_{i \in Q_r} x^i \quad \text{and} \quad \sum_{i \in N_r} x^i,$$

respectively. As stated previously, these are equivalent codes. They both correspond to the code given in the following definition.

Definition 4.1. [6, page 401] The *(perfect) binary Golay code* $\mathcal{G}_{23}$ is a a linear $(23, 12, 7)$ - code corresponding to the quadratic residue - code of length 23 over $\mathbb{Z}_2$.

The *extended binary Golay code* $\mathcal{G}_{24}$ is the $(24, 12, 8)$ - code obtained when adding a parity check to the codewords of $\mathcal{G}_{23}$.

Now let $\mathcal{G}_{24} = \widehat{\mathcal{G}}_{23}$ with $\mathcal{G}_{23} = \langle q(x) \rangle$. Since $\sum_{i \in Q_r} x^i$ and $\sum_{i=0}^{22} x^i$ are codewords in $\mathcal{G}_{23}$, we see that

$$\begin{aligned} e(x) &= \sum_{i \in Q_r} x^i + x^\infty + \sum_{i=0}^{22} x^i + x^\infty \\ &= 1 + \sum_{i \in N_r} x^i, \end{aligned}$$

is a codeword in $\mathcal{G}_{24}$. Note that $e(x)$ is the generating idempotent for the quadratic residue code $\langle(1-x)q(x)\rangle$ in $\mathbb{Z}_2[x]/(x^{23}-1)$ by [6, Theorem 6.6.5]. In order to generate all of $\mathcal{G}_{24}$ however, we use the following set of codewords.

$$c_j \;=\; e(x)\cdot x^j, \text{ for } j \;=\; 0,\ldots,22 \quad \text{and} \quad c_{23} \;=\; x^{\infty} + \sum_{i=0}^{22} x^i. \tag{6}$$

We describe one way of finding a generator matrix for $\mathcal{G}_{24}$. Let D be the 24×24 binary matrix whose rows correspond to the codewords $c_0,\ldots,c_{22},c_{23}$. Note that N_{23} equals the 2-cyclotomic coset given as $C_{23}=\{5\cdot 2^j \mid j<(23-1)/2\}$. We arrange the columns of D corresponding to x^i in the order given by

$$\begin{aligned} i \;&=\; \infty, 5\cdot 2^{11},\ldots,5\cdot 2,5,0,-5,-5\cdot 2.\ldots,-5\cdot 2^{11} \\ &=\; \infty,14,7,15,19,21,22,11,17,20,10,5,0,18,13,3,6,12,1,2,4,8,16,9. \end{aligned}$$

Now the reduced row echelon form of D with the resulting all zero rows removed is the matrix

$$G = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&0&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&0&0&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0&1&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&1&0&0&0&1&1&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&1&1&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&1&1&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&1&1&0&1&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&1&0&1&0&0
\end{bmatrix}.$$

Here the dimension of $\mathcal{G}_{24}$ is given by the row rank of G.

We list some additional properties of $\mathcal{G}_{24}$ that will be used in this thesis. Remember that the (maximal) number of errors corrected by a code with minimal weight d is $\lfloor (d-1)/2\rfloor$. As stated in Definition 4.1, the minimum weight of $\mathcal{G}_{24}$ is 8. Since the code $\mathcal{G}_{24}$ is a rather well-established code with many uses and constructions, then the following facts are well-known and will therefore not be explicitly proven.

Lemma 4.2. *[6] For the binary Golay code $\mathcal{G}_{24}$ the following hold*

(i) It is a *self-dual* code, meaning that $\mathcal{G}_{24}=\mathcal{G}_{24}^{\perp}$.

(ii) It is 3-error correcting and 7-error detecting.

(iii) The weight of any codeword $c\in\mathcal{G}_{24}$ is divisible by 4.

Note that since $\mathcal{G}_{24}$ has minimum weight 8, it follows from the last point in Lemma 4.2 that the codewords in $\mathcal{G}_{24}$ have weight of either 8, 12, and 16.

Now, in order to construct $\mathcal{G}_{24}$ as an ideal in a group algebra we first need to construct that algebra from a suitable group basis. We do so by looking at the subgroups of the group of automorphisms.

4.1 Constructing the group algebra $\mathbb{Z}_2 S_4$ from automorphisms of $\mathcal{G}_{24}$

We begin by outlining the knowledge we have about the automorphism groups of $\mathcal{G}_{24}$ when applying the theory established in Chapter 2.1. It follows from Proposition 2.4 and Theorem 2.5 that

$$\mathrm{PSL}_2(23) \;\cong\; \langle s_{23}, \mu, \alpha_{24} \rangle \;\leq\; \mathrm{PAut}(\mathcal{G}_{24}),$$

where

$$\begin{aligned} s_{23} &= (0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,21,22), \\ \alpha_{24} &= (0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21) \\ &\quad (14,18). \end{aligned}$$

Note that $\mathrm{PAut}(\mathcal{G}_{24})$ is the Mathieu group M_{24}, which is known to have order $24^2 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 2$, see [6, page 402]. For the results that remain in this section to make sense, we need to understand the following property.

Definition 4.3. Let S be a set with a group action from a group G. An element $g \in G$ is called *fixed-point-free* if $gs \neq s$ for all $s \in S$. We say that G *acts fixed-point-freely on* S if g is fixed-point-free for all $g \in G$, $g \neq 1$.

There is a general result [7, Chapter II, Theorem 8.18] stating that $\mathrm{PSL}_2(r)$ contains a copy of S_4, the symmetric group of four digits, whenever $r^2 - 1 \equiv 0 \pmod{16}$. This holds for $r = 23$. The following Lemma defines a *fixed-point-free* group acting on $P(23)$ that can be embedded in $\mathrm{PSL}_2(23)$ and is isomorphic to S_4. We denote by π^ρ the element $\rho^{-1}\pi\rho$ for two elements π and ρ in a group.

Lemma 4.4. *Let $\alpha = \alpha_{24}$. Let β, γ and δ be fixed-point-free permutations on $P(23)$ such that*

1. $\alpha^2 = \beta^2 = \delta^2 = \gamma^3 = 1$.
2. $\alpha^\gamma = \beta$, $\beta^\gamma = \alpha\beta$, *or* $\alpha^\gamma = \alpha\beta$, $\beta^\gamma = \alpha$.
3. $\alpha^\delta = \alpha$, $\beta^\delta = \alpha\beta$, *or* $\alpha^\delta = \beta$, $\beta^\delta = \alpha$ *or* $\alpha^\delta = \alpha\beta$, $\beta^\delta = \beta$.

Then

$$S_4 \;\cong\; \langle \alpha, \beta, \gamma, \delta \rangle \;\leq\; \mathrm{PSL}_2(23).$$

A proof that this Lemma holds for a particular choice of α, β, γ, and δ in $\mathrm{PSL}_2(23)$ is found in Appendix 7.1.

As of now, we have defined $\mathcal{G}_{24}$ as a $\mathrm{Span}_{\mathbb{Z}_2}\langle x^0, \ldots, x^\infty\rangle$ - module. In order to find an embedding of $\mathcal{G}_{24}$ inside $\mathbb{Z}_2S_4$ we evaluate the module structure of $\mathbb{Z}_2S_4$. We first show that $\mathbb{Z}_2S_4$ can be written as a sum of indecomposable right ideals.

Lemma 4.5. *The group algebra $\mathbb{Z}_2S_4$ can be decomposed into a direct sum of right projective modules*

$$\mathbb{Z}_2S_4 \;\cong\; P_1 \oplus P_2 \oplus P_3,$$

where $P_2 \cong P_3$ and $\dim(P_1) = \dim(P_2) \;=\; \dim(P_3) = 8$.

Proof. Let $A = \mathbb{Z}_2S_4$ and $\mathfrak{r} = \mathrm{rad}(A)$. Then $\mathbb{Z}_2$ is a splitting field for $A/\mathfrak{r}$, that is

$$\begin{aligned} A/\mathfrak{r} &\cong \mathbb{Z}_2 \oplus M_2(\mathbb{Z}_2) \\ &\cong \mathbb{Z}_2 \oplus \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} M_2(\mathbb{Z}_2) \oplus \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} M_2(\mathbb{Z}_2) \;=\; L_1 \oplus L_2 \oplus L_3. \end{aligned}$$

for simple modules L_1, L_2 and L_3. Thus $A/\mathfrak{r}$ is a direct sum of three simple modules. Recall that for projective modules P and P' we have $P \cong P'$ if and only if $P/P\mathfrak{r} \cong P'/P'\mathfrak{r}$. Let P_1, P_2, P_3 be the projective covers of L_1, L_2 and L_3, respectively. Thus we have

$$\begin{aligned} (P_1 \oplus P_2 \oplus P_3)/(P_1 \oplus P_2 \oplus P_3)\mathfrak{r} &\cong P_1/P_1\mathfrak{r} \oplus P_2/P_2\mathfrak{r} \oplus P_3/P_3\mathfrak{r} \\ &= L_1 \oplus L_2 \oplus L_3 \;=\; A/\mathfrak{r}. \end{aligned}$$

Since A is a finite dimensional $\mathbb{Z}_2$-algebra then $A \cong P_1 \oplus P_2 \oplus P_3$. Moreover, since P_2 and P_3 are projective then $P_2/P_2\mathfrak{r} = L_2 \cong L_3 = P_3/P_3\mathfrak{r}$ implies that $P_2 \cong P_3$. □

We also want to evaluate how these ideals are built according to the irreducible modules in A. From basic group theory we know that K_4, the Klein-4-group, is a subgroup of S_4 and that K_4 acts trivially on any irreducible $\mathbb{Z}_2S_4$-module. Also, $S_4/K_4 \cong S_3$, such that any irreducible submodule of $\mathbb{Z}_2S_4$ is also an irreducible submodule of $\mathbb{Z}_2S_3$. It is known that $\mathbb{Z}_2S_3$ has only two irreducible submodules, including the trivial one. Hence the only irreducible submodules of $\mathbb{Z}_2S_4$ are the trivial module, $\mathbb{Z}_2$, and a 2-dimensional $\mathbb{Z}_2S_3$-module, V. From Lemma 4.4 we find that $K_4 \cong \langle\alpha, \beta\rangle$, and $S_3 \cong \langle\gamma, \delta\rangle$. The action of $\langle\gamma, \delta\rangle$ on V must thereby be defined in a way that satisfies $\gamma^3 = \delta^2 = 1$. We let $V = \mathrm{Span}_{\mathbb{Z}_2}\langle v, v'\rangle$ and

$$\begin{aligned} \gamma &: \; v \mapsto v', \quad v' \mapsto v + v', \\ \delta &: \; v \mapsto v + v', \quad v' \mapsto v'. \end{aligned}$$

Our next step is to examine the inclusions of indecomposable submodules in $\mathbb{Z}_2S_4$. We make the following definition.

Definition 4.6. [1, Page 161] 1. The *socle* of a module M, denoted $\mathrm{Soc}(M)$, is the sum of all simple submodules of M.
2. The *socle-series* of M is the inclusion series

$$0 \subset \mathrm{Soc}(M) \subset \mathrm{Soc}^2(M) \subset \cdots \subset M,$$

where $\mathrm{Soc}^{i+1}(M)$ is defined by the identity $\mathrm{Soc}(M/\mathrm{Soc}^i(M)) = \mathrm{Soc}^{i+1}(M)/\mathrm{Soc}^i(M)$.

The socle series is also called the upper Loewy series. It is shown in [8, Example 15.10 a)] that the composition factors of the socle series of the ideal P_1 are given as

$$\mathrm{Soc}^{i+1}(P_1)/\mathrm{Soc}^i(P_1) \cong \begin{cases} \mathbb{Z}_2 & i=3 \\ \mathbb{Z}_2 \oplus V & \text{for } i=2 \\ \mathbb{Z}_2 \oplus V & i=1 \\ \mathbb{Z}_2 & i=0. \end{cases} \tag{7}$$

Likewise for P_2 we have

$$\mathrm{Soc}^{i+1}(P_2)/\mathrm{Soc}^i(P_2) \cong \begin{cases} V & i=3 \\ \mathbb{Z}_2 & i=2 \\ \mathbb{Z}_2 \oplus V & \text{for } i=1 \\ V & i=0. \end{cases} \tag{8}$$

We later use this to show that we have found suitable generators for the ideals in A.

Definition 4.7. [9, Chapter 11] Let G be a finite group, R a commutative ring and let M be a nonzero RG-module. Then M is called a *permutation module* if M is a free R-module and G acts as a permutation group on an R-basis of M.

The following result lays the foundation for our next chapter.

Lemma 4.8. *The extended binary Golay code $\mathcal{G}_{24}$ is a right $\mathbb{Z}_2S_4$-permutation (sub)module. In particular, $\mathcal{G}_{24}$ is a right ideal in the group algebra $\mathbb{Z}_2S_4$.*

Proof. Let $A = \mathbb{Z}_2S_4$. We first show that $\mathcal{G}_{24}$ is a A-permutation module. That is, that $\mathcal{G}_{24}$ is a A-module, a free $\mathbb{Z}_2$-module and that S_4 acts as a permutation group on an $\mathbb{Z}_2$-basis of $\mathcal{G}_{24}$.

Let $X = \{1, x, \ldots, x^{22}, x^\infty\}$. Then $\mathbb{Z}_2X = \mathrm{Span}_{\mathbb{Z}_2}X$ is by definition a free $\mathbb{Z}_2$-module with basis X, and the same holds for $\mathcal{G}_{24}$ as a submodule of $\mathbb{Z}_2X$. We know that any $g \in S_4$ is a permutation of the set $P(23) = \mathbb{F}_{23} \cup \{\infty\}$. write $g : i \mapsto i_g$. We have a bijection between X and $P(23)$ given by the correspondence

$$x^i \longleftrightarrow i.$$

Thus we can let

$$x^i \cdot g = x^{i_g}.$$

Let $a = \sum_{g \in S_4} a_g g$ where $a_g \in \mathbb{Z}_2$. Then we have

$$x^i \cdot a \;=\; x^i \left(\sum_{g \in S_4} a_g g \right) \;=\; \sum_{g \in S_4} a_g x^i g \;=\; \sum_{g \in S_4} a_g x^{i_g}.$$

Thus for some $c = \sum_{i \in P(23)} c_i x^i$ with $c_i \in \mathbb{Z}_2$ then

$$c \cdot a = \sum_{i \in P(23)} c_i \left(\sum_{g \in S_4} a_g x^{i_g} \right) = \sum_{\substack{i \in P(23) \\ g \in S_4}} (c_i a_g) x^{i_g}.$$

Thus $\mathcal{G}_{24}$ is an A-permutation module. It now remains to show that $\mathcal{G}_{24}$ can be embedded as a ideal in $\mathbb{Z}_2 S_4$. We start by defining a map

$$\begin{aligned} X &\;\to\; S_4 \\ x^0 \cdot g &\;\mapsto\; g, \end{aligned}$$

for $g \in S_4$. First we show that this map is well-defined. Suppose that $x^0 g = x^0 g'$. Then $x^0 g (g')^{-1} = x^0$. Since S_4 acts fixed point freely on $P(23)$, it also acts fixed-point freely on X. Hence the only element of S_4 keeping any x^0 fixed is 1. It follows that $g(g')^{-1} = 1$, and thus $g = g'$. Since S_4 and X also have the same number of elements, it follows that the action of S_4 is transitive. Hence for any $x^i \in X$ we can write $x^i g \mapsto g$. We then see that $\mathcal{G}_{24}$ can be identified with the submodule of $\mathbb{Z}_2 S_4$ by

$$\begin{aligned} \mathcal{G}_{24} \;\hookrightarrow\; \mathrm{Span}_{\mathbb{Z}_2} X &\;\to\; \mathbb{Z}_2 S_4 \\ x^0 \cdot g &\;\mapsto\; g. \end{aligned}$$

Thus $\mathcal{G}_{24}$ is a right ideal in $\mathbb{Z}_2 S_4$. □

4.2 The structure of $\mathcal{G}_{24}$ as an ideal in $\mathbb{Z}_2 S_4$

From now on we let $A = \mathbb{Z}_2 S_4$. We want to show that the structure of A allows for $\mathcal{G}_{24}$ to be embedded into A in such a way that $\mathcal{G}_{24}$ is an idempotent code. In order for the codewords of $\mathcal{G}_{24}$ to be written as vectors in A, we need to find a bijection between the 24 canonical basis vectors and the basis elements of $S_4 \cong \langle \alpha, \beta, \gamma, \delta \rangle$. We first need to define all generators of S_4 as permutations of $P(23)$. Remember that

$$\begin{aligned} \alpha \;=\; & (0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21) \\ & (14,18). \end{aligned}$$

There are many ways of choosing β, γ and δ that satisfy the identities given in Lemma 4.4. We here let

$$\begin{aligned}
\beta &= (0,11)(1,20)(2,\infty)(3,7)(4,16)(5,19)(6,9)(8,22)(10,17)(12,14)(13,15)\\
&\quad (18,21),\\
\gamma &= (0,18,9)(1,10,3)(2,21,5)(4,7,22)(6,\infty,12)(8,17,15)(13,20,16)\\
&\quad (11,14,19),\\
\delta &= (0,15)(1,19)(2,7)(3,11)(4,21)(5,22)(6,20)(8,9)(10,14)(12,16)(13,\infty)\\
&\quad (17,18).
\end{aligned}$$

Then multiplication in S_4 yields

$$\alpha^\gamma = \alpha\beta, \quad \alpha^\delta = \beta, \quad \beta^\gamma = \beta\delta = \alpha.$$

Thus $\langle \alpha, \beta, \gamma, \delta \rangle$ satisfies the requirements for S_4 stated in Lemma 4.4. (Note that we have defined β and γ equal to those given in [2], while our choice of δ equals $\gamma\delta$ in [2]).

We now look for a bijection between the 24 canonical basis vectors given as $x^0, \ldots, x^{22}, x^\infty$ and the 24 group elements of S_4 that identifies the result of the action of any $\pi \in S_4$ on the position of some x^i with the result of multiplying on the right by π on the element corresponding to i in S_4. Let $1 \in S_4$ correspond to x^0. Then each π in $\langle \alpha, \beta, \gamma, \delta \rangle$ can be identified with the number for which π permutes 0. We thereby have

$$\begin{array}{llll}
0 \Leftrightarrow 1, & \infty \Leftrightarrow \alpha, & 11 \Leftrightarrow \beta, & 2 \Leftrightarrow \alpha\beta,\\
18 \Leftrightarrow \gamma, & 12 \Leftrightarrow \alpha\gamma, & 14 \Leftrightarrow \beta\gamma, & 21 \Leftrightarrow \alpha\beta\gamma,\\
9 \Leftrightarrow \gamma^2, & 6 \Leftrightarrow \alpha\gamma^2, & 19 \Leftrightarrow \beta\gamma^2, & 5 \Leftrightarrow \alpha\beta\gamma^2,\\
15 \Leftrightarrow \delta, & 13 \Leftrightarrow \alpha\delta, & 3 \Leftrightarrow \beta\delta, & 7 \Leftrightarrow \alpha\beta\delta,\\
17 \Leftrightarrow \gamma\delta, & 16 \Leftrightarrow \alpha\gamma\delta, & 10 \Leftrightarrow \beta\gamma\delta, & 4 \Leftrightarrow \alpha\beta\gamma\delta,\\
8 \Leftrightarrow \gamma^2\delta, & 20 \Leftrightarrow \alpha\gamma^2\delta, & 1 \Leftrightarrow \beta\gamma^2\delta, & 22 \Leftrightarrow \alpha\beta\gamma^2\delta.
\end{array} \tag{9}$$

For some of the results in this chapter and onward we use a combination of computations in GAP and calculations by hand. In those cases we use the following bijection to identify the elements in the representation $\langle \alpha, \beta, \gamma, \delta \rangle$ with original elements in S_4.

$$\begin{array}{lll}
1 \Leftrightarrow 1, & \gamma \Leftrightarrow (2,3,4), & \gamma^2 \Leftrightarrow (2,4,3),\\
\alpha \Leftrightarrow (1,4)(2,3), & \alpha\gamma \Leftrightarrow (1,2,4), & \alpha\gamma^2 \Leftrightarrow (1,3,4),\\
\beta \Leftrightarrow (1,3)(2,4), & \beta\gamma \Leftrightarrow (1,4,3), & \beta\gamma^2 \Leftrightarrow (1,2,3),\\
\alpha\beta \Leftrightarrow (1,2)(3,4), & \alpha\beta\gamma \Leftrightarrow (1,3,2), & \alpha\beta\gamma^2 \Leftrightarrow (1,4,2),\\
\delta \Leftrightarrow (3,4), & \gamma\delta \Leftrightarrow (2,4), & \gamma^2\delta \Leftrightarrow (2,3),\\
\alpha\beta\delta \Leftrightarrow (1,2), & \beta\gamma\delta \Leftrightarrow (1,3), & \alpha\gamma^2\delta \Leftrightarrow (1,4),\\
\alpha\delta \Leftrightarrow (1,3,2,4), & \alpha\beta\gamma\delta \Leftrightarrow (1,4,3,2), & \beta\gamma^2\delta \Leftrightarrow (1,2,4,3),\\
\beta\delta \Leftrightarrow (1,4,2,3), & \alpha\gamma\delta \Leftrightarrow (1,2,3,4), & \alpha\beta\gamma^2\delta \Leftrightarrow (1,3,4,2).
\end{array}$$

The purpose of constructing $\mathcal{G}_{24}$ as an ideal in A is to give $\mathcal{G}_{24}$ a structure so it can be generated by a sum of idempotents. In order to understand this structure thoroughly we look at the embedding of $\mathcal{G}_{24}$ in relation to the decomposition of A as given by Lemma 4.5. Now let $e_1 = 1 + \gamma + \gamma^2$ and $P_1 = e_1 A$. Also let $S = \langle \alpha, \beta, \delta \rangle$ ($\cong S_4/\langle \gamma \rangle$). Since $e_1\gamma = \gamma e_1 = e_1$, the dimension of P_1 is the same as that of $|S| = 2^3 = 8$. We find that P_1 can be spanned by

$$\begin{aligned}
v_1 &= e_1 \sum_{g \in S} g, \\
v_2 &= e_1(1 + \alpha + \beta + \alpha\beta), \\
v_3 &= e_1(1 + \alpha + \delta + \alpha\beta\delta), \\
v_4 &= v_3\gamma = e_1(1 + \alpha\beta + \delta + \alpha\delta), \\
v_5 &= e_1(1 + \beta + \delta + \alpha\delta), \\
v_6 &= v_1\gamma = e_1(1 + \alpha + \delta + \beta\delta), \\
v_7 &= e_1(1 + \delta), \\
v_8 &= e_1.
\end{aligned}$$

We outline in Appendix 7.2 how $v_1, \ldots, v_8$ span indecomposable submodules of P_1, and that this yields the same composition factors as those stated by (7). Note that the socle of P_1 is 1-dimensional and spanned by v_1. In particular, since v_1 corresponds to the all-one codeword, then $v_1 \in \mathcal{G}_{24}$. Further examination confirms that we have $v_2, v_3, v_4 \in \mathcal{G}_{24}$ as well. We find that

$$M_1 = \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2, v_3, v_4\},$$

is an indecomposable submodule of P_1 (See Appendix 7.2). Here the maximum proper indecomposable submodule of M_1 is $\mathrm{Span}\{v_1, v_2\}$. In particular, since $v_3\gamma = v_3\delta = v_4$, $v_4\gamma = v_4 + v_3 + v_1$ and $v_4\delta = v_3$, it follows that

$$M_1/\mathrm{Span}\{v_1, v_2\} \cong V.$$

Note that then v_3 and v_4 are both generators for M_1.

Altogether, we find that the composition factors of the socle series of M_1 can be given as

$$\mathrm{Soc}^{i+1}(M_1)/\mathrm{Soc}^{i}(M_1) \cong \begin{cases} V & i = 2 \\ \mathbb{Z}_2 \quad \text{for} & i = 1 \\ \mathbb{Z}_2 & i = 0. \end{cases}$$

This shows that M_1 has dimension 4. Now in order to generate the 12-dimensional module that is $\mathcal{G}_{24}$, we look for some 8-dimensional module that is contained in $\mathcal{G}_{24}$ but disjoint with P_1. We know that any primitive idempotent in $\mathcal{G}_{24}$ generates an ideal that is exactly 8-dimensional. This follows from $\mathcal{G}_{24}$ being 12-dimensional and that A is a disjoint sum of 8-dimensional ideals so any ideal generated by an idempotent in A must have dimension divisible by 8. We have confirmed by computation that there are exactly 64 non-zero idempotents in

$\mathcal{G}_{24}$. We are looking for an idempotent that is orthogonal with e_1. One such idempotent is

$$e_2 \;=\; 1+\gamma+\alpha\gamma\delta+\beta\gamma\delta+\alpha\beta\gamma\delta+\alpha\gamma^2\delta+\beta\gamma^2\delta+\alpha\beta\gamma^2\delta.$$

as given in [2]. That is, we have $e_2 \in \mathcal{G}_{24}$, $e_2 = e_2^2$, and $e_1e_2 = e_2e_1 = 0$. We let $P_2 = e_2A$. It follows that

$$\mathcal{G}_{24} \;\cong\; M_1 \oplus P_2. \tag{10}$$

We find that the following list of vectors span P_2.

$$\begin{aligned}
w_1 &= e_2(1+\alpha+\beta+\alpha\beta),\\
w_2 &= w_1\gamma \;=\; e_2(\delta+\alpha\delta+\beta\delta+\alpha\beta\delta),\\
w_3 &= e_2(1+\alpha+\delta+\alpha\delta),\\
w_4 &= e_2(1+\alpha\beta+\delta+\beta\delta),\\
w_5 &= e_2(1+\alpha\beta+\delta+\alpha\delta),\\
w_6 &= w_5\gamma \;=\; e_2(1+\alpha+\alpha\delta+\beta\delta),\\
w_7 &= e_2(\alpha+\beta+\alpha\beta),\\
w_8 &= w_7\gamma \;=\; e_2\delta.
\end{aligned}$$

The detailed structure of the submodules of P_2 as spanned by $w_1,\ldots,w_8$ is outlined in Appendix 7.3. We note here that w_7 and w_8 are both generators for P_2. In particular we find that $v_4w_7 = w_7v_4 = 0$ and $v_3w_8 = w_8v_3 = 0$. So it follows from (10) that

$$\mathcal{G}_{24} \;\cong\; (v_4+w_7)A \;\cong\; (v_3+w_8)A.$$

Hence $\mathcal{G}_{24}$ is principal and has at least two generators. However, we want to find a generator for $\mathcal{G}_{24}$ that is also a sum of idempotents. We first look at the following idempotent that is given in [2]).

$$e' \;=\; 1+\alpha\beta\gamma+\alpha\gamma^2+\alpha\beta\gamma^2+\alpha\delta+\alpha\beta\delta+\gamma\delta+\alpha\beta\gamma^2\delta.$$

Our calculations confirm that e' is an idempotent and that $e' \in \mathcal{G}_{24}$. Moreover, we find that $(e_1+e_2)e' = e'$ and $e_1e' = v_3$. Thus $M_1 \subseteq e'A \subseteq \mathcal{G}_{24}$, It thereby follows that

$$e'A + e_2A \;\cong\; M_1 \oplus P_2 \;\cong\; \mathcal{G}_{24},$$

as stated by Lemma 2.5 in [2].

Now, the article also claims that $f = e' + e_2$ generates a 12-dimensional ideal, thus is equal to $\mathcal{G}_{24}$. We however find that

$$\begin{aligned}
f' &= e'+e_2\\
&= (e_1+e_2)e'+e_2\\
&= e_1e'+e_2(e'+1)\\
&= e_1(1+\alpha+\delta+\alpha\beta\delta)+e_2(1+\alpha+\delta+\alpha\delta)\\
&= v_3+w_3.
\end{aligned}$$

It turns out that w_3A is in fact 3-dimensional, which suggests that $f'A$ is 7-dimensional. We have confirmed both by multiplication on the right of f' with elements in S_4, and by computer calculation, that this is in fact the case. So $f'A$ is properly contained $\mathcal{G}_{24}$, but f' is not a generator for $\mathcal{G}_{24}$.

However, our computations show that such idempotents do exist. In fact, we find that there are a total of 16 idempotents in $\mathcal{G}_{24}$ with the property that when adding e_2 to that idempotent yields a generator for $M_1 \oplus P_2$. The shortest one is

$$e = 1 + \alpha + \alpha\beta + \beta\gamma + \alpha\beta\gamma + \beta\gamma^2 + \delta + \alpha\gamma^2\delta.$$

Calculations show that $e_1 e = v_3 + v_4$, and $(e_1 + e_2)e = e$, which confirms that $\mathcal{G}_{24} \cong eA + e_2A$. Now let

$$\begin{aligned} f &= e + e_2 \\ &= \alpha + \alpha\beta + \gamma + \beta\gamma + \alpha\beta\gamma + \beta\gamma^2 + \delta + \alpha\gamma\delta + \beta\gamma\delta + \alpha\beta\gamma\delta + \beta\gamma^2\delta + \alpha\beta\gamma^2\delta. \end{aligned}$$

Further evaluation of f shows that

$$\begin{aligned} f &= (e_1 + e_2)e + e_2 \\ &= e_1 e + e_2(1 + e) \\ &= e_1(1 + \beta + \delta + \beta\delta) + e_2(1 + \alpha + \beta + \alpha\beta + \beta\delta) \\ &= v_1 + v_3 + v_4 + w_1 + w_3 + w_6 + w_8. \end{aligned}$$

We find that f generates $v_1, \ldots, v_4, w_1, \ldots, w_8$, the details of this argument are found in Appendix 7.4. This shows that $\mathcal{G}_{24} \subseteq fA$. We thereby conclude that

$$fA \cong \mathcal{G}_{24}.$$

Computations in GAP confirm that fA is indeed 12-dimensional.

4.3 Decoding $\mathcal{G}_{24}$

We will now show how to decode codewords in $\mathcal{G}_{24}$ using the method introduced in Chapter 3. The following arguments are also given in [2, Section 4.3(a)]. For an arbitrary codeword $c \in \mathcal{G}_{24}$, let $c' = c + \Delta$ be the received codeword with error Δ. Since $\mathcal{G}_{24}$ is 3-error correcting, we assume that Δ has weight at most 3. It then follows from Lemma 3.9 that $\tau(e)c = 0 = \tau(e_2)c$. Hence we have $\tau(e)c' = \tau(e)\Delta$ and $\tau(e_2)c' = \tau(e_2)\Delta$. Knowing what these idempotent look like we can uniquely determine Δ and thereby find c. We here have that

$$\begin{aligned} \tau(e_2) &= 1 + \gamma^2 + \alpha\gamma\delta + \beta\gamma\delta + \alpha\beta\gamma\delta + \alpha\gamma^2\delta + \beta\gamma^2\delta + \alpha\beta\gamma^2\delta \\ \tau(e) &= 1 + \alpha + \alpha\beta + \alpha\beta\gamma + \alpha\gamma^2 + \beta\gamma^2 + \delta + \alpha\gamma^2\delta. \end{aligned}$$

This gives us all the information we need to decode a received codeword from $\mathcal{G}_{24}$.

5 The endomorphism ring of $\mathbb{Z}_2 S_4$

We have established that $\mathcal{G}_{24}$ is an ideal in the group algebra $A = \mathbb{Z}_2 S_4$. A group algebra comes with a lot of structure and further exploration into the structural properties of A may offer a new and better understanding of $\mathcal{G}_{24}$. The results outlined in this chapter are based on the following lemma, showing that the ring of endomorphisms of A as an A-module offers a further decomposition of A.

Lemma 5.1. *As rings, there is an isomorphism*

$$A^{\mathrm{op}} \cong \begin{bmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ B_{2,1} & B_{2,2} & B_{2,3} \\ B_{3,1} & B_{3,1} & B_{3,3} \end{bmatrix} \text{ where } B_{i,j} = e_i A e_j.$$

Proof. We know that $A \cong (\mathrm{End}_A A)^{\mathrm{op}}$, meaning that

$$A^{\mathrm{op}} \cong \mathrm{End}_A A \cong \mathrm{Hom}_A(A, A).$$

Since A is a direct sum of indecomposable modules with $A \cong P_1 \oplus P_2 \oplus P_3$ with $P_i = e_i A$, we have a general result [3, Chapter 19, Theorem 1.1] saying that

$$\begin{aligned} \mathrm{Hom}_A(A, A) &\cong \mathrm{Hom}_A(e_1A \oplus e_2A \oplus e_3A, e_1A \oplus e_2A \oplus e_3A) \\ &\cong \begin{bmatrix} \mathrm{Hom}_A(e_1A, e_1A) & \mathrm{Hom}_A(e_2A, e_1A) & \mathrm{Hom}_A(e_3A, e_1A) \\ \mathrm{Hom}_A(e_1A, e_2A) & \mathrm{Hom}_A(e_2A, e_2A) & \mathrm{Hom}_A(e_3A, e_2A) \\ \mathrm{Hom}_A(e_1A, e_3A) & \mathrm{Hom}_A(e_2A, e_3A) & \mathrm{Hom}_A(e_3A, e_3A) \end{bmatrix}. \end{aligned}$$

But we have $\mathrm{Hom}_A(e_jA, e_iA) = e_i A e_j$, hence the Lemma holds. □

From Lemma 5.1, let $\mathcal{M}_A$ denote the given matrix ring, and from the isomorphism given in Lemma 5.1 we obtain the isomorphism $\varphi : A \to \mathcal{M}_A$ for which

$$\varphi(a) = \begin{pmatrix} e_1ae_1 & e_1ae_2 & e_1ae_3 \\ e_2ae_1 & e_2ae_2 & e_2ae_3 \\ e_3ae_1 & e_3ae_2 & e_3ae_3 \end{pmatrix}.$$

Since $e_1 + e_2 + e_3 = 1$ and thereby $A = (e_1 + e_2 + e_3)A(e_1 + e_2 + e_3)$, we have

$$A \cong \bigoplus_{i,j=1}^{3} B_{i,j}.$$

From computations in GAP, we find that the dimension of each of the entries in $\mathcal{A}$ is as illustrated by the matrix

$$\begin{bmatrix} 4 & 2 & 2 \\ 2 & 3 & 3 \\ 2 & 3 & 3 \end{bmatrix}. \tag{11}$$

In order to find a suitable embedding of $\mathcal{G}_{24}$, we need to find basis elements for each of the entries $B_{i,j}$ of $\mathcal{M}_A$. We just saw in the proof of Lemma 5.1 that each right submodule P_i in Lemma 4.5 corresponds to a row of $\mathcal{M}_A$. That is,

$$P_i \;\cong\; e_iA \;\cong\; B_{i,1} \oplus B_{i,2} \oplus B_{i,3}.$$

Likewise, the columns in $\mathcal{M}_A$ provide a similar decomposition of A into left ideals. Thus $A \cong I_1 \oplus I_2 \oplus I_3$ where I_j are indecomposable left ideals and

$$I_j \;\cong\; Ae_j \;\cong\; B_{1,j} \oplus B_{2,j} \oplus B_{3,j}.$$

Note that $A_i = B_{i,i}$ is an algebra for all $i = 1, 2, 3$ since

$$A_i \;=\; e_iAe_i \;=\; \mathrm{Hom}_A(e_iA, e_iA) \;=\; \mathrm{End}_A(e_iA).$$

We let $P_1 = e_1A$ and $P_2 = e_2A$ be defined by the same idempotent generators as in Section 4.2. Then the last row of $\mathcal{M}_A$ corresponds to the ideal $P_3 = e_3A$ with

$$\begin{aligned} e_3 \;&=\; 1 - (e_1 + e_2) \\ &=\; 1 + \gamma^2 + \alpha\gamma\delta + \beta\gamma\delta + \alpha\beta\gamma\delta + \alpha\gamma^2\delta + \beta\gamma^2\delta + \alpha\beta\gamma^2\delta. \end{aligned}$$

As a consequence of how the e_i's and the group generators have been chosen, we find that, for any $b = \sum_{g\in S_4} b_g g \in B_{i,j}$ where $b_g \in \mathbb{Z}_2$ and $i = 1, 2, 3$, we can write

$$b \;=\; e_id \;=\; de_j \qquad \text{where} \quad d \;=\; \sum_{g\in S} d_g g, \;\; d_g \in \mathbb{Z}_2, \;\; S = \langle \alpha, \beta, \delta \rangle.$$

Now remember that we defined τ as the antipode of A. That is, for $a = \sum_{g\in S_4} a_g g$ then

$$\tau(a) \;=\; \sum_{g\in S_4} a_g g^{-1},$$

where $\tau(\tau(a)) = a$ and $\tau(aa') = \tau(a')\tau(a)$. For $b \in B_{i,j}$ in particular we then have

$$\tau(b) \;=\; \tau(e_ide_j) \;=\; \tau(e_j)\tau(d)\tau(e_i).$$

In general, we see that

$$\tau(B_{i,j}) \;=\; \tau(e_iAe_j) \;=\; \tau(e_j)\tau(A)\tau(e_i) \;=\; \tau(e_j)A\tau(e_i).$$

We see that $\tau(e_2) = e_3$ from Section 4.3. Then $\tau(e_3) = e_2$ as well. We also see that $\tau(e_1) = e_1$. Altogether it follows that

$$\mathcal{M}_A \;\cong\; \begin{bmatrix} B_{1,1} & B_{1,2} & \tau(B_{2,1}) \\ B_{2,1} & B_{2,2} & B_{2,3} \\ \tau(B_{1,2}) & B_{3,2} & \tau(B_{2,2}) \end{bmatrix}.$$

In particular, if $h = 1 - e_3 = e_1 + e_2$ and $h' = \tau(h) = e_1 + e_3$ we have

$$\begin{aligned}
\tau(hAh) &\cong \tau(hAe_1 \oplus hAe_2) \\
&\cong \tau(hAe_1) \oplus \tau(hAe_2) \\
&\cong \tau(e_1)\tau(A)\tau(h) \oplus \tau(e_2)\tau(A)\tau(h) \\
&\cong e_1Ah' \oplus e_3Ah' \\
&\cong h'Ah'.
\end{aligned}$$

Since $A \cong e_1A \oplus e_2A \oplus e_3A$ and $e_3A \cong e_2A$, then there is a quiver with relations (Γ, ρ) such that $\Lambda = \mathbb{Z}_2\Gamma/\langle\rho\rangle \cong hAh$. We find that

$$\Gamma: \quad a_1 \circlearrowright 1 \underset{a_3}{\overset{a_2}{\rightleftarrows}} 2 \circlearrowright a_4 \quad .$$

Letting e_1 and e_2 be trivial paths, we find, by a combination of calculations by hand and computations in QPA, that the arrows in Γ can be given as

$$\begin{aligned}
a_1 &= e_1(1 + \delta) && \in A_1, \\
a_2 &= e_1(\alpha + \beta + \alpha\delta + \alpha\beta\delta) && \in B_{1,2}, \\
a_3 &= e_2(\alpha + \beta + \alpha\delta + \alpha\beta\delta) && \in B_{2,1}, \\
a_4 &= e_2(\alpha + \beta + \beta\delta + \alpha\beta\delta) && \in A_2.
\end{aligned}$$

We can now determine the relations and remaining nonzero paths in Λ from calculation by hand. We find that the set relations in Λ can be given as

$$\begin{aligned}
\rho = \{&a_1^2,\ a_2a_4,\ a_4a_3,\ a_2a_3a_2,\ a_3a_2a_3,\ a_4^3, \\
&a_3a_2 + a_4^2,\ a_3a_1a_2 + a_4^2,\ a_1a_2a_3 + a_2a_3a_1\}.
\end{aligned}$$

On the other hand, if $\Lambda' = \mathbb{Z}_2\Gamma'/\langle\rho'\rangle$ where $\rho' = \tau(\rho)$ and

$$\Gamma': \quad \tau(a_1) \circlearrowright 1 \underset{\tau(a_2)}{\overset{\tau(a_3)}{\rightleftarrows}} 3 \circlearrowright \tau(a_4) \quad ,$$

it follows that $\Lambda' \cong h'Ah'$. Note that $\tau(a_1) = a_1$. The remaining arrows can be given as

$$\begin{aligned}
\tau(a_2) &= e_3(\alpha + \beta + \beta\delta + \alpha\beta\delta) && \in B_{3,1}, \\
\tau(a_3) &= e_1(\alpha + \beta + \beta\delta + \alpha\beta\delta) && \in B_{1,3}, \\
\tau(a_4) &= e_3(\alpha + \beta + \alpha\delta + \alpha\beta\delta) && \in A_3.
\end{aligned}$$

Given the set of relations in ρ, we find that the remaining nonzero basis elements

in A_1, $B_{1,2}$, $B_{2,1}$ and A_2 are the paths

$$\begin{aligned} a_2a_3 &= e_1(1+\alpha+\beta+\alpha\beta), \quad a_1a_2a_3 = \sum_{g\in S_4} g, \\ a_1a_2 &= e_1(\alpha+\alpha\beta+\beta\delta+\alpha\beta\delta), \\ a_3a_1 &= e_2(\beta+\alpha\beta+\beta\delta+\alpha\beta\delta), \\ a_4^2 &= e_2(1+\alpha+\beta+\alpha\beta). \end{aligned}$$

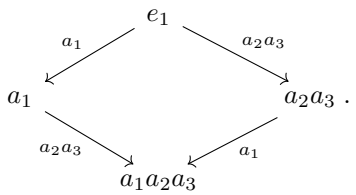
Similarly, for Λ', the remaining basis elements in $B_{1,3}$, $B_{3,1}$ and $B_{3,3}$ can be defined as the antipode of the nonzero paths in Λ. We have

$$\begin{aligned} a_1\tau(a_3) &= \tau(a_3a_1) = e_1(\beta+\alpha\beta+\alpha\delta+\alpha\beta\delta), \\ \tau(a_2)a_1 &= \tau(a_1a_2) = e_3(\alpha+\alpha\beta+\alpha\delta+\alpha\beta\delta), \\ \tau(a_4)^2 &= \tau(a_4^2) = e_3(1+\alpha+\beta+\alpha\beta). \end{aligned}$$

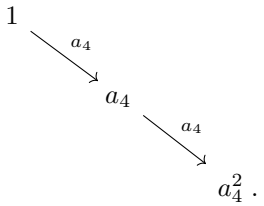
Note that the paths that are elements in A_1 can be equally defined as the products of paths in $B_{1,3}$ and $B_{3,1}$. Here

$$\begin{aligned} \tau(a_3)\tau(a_2) &= \tau(a_2a_3) = a_2a_3 \\ \tau(a_3a_1)\tau(a_2) &= \tau(a_3)\tau(a_1a_2) = \tau(a_1a_2a_3) = a_1a_2a_3. \end{aligned}$$

We see that $U = \{e_1, a_1, a_2a_3, a_1a_2a_3\}$ can be given as a basis for A_1. Thus A_1 has two generators, here a_1 and a_2a_3. From ρ, we see that $a_1^2 = 0$, $(a_2a_3)^2 = 0$ and $a_1a_2a_3 = a_3a_2a_1$. Hence a basis of A_1 can be illustrated as



As for the algebra A_2, we see that $W = \{e_2, a_4, a_4^2\}$ is a basis and a_4 a single generator. Similarly, A_3 is spanned by $\tau(W) = \{\tau(e_2), \tau(a_4), \tau(a_4^2)\}$ with generator $\tau(a_4)$. Here we have



It remains to say something about the nature of elements in the modules $B_{2,3}$ and $B_{3,2}$. We observe that $\tau(e_2) = e_3 = \delta e_2 \delta$ in A_3. Thus $e_2\delta = \delta e_3 \in B_{2,3}$ and

$e_3\delta = \delta e_2 \in B_{3,2}$. Hence a basis for $B_{2,3}$ can be given as $W\delta = \{e_2\delta, a_4\delta, \delta a_4^2\}$. Likewise, we have that $\delta W = \{\delta e_2, \delta a_4, \delta a_4^2\}$ is a basis for $B_{3,2}$. We calculate

$$\begin{aligned} a_4\delta &= e_2(\beta + \alpha\beta + \alpha\delta + \beta\delta), \quad & a_4^2\delta &= e_2(\delta + \alpha\delta + \beta\delta + \alpha\beta\delta), \\ \delta a_4 &= e_3(\alpha + \alpha\beta + \alpha\delta + \beta\delta), \quad & \delta a_4^2 &= e_3(\delta + \alpha\delta + \beta\delta + \alpha\beta\delta). \end{aligned}$$

Now let $U_1 = \{e_1, a_1\} \subseteq U$. Then every $\tau(a) \in A$ can be given as a sum of elements from the entries of the subset of $\mathcal{M}_A$ given as

$$\begin{bmatrix} U & U_1a_2 & U_1\tau(a_3) \\ a_3U_1 & W & W\delta \\ \tau(a_2)U_1 & \delta W & \tau(W) \end{bmatrix}. \tag{12}$$

In general multiplication in $\mathcal{M}_A$ is defined as the collection of all maps of the form

$$\begin{aligned} B_{i,k} \otimes B_{k,j} &\to B_{i,j} \\ b \otimes b' &\mapsto bb', \end{aligned} \tag{13}$$

where $i, j, k = 1, 2, 3$. We see that each of the nine modules $B_{i,j}$ is the codomain of exactly three of these maps for $k = 1, 2, 3$, respectively. Hence (13) defines a total of 27 different mappings for various values of i, j, k. However, we do not need to examine all these separately. We see that most of these operations follow from what we have already found about concatenation of arrows into paths in Λ and Λ'. However, we make some final notes regarding those maps that do not involve any of the algebras. We see that $B_{2,1} \otimes B_{1,3} \to B_{2,3}$ and $B_{3,1} \otimes B_{1,2} \to B_{3,2}$ yield

$$\begin{aligned} a_3\tau(a_3) &= 0, \quad & a_3\tau(a_3a_1) &= a_3a_1\tau(a_3) = a_4^2\delta, \\ \tau(a_2)a_2 &= 0, \quad & \tau(a_1a_2)a_2 &= \tau(a_2)a_1a_2 = \delta a_4^2. \end{aligned}$$

It may also be useful to note that for $B_{1,2} \otimes B_{2,3} \to B_{1,3}$, $B_{2,3} \otimes B_{3,1} \to B_{2,1}$, $B_{3,2} \otimes B_{2,1} \to B_{1,3}$ and $B_{1,3} \otimes B_{3,2} \to B_{1,2}$ we have

$$\begin{aligned} a_2\delta &= \tau(a_3) + \tau(a_3a_1) \iff \delta\tau(a_2) = \tau(a_2\delta) = a_3 + a_3a_1, \\ \delta a_3 &= \tau(a_2) + \tau(a_1a_2) \iff \tau(a_3)\delta = \tau(\delta a_3) = a_2 + a_1a_2. \end{aligned}$$

We should now have provided a good understanding of how multiplication in $\mathcal{M}_A$ works.

The action of S_4 on $\mathcal{M}_A$ is given by the multiplication on the right by $\varphi(g)$

for $g \in S_4$. The group generators from A in $\mathcal{M}_A$ can be given as

$$\begin{aligned}
\varphi(\alpha) &= \begin{pmatrix} e_1 + a_2a_3 & a_1a_2 & \tau(a_3) \\ a_3 & e_2 + a_4 + a_4^2 & a_4\delta \\ \tau(a_1a_2) & 0 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix}, \\
\varphi(\beta) &= \begin{pmatrix} e_1 + a_2a_3 & a_2 & \tau(a_3a_1) \\ a_3a_1 & e_2 + a_4 + a_4^2 & 0 \\ \tau(a_2) & \delta a_4 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix}, \\
\varphi(\gamma) &= \begin{pmatrix} e_1 & 0 & 0 \\ 0 & 0 & (e_2 + a_4^2)\delta \\ 0 & \delta(e_2 + a_4^2) & e_3 \end{pmatrix}, \\
\varphi(\delta) &= \begin{pmatrix} e_1 + a_1 & 0 & 0 \\ 0 & 0 & e_2\delta \\ 0 & \delta e_2 & 0 \end{pmatrix},
\end{aligned}$$

which defines our group basis in $\mathcal{M}_A$. The image of all 24 elements in S_4 under φ is listed in Appendix 7.5.

5.1 Embedding of $\mathcal{G}_{24}$

We are looking for a suitable basis for $\mathcal{G}_{24}$ in $\mathcal{M}_A$. We saw earlier that $\mathcal{G}_{24}$ was spanned by $v_1, \ldots, v_4 \in P_1$ and $w_1, \ldots, w_8 \in P_2$. Given that $v_1, \ldots v_4$ span the module M_1, and since v_1 generates the socle of P_1, we find that

$$\varphi(v_1) = \begin{pmatrix} a_1a_2a_3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_2) = \begin{pmatrix} a_2a_3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\varphi(v_3 + v_1) = \begin{pmatrix} 0 & a_2 + a_1a_2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_4 + v_1) = \begin{pmatrix} 0 & 0 & \tau(a_3) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

is a basis for $\varphi(M_1)$. Likewise we see that $\varphi(P_2)$ is spanned by

$$\begin{aligned}
\varphi(a_3a_1) &= \begin{pmatrix} 0 & 0 & 0 \\ a_3a_1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & \varphi(a_3) &= \begin{pmatrix} 0 & 0 & 0 \\ a_3 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\
\varphi(a_4^2) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_4^2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & \varphi(a_4^2\delta) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_4^2\delta \\ 0 & 0 & 0 \end{pmatrix}, \\
\varphi(a_4) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_4 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & \varphi(a_4\delta) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_4\delta \\ 0 & 0 & 0 \end{pmatrix}, \\
\varphi(e_2) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & e_2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, & \varphi(e_2\delta) &= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & e_2\delta \\ 0 & 0 & 0 \end{pmatrix}.
\end{aligned}$$

For the details we refer to Appendix 7.6. It now follows that an arbitrary element in $u \in \mathcal{G}_{24}$ can be written on the form

$$\tau(u) = \begin{pmatrix} c_1a_1a_2a_3 + c_2a_2a_3 & c_3(a_2 + a_1a_2) & c_3\tau(a_3) \\ c_5a_3a_1 + c_6a_3 & c_7 + c_8a_4 + c_9a_4^2 & c_{10}\delta + c_{11}a_4\delta + c_{12}a_4^2\delta \\ 0 & 0 & 0 \end{pmatrix}.$$

Note that, since e_1 has weight 3 and the codewords in $\mathcal{G}_{24}$ have weight 8, 12, 16 or 24, then any codeword in $\mathcal{G}_{24}$ contained in either the first row or column of $\mathcal{M}_A$ has weight divisible by 3. That is, it either corresponds to $v_1 = a_1a_2a_3$, or has weight 12.

Now that we have defined a way to express any $c \in \mathcal{G}_{24}$ inside $\mathcal{M}_A$, we can also determine how decoding looks like.

5.1.1 Decoding in $\mathcal{M}_A$

We now check that decoding works as intended in $\mathcal{M}_A$. For $f = e + e_2$ as a generating element for $\mathcal{G}_{24}$ we have

$$\varphi(f) = \begin{pmatrix} 0 & a_2 + a_1a_2 & \tau(a_3) \\ a_3a_1 & a_4^2 & (e_2 + a_4 + a_4^2)\delta \\ 0 & 0 & 0 \end{pmatrix}.$$

Then the idempotent e embedded in $\mathcal{M}_A$ can be given as

$$\varphi(e) = \varphi(f + e_2) = \varphi(f) + \varphi(e_2).$$

In order to decode in $\mathcal{M}_A$ we need to determine the antipodes of the idempotents e and e_3. Mapping $\tau(e)$ into $\mathcal{M}_A$ yields

$$\varphi(\tau(e)) = \begin{pmatrix} a_1a_2a_3 & 0 & \tau(a_3a_1) \\ a_3 & 0 & e_2\delta + a_4\delta + a_4^2\delta \\ \tau(a_2 + a_1a_2) & 0 & \tau(e_2 + a_4^2) \end{pmatrix}.$$

We now check that $\tau(e)c = 0$ in A implies that $\varphi(\tau(e)c) = 0$ in $\mathcal{M}_A$ for some arbitrary codeword $c \in \mathcal{G}_{24} \subseteq A$. Consider the word c_1 as defined in (6). From (9), we find that the corresponding vector in A is

$$c_1 = 1 + \beta + \gamma + \alpha\gamma + \alpha\beta\gamma + \alpha\gamma^2 + \delta + \alpha\gamma\delta + \gamma^2\delta + \alpha\gamma^2\delta + \beta\gamma^2\delta + \alpha\beta\gamma^2\delta.$$

Calculations yield that in $\mathcal{M}_A$ we have

$$\varphi(c) = \begin{pmatrix} 0 & a_2 + a_1a_2 & 0 \\ a_3a_1 & a_4 + a_4^2 & e_2\delta + a_4^2\delta \\ 0 & 0 & 0 \end{pmatrix}.$$

We see that $\varphi(\tau(e)) \cdot \varphi(c) = 0$. Now let $c' = c + \Delta$ be some received codeword with error Δ of weight at most 3. Since $\varphi(c') = \varphi(c) + \varphi(\Delta)$ then

$$\varphi(\tau(e)) \cdot \varphi(c') = \varphi(\tau(e)) \cdot \varphi(\Delta) = \varphi(\tau(e)\Delta),$$

in $\mathcal{M}_A$.

6 Constructing new codes

We want to see if we can start with the decomposition of some group algebra and from there find an ideal within this new algebra that is an error-correcting code. We here try two different cases or strategies. In the first, we begin with the endomorphism ring $\mathcal{M}'_A$ of some unidentified algebra A', for which we assume that $\mathcal{M}'_A$ is a 3×3 - matrix, but with entries of twice the dimensions as that in $\mathcal{M}_A$. In the second case we consider groups of twice the dimension as that of S_4, that is $2 \cdot 24 = 48$, in order to find a group algebra with similar decomposition as A.

For the first case we suppose A is some algebra with the same block decomposition as in Lemma 4.5 such that the ring of endomorphisms of A' as a module over itself is a 3×3 matrix ring

$$\mathcal{M}_{A'} = \begin{bmatrix} A'_1 & B'_{1.2} & B'_{1.3} \\ B'_{2.1} & A'_2 & B'_{2.3} \\ B'_{3.1} & B'_{3.2} & A'_3 \end{bmatrix}.$$

We assume that the dimensions of all entries of $\mathcal{M}_{A'}$ is twice of that given in (11). We then have

$$|\mathcal{M}_{A'}| = \begin{bmatrix} 8 & 4 & 4 \\ 4 & 6 & 6 \\ 4 & 6 & 6 \end{bmatrix}. \tag{14}$$

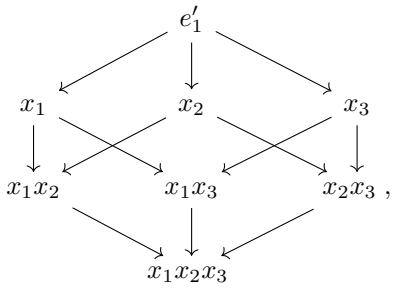
We now approach the problem by choosing possible structures for the algebras A'_i given that these are algebras of twice the dimensions of the A_is in $A = \mathbb{Z}_2 S_4$ in the previous chapter. We saw that the algebra A_1 had 2 generators for a basis of size $4 = 2^2$. Since A'_1 has dimension $8 = 2^3$, we let A'_1 be an algebra spanned by a basis with 3 generators, and with similar relations as for A_1. That is, we suppose that

$$A'_1 \cong \mathbb{Z}_2[x_1, x_2, x_3]/(r),$$

where

$$r = \{x_1^2, x_2^2, x_3^2, x_1x_2 + x_2x_1, x_1x_3 + x_3x_1, x_2x_3 + x_3x_2\}.$$

If so, then we have three vectors x_1, x_2 and x_3 in A'_1, that generate a basis X for A_1 as illustrated by the diagram



where e_1 is an idempotent generator for the submodule of A corresponding to the first row in $\mathcal{M}'_A$ for A'_1. Similarly, since 6 is not the power of a smaller natural number, we let for A'_2 and A'_3 be 6-dimensional algebras with a single generator, that is

$$A'_2 \;\cong\; A'_3 \;\cong\; \mathbb{Z}_2[y]/(y^6).$$

Let $Y = \{e'_2, y, y^2, \dots y^5\}$ define a basis for A'_2, and $Z = \{e'_2, z, z^2, \dots z^5\}$ a basis for A'_3. We suppose that a basis for $B_{1,2}$ can be defined by some $b \in B_{1,2}$ over a subset of X with four elements, say $X_2 = \{e'_1, x_1, x_2, x_1x_2\}$. Then altogether, a basis $\mathcal{M}_A$ could be given as

$$\begin{bmatrix} X & X_2b_1 & X_2b_2 \\ b_3X_2 & Y & \nu(Y) \\ b_4X_2 & \nu(Z) & Z \end{bmatrix},$$

where ν is some automorphism in A'. Let $X_1 = \{e'_1, x_1\}$. Given what we know about $\mathcal{G}_{24}$ from the previous section we suggest that a possible code in A could be that which is spanned by the sets in

$$\begin{bmatrix} X - X_2 & X_1b_1 & X_1b_2 \\ b_3X_2 & Y & \nu(Y) \\ 0 & 0 & 0 \end{bmatrix}.$$

for $b_1 \in B'_{1,2}$ and $b_2 \in B'_{1,3}$, $b_3 \in B'_{1,2}$ and $b_4 \in B'_{1,3}$, where $0 \neq b_1b_3 \in X$. If e'_2 has weight 16, it is reasonable to suggest that this would also be the minimal weight of the code. However, we see that there is not an obvious way to go from this construction to thereby find a set of generators that could be identified with a set canonical basis vectors for a code.

Instead, we choose another approach. We start by looking for a group G such that if $\tilde{A} = FG$ for some field F then $\mathcal{M}_{\tilde{A}}$ satisfies (14). Since we are looking for a (non-abelian) group that is the basis of a 48-dimensional group algebra, a natural place to begin is with groups of order 48 over $\mathbb{Z}_2$. We use GAP to look for groups with the property that

$$\mathbb{Z}_2G/\mathrm{rad}(\mathbb{Z}_2G) \;\cong\; \mathbb{Z}_2 \oplus M_2(\mathbb{Z}_2). \tag{15}$$

In total, there are 5 abelian and 47 non-abelian groups of dimension 48 size. When evaluating their decomposition as algebras over $\mathbb{Z}_2$, our output was somewhat inconsistent as to how many of these algebras that satisfy (15). It seems however, that one such algebra is that with group basis the *binary octahedral group*, denoted $2O$ [4, Chapter 6.5]. This group can be represented as

$$2O \;\cong\; \langle r, s, t, \mid\; r^2 = s^3 = t^4 = rst \rangle,$$

where $(rst)^2 = 1$. It follows that $r = st$ and $t^3 = rs$. Moreover, $s^2 = tr$.

Altogether the different group elements of $2O$ can be listed as

$$\begin{array}{llllllll}
e, & t, & t^2, & t^3, & r^2, & t^5, & t^6, & t^7, \\
s, & r, & st^2, & st^3, & s^4, & s^4t, & s^4t^2, & s^4t^3, \\
s^2, & s^2t, & s^2t^2, & t^5s, & s^5, & s^5t, & s^5t^2, & ts, \\
t^2s, & ts^2, & ts^2t, & ts^2t^2, & t^6s, & t^5s^2, & t^5s^2t, & t^5s^2t^2, \\
st^2s, & t^3s, & t^2s^2, & t^2s^2t, & s^4t^2s. & t^7s, & t^6s^2, & t^6s^2t, \\
s^2t^2s, & st^3s, & st^2s^2, & st^2s^2t, & s^5t^2s, & s^4t^3s, & s^4t^2s^2, & s^4t^2s^2t.
\end{array}$$

Now let $\tilde{A} = \mathbb{Z}_2 2O$. Given that (15) holds for $\tilde{A}$, then $\tilde{A}$ has a subalgebra that corresponds to the representation of some quiver with relation $(\tilde{\Gamma})$. That is,

$$\tilde{\Lambda} \;=\; \tilde{\Gamma}/(\rho) \;\cong\; \mathbb{Z}_2 \oplus \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} M_2(\mathbb{Z}_2).$$

Using QPA we find that this is indeed the case, and that the quiver $\tilde{\Gamma}$ can be given as

$$\tilde{\Gamma}: \quad \tilde{a}_1 \circlearrowright 1 \underset{\tilde{a}_3}{\overset{\tilde{a}_2}{\rightleftarrows}} 2 \circlearrowright \tilde{a}_4 \quad .$$

We let $\tilde{e}_1$ and $\tilde{e}_2$ be idempotents in $\tilde{A}$ representing the trivial paths in vertices 1 and 2, respectively. Now let $\tilde{A}_1 = \tilde{e}_1\tilde{A}\tilde{e}_1$, $\tilde{A}_2 = \tilde{e}_2\tilde{A}\tilde{e}_2$, $\tilde{B}_{1,2} = \tilde{e}_1\tilde{A}\tilde{e}_2$ and $\tilde{B}_{2,1} = \tilde{e}_2\tilde{A}\tilde{e}_1$. Then $\tilde{a}_1$, $\tilde{a}_2$, $\tilde{a}_3$ and $\tilde{a}_4$ can be given as $\tilde{a}_1 \in \tilde{A}_1$, $\tilde{a}_2 \in \tilde{B}_{1,2}$, $\tilde{a}_3 \in \tilde{B}_{2,1}$ and $\tilde{a}_4 \in \tilde{A}_2$. We are outputted the following set of relations in Λ.

$$\rho \;=\; \left\{ \begin{array}{c}
\tilde{a}_1^4,\;\; \tilde{a}_2\tilde{a}_4^2,\;\; \tilde{a}_3\tilde{a}_2\tilde{a}_4,\;\; \tilde{a}_4\tilde{a}_3\tilde{a}_2,\;\; \tilde{a}_4^2\tilde{a}_3,\;\; \tilde{a}_1^2\tilde{a}_2\tilde{a}_3 + \tilde{a}_2\tilde{a}_3\tilde{a}_1^2, \\
\tilde{a}_1^3 + \tilde{a}_2\tilde{a}_4\tilde{a}_3 + \tilde{a}_1\tilde{a}_2\tilde{a}_3\tilde{a}_1,\;\; \tilde{a}_1^2\tilde{a}_2 + \tilde{a}_2\tilde{a}_3\tilde{a}_2,\;\; \tilde{a}_1^2\tilde{a}_2 + \tilde{a}_2\tilde{a}_3\tilde{a}_1\tilde{a}_2, \\
\tilde{a}_1\tilde{a}_2\tilde{a}_4 + \tilde{a}_1^3\tilde{a}_2,\;\; \tilde{a}_3\tilde{a}_1^2 + \tilde{a}_3\tilde{a}_2\tilde{a}_3,\;\; \tilde{a}_3\tilde{a}_1^2 + \tilde{a}_3\tilde{a}_1\tilde{a}_2\tilde{a}_3,\;\; \tilde{a}_4\tilde{a}_3\tilde{a}_1 + \tilde{a}_3\tilde{a}_1^3, \\
\tilde{a}_2\tilde{a}_4 + \tilde{a}_1^2\tilde{a}_2 + \tilde{a}_1\tilde{a}_2\tilde{a}_4,\;\; \tilde{a}_3\tilde{a}_2 + \tilde{a}_3\tilde{a}_1\tilde{a}_2 + \tilde{a}_4^3,\;\; \tilde{a}_4\tilde{a}_3 + \tilde{a}_3\tilde{a}_1^2 + \tilde{a}_4\tilde{a}_3\tilde{a}_1, \\
\tilde{a}_1^2 + \tilde{a}_1\tilde{a}_2\tilde{a}_3 + \tilde{a}_2\tilde{a}_3\tilde{a}_1 + \tilde{a}_1\tilde{a}_2\tilde{a}_3\tilde{a}_1,
\end{array} \right\}.$$

In order to understand the structural properties of $\tilde{A}$ and possibly find some similarities to $A = \mathbb{Z}_2 S_4$ that could offer a way to define some code, we look at relations in $\tilde{A}_1$ and $\tilde{A}_2$ as given by ρ. First note that ρ yields the following identities between paths from in $\tilde{B}_{1,2}$ and $\tilde{B}_{2,1}$.

$$\begin{aligned}
\tilde{a}_1^2\tilde{a}_2 \;&=\; \tilde{a}_2\tilde{a}_3\tilde{a}_1\tilde{a}_2 \;=\; \tilde{a}_2\tilde{a}_3\tilde{a}_2 \;=\; \tilde{a}_2\tilde{a}_4 + \tilde{a}_1\tilde{a}_2\tilde{a}_4, \\
\tilde{a}_1^3\tilde{a}_2 \;&=\; \tilde{a}_1\tilde{a}_2\tilde{a}_3\tilde{a}_2 \;=\; \tilde{a}_1\tilde{a}_2 v_4, \\
\tilde{a}_3\tilde{a}_1^2 \;&=\; \tilde{a}_3\tilde{a}_1\tilde{a}_2\tilde{a}_3 \;=\; \tilde{a}_3\tilde{a}_2\tilde{a}_3 \;=\; \tilde{a}_4\tilde{a}_3 + b_4 b_3 b_1, \\
\tilde{a}_3\tilde{a}_1^3 \;&=\; \tilde{a}_3\tilde{a}_2\tilde{a}_3\tilde{a}_1 \;=\; \tilde{a}_4\tilde{a}_3\tilde{a}_1.
\end{aligned}$$

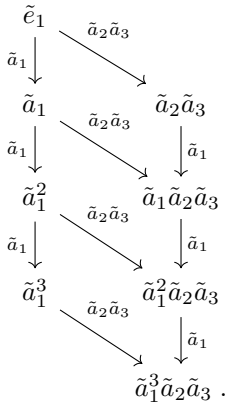
We see that in $\tilde{A}_1$ we then have

$$\tilde{a}_2\tilde{a}_3\tilde{a}_1^2 \;=\; \tilde{a}_1^2\tilde{a}_2\tilde{a}_3 \;=\; (\tilde{a}_2\tilde{a}_3)^2.$$

From that we deduce that a basis for $\tilde{A}_1$ can be given as

$$\tilde{U} \;=\; \{\tilde{e}_1, \tilde{a}_1, \tilde{a}_1^2, \tilde{a}_1^3, \tilde{a}_2\tilde{a}_3 + \tilde{a}_1^2\tilde{a}_2\tilde{a}_3, \tilde{a}_1\tilde{a}_2\tilde{a}_3 + \tilde{a}_1^3\tilde{a}_2\tilde{a}_3, \tilde{a}_1^2\tilde{a}_2\tilde{a}_3, \tilde{a}_1^3\tilde{a}_2\tilde{a}_3\}.$$

We see that $\tilde{A}_1$ then has two nontrivial generating paths, here $\tilde{a}_1$ and $\tilde{a}_2\tilde{a}_3$, which generate a basis for $\tilde{A}_1$ according to the following diagram.



Now for $\tilde{A}_2$ we get the following identities.

$$\begin{aligned} \tilde{a}_3\tilde{a}_1\tilde{a}_2 \;&=\; \tilde{a}_3\tilde{a}_2 + \tilde{a}_4^3, \\ \tilde{a}_3\tilde{a}_1^2\tilde{a}_2 \;&=\; (\tilde{a}_3\tilde{a}_2)^2 \;=\; \tilde{a}_4^4. \end{aligned}$$

From this we see that a basis for $\tilde{A}_2$ can be given as

$$\tilde{W} \;=\; \{\tilde{e}_2, \tilde{a}_4, \tilde{a}_4^2, \tilde{a}_4^3, \tilde{a}_4^4, \tilde{a}_3\tilde{a}_2\}.$$

Now let $\tilde{U}_1 = \{\tilde{e}_1, \tilde{a}_1\}$ and $\tilde{U}_2 = \{\tilde{e}_1, \tilde{a}_1, \tilde{a}_1^2, \tilde{a}_1^3\}$. Then bases for $\tilde{B}_{1,2}$ and $\tilde{B}_{2,1}$ can be given as

$$\begin{aligned} \tilde{X}_2\tilde{a}_2 \;&=\; \{\tilde{a}_2, \tilde{a}_1\tilde{a}_2, \tilde{a}_1^2\tilde{a}_2, \tilde{a}_1^3\tilde{a}_2\}, \\ \tilde{a}_3\tilde{X}_2 \;&=\; \{\tilde{a}_3, \tilde{a}_3\tilde{a}_1, \tilde{a}_3\tilde{a}_1^2, \tilde{a}_3\tilde{a}_1^3\}. \end{aligned}$$

Let $\tilde{e}_3 = 1 - \tilde{e}_1 - \tilde{e}_2$ where $\tilde{e}_3\tilde{A} \cong \tilde{e}_2\tilde{A}$. Assume that $\tilde{e}_3 = \tau(\tilde{e}_2)$. Then a basis for all of $\mathcal{M}_{\tilde{A}}$ could be given as

$$\begin{bmatrix} \tilde{U} & \tilde{U}_2\tilde{a}_2 & \tau(\tilde{a}_3\tilde{U}_2) \\ \tilde{a}_3\tilde{U}_2 & \tilde{W} & \tilde{W}g \\ \tau(\tilde{U}_2 b_2) & g\tilde{W} & \tau(\tilde{W}) \end{bmatrix},$$

for some $g \in 2O$ such that $\tau(\tilde{e}_2) = g\tilde{e}_2 g$. Now a natural suggestion for a basis for some code in $\tilde{A}$, given what we learned in the previous section, is

$$\begin{bmatrix} \tilde{U} - \tilde{U}_2 & \tilde{U}_1\tilde{a}_2 & \tilde{U}_1\tilde{a}_2 g \\ \tilde{a}_3\tilde{U}_2 & \tilde{W} & \tilde{W}g \\ 0 & 0 & 0 \end{bmatrix},$$

Assuming that $\tau(\tilde{a}_2 g) \in \tilde{B}_{2,1}$, then the above is a right ideal. We see that, although we would be able to identify the group elements of $2O$ in $\mathcal{M}_{\tilde{A}}$ by computations in GAP, there is still not an obvious way to go from this point unless we already know about some particular code inside $\tilde{A}$. Like in the previous case we could suggest that the minimal weight of a codeword is 16, and that all codeword with minimal weight are contained in the second row above. But we have also seen that $\tilde{A}$ has a more complicated structure than A, which suggest that the same is true for some right ideal or vector space in $\tilde{A}$. We have made a final attempt by searching for some idempotent $\tilde{e}$ in GAP such that $\tilde{e} + \tilde{e}_2$ generates a 12-dimensional submodule in the first and second row of $\mathcal{M}_{\tilde{A}}$. It turns out there are too many candidates to search through in order to get a result.

7 Appendix

7.1 The symmetric group S_4 as a subgroup of $\mathrm{PSL}_2(23)$

We are going to check that Lemma 4.4 holds for $S_4 \cong \langle \alpha, \beta, \gamma, \delta \rangle$, given representatives for α, β, γ and δ in $\mathrm{PSL}_2(23)$. Note that α and γ are defined similarly as in [2, Section 2]. We let

$$\alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \beta = \begin{pmatrix} -3 & 6 \\ 6 & 3 \end{pmatrix}, \ \gamma = \begin{pmatrix} 2 & 5 \\ 4 & -1 \end{pmatrix} \text{ and } \delta = \begin{pmatrix} -4 & -1 \\ -6 & 4 \end{pmatrix}.$$

Calculations show that then $\alpha^2 = \beta^2 = \delta^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and γ^3. Moreover, we have $\alpha^\delta = \delta\alpha\delta = \beta$ and $\alpha^y = \gamma^2\alpha\gamma = \alpha\beta$. This satisfies all three requirements given in Lemma 4.4.

7.2 A basis for P_1

We are going to show that if P_1 is an 8-dimensional projective submodule of $A = \mathbb{Z}_2 S_4$ with socle series

$$\mathrm{Soc}^{i+1}(P_1)/\mathrm{Soc}^i(P_1) \cong \begin{cases} \mathbb{Z}_2 & i = 3 \\ \mathbb{Z}_2 \oplus V & \text{for} \quad i = 2 \\ \mathbb{Z}_2 \oplus V & i = 1 \\ \mathbb{Z}_2 & i = 0. \end{cases}$$

where $P_1 = e_1 A$ for $e_1 = 1 + \gamma + \gamma^2$, then the following set of vectors is a basis for P_1.

$$\begin{aligned} v_1 &= \sum_{g \in S_4} g, \\ v_2 &= e_1(1 + \alpha + \beta + \alpha\beta), \\ v_3 &= e_1(1 + \alpha + \delta + \alpha\beta\delta), \\ v_4 &= v_3\gamma = e_1(1 + \alpha\beta + \delta + \alpha\delta), \\ v_5 &= e_1(1 + \beta + \delta + \alpha\delta), \\ v_6 &= v_5\gamma = e_1(1 + \alpha + \delta + \beta\delta), \\ v_7 &= e_1(1 + \delta), \\ v_8 &= e_1. \end{aligned}$$

First note that v_1 corresponds to the full-length vector in $\mathbb{Z}_2 S_4$, hence all permutations in S_4 act trivially on v_1. It follows that $\{v_1\} \cong \mathbb{Z}_2$. As for v_2 we calculate

$$v_2\alpha = v_2\beta = v_2\gamma = v_2, \quad v_2\delta = v_2 + v_1.$$

Thus $\mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2\}$ is closed upon action by S_4 and is thereby an indecomposable submodule of P_1 with composition factors two times $\mathbb{Z}_2$. Now for v_3 and v_4 we see that

$$\begin{aligned} v_3\alpha &= v_3 + v_1 + v_2, & v_4\alpha &= v_4 + v_1, \\ v_3\beta &= v_3 + v_1, & v_4\beta &= v_4 + v_2, \\ v_3\gamma &= v_4, & v_4\gamma &= v_3 + v_4 + v_1, \\ v_3\delta &= v_4, & v_4\delta &= v_3. \end{aligned}$$

Letting $M_1 = \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2, v_3, v_4\}$, we see that M_1 is a 4-dimensional indecomposable right submodule of P_1. Moreover, we have $\mathrm{Soc}(M_1) = \mathrm{Span}_{\mathbb{Z}_2}\{v_1\}$ and $\mathrm{Soc}^2(M_1) = \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2\}$. Hence P_1 has composition factors given by

$$\mathrm{Soc}^{i+1}(M_1)/\mathrm{Soc}^i(M_1) \cong \begin{cases} V & i = 2 \\ \mathbb{Z}_2 \quad \text{for} & i = 1 \\ \mathbb{Z}_2 & i = 0. \end{cases} \tag{16}$$

Now for v_5, v_6 and v_7 we have

$$\begin{aligned} v_5\alpha &= v_5 + v_1, & v_6\alpha &= v_6, & v_7\alpha &= v_7 + v_6, \\ v_5\beta &= v_5, & v_6\beta &= v_6 + v_1, & v_7\beta &= v_7 + v_5, \\ v_5\gamma &= v_6, & v_6\gamma &= v_5 + v_6 + v_1, & v_7\gamma &= v_7, \\ v_5\delta &= v_6, & v_6\delta &= v_5, & v_7\delta &= v_7. \end{aligned}$$

Thus $M_2 = \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_5, v_6, v_7\}$ is an indecomposable module. We have $\mathrm{Soc}(M_2) = \{v_1\}$. and and $\mathrm{Soc}^2(M_2) = \mathrm{Span}_{\mathbb{Z}_2} = \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_5, v_6\}$. Thus M_2 has composition factors given by

$$\mathrm{Soc}^{i+1}(M_2)/\mathrm{Soc}^i(M_2) \cong \begin{cases} \mathbb{Z}_2 & i = 2 \\ V \quad \text{for} & i = 1 \\ \mathbb{Z}_2 & i = 0, \end{cases} \tag{17}$$

and is thereby 4-dimensional.

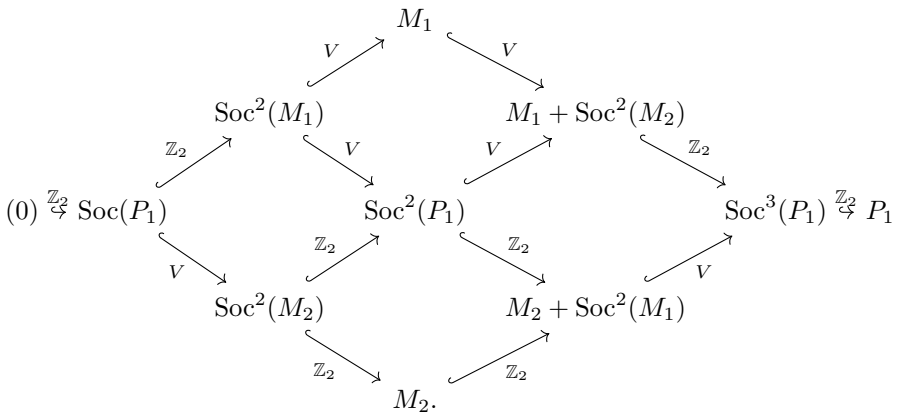
Since v_8 generate P_1, then the largest proper indecomposable submodule of P_1 is $M_1 + M_2$. Thus we have $\mathrm{Soc}^i(P_2) = \mathrm{Soc}^i(M_1) + \mathrm{Soc}^i(M_2)$ for $i = 1, 2$ and $\mathrm{Soc}^3(P_1) = M_1 + M_2$. Hence the iterated socle series is the union of that of M_1 and M_2, that is

$$\begin{aligned} \mathrm{Soc}(P_1) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{v_1\}, \\ \mathrm{Soc}^2(P_1) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2, v_5, v_6\}, \\ \mathrm{Soc}^3(P_1) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{v_1, v_2, v_5, v_6, v_3, v_4, v_7\}. \end{aligned}$$

And so the combining (16) and (17) yields the following composition factors

$$\mathrm{Soc}^{i+1}(P_1)/\mathrm{Soc}^i(P_1) \cong \begin{cases} \mathbb{Z}_2 & i = 3 \\ \mathbb{Z}_2 \oplus V & i = 2 \\ \mathbb{Z}_2 \oplus V \quad \text{for} & i = 1 \\ \mathbb{Z}_2 & i = 0. \end{cases} \tag{7}$$

Now the following diagram illustrates the module structure of P_1, for which the arrows are inclusion maps.



The labels of the maps are the cokernel of the inclusion maps, we have for example that $\mathrm{Soc}^2(M_1)/\mathrm{Soc}(P_1) \cong \mathbb{Z}_2$.

7.3 A basis for P_2

We are going to show that if $P_2 = e_2 A$, then P_2 is a module such that

$$\mathrm{Soc}^{i+1}(P_2)/\mathrm{Soc}^i(P_2) \;\cong\; \begin{cases} V & i=3 \\ \mathbb{Z}_2 & i=2 \\ \mathbb{Z}_2 \oplus V & i=1 \\ V & i=0, \end{cases} \quad \text{for}$$

and a set of vectors spanning all of P_2 is

$$\begin{aligned} w_1 &= e_2(1+\alpha+\beta+\alpha\beta), \\ w_2 &= w_1\gamma = e_2(\delta+\alpha\delta+\beta\delta+\alpha\beta\delta), \\ w_3 &= e_2(1+\alpha+\delta+\alpha\delta), \\ w_4 &= e_2(1+\alpha\beta+\delta+\beta\delta), \\ w_5 &= e_2(1+\alpha\beta+\delta+\alpha\delta), \\ w_6 &= w_5\gamma = e_2(1+\alpha+\alpha\delta+\beta\delta), \\ w_7 &= e_2(\alpha+\beta+\alpha\beta), \\ w_8 &= w_7\gamma = e_2\delta. \end{aligned}$$

We first note that $\langle \alpha, \beta \rangle$ acts trivially on w_1 and w_2, while $w_1\gamma = w_1\delta = w_2$, $w_2\gamma = w_1 + w_2$ and $w_2\delta = w_1$. Thus $V \cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2\} \subseteq \mathrm{Soc}(P_2)$. Now for w_3 we find that

$$\begin{aligned} w_3\alpha &= w_3 + w_2, \quad & w_3\beta &= w_3 + w_1, \\ w_3\gamma &= w_3 + w_2, \quad & w_3\delta &= w_3. \end{aligned}$$

Moreover, for w_4 we have

$$\begin{aligned} w_4\alpha &= w_4 + w_1, & w_4\beta &= w_4 + w_2 + w_1, \\ w_4\gamma &= w_4 + w_2, & w_4\delta &= w_4 + w_3 + w_2 + w_1. \end{aligned}$$

Let $N_1 = \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2, w_3, w_4\}$. Hence N_1 is a 4-dimensional indecomposable right submodule of P_2. Moreover, $\mathrm{Soc}(N_1) \cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2\}$ and $\mathrm{Soc}^2(N_1) \cong \{w_1, w_2, w_3\}$. Thereby, we have

$$\mathrm{Soc}^{i+1}(N_1)/\mathrm{Soc}^i(N_1) \cong \begin{cases} \mathbb{Z}_2 & i = 2 \\ \mathbb{Z}_2 \quad \text{for} & i = 1 \\ V & i = 0. \end{cases} \tag{18}$$

Now for w_5 and w_6 we find that

$$\begin{aligned} w_5\alpha &= w_5 + w_1 + w_2, & w_6\alpha &= w_6 + w_2, \\ w_5\beta &= w_5 + w_1, & w_6\beta &= w_6 + w_1 + w_2, \\ w_5\gamma &= w_6, & w_6\gamma &= w_6 + w_5, \\ w_5\delta &= w_6 + w_2, & w_6\delta &= w_5 + w_1. \end{aligned}$$

We find that $N_2 \cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2, w_5, w_6\}$ is a 4-dimensional indecomposable right submodule of P_2 with $\mathrm{Soc}(N_2) = \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2\}$. Hence N_2 has composition factors given by

$$\mathrm{Soc}^{i+1}(N_2)/\mathrm{Soc}^i(N_2) \cong \begin{cases} V & i = 1 \\ V \quad \text{for} & i = 0. \end{cases} \tag{19}$$

At last for w_7, and w_8 we have

$$\begin{aligned} w_7\alpha &= w_7 + w_6 + w_5 + w_4, & w_8\alpha &= w_8 + w_6 + w_3, \\ w_7\beta &= w_7 + w_5 + w_3 + w_1, & w_8\beta &= w_8 + w_6 + w_5 + w_4 + w_3, \\ w_7\gamma &= w_8, & w_8\gamma &= w_8 + w_7, \\ w_7\delta &= w_8 + w_2, & w_8\delta &= w_7 + w_1. \end{aligned}$$

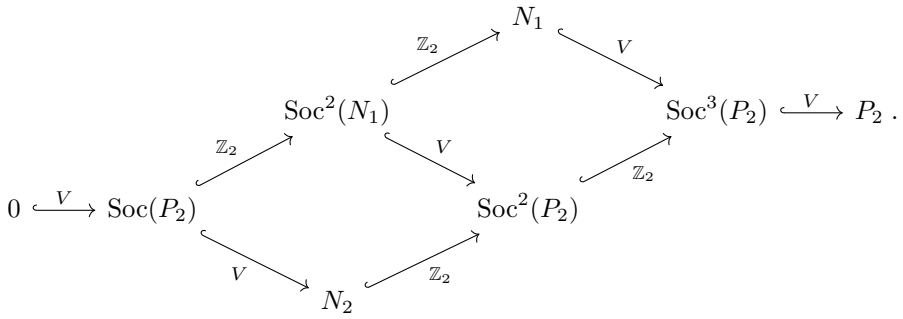
Thus $V \cong \mathrm{Span}_{\mathbb{Z}_2}\{w_7, w_8\} \cong P_2/\mathrm{Soc}^3(P_2)$. It follows that the largest indecomposable proper right submodule of P_2 is $N_1 + N_2 = \mathrm{Span}_{\mathbb{Z}_2}\{w_1, \ldots, w_6\}$. Thus $\mathrm{Soc}^i(P_2) = \mathrm{Soc}^i(N_1) + \mathrm{Soc}^i(N_2)$, meaning that

$$\begin{aligned} \mathrm{Soc}(P_2) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2\}, \\ \mathrm{Soc}^2(P_2) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2, w_3, w_5, w_6\}, \\ \mathrm{Soc}^3(P_2) &\cong \mathrm{Span}_{\mathbb{Z}_2}\{w_1, w_2, w_3, w_4, w_5, w_6\}. \end{aligned}$$

Thus combining (18) and (19) yields

$$\mathrm{Soc}^{i+1}(P_2)/\mathrm{Soc}^i(P_2) \cong \begin{cases} V & i = 3 \\ \mathbb{Z}_2 & i = 2 \\ \mathbb{Z}_2 \oplus V \quad \text{for} & i = 1 \\ V & i = 0. \end{cases} \tag{8}$$

In detail the structure of P_2 can then be given by the following diagram.



Here the arrows illustrate the inclusion maps of the indecomposable submodules, labeled by the cokernel.

7.4 The element f as a generator for $\mathcal{G}_{24}$

In the end of Chapter 4.2, we claimed that $f = e + e_2$ generates $\mathcal{G}_{24}$, where $\mathcal{G}_{24}$ is spanned by the vectors $v_1, \ldots, v_4, w_1, \ldots, w_8$. We find that f generate the following linearly independent vectors, given as sums of vectors in this basis.

$$
\begin{aligned}
f \cdot 1 &= v_1 + v_3 + v_4 + w_1 + w_3 + w_6 + w_8, \\
f \cdot \alpha &= v_1 + v_2 + v_3 + v_4 + w_1 + w_8, \\
f \cdot \beta &= v_2 + v_3 + v_4 + w_1 + w_2 + w_4 + w_5 + w_8, \\
f \cdot \alpha\beta &= v_3 + v_4 + w_1 + w_3 + w_4 + w_5 + w_6 + w_8, \\
f \cdot \delta &= v_1 + v_3 + v_4 + w_2 + w_3 + w_5 + w_7, \\
f \cdot \alpha\delta &= v_2 + v_3 + v_4 + w_1 + w_2 + w_7, \\
f \cdot \beta\delta &= v_1 + v_2 + v_3 + v_4 + w_1 + w_2 + w_3 + w_4 + w_6 + w_7, \\
f \cdot \alpha\beta\delta &= v_3 + v_4 + w_1 + w_2 + w_4 + w_5 + w_6 + w_7, \\
f \cdot \gamma &= v_3 + w_3 + w_5 + w_6 + w_7 + w_8, \\
f \cdot \alpha\gamma &= v_2 + v_3 + w_2 + w_7 + w_8, \\
f \cdot \gamma\delta &= v_4 + w_3 + w_5 + w_6 + w_7 + w_8, \\
f \cdot \alpha\gamma\delta &= v_1 + v_4 + w_2 + w_7 + w_8.
\end{aligned}
$$

We thereby find $v_1, \ldots, v_4$ and $w_1, \ldots, w_8$ can be given as

$$\begin{aligned}
v_1 &= f(\alpha + \beta + \alpha\delta + \beta\delta + \gamma\delta + \alpha\gamma\delta),\\
v_2 &= f(\alpha + \beta + \alpha\delta + \beta\delta + \gamma + \alpha\gamma),\\
v_3 &= f(\alpha + \alpha\delta + \gamma + \gamma\delta + \alpha\gamma\delta),\\
v_4 &= f(\alpha + \alpha\delta + \alpha\gamma\delta),\\
w_1 &= f(\delta + \alpha\delta + \beta\delta + \alpha\beta\delta)\\
w_2 &= f(1 + \alpha + \beta + \alpha\beta),\\
w_3 &= f(\beta + \alpha\beta + \beta\delta + \alpha\beta\delta + \gamma\delta + \alpha\gamma\delta),\\
w_4 &= f(1 + \alpha + \alpha\delta + \beta\delta + \gamma + \alpha\gamma + \gamma\delta + \alpha\gamma\delta),\\
w_5 &= f(\beta + \alpha\beta + \gamma + \alpha\gamma),\\
w_6 &= f(1 + \alpha\beta + \alpha\delta + \alpha\beta\delta + \gamma + \alpha\gamma + \gamma\delta + \alpha\gamma\delta),\\
w_7 &= f(1 + \alpha + \alpha\beta\delta + \delta + \alpha\delta + \alpha\beta\delta + \alpha\gamma + \gamma\delta),\\
w_8 &= f(\delta + \alpha\delta + \beta\delta + \alpha\beta\delta + \alpha\gamma + \alpha\gamma\delta).
\end{aligned}$$

This proves that all the given vectors are generated by f and so the same holds for $\mathcal{G}_{24}$.

7.5 Embedding of S_4 in $\mathcal{M}_A$

In Section 5, we defined the homomorphism $\varphi : A \to M_A$ and gave the image of the generators of S_4 under this map. We here do the same for all elements

in S_4. We find that

$$\varphi(1) = \begin{pmatrix} e_1 & 0 & 0 \\ 0 & e_2 & 0 \\ 0 & 0 & e_3 \end{pmatrix}, \quad \varphi(\delta) = \begin{pmatrix} e_1 + a_1 & 0 & 0 \\ 0 & 0 & e_2\delta \\ 0 & \delta e_2 & 0 \end{pmatrix},$$

$$\varphi(\gamma) = \begin{pmatrix} e_1 & 0 & 0 \\ 0 & 0 & e_2\delta + a_4^2\delta \\ 0 & \delta e_2 + \delta a_4^2 & e_3 \end{pmatrix},$$

$$\varphi(\gamma^2) = \begin{pmatrix} e_1 & 0 & 0 \\ 0 & e_2 & e_2\delta + a_4^2\delta \\ 0 & \delta e_2 + \delta a_4^2 & 0 \end{pmatrix},$$

$$\varphi(\gamma\delta) = \begin{pmatrix} e_1 + a_1 & 0 & 0 \\ 0 & e_2 + a_4^2 & 0 \\ 0 & \delta e_2 & \tau(e_2 + a_4^2) \end{pmatrix},$$

$$\varphi(\gamma^2\delta) = \begin{pmatrix} e_1 + a_1 & 0 & 0 \\ 0 & e_2 + a_4^2 & e_2\delta \\ 0 & 0 & \tau(e_2 + a_4^2) \end{pmatrix},$$

$$\varphi(\alpha) = \begin{pmatrix} e_1 + a_2a_3 & a_1a_2 & \tau(a_3) \\ a_3 & e_2 + a_4 + a_4^2 & a_4\delta \\ \tau(a_1a_2) & 0 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix},$$

$$\varphi(\beta) = \begin{pmatrix} e_1 + a_2a_3 & a_2 & \tau(a_3a_1) \\ a_3a_1 & e_2 + a_4 + a_4^2 & 0 \\ \tau(a_2) & \delta a_4 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix},$$

$$\varphi(\alpha\beta) = \begin{pmatrix} e_1 + a_2a_3 & a_2 + a_1a_2 & \tau(a_3 + a_3a_1) \\ a_3 + a_3a_1 & e_2 + a_4^2 & a_4\delta \\ \tau(a_2 + a_1a_2) & \delta a_4 & \tau(e_2 + a_4^2), \end{pmatrix},$$

$$\varphi(\alpha\gamma) = \begin{pmatrix} e_1 + a_2a_3 & a_2 + a_1a_2 & \tau(a_3 + a_3a_1) \\ a_3 & a_4 & e_2\delta \\ \tau(a_1a_2) & \delta e_2 + \delta a_4 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix},$$

$$\varphi(\beta\gamma) = \begin{pmatrix} e_1 + a_2a_3 & a_1a_2 & \tau(a_3) \\ a_3a_1 & 0 & e_2\delta + a_4\delta \\ \tau(a_2) & \delta e_2 + \delta a_4 & \tau(e_2 + a_4^2) \end{pmatrix},$$

$$\varphi(\alpha\beta\gamma) = \begin{pmatrix} e_1 + a_2a_3 & a_1 + a_1a_2 & \tau(a_3 + a_3x_1) \\ a_3 + a_3a_1 & a_4 & e_2\delta + a_4\delta \\ \tau(a_2 + a_1a_2) & \delta e_2 & \tau(e_2 + a_4 + a_4^2) \end{pmatrix},$$

$$
\begin{aligned}
\varphi(\alpha\gamma^2) &= \begin{pmatrix} e_1+a_2a_3 & a_2 & \tau(a_3a_1) \\ a_3 & e_2+a_4^2 & e_2\delta+a_4\delta \\ \tau(a_1a_2) & \delta e_2+\delta a_4 & 0 \end{pmatrix}, \\
\varphi(\beta\gamma^2) &= \begin{pmatrix} e_1+a_2a_3 & a_2+a_1a_2 & \tau(a_3+a_3a_1) \\ a_3a_1 & e_2+a_4+a_4^2 & e_2\delta+a_4\delta \\ \tau(a_2) & \delta e_2 & \tau(a_4) \end{pmatrix}, \\
\varphi(\alpha\beta\gamma^2) &= \begin{pmatrix} e_1+a_2a_3 & a_1a_2 & \tau(a_3) \\ a_3+a_3a_1 & e_2+a_4+a_4^2 & e_2\delta \\ \tau(a_2+a_1a_2) & \delta e_2+\delta a_4 & \tau(a_4) \end{pmatrix},
\end{aligned}
$$

$$
\begin{aligned}
\varphi(\alpha\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_2+a_1a_2 & \tau(a_3a_1) \\ a_3+a_3a_1 & a_4 & e_2\delta+a_4\delta+a_4^2\delta \\ \tau(a_1a_2) & \delta e_2+\delta a_4+\delta a_4^2 & 0 \end{pmatrix}, \\
\varphi(\beta\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_1a_2 & \tau(a_3+a_3a_1) \\ a_3a_1 & 0 & e_2\delta+a_4\delta+a_4^2\delta \\ \tau(a_2+a_1a_2) & \delta e_2+\delta a_4+\delta a_4^2 & \tau(a_4) \end{pmatrix}, \\
\varphi(\alpha\beta\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_2 & \tau(a_3) \\ a_3 & a_4 & e_2\delta+a_4^2\delta \\ \tau(a_2) & \delta e_2+\delta a_4+\delta a_4^2 & \tau(a_4) \end{pmatrix},
\end{aligned}
$$

$$
\begin{aligned}
\varphi(\alpha\gamma\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_2 & \tau(a_3) \\ a_3+a_3a_1 & e_2 & a_4\delta \\ \tau(a_1a_2) & \delta e_2+\delta a_4+\delta a_4^2 & \tau(e_2+a_4) \end{pmatrix}, \\
\varphi(\beta\gamma\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_2+a_1a_2 & \tau(a_3a_1) \\ a_3a_1 & e_2+a_4 & 0 \\ \tau(a_2+a_1a_2) & \delta e_2+\delta a_4^2 & \tau(e_2+a_4) \end{pmatrix}, \\
\varphi(\alpha\beta\gamma\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_1a_2 & \tau(a_3+a_3a_1) \\ a_3 & e_2+a_4 & a_4\delta \\ \tau(a_2) & \delta e_2+\delta a_4+\delta a_4^2 & \tau(e_2) \end{pmatrix},
\end{aligned}
$$

$$
\begin{aligned}
\varphi(\alpha\gamma^2\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_1a_2 & \tau(a_3+a_3a_1) \\ a_3+a_3a_1 & e_2+a_4 & e_2\delta+a_4^2\delta \\ \tau(a_1a_2) & 0 & \tau(e_2+a_4) \end{pmatrix}, \\
\varphi(\beta\gamma^2\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_2 & \tau(a_3) \\ a_3a_1 & e_2+a_4 & e_2\delta+a_4\delta+a_4^2\delta \\ \tau(a_2+a_1a_2) & \delta e_2 & \tau(e_2) \end{pmatrix}, \\
\varphi(\alpha\beta\gamma^2\delta) &= \begin{pmatrix} e_1+a_1+a_2a_3+a_1a_2a_3 & a_1a_2 & \tau(a_3a_1) \\ a_3 & e_2 & e_2\delta+a_4\delta+a_4^2\delta \\ \tau(a_2) & \delta a_4 & \tau(e_2+a_4) \end{pmatrix}.
\end{aligned}
$$

7.6 Bases for P_1 and P_2 in $\mathcal{M}_A$

We have seen that a set of vectors spanning P_1 as a right A-module is the set $\{v_1, \ldots, v_8\}$, defined in Chapter (4). We find that these vectors are equal to the following sums of basis elements for the entries of $\mathcal{M}_A$.

$$v_1 = a_1a_2a_3, \quad v_2 = a_2a_3, \quad v_3 = a_2 + a_1a_2 + a_1a_2a_3, \quad v_4 = \tau(a_3) + a_1a_2a_3,$$
$$v_5 = a_1a_2 + a_1a_2, \quad v_6 = \tau(a_3a_1) + a_1a_2a_3, \quad v_7 = a_1, \quad v_8 = e_1.$$

Given what we know about the socle layers of P_1, as outlined in Appendix 7.2, we deduce that a basis for $\varphi(P_1)$ can be given as

$$\varphi(v_1) = \begin{pmatrix} a_1a_2a_3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_2) = \begin{pmatrix} a_2a_3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\varphi(v_3 + v_5 + v_1) = \begin{pmatrix} 0 & a_2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_4 + v_1) = \begin{pmatrix} 0 & 0 & \tau(a_3) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\varphi(v_5 + v_1) = \begin{pmatrix} 0 & a_1a_2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_6 + v_1) = \begin{pmatrix} 0 & 0 & \tau(a_3a_1) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$
$$\varphi(v_7) = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(v_8) = \begin{pmatrix} e_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We saw that $P_2 = e_2A$ as a right module was spanned by the set of vectors $w_1, \ldots, w_8$, that are equal to the following sums of basis elements for various entries in $\mathcal{M}_A$.

$$w_1 = a_4^2, \quad w_2 = a_4^2\delta, \quad w_3 = a_3a_1 + a_4^2 + a_4^2\delta,$$
$$w_4 = a_3 + a_4^2 + a_4^2\delta, \quad w_5 = a_4 + a_4^2 + a_4^2\delta, \quad w_6 = a_4\delta + a_4^2 + a_4^2\delta,$$
$$w_7 = e_2 + a_4^2, \quad w_8 = e_2\delta.$$

Then, given what we know about the socle layers of P_2 from Appendix 7.3, in particular that $w_1, w_2 \in \mathrm{Soc}(P_2)$, then a basis for $\varphi(P_2)$ is

$$\varphi(w_1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_4^2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(w_2) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_4^2\delta \\ 0 & 0 & 0 \end{pmatrix},$$

$$\varphi(w_3 + w_2 + w_1) = \begin{pmatrix} 0 & 0 & 0 \\ a_3a_1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(w_4 + w_2 + w_1) = \begin{pmatrix} 0 & 0 & 0 \\ a_3 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\varphi(w_5 + w_2 + w_1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_4 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(w_6 + w_2 + w_1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_4\delta \\ 0 & 0 & 0 \end{pmatrix},$$

$$\varphi(w_7 + w_1) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & e_2 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \varphi(w_8) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & e_2\delta \\ 0 & 0 & 0 \end{pmatrix}.$$

References

[1] I. Assem, D. Simson, A. Skowroński, Elements of the representation theory of associative algebras, Vol. 1., Techniques of representation theory, London Math. Soc. Stud. Texts, 65, *Cambridge University Press, Cambridge*, 2006.

[2] F. Bernhardt, P. Landrock, O. Manz, The extended Golay codes considered as ideals, J. Combin. Theory Ser. A 55(1990), no. 2, 235–246.

[3] P.B. Bhattacharya, S.K. Jain, S.R. Nagpaul, Basic abstract algebra, *Cambridge University Press, Cambridge*, 1994.

[4] H.S.M. Coxeter, W.O.J. Moser, Generators and relations for discrete groups, Fourth edition, Ergeb. Math. Grenzgeb., 14, *Springer-Verlag, Berlin-New York*, 1980.

[5] J.D. Dixon, B. Mortimer, Permutation groups, Grad. Texts in Math., 163, *Springer-Verlag, New York*, 1996.

[6] W.C. Huffman, V. Pless, Fundamentals of error-correcting codes, *Cambridge University Press, Cambridge*, 2010.

[7] B. Huppert, Endliche Gruppen. I, Die Grundlehren der mathematischen Wissenschaften, Band 134, *Springer-Verlag, Berlin-New York*, 1967.

[8] B. Huppert, N. Blackburn, Finite groups. II, Grundlehren der Mathematischen Wissenschaften, 242, *Springer-Verlag, Berlin-New York*, 1982.

[9] G. Karpilovsky, Group representations. Vol. 4, North-Holland Math. Stud., 182, *North-Holland Publishing Co., Amsterdam*, 1995.

[10] F.J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. II, North-Holland Math. Library, Vol. 16, *North-Holland Publishing Co., Amsterdam-New York-Oxford*, 1977.

[11] I. McLoughlin, T. Hurley, A group ring construction of the extended binary Golay code, IEEE Trans. Inform. Theory 54 (2008), no. 9, 4381-4383.

NTNU

Norwegian University of
Science and Technology