THE EXTENDED GOLAY CODES AS IDEALS

ERLEND HOV

Contents

1. Introduction

The inspiration for this text was an article by Bernhart, Landrock and Manz called "The Extended Golay Codes Considered as Ideals" (see [1]), wherein they use fixed point free subgroups of the Mathieu groups M_{24} and M_{12} to turn the extended Golay codes into right ideals in their ambient vector spaces. We take a

Date: December 1, 2016.

more explicit approach to recreating their findings and build on them. Bernhart, Landrock and Manz use known facts about the subgroups of M_{24} and M_{12}, along with more algebraic machinery than this author was able to follow, to achieve their results. They find a way to define multiplication such that a right ideal must exist that equals an extended Golay code, and finally they show what this ideal must be.

To arrive at the same results, but requiring less deep algebraic knowledge on the parts of the reader and the writer, we instead start with explicit versions of the extended binary and ternary Golay codes. We believe an additional benefit of this explicit approach is the ease with which it can be applied to other codes, or other cases for the same codes.

Although we have only applied this approach to one additional code, the extended Hamming(7,4) code, it seems reasonable to assume that this can be done with many, if not all, other linear codes as well. What is required to have hopes that this approach will yield fruit is a decently sized chunk of equi-cyclic (Definition 4.3) automorphisms of the code in question.

2. Linear codes

This and the following chapter aims to give a brief introduction to linear codes and a subset of them, the quadratic residue codes and extended quadratic residue codes. This whole text deals with extended quadratic residue codes. Still, very little knowledge of coding theory is required of the reader. We include the following two chapters mainly to highlight what kind of objects are being dealt with, giving some context.

Linear codes are error-correcting codes that employ a **generator matrix**, G, to encode messages. They are so named because any linear combination of the row vectors of G is a valid code word.

Let G be an $n \times m$ matrix, with $n < m$. A **message**, v, is a vector of length n, and its corresponding **code word**, w, is a vector of length m. The **encoding** of v is

$$w = vG$$

To look at an example, let

$$G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right]$$

If this matrix has entries in $\mathbb{Z}_2$, it describes a linear code that takes a four digit binary number and encodes it as an eight digit number.

Error-correction is useful when information is sent over a channel that can not be expected to deliver messages exactly as they were sent. We say these errors are due to **noise**, and call the channel **noisy**.

Let w_1, w_2, w_3, w_4 be the rows of G. To briefly examine the error-correcting properties of G, assume we receive the words

$$w' = (1, 1, 0, 0, 1, 1, 0, 0)$$
$$w'' = (1, 1, 1, 0, 0, 1, 1, 0)$$
$$w''' = (1, 1, 1, x, 1, 1, 1, 1)$$

over a noisy channel. The x represents a digit that can not be determined to be either 0 or 1. We see that

$$w_1 + w_2 = w'$$

and conclude that w is, probably, the encoding of $(1, 1, 0, 0)$. However

$$w'' + w_1 + w_2 + w_3 = (0, 0, 0, 0, 0, 1, 1, 0)$$

which is not expressible as a linear combination of $\{w_i\}$, and therefore w'' contains at least one error. The word w''' becomes valid if we set $x = 1$, but not if we set $x = 0$.

If we partition the matrix G into

$$G = [I_4|G']$$

we can create the **parity-check matrix**

$$H = [G'^T|I_4] = \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

The rows of the matrix H show which entries in a valid code word need to add up to zero. We can test if a candidate is a valid code word because

$$wH^T = 0$$

if w is a code word. Applying this to the above examples, we see

$$w'H^T = (0, 0, 0, 0)$$

$$w''H^T = (0, 1, 1, 1)$$

$$w'''H^T = (1 + x, 1 + x, 1 + x, 0)$$

This shows clearly that $x = 1$.

The **weight of a code word** is the number of its entries that are non-zero and the **distance** between two code words is the number of places they are not equal in. Thus the distance between two words, w and w', is the same as the weight of $w - w'$.

The **weight of a code** is the smallest non-zero weight of all code words it contains. Thus the weight of a code is also the smallest distance between two valid code words.

The weight of the code with the above generator matrix, G, over $\mathbb{Z}_2$ is 4. In fact, the smallest distance from one code word to any of the closest code words is always 4 (compare any non-zero code word to $w_1 + w_2 + w_3 + w_4 = (1, 1, 1, 1, 1, 1, 1, 1)$). If we receive a word that is one position away from being valid, the second closest word is therefore at least 3 positions off. This lets us have a good guess at what the original message was. Of course, the more noise on the channel, the less certain we can be of this guess.

We see that the code with generator matrix G guesses correctly with one error and with two errors no guess is better than all others. With three errors, it detects the error but guesses incorrectly at the original message.

3. Extended quadratic residue codes

This text focuses on the extended binary and ternary Golay codes, with examples in the extended Hamming(7,4)-code. All of these are extended quadratic residue codes, which is defined below.

If G is the $n \times m$ generator matrix of a linear code, the **block length** of this code is m and its **dimension** is n. This is the same as the lengths of an encoded message and an original message, respectively.

A **cyclic code** is one that can be generated from one of its code words in the following manner. Let w_1 be this code word, and let w_{i+1} be the word obtained by shifting all entries in w_i one position to the right, sending the last position to the first. Then the span of $\{w_1, w_2, ..., w_m\}$ is the whole code.

Given primes p and q, where $p > q$ and q is a quadratic residue modulo p, there exists a cyclic code of block length p with entries from $\mathbb{Z}_q$. Such a code is called a **quadratic residue code**. Let ϵ be a primitive p'th root of unity in a finite extension field of $\mathbb{Z}_q$, and let $X = \{1, ...\}$ be the integers between zero and p that are quadratic residues modulo p. It can be shown there are $\frac{p-1}{2}$ distinct such integers. The polynomial

$$f(x) = \prod_{i \in X} (x - \epsilon^i)$$

is in $\mathbb{Z}_q[x]$, and form a word that generates the quadratic residue code in the manner of a cyclic code.

Adding a parity bit (1 if a row contains an odd number of 1's, 0 otherwise) to a quadratic residue code, results in an **extended quadratic residue code**. Apart from the described method, there are many other ways to generate an extended quadratic residue code. We do not bother with detailing the construction of the codes in use here, merely present their generator matrix.

An extended quadratic residue code has block length $p + 1$ and dimension $\frac{p+1}{2}$. The **ambient space**, $\mathcal{A}$, of a code with an $n \times m$ generator matrix with entries in $\mathbb{Z}_q$ is the vector space $(\mathbb{Z}_q)^m$, of which the code, $\mathcal{C}$, itself is a subspace. For an extended quadratic residue code, the ambient space is $(\mathbb{Z}_q)^{p+1}$ and the code, or code space, is $(\mathbb{Z}_q)^{\frac{p+1}{2}}$ as a vector space. In the example in Section 2 of the generator matrix G, $\mathcal{A} = (\mathbb{Z}_2)^8$ and $\mathcal{C} = (\mathbb{Z}_2)^4$.

3.1. The extended Hamming(7,4)-code.

The smallest prime with a prime quadratic residue is 7, where $3^2 = 2 \mod 7$. The quadratic residue code that arises from the primes 2 and 7 is called The Hamming(7,4)-code. We use the exended version of this code for illustrative purposes throughout this text. A generator matrix for this code is

$$\text{ham} = G = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right]$$

This is the familiar example from Section 2.

3.2. Automorphisms of an extended quadratic residue code.

Automorphisms of extended quadratic residue codes are central to this text.

Definition 3.1. An **automorphism** of a linear code, $\mathcal{C}$, is a homomorphism of $\mathcal{A}$ that maps $\mathcal{C}$ to itself and **preserves the weight** of code words.

We denote the automorphism group of $\mathcal{C}$ by $\mathrm{Aut}(\mathcal{C})$.

For $q = 2$, the automorphisms of an extended quadratic residue code are permutations of the basis of the ambient space (see [2] page 229).

For $q > 2$, the automorphisms are instead monomial matrices (see Section 12.1), a generalization of the case for $q = 2$ (see [2] page 238).

For now we look only at the case $q = 2$.

4. Fixed-point-free permutation groups

Fixed-point-free permutation groups are crucial in how we intend to define multiplication on the ambient space. This chapter defines such groups and lays out a number of results about them that will be applied in the remainder of this text.

Consider any symmetric group S_n, the group of all permutations of n elements. If a permutation, $p \in S_n$, sends x to itself, $p(x) = x$, we call x a **fixed point** of p. A **fixed-point-free permutation** is one with no fixed points.

A **fixed-point-free permutation group** is a subgroup of S_n, for some n, where the identity is the only permutation that contains fixed points.

From here on, $\{p_i\}$, will refer to a fixed-point-free permutation group with p_1 as the identity permutation.

Theorem 4.1. *When $j \neq k$, this implies that $p_j(x) \neq p_k(x)$ for all x in $\{1, 2, ..., n\}$.*

Proof. Assume $j \neq k$ and $p_j(x) = p_k(x)$ for some x. Then

$$p_j p_k^{-1}(p_k(x)) = p_j(x) = p_k(x)$$

Thus $p_k(x)$ is a fixed point of $p_j p_k^{-1}$, which is a contradiction. □

From the next chapter and onwards, fixed-point-free permutation groups of order n will be central to this text. The following shows that these exist, and are the largest fixed-point-free subgroups of S_n.

Corollary 4.2. *The largest possible order of a fixed-point-free subgroup of S_n is n.*

Proof. For any point, x, since $p_j(x) \neq p_k(x)$ whenever $j \neq k$, all permutations $p_l \in \{p_i\}$ must send x to different positions. There are only n positions to choose from, showing that $\{p_i\}$ can be no larger than n.

To see that fixed-point-free groups of order n exist, observe the group $\{p, p^2, ..., p^n = 1\}$, where p is of order n. □

Definition 4.3. If a permutation is made up exclusively of cycles of the same length, with no fixed points, we will call this an **equi-cyclic permutation**.

This definition gives a name to the building blocks we will make order n fixed-point-free permutation groups out of.

Interpreting fixed points as cycles of length one means the identity is also equi-cyclic.

The following theorem shows why being interested in fixed-point-free permutation groups leads us to be interested in equi-cyclic permutations.

Theorem 4.4. *The permutations in a fixed-point-free permutation group are all equi-cyclic.*

Proof. Assume a fixed-point-free permutation group contains a permutation, p, that is not equi-cyclic. Let a and b be the lengths of two cycles in p, where $a > b$. Then p^b will have fixed points at every point that is in a cycle of length b in p, but the points in a cycle of length a in p will not be fixed in p^b. Thus p^b has both fixed points and non-fixed points, which is a contradiction. □

The results in this text consist largely of finding various order n groups as fixed-point-free subgroups of $\mathrm{Aut}(\mathcal{C})$, a subgroup of S_n (for the appropriate n). It seems prudent to first show that:

Theorem 4.5. *Any group of order n can be represented by a fixed-point-free subgroup of S_n.*

Proof. Let $\{g_i\}$ be a group of order n, with $g_1 = 1$. Let p_i be the permutation that acts on $S = \{g_1, g_2, ..., g_n\}$ by:

$$p_i = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_i g_1 & g_i g_2 & \cdots & g_i g_n \end{pmatrix}$$

This is clearly fixed-point-free when $i \neq 1$. Let f be the mapping that sends g_i to p_i.

Then $f(1) = 1$, $f(g_i)f(g_j) = p_i p_j = f(g_i g_j)$ and if $f(x) = 1$, then $x = g_1 = 1$, thus f is a group isomorphism. □

Lemma 4.6. *Any order n subgroup, $\{p_i\}$, of S_n, where $j \neq k$ implies $p_j(x) \neq p_k(x)$ for all x, is fixed-point-free.*

Proof. Let $p_j(x) = x$, where p_j is not the identity. Then $j \neq 1$, but $p_j(x) = p_1(x) = 1(x)$, since p_1 is the identity. This is a contradiction. □

This lemma, combined with Theorem 4.1, gives the following characterization of fixed-point-free subgroups of S_n

Theorem 4.7. *For an order n subgroup, P, of S_n, the following are equivalent:*
-The group P is fixed-point-free.
-If $p, q \in P$ and $p \neq q$, then $p(x) \neq q(x)$ for all x.

Proof. Theorem 4.1 and Lemma 4.6. □

Finally, we introduce a numbering of the elements of any maximal order fixed-point-free permutation group.

Definition 4.8. Whenever we have a fixed-point-free permutation group, $\{p_i\}$, of maximal order, we will let p_i refer to the permutation that sends 1 to i;

$$p_i(1) = i$$

5. Multiplication in the ambient space

We now define a multiplication on the ambient space, $\mathcal{A}$, of an extended quadratic residue code, and then show how this makes the code space, $\mathcal{C}$, a left ideal in the resulting algebra.

Let $\{e_i\}$ be the basis of $\mathcal{A}$ and let $\{p_i\}$ be a fixed-point-free subgroup of S_n, with order n.

Definition 5.1. $e_n e_m := e_{p_n(m)}$.

With this definition, e_1 becomes the multiplicative identity of the algebra $\mathcal{A}$, since by Definition 4.8;

$$e_1 e_n = e_{p_1(n)} = e_n = e_{p_n(1)} = e_n e_1$$

Let f be the canonical bijection from $\{e_i\}$ to $\{p_i\}$, so $f(e_x) = p_x$. To have more ways of looking at the multiplication we mention:

Proposition 5.2. *The following are two definitions of multiplication that are equivalent to* Definition 5.1*:*

$$e_n e_m = e_{p_n p_m(1)}$$
$$e_n e_m = f^{-1}(p_n p_m)$$

Now we argue that this definition makes $\mathcal{C}$ a left ideal in $\mathcal{A}$.
Let $r \in \mathcal{A}$, $w \in \mathcal{C}$ and $\{w_i\}$ be the basis of $\mathcal{C}$. Then

$$rw = \sum_{i \in X} e_i * \sum_{i \in Y} w_j = \sum_{i \in X, j \in Y} e_i w_j$$

where X and Y are the positions of the non-zero coefficients of r and w. For $\mathcal{C}$ to be a left ideal in $\mathcal{A}$ it is necessary and sufficient that $e_i w_j \in \mathcal{C}$ for all $i \in \{1, 2, ..., n\} and j \in \{1, 2, ..., n/2\}$.
With Definition 5.1 this becomes

$$e_i w_j = e_i \sum_{k \in S} c_k e_k = \sum_{k \in S} c_k e_{p_i(k)}$$

where $S = \{1, 2, ..., n\}$ and c_k is the k'th coefficient of w_j. Thus, multiplication on the left by e_i is the same as letting the permutation p_i act on S. To sum this up:

Proposition 5.3. *If p_i is an automorphism of $\mathcal{C}$, then $e_i w_j \in \mathcal{C}$ for all j.*

This next proposition tells us the structure of the ambient space, $\mathcal{A}$, as an algebra when using the multiplication in Definition 5.1. Since $e_i e_j = f^{-1}(p_i p_j)$:

Proposition 5.4. *If P is the group $\{p_i\}$, then $\mathcal{A}$, with multiplication as in Definition 5.1, now has the structure of the group ring $\mathbb{Z}_q[P]$.*

Now, to see why we demand the group $\{p_i\}$ be fixed-point-free, assume a case where

$$p_i(k) = p_j(k), i \neq j$$

Then

$$e_i e_k = e_{p_i(k)} = e_{p_j(k)} = e_j e_k$$

and since $\{p_i\}$ is a group

$$e_i = e_i e_k e_k^{-1} = e_j e_k e_k^{-1} = e_j$$

This would set two distinct basis elements of the ambient space as equal.

6. Two examples in the extended Hamming(7,4)-code

In this section we give two explicit examples of constructions that render the extended Hamming(7,4)-code a left ideal in its ambient space. These examples will show up again in Section 7 and Section 9.

The following permutations can be used to define multiplication, as above, on the extended Hamming(7,4)-code as presented earlier (we denoted its generator matrix by ham).

$$a_{\text{ham}} = (1,4,3,2)(5,8,7,6)$$

$$b_{\text{ham}} = (1,5)(4,6)(3,7)(2,8)$$

These are automorphisms of ham. To verify this, let the permutations act on the columns of the matrix ham, and see that the resulting rows can express the rows of the original matrix under addition modulo 2;

$$a_{\text{ham}}(\text{ham}) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Actually, a_{ham} simply reorders the rows of ham.

$$b_{\text{ham}}(\text{ham}) = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The sum of any three rows of the above matrix gives a row in ham.

Observe that

$$a_{\text{ham}} b_{\text{ham}} = (1,8)(2,7)(3,6)(4,5) = b_{\text{ham}} a_{\text{ham}}^{-1}$$

This relationship describes the group D_4 (sometimes called D_8, the symmetries of a square).

Let $a_{\text{ham}}^i b_{\text{ham}}^j$, where $i \in \{0,1,2,3\}$ and $j \in \{0,1\}$, be our normal form of the elements in this group and assume $a_{\text{ham}}^r b_{\text{ham}}^s(x) = x$. If $s = 0$, then $r = 0$, which represents the identity. If $s = 1$, then b_{ham} sends the points of one cycle of a_{ham} to the other, and no choice for r can send them back. This demonstrates that the group $\langle a_{\text{ham}}, b_{\text{ham}} \rangle$ is fixed-point-free.

For a second example, the permutations

$$a'_{\text{ham}} = (1,2,3,8)(4,5,6,7)$$

$$b'_{\text{ham}} = (1,4)(2,7)(3,6)(5,8)$$

are also both automorphisms of ham. They generate a fixed-point-free permutation group with the structure D_4 as well.

7. A test for right ideals

We now have a multiplication that renders $\mathcal{C}$ a left ideal in the algebra $\mathcal{A}$. In many cases it may be desirable for $\mathcal{C}$ to be a double sided ideal. Although we have not found a way to look directly for such ideals, we can at least test the left ideals we have found.

For $\mathcal{C}$ to be a right ideal it is necessary and sufficient that $w_i e_j \in \mathcal{C}$ for all $i \in \{1, 2, ..., n/2\}$ and $j \in \{1, 2, ..., n\}$. Let $(c_1, c_2, ..., c_n)$ be the coefficients of w_i, then

$$w_i e_j = (c_1 e_1, c_2 e_2, ..., c_n e_n) e_j = (c_1 e_{p_1(j)}, c_2 e_{p_2(j)}, ..., c_n e_{p_n(j)})$$

Theorem 4.1 ensures this is a permutation of the coefficients of w_i. This permutation depends on the group $\mathcal{S} = \{p_i\}$ and on p_j specifically. We denote it by $\mathcal{S}(p_j)$:

$$\mathcal{S}(p_j) = \begin{pmatrix} 1 & 2 & ... & n \\ p_1(j) & p_2(j) & ... & p_n(j) \end{pmatrix}$$

This sends c_x to position $p_x(j)$. For $\mathcal{C}$ to be a right ideal in $\mathcal{A}$, the permutation $\mathcal{S}(p_j)$ must be an automorphism for any $j \in \{1, 2, ..., n\}$.

Definition 7.1. The **right ideal test** for a maximal order fixed-point-free subgroup, P, of $\mathrm{Aut}(\mathcal{C})$, **applied to the element** $p_j \in P$, passes if $\mathcal{S}(p_j) \in \mathrm{Aut}(\mathcal{C})$ and fails otherwise.

The right ideal test **applied to** P **itself** passes if it passes for every element in a generator set of P.

We now perform this test on the examples $\langle a_{\mathrm{ham}}, b_{\mathrm{ham}} \rangle$ and $\langle a'_{\mathrm{ham}}, b'_{\mathrm{ham}} \rangle$.

For a tidier display, we write a_{ham} and b_{ham} simply as a and b in the following:

$$\begin{aligned} \mathcal{S}(a) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & a^3(4) & a^2(4) & a(4) & b(4) & a^3b(4) & a^2b(4) & ab(4) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 6 & 7 & 8 & 5 \end{pmatrix} \\ &= (1, 2, 3, 4)(5, 8, 7, 6) \end{aligned}$$

To investigate $\mathcal{S}(a)$, apply it to the first row of ham to get (0,1,0,0,1,1,1,0). Add the second row of ham to this to get (0,0,0,0,0,1,0,1), which has weight 2, and can therefore not be part of a code of weight 4. This verifies that the permutation $\mathcal{S}(a)$ is not an automorphism of $\mathcal{C}$ and therefore the group $\langle a_{ham}, b_{ham} \rangle$ does not induce a right ideal.

However, the same test on $\langle a'_{\mathrm{ham}}, b'_{\mathrm{ham}} \rangle$ yields:

$$\mathcal{S}'(a'_{\mathrm{ham}}) = (1, 8, 3, 2)(4, 5, 6, 7)$$

$$\mathcal{S}'(b'_{\mathrm{ham}}) = (1, 4)(2, 5)(3, 6)(7, 8)$$

$\mathcal{S}'(a'_{\mathrm{ham}})$ and $\mathcal{S}'(b'_{\mathrm{ham}})$ are both automorphisms of ham, and therefore $\langle a'_{\mathrm{ham}}, b'_{\mathrm{ham}} \rangle$ does induce a two-sided ideal.

Remark. The ratio of automorphisms of $\mathcal{C}$ to the order of S_n, for the relevant n, implies the chance for a random permutation to be an automorphism. It is the case that this ratio is a lot higher for the extended Hamming(7,4)-code than for

the extended binary Golay code, and the right ideal test seems to pass a lot more frequently for ham than for bin.

8. Conjugacy classes of automorphism groups

To find various fixed-point-free subgroups of the automorphism group of a given code we used computer searches. Particularly for the extended binary Golay code, the size of the automorphism group (M_{24}) and the size of S_{24} meant we needed some techniques to reduce the search time. The concept of conjugacy classes was one very helpful tool for this.

We shall see that if P and P' are conjugate fixed-point-free order n subgroups of $\mathrm{Aut}(\mathcal{C})$, then using Definition 5.1 to define multiplication on $\mathcal{A}$ yields the same behavior whether we base multiplication on P or P'.

These first three definitions and one theorem should be familiar.

Definition 8.1. Let a and r be elements of some group. The **conjugate of a by r** is rar^{-1}.

Definition 8.2. Let $P = \{p_i\}$ be a subgroup of some group, G, and let $r \in G$. Then the **conjugate of P by r** is $rPr^{-1} = \{rp_ir^{-1}\}$.

Theorem 8.3. *Conjugation is a group isomorphism.*

Proof. It is easily verified that $r1r^{-1} = 1$ and $r(ab)r^{-1} = rar^{-1}rbr^{-1}$. Also, if $rar^{-1} = 1$, then $a = 1$. □

Definition 8.4. Let a and b be elements in some permutation group, P. Then a and b are in the same **conjugacy class** of P if, and only if, there exists some $r \in P$ such that $rar^{-1} = b$.

Given that we are so concerned with permutations that are equi-cyclic and of appropriate order, the following fact will be useful.

Theorem 8.5. *Conjugation of permutations preserves cycle structure.*

Proof. Let $a, r \in S_n$ for some n and let $x \in \{1, 2, ..., n\}$ be in a cycle of length l in a. Now

$$(rar^{-1})^l(r(x)) = ra^lr^{-1}(r(x)) = ra^l(x) = r(x)$$

So $r(x)$ is a fixed point for $(rar^{-1})^l$ and therefore $r(x)$ is in a cycle in rar^{-1} with length dividing l. Let $0 < l' < l$. Then

$$(rar^{-1})^{l'}(r(x)) = ra^{l'}r^{-1}(r(x)) = ra^{l'}(x) \neq r(x)$$

Thus $r(x)$ is in a cycle in rar^{-1} with length not shorter than l, so the cycle in a containing x and the cycle in rar^{-1} containing $r(x)$ are both of length l. The same holds for any cycle in a. □

We are out to find a way of inspecting large sets of fixed-point-free subgroups of some group, P, by inspecting a single representative group, $\{p_i\}$. The next result tells us that the set of groups $\{rp_ir^{-1}\}$ for $r \in P$ is such a set.

Corollary 8.6. *Let $\{p_i\}$ be a fixed-point-free subgroup of the automorphism group, $\mathrm{Aut}(\mathcal{C})$, of an extended quadratic residue code. Then $\{rp_ir^{-1}\}$ is a fixed-point-free subgroup with the same structure whenever $r \in \mathrm{Aut}(\mathcal{C})$.*

Proof. Preservation of the group structure is guaranteed by Theorem 8.3. Theorem 8.5 ensures the elements of $\{rp_ir^{-1}\}$ are all equi-cyclic, and therefore fixed-point-free (save the identity). □

Finally we show that the right ideal test, Definition 7.1, need also only be carried out on one representative group.

Theorem 8.7. *The right ideal test gives the same result for any two order n fixed-point-free permutation groups that are conjugate.*

Proof. Let $P = \{p_i\}$ and $P' = \{p'_i\}$ be order n fixed-point-free subgroups of $\mathrm{Aut}(\mathcal{C})$, where $p_i(1) = i$ and $p'_i = rp_jr^{-1}$, for some j such that $p'_i(1) = i$ and some $r \in \mathrm{Aut}(\mathcal{C})$. Let f be the permutation such that $p'_{f(i)} = rp_ir^{-1}$.

We have $p'_{f(i)}(1) = f(i) = rp_ir^{-1}(1)$, thus $r^{-1}f(i) = p_ir^{-1}(1)$. Then

$$r^{-1}f = \begin{pmatrix} 1 & 2 & ... & n \\ p_1(r^{-1}(1)) & p_2(r^{-1}(1)) & ... & p_n(r^{-1}(1)) \end{pmatrix}$$

Assume that the right ideal test passes for P. Notice how $r^{-1}f$ is precisely the right ideal test for P on the permutation $p_x \in P$, where $p_x(1) = r^{-1}(1)$. This means f is an automorphism of $\mathcal{C}$.

Now the right ideal test for P' on the permutation $p'_i \in P'$ is

$$\begin{aligned} \mathcal{S}'(p'_i) &= \begin{pmatrix} 1 & 2 & ... & n \\ p'_1(i) & p'_2(i) & ... & p'_n(i) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & ... & n \\ rp_{f^{-1}(1)}r^{-1}(i) & rp_{f^{-1}(2)}r^{-1}(i) & ... & rp_{f^{-1}(n)}r^{-1}(i) \end{pmatrix} \end{aligned}$$

Because the permutation f^{-1} applied to the elements of P gives $f^{-1}(p_x) = p_{f^{-1}(x)}$ we have $\mathcal{S}'(p'_i) = rf^{-1}\mathcal{S}(p_{r^{-1}(i)})$, where

$$\mathcal{S}(p_{r^{-1}(i)}) = \begin{pmatrix} 1 & 2 & ... & n \\ p_1(r^{-1}(i)) & p_2(r^{-1}(i)) & ... & p_n(r^{-1}(i)) \end{pmatrix}$$

But $\mathcal{S}(p_{r^{-1}(i)})$ is precisely the right ideal test for P applied to $p_{r^{-1}(i)}$, showing that the right ideal test for P' passes.

The same argument shows implication the other way.

□

9. More solutions for the extended Hamming(7,4)-code

When looking for maximal order fixed-point-free subgroups of the automorphism group of an extended quadratic residue code, we have argued the usefulness of observing the equi-cyclic conjugacy classes of said automorphism group. A brute force search is good enough to find these classes for the extended Hamming(7,4)-code, due to its small size. Below are the results of such a search, showing structure, size and one representative element.

structure	size	representative
2^4	7	(1,2)(3,8)(4,7)(5,6)
2^4	42	(1,2)(3,4)(5,6)(7,8)
4^2	84	(1,2,3,8)(4,5,6,7)
4^2	168	(1,4,3,2)(5,8,7,6)

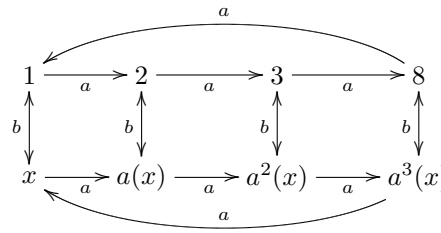
A **structure of** 2^4 means four 2-cycles, and vice versa. Throughout this section we fix

$$a = (1, 2, 3, 8)(4, 5, 6, 7)$$

$$a' = (1, 4, 3, 2)(5, 8, 7, 6)$$

The group $\mathbb{Z}_8$ is discarded immediately, as it contains elements of order 8, for which no conjugacy class exists.

9.1. **Applying** $(\mathbb{Z}_4) \times (\mathbb{Z}_2)$**.** We use the element $a = (1, 2, 3, 8)(4, 5, 6, 7)$ to illustrate our approach.



Here, x is an element of the cycle $(4, 5, 6, 7)$. This diagram shows the options for choice of b. The squares commuting captures the equality $ab = ba$.

If $x = 4$, then

$$b = (1, 4)(2, 5)(3, 6)(7, 8)$$

If instead we choose $x = 5$, we get

$$b^* = (1, 5)(2, 6)(3, 7)(4, 8)$$

Both b and b^* are automorphisms of ham, so $\langle a, b\rangle$ and $\langle a, b^*\rangle$ are both valid groups.

We point out that b and b^* are in different conjugacy classes and that the results for $x = y$ and $x = a^2(y)$ generate the same group.

Similarly, building on the element a', from the second conjugacy class of structure 4^2:

$$a' = (1, 4, 3, 2)(5, 8, 7, 6)$$

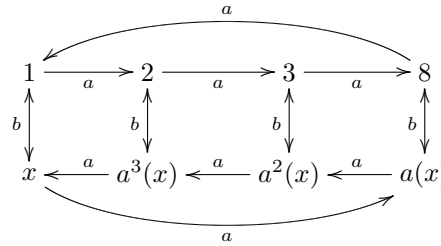
If $b'(1) = 5$ we get

$$b' = (1, 5)(2, 6)(3, 7)(4, 8) = b^*$$

which we already claimed is an automorphism. If we set $b''(1) = 8$, the result is not an automorphism.

The first conjugacy class of structure 4^2 gives a valid group for both options of x, but for the second class only one of the options does.

9.2. **Applying D_4.** Although this case has been used as an example in chapter 6, it is helpful to revisit it before tackling the cases D_{12} and D_6 of the binary and ternary extended Golay codes. Similar to the case $(\mathbb{Z}_4) \times (\mathbb{Z}_2)$, here is a diagram illustrating our choices when building on the automorphism a from above.

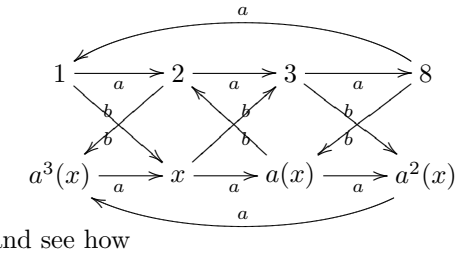


Notice that the bottom cycle has switched direction, and the squares commuting now reflects the identity $ab = ba^{-1}$. Two possible options for b are described by $b(1) = 4$ and $b'(1) = 5$. But then $b = b'a$. In this manner, $\langle a, b\rangle$ generates the same group, no matter the choice of $b(1)$. Therefore, the two cases described in chapter 6 are all possible solutions, up to conjugation.

9.3. **Applying the quaternion group.** We build the following diagram on

$$a = (1, 2, 3, 8)(4, 5, 6, 7)$$

The arrows for $b(a^3(x)) = 8$ and $(b(a^2(x)) = 1$ are omitted for a neater display.



Here, let $ab = c$, and see how

$$ac = b^{-1}$$
$$ba = c^{-1}$$
$$bc = a$$
$$ca = b$$
$$cb = a^{-1}$$
$$a^2 = b^2 = c^2$$
$$(a^2)^2 = 1$$

This describes the quaternion group. We have set $b(1) = x$, and this means $c(1) = a(x)$, $b^{-1}(1) = a^2(x)$ and $c^{-1}(x) = a^3(x)$. Any of these elements would, along with a, generate $\langle a, b\rangle$, meaning any choice of x is as good as an other. We test

$$b = (1, 4, 3, 6)(2, 7, 8, 5)$$

which is indeed an automorphism.

For the right ideal test, see that

$$(p_1, p_2, ..., p_3) =$$
$$(1, a, a^2, b, ab, a^2b, a^3b, a^3)$$

$$\mathcal{S}(a) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & a(2) & a^2(2) & b(2) & ab(2) & a^2b(2) & a^3b(2) & a^3(2) \end{pmatrix}$$
$$= (1,8,3,2)(4,5,6,7),$$

which is an automorphism of ham, and

$$\mathcal{S}(b) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & a(4) & a^2(4) & b(4) & ab(4) & a^2b(4) & a^3b(4) & a^3(4) \end{pmatrix}$$
$$= (1,4)(2,5)(3,6)(7,8)$$

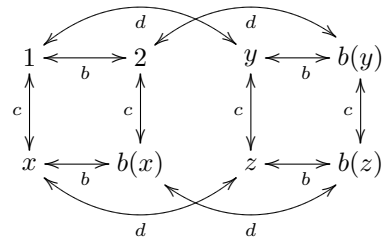
is also an automorphism.

If we build on $a' = (1,4,3,2)(5,8,7,6)$ instead, and set $b'(1) = 5$, we get

$$b' = (1,5,3,7)(2,8,4,6),$$

which is not an automorphism, so $\langle a, b\rangle$ is a double sided ideal.

9.4. **Applying $(\mathbb{Z}_2)^3$.** We use the following diagram, building on $b = (1,2)(3,4)(5,6)(7,8)$:



Not surprisingly, this diagram is a cube. We need one permutation that sends 1 to x for every x (Theorem 4.1), and from the diagram we see if 1 goes to x, then 2 goes to $b(x)$. This forces the following permutations:

$$p_2 = (1,2)(3,4)(5,6)(7,8)$$
$$p_3 = (1,3)(2,4)(-,-)(-,-)$$
$$p_4 = (1,4)(2,3)(-,-)(-,-)$$
$$p_5 = (1,5)(2,6)(-,-)(-,-)$$
$$p_6 = (1,6)(2,5)(-,-)(-,-)$$
$$p_7 = (1,7)(2,8)(-,-)(-,-)$$
$$p_8 = (1,8)(2,7)(-,-)(-,-)$$

Now the first blank cycle of p_3 can be either $(5,7)$ or $(5,8)$. This choice forces p_3 and, because $p_4 = p_2p_3$, p_4 in to place. The first blank cycle of p_5 can be either $(3,7)$ or $(3,8)$. This choice forces the remaining blank cycles in to place, because $p_6 = p_1p_5$ and so forth. We test the two versions of p_3 and p_5:

$$p_3 = (1,3)(2,4)(5,7)(6,8)$$
$$p_3' = (1,3)(2,4)(5,8)(6,7)$$
$$p_5 = (1,5)(2,6)(3,7)(4,8)$$
$$p_5' = (1,5)(2,6)(3,8)(4,7)$$

Verify that p_3 is an automorphism of ham, while p_3' is not, and that p_5 and p_5' are both automorphisms.

10. Guidelines on constructing permutation group diagrams

When looking for a fixed-point-free representation of some group structure to base multiplication in $\mathcal{A}$ on, we use permutation group diagrams of the type seen in the previous chapter. These diagrams are based on one suitable equi-cyclic automorphism, a, and they highlight the options for permutations that will, along with a, generate the desired group. This chapter lays out some guidelines we follow to create useful diagrams of this sort, although other approaches may certainly be viable.

Find a minimal generator set, $\langle a, b, ... \rangle$, for the desired group structure. This minimizes the number of arrows, making the diagram easier to use. Let a be the highest order element in the generator set. Minimal sets containing one high order element and the rest elements of order two are preferred, since elements of order two require only one arrow to represent their effect on two points.

Pick an $a \in \mathrm{Aut}(\mathcal{C})$ from some appropriate conjugacy class we wish to examine. Draw one cycle of a explicitly, and the rest with symbols. This lets us draw arrows of b while maintaining generality.

Keep aiming for symmetry when adding the arrows of b; we are drawing a group, so symmetry should exist. Sometimes it will be best to finish a diagram before starting to move the pieces around to find the neatest representation.

The first arrow for b can be sent anywhere between two cycles. Sending a point in a cycle of a to another point in the same cycle, via b, would violate Theorem 4.1. Having drawn the first arrow of b, use equalities in the group to find if this forces other arrows in to place. For instance, in the diagram in Section 9.2, we first draw the arrow for $b(1)$. Then all other arrows of b are forced by the equality $ab = ba^{-1}$. The number of arrows needed to start forcing new arrows in place will depend on the group in question.

For an example, we now use this approach to find a diagram for S_4 fixed-point-free inside S_{24}.

10.1. **Constructing the diagram for S_4 inside S_{24}.** A minimal generator set for S_4 is

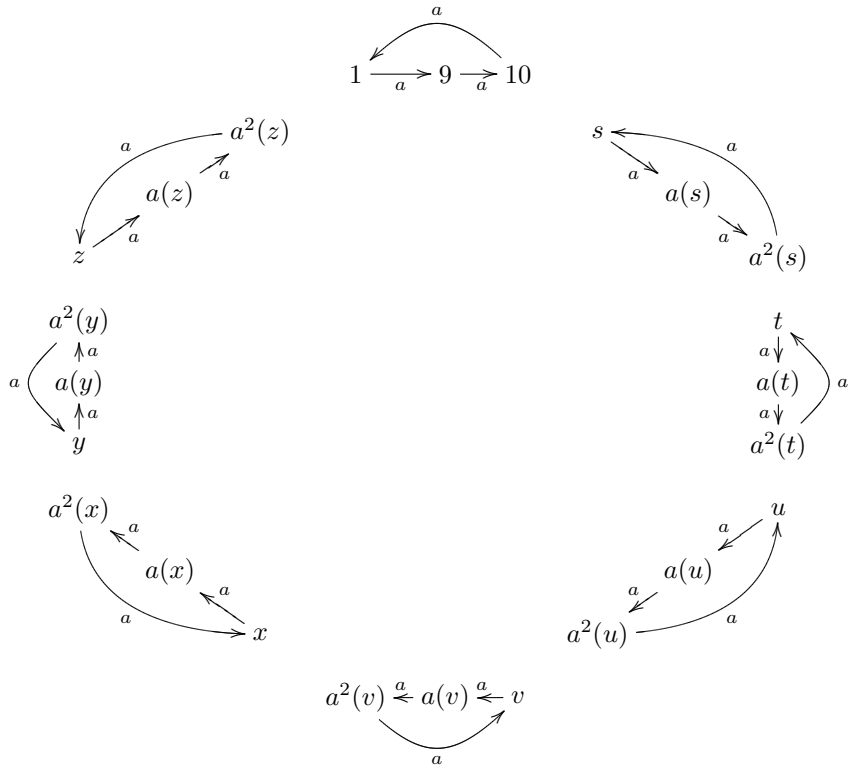
$$a' = (1, 2, 3), b' = (1, 4)$$

A fixed-point-free representation of S_4 in S_{24} will contain permutations a and b that correspond to a' and b'. We will draw the diagram for these equi-cyclic elements of S_{24} that correspond to a' and b'.

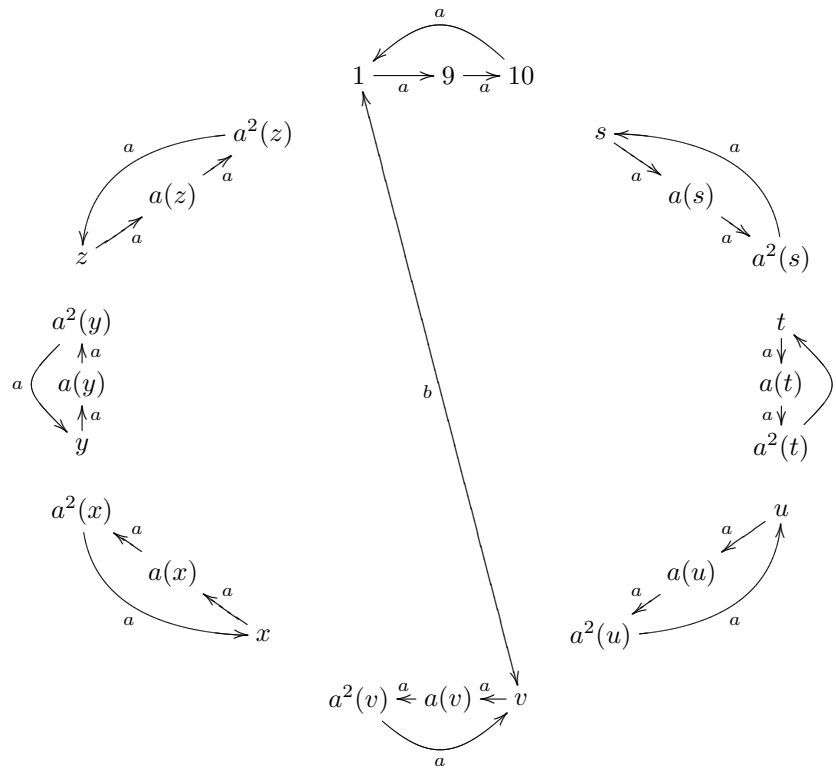
Corresponding to a', we choose

$$a = (1, 9, 10)(2, 11, 8)(3, 7, 12)(4, 5, 6)(13, 21, 22)(14, 23, 20)(15, 19, 24)(16, 17, 18)$$

This means b, corresponding to b', will have the cycle structure 2^{12}. We start by representing a in a fashion that will help us see symmetries, and maintain generality whenever possible:


a
1
a
9
a
10
a
a²(z)
a
a(z)
a
z
a
s
a
a
a(s)
a
a²(s)
a²(y)
a
a
a(y)
a
y
a
t
a
a(t)
a
a²(t)
a
a²(x)
a
a(x)
a
a
x
u
a
a(u)
a
a²(u)
a
a²(v)
a
a(v)
a
v
a

Now we draw $b(1)$. Clearly, this must point to some other cycle than $(1, 9, 10)$, otherwise we would be violating Theorem 4.1. Because we are using (s, t, u, v, x, y, z) to identify the remaining cycles, we can say $b(1) = v$ without loss of generality:



The following results about a' and b' will help us place $b(9)$ and $b(10)$:

$$a'b'a' = (1, 3, 4, 2)$$

$$a'^2b'a' = (3, 4)$$

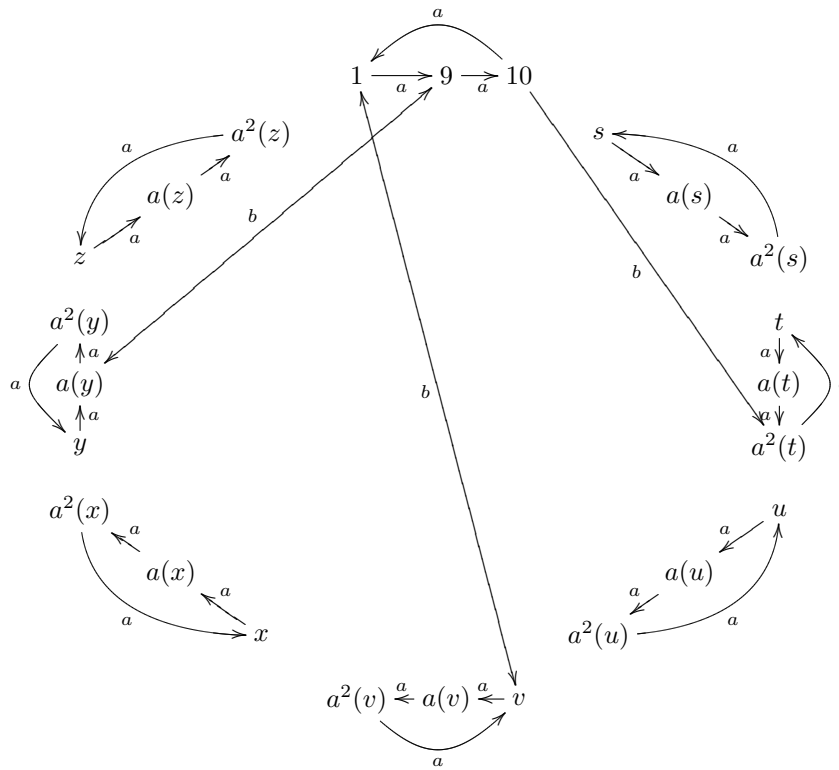
$$a'b'a'^2 = (2, 4)$$

$$a'^2b'a'^2 = (1, 2, 4, 3)$$

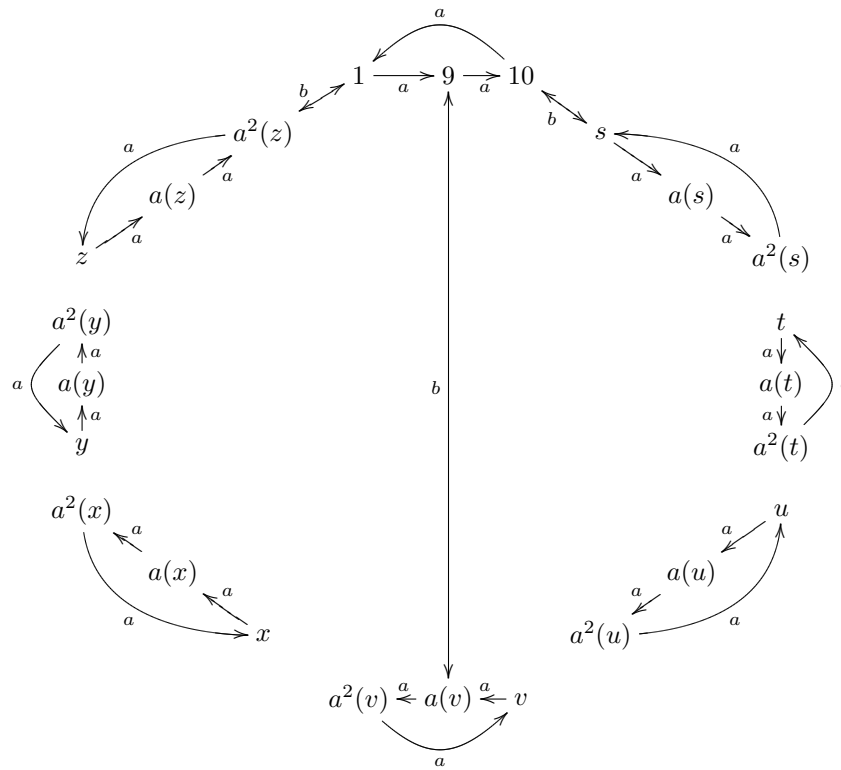
Notice that none of these are equal to b'. If $b(1) = aba(1)$, then $b = aba$, by Theorem 4.1. Therefore $aba(1) \neq b(1)$, and similar for the three other cases.

This tells us neither $b(9)$ or $b(10)$ are equal to $a(v)$ or $a^2(v)$.

A similar argument also says b must send 9 and 10 to different cycles of a. Without loss of generality we can draw:



Our plans of symmetry have not panned out, due to a poor choice for $b(1)$. Without loss of generality we redraw what we have so far, hoping now to connect opposite cycles at the middle:



Now lets look at where b can send v.

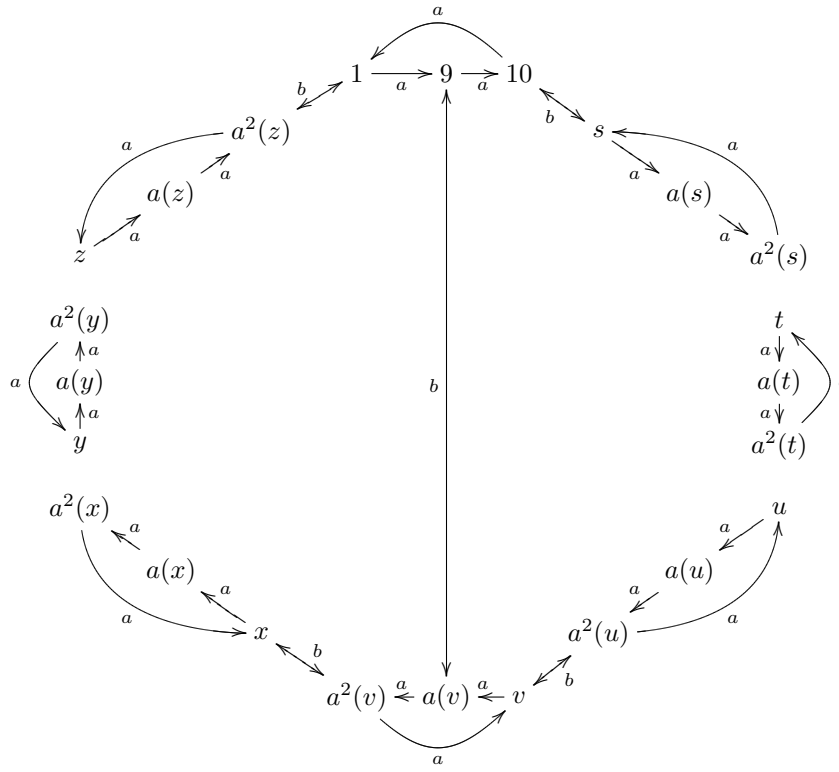
If $b(v) = a(s)$, then $(a^2b)(a^2b)(a^2b) = 1$. To see this, start at the point 9 and apply a^2b thrice to end up back at 9. Since $a'^2b' = (1, 4, 3, 2)$, this is not possible.

Similarly, if $b(v) = a^2(s)$, then $(a^2b)(ab)(a^2b) = 1$. But $(a'^2b')(a'b')(a'^2b') = (2, 3)$, excluding this possibility.

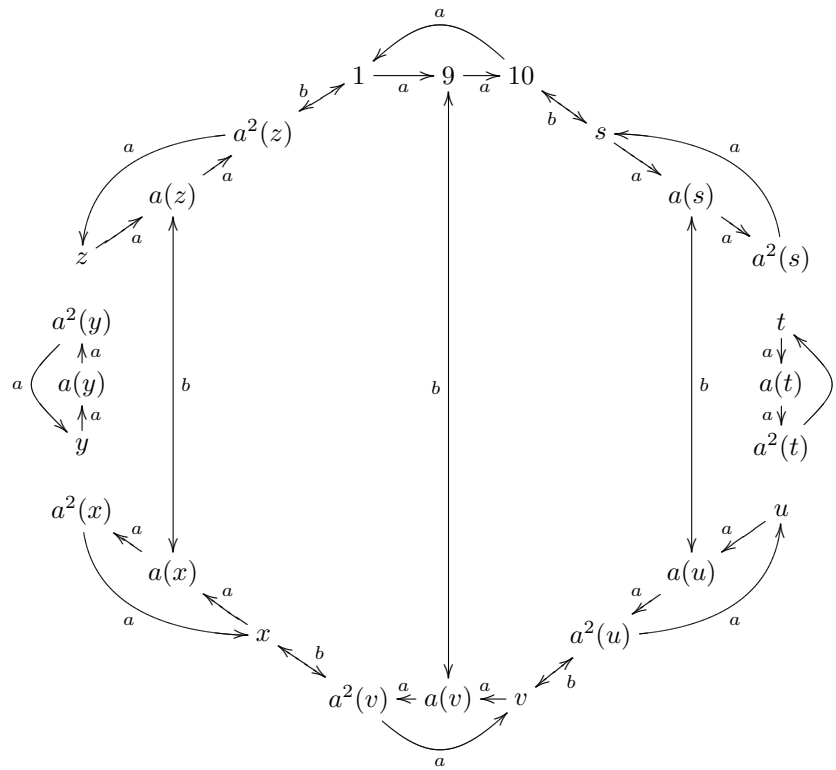
If $b(v) = z$, then $(ab)(a^2b)(a^2b) = 1$. But $(a'b')(a'^2b')(a'^2b') = (1, 3)$.

Finally, if $b(v) = a(z)$, then $(ab)(ab)(a^2b) = 1$. But $(a'b')(a'b')(a'^2b') = (3, 4)$.

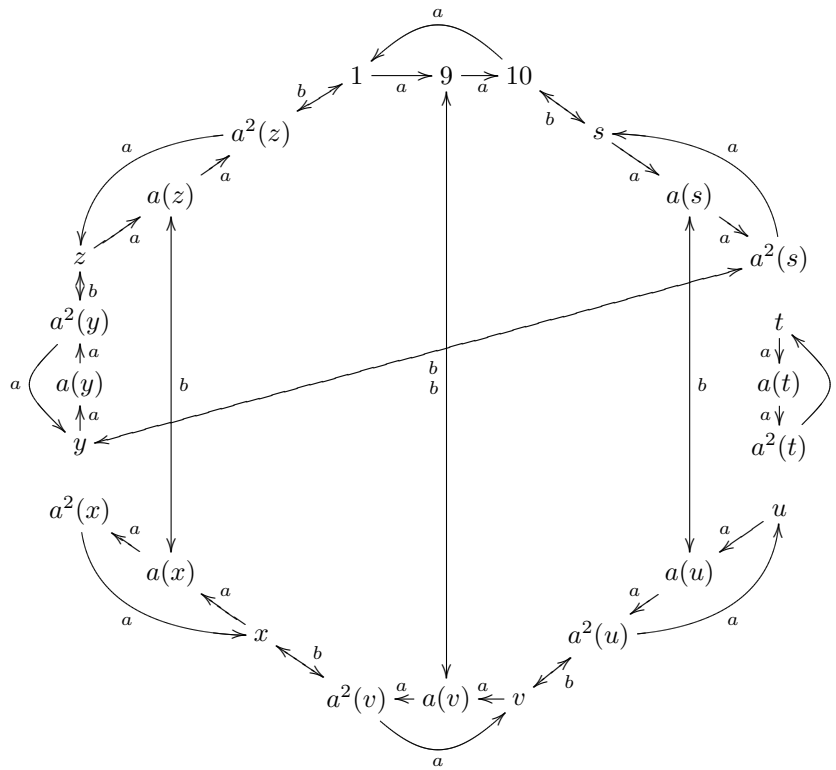
This means $b(v)$ must be one of the unconnected cycles, and by a similar agrument, so must $b(a^2(v))$. Also, we saw earlier that the three b-arrows emanating from one cycle must all go to different cycles:



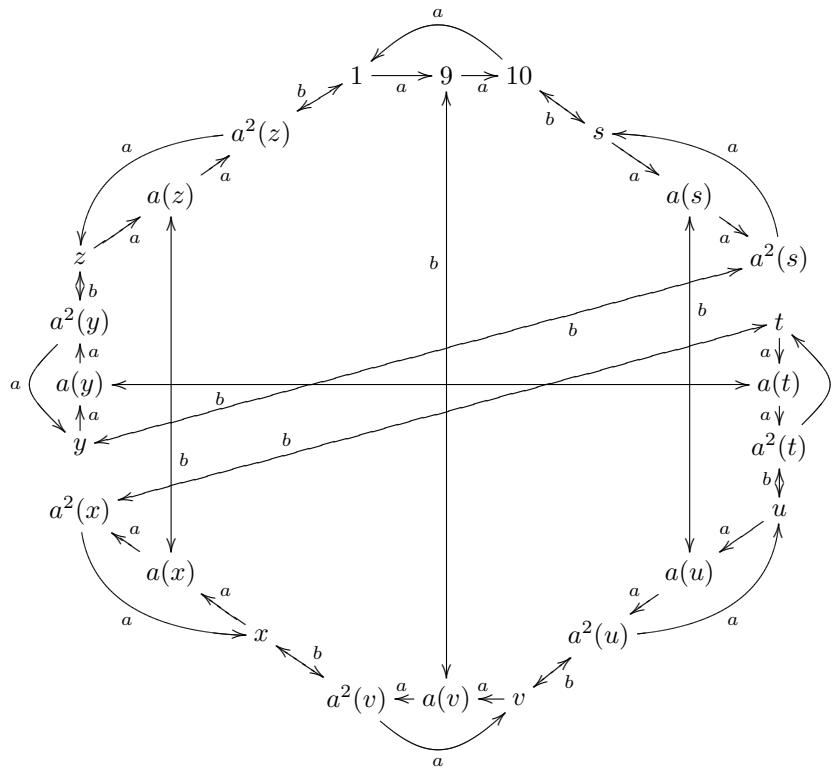
Since $a'b' = (1, 4, 2, 3)$, we know $(ab)^4 = 1$. Starting at $a^2(z)$, we now require $b(a(x)) = a(z)$ to complete the lap in the diagram that is described by $(ab)^4$. A similar argument says $b(a(u)) = a(s)$.



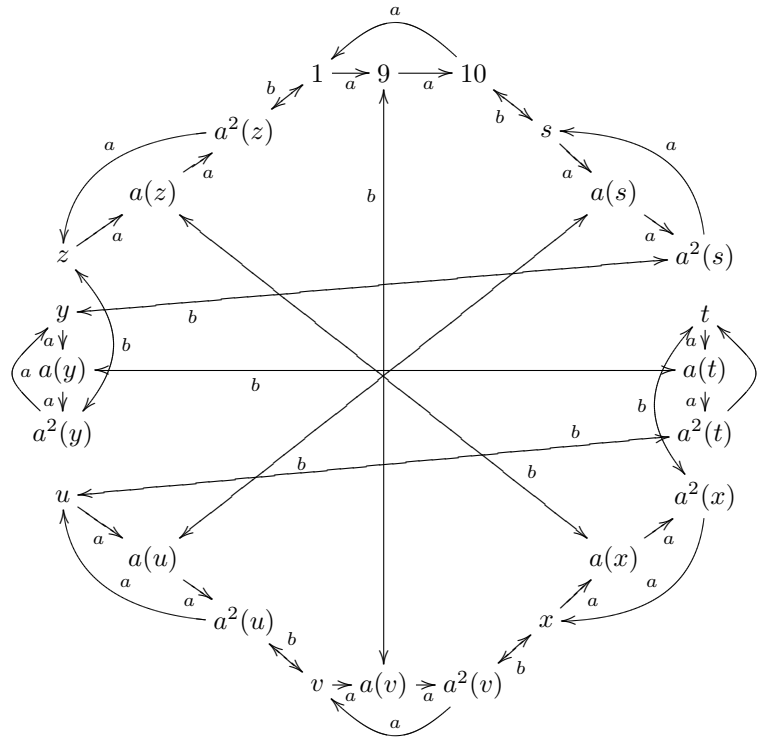
For the cycle containing y, there are now two structurally distinct choices for target of b; the cycle containing t, and any other point with no b-connection. At most one arrow can go from the y-cycle to the t-cycle, so without loss of generality we say $b(a^2(y)) = z$. Recall that a^2b is of odrder 4, thus $(a^2b)^4 = 1$. Starting at $a^2(y)$, we apply $(a^2b)^3$, landing at $a^2(s)$. To complete the lap described by $(a^2b)^4$, we require $b(y) = a^2(s)$.



The cycle containing t now only has three possible places left to link to. The symmetrical choice for $b(t)$ is $b(t) = a^2(x)$.

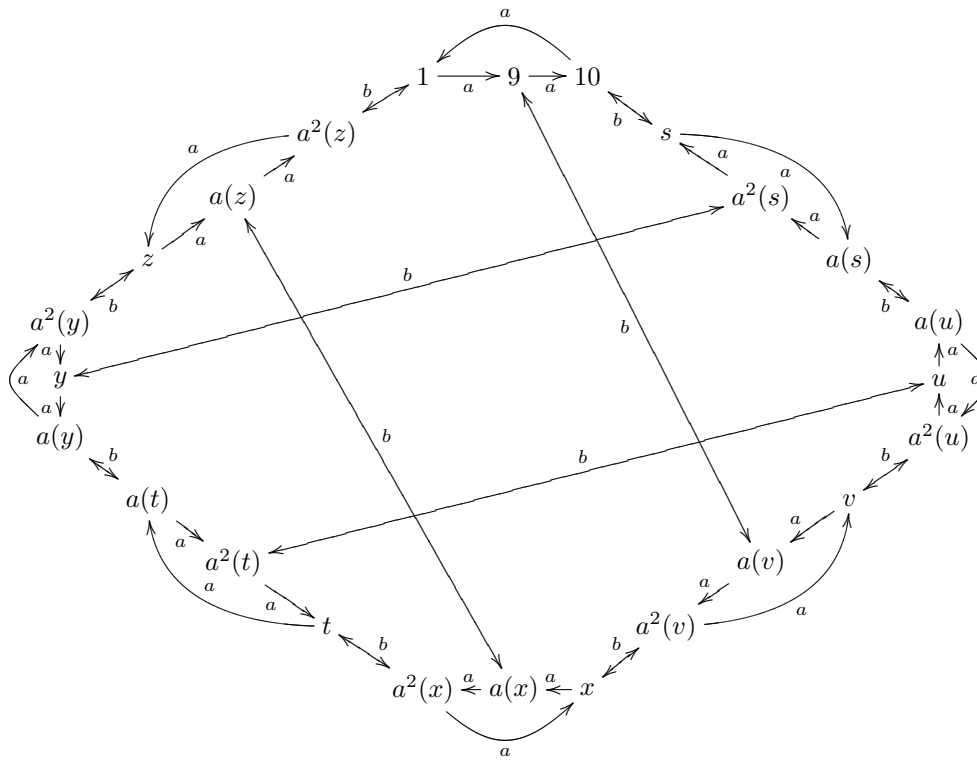


To highlight the symmetry more, we keep manipulating this diagram. First, lets mirror the bottom portion, and the y-cycle, in order to connect opposite cycles at the middle while maintaining symmetry.



At this point we abandon the plan of having b connect the middles of opposite cycles. We instead aim connect the "sides" of each cycle to its nearest neighbor, resulting in a more presentable diagram.

10.2. **The diagram for S_4 inside S_{24}.** Finally we have:



11. Solutions for the extended binary Golay code

In this section we examine some of the groups of order 24 to see if they can define a multiplication that renders the extended binary Golay code an ideal in its ambient space. Unfortunately, we did not get around to testing all such groups, but how this would have been approached should be clear.

We also see that $\mathbb{Z}_{24}$, as well as any group containing an element of order 8, can be immediately discarded.

This is the generator matrix we work with for the extended binary Golay code

$$\text{bin} = \left[\begin{array}{cccccccccccc|cccccccccc|cc}
1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&1&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&1&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1&1&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&0&0&1&1&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&1&0&0&1&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&1&0&0&1&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0&0&1&1&0\\
\hline
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&0&1&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&0&1&0&1&1
\end{array}\right]$$

The additional lines higlight that the 10×10 block consist of the same string, shifted right for each row. The 2×10 and 10×2 blocks have a zig-zag pattern of 1's (and 0's) and are transposes of each other, as is the whole second 12×12 block.

11.1. **Equi-cyclic conjugacy classes of** bin**.** The automorphism group of the extended binary Golay code is the Mathieu group M_{24} (see [3] page 640). The conjugacy classes of M_{24} are known, we simply state the relevant parts here.

For the cycle structures 8^3 (three 8-cycles) and 24, no conjugacy classes exist, meaning no automorphism of bin has one of these cycle structures.

For the remaining equi-cyclic structures, 2^{12}, 3^8, 4^6, 6^4 and 12^2, there is precisely one conjugacy class of each.

The permutation

$$a_{\text{bin}} = (1,7,5,8,9,12,6,2,10,3,4,11)(13,14,17,15,21,23,18,19,22,20,16,24)$$

is an automorphism of bin. Raising a_{bin} to the relevant powers also gives representative elements for the remaining equi-cyclic structures.

11.2. **Applying** D_{12}**.** As in Section 9.2, this whole case can be fully examined by one permutation b. Let a be the above automorphism and $b(1) = 13$, say, then

$$b = (1,13)(2,23)(3,15)(4,17)(5,16)(6,18)(7,24)(8,20)(9,22)(10,21)(11,14)(12,19)$$

To verify that b is indeed an automorphism of bin, apply b to the columns of bin, then add rows together until the first half of the matrix is back to the pattern of the 12×12 identity matrix and observe that the latter half is now identical to the latter half of bin.

There exists a canonical group isomorphism between the permutations of n elements and the $n \times n$ permutation matrices. Let π be this automorphism, such that $\pi(p)$ is the permutation matrix corresponding to the permutation p. Then, with matrix multiplication, the previous verification is the same as saying

$$\text{bin} \times (\pi(p))^T = (\pi(p) \times (\text{bin}^T))^T$$

is row-equivalent to bin.

To test if this group induces a right ideal, find p' in

$$\mathcal{S}(b) = (13, p_2(13), ..., p_{23}(13), p_{24}(13)) = p'(S)$$

where $p_n(1) = n$ identifies the permutations p_i. We include this calculation as an example:

$p_1(13) = 1(13) = 13$
$p_2(13) = a^7(13) = 19$
$p_3(13) = a^9(13) = 20$
$p_4(13) = a^{10}(13) = 16$
$p_5(13) = a^2(13) = 17$
$p_6(13) = a^6(13) = 18$
$p_7(13) = a(13) = 14$
$p_8(13) = a^3(13) = 15$
$p_9(13) = a^4(13) = 21$
$p_{10}(13) = a^8(13) = 22$
$p_{11}(13) = a^{11}(13) = 24$
$p_{12}(13) = a^5(13) = 23$
$p_{13}(13) = b(13) = 1$
$p_{14}(13) = ab(13) = 7$
$p_{15}(13) = a^3b(13) = 8$
$p_{16}(13) = a^{10}b(13) = 4$
$p_{17}(13) = a^2b(13) = 5$
$p_{18}(13) = a^6b(13) = 6$
$p_{19}(13) = a^7b(13) = 2$
$p_{20}(13) = a^9b(13) = 3$
$p_{21}(13) = a^4b(13) = 9$
$p_{22}(13) = a^8b(13) = 10$
$p_{23}(13) = a^5b(13) = 12$
$p_{24}(13) = a^{11}b(13) = 11$

$$p' = (1,13)(2,19)(3,20)(4,16)(5,17)(6,18)(7,14)(8,15)(9,21)(10,22)(11,24)(12,23)$$

It can be verified that p' is not an automorphism of bin, thus $\langle a_{\text{bin}}, b\rangle$ does not induce a right ideal.

11.3. **Applying S_4.** We refer to the diagram in Section 10.2. There are $24-3$ options for choice of s, then $24-3-3$ options for choice of t, and so forth. In total this is $3^7 7! = 11022480$ different options for b, although they come in sets of three that all generate the same group, since b' (from Section 10.1) could have been any one of $(1,4)$, $(2,4)$ or $(3,4)$.

These cases were examined with a computer algorithm.

Although we did not think to count, roughly 700 of these options result in an automorphism, none of which passed the right ideal test.

Here is one generator set for a fixed-point-free representation of S_4 inside S_{24} consisting entirely of automorphisms of bin:

$$a = (1,9,10)(2,11,8)(3,7,12)(4,5,6)(13,21,22)(14,23,20)(15,19,24)(16,17,18)$$

$$b = (1,7)(2,13)(3,21)(4,15)(5,10)(6,14)(8,9)(11,23)(12,24)(16,20)(17,22)(18,19)$$

12. Automorphisms of the extended ternary Golay code

So far, automorphisms of a code have taken the form of permutations. A permutation, p, has a corresponding permutation matrix, $\pi(p)$, that carries the same information. Permutation notation saves space, and highlights the cycle structure more clearly. Both p and $\pi(p)$ act on the code in the same way:

$$p(\text{bin}) = \text{bin} \times \pi(p)^T = (\pi(p) \times (\text{bin}^T))^T$$

To talk about automorphisms of the extended ternary Golay code we will need to talk about monomial matrices, a generalization of permutation matrices.

Definition 12.1. A **monomial matrix** is a $n \times n$ matrix with precisely one nonzero entry in each row and column.

Recall that the ambient space of an extended quadratic residue code is of the form $(\mathbb{Z}_q)^{p+1}$. We have been dealing only with codes where $q = 2$. When $q > 2$, the structure of the automorphisms generalize from permutations (via permutation matrices) to monomial matrices.

Now we lay out some notation that allows us to view the same monomial matrix in different ways. Here is a **monomial matrix**:

$$A_{\text{ter}} = \pi(a_{\text{ter}}) = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The mapping π is now the canonical bijection between monomial permutations (illustrated next) and monomial matrices. This is a generalization of our previous use of π.

Here is the **monomial permutation form** of A_{ter}

$$a_{\text{ter}} = (1_2, 2, 3, 4_2, 5, 8_2)(6_2, 7_2, 9_2, 10, 12, 11)$$

The subscript shows the points a_{ter} multiplies by 2 when passing them along. So, for example

$$a_{\text{ter}}(e_1) = 2e_2$$
$$a_{\text{ter}}(e_2) = e_3$$
$$a^2_{\text{ter}}(e_1) = 2e_3$$
$$a^4_{\text{ter}}(e_1) = e_5$$
$$a^6_{\text{ter}}(x) = 2x$$

and still

$$a_{\text{ter}}(\text{ter}) = \text{ter} \times \pi(a_{\text{ter}})^T$$

Notice how

$$a^6_{\text{ter}}(e_i) = 2e_i$$

for all e_i. This means that a_{ter} really is of order 12:

$$\hat{a}_{\text{ter}} = (e_1, 2e_2, 2e_3, 2e_4, e_5, e_8, 2e_1, e_2, e_3, e_4, 2e_5, 2e_8)$$
$$(e_6, 2e_7, e_9, 2e_{10}, 2e_{12}, 2e_{11}, 2e_6, e_7, 2e_9, e_{10}, e_{12}, e_{11})$$

To write this more simply:

$$\hat{a}_{\text{ter}} = (1, \bar{2}, \bar{3}, \bar{4}, 5, 8, \bar{1}, 2, 3, 4, \bar{5}, \bar{8})(6, \bar{7}, 9, \bar{10}, \bar{12}, \bar{11}, \bar{6}, 7, \bar{9}, 10, 12, 11)$$

We call this the **unpacked monomial permutation**, $\hat{a}_{\text{ter}}$, of a_{ter}.

The **underlying permutation** of a_{ter} is

$$\breve{a}_{\text{ter}} = (1, 2, 3, 4, 5, 8)(6, 7, 9, 10, 12, 11)$$

The automorphism group of the extended ternary Golay code is known to be a double covering of the Mathieu group M_{12} (see [3] page 647). For any permutation like a_{ter}, let its **twin permutation** be

$$\bar{a}_{\text{ter}} = (1, 2_2, 3_2, 4, 5_2, 8)(6, 7, 9, 10_2, 12_2, 11_2)$$

where, if

$$p(e_i) = e_j$$

then

$$\bar{p}(e_i) = 2e_j = \bar{e}_j$$

for all i, j. Above we also introduce the convention that $2e_i = \bar{e}_i$.

The twin of an automorphism is also an automorphism, and these two automorphisms correspond to the same underlying permutation in M_{12}.

For a monomial permutation, a, we write A for the corresponding monomial matrix:

$$\pi(a) = A$$
$$\pi(\check{a}) = \check{A}$$

The conjugacy classes of M_{12} are known. We list the relevant ones:

structure	size	representative
1^{12}	1	()
2^6	396	a^3
3^4	2640	a^2
6^2	7920	$a = (1, 2, 3, 4, 5, 8)(6, 7, 9, 10, 12, 11)$

For every element in a conjugacy class of M_{12} there are two automorphisms of ter that map to it as their underlying permutation and these automorphisms are twins. The conjugacy class of an automorphism, p, is clearly at least as large as the conjugacy class of $\check{p}$, since for any $\check{r}\check{p}\check{r}^{-1}$ in M_{12}, this is the underlying permutation of rpr^{-1}. Either p is in a conjugacy class twice the size of $\check{p}$, or there are two twin conjugacy classes, one containing p and the other $\bar{p}$. In either case we need only examine one representative element.

All equi-cyclic automorphisms of ter taken to the power of the order of their underlying permutation is $2 * I_{12}$, the monomial matrix with all 2's on the diagonal.

In the $q = 2$ case, we dealt with fixed point free permutation groups permuting the ambient basis $\{e_i\}$. For $q = 3$ we instead have to look at permutations of $\{e_i, \bar{e}_i\}$. We still name the (monomial) permutations such that $p_i(1) = i$, where

$$\bar{p}_i = p_{\bar{i}}$$
$$\bar{p}_i(e_i) = \bar{e}_i$$

and multiplication in the ambient space is defined as before.

Previously, our multiplication on the ambient basis was isomorphic to a fixed point free permutation group of order n acting on $\{e_1, e_2, ..., e_n\}$. Now it is instead isomorphic to a fixed point free permutation group of order $2m$ acting on $\{e_1, e_2..., e_m, \bar{e}_1, \bar{e}_2, ..., \bar{e}_m\}$.

Let $\{\check{p}_i\}$ be a fixed point free order 12 permutation group consisting of underlying permutations of automorphisms of ter. Then each of $\check{p}_i$ is the underlying permutation of two automorphisms, p_i and $\bar{p}_i$. Thus $\{p_i, \bar{p}_i\}$ is of order 24.

Theorem 12.2. *$\{p_i, \bar{p}_i\}$ is transitive.*

Proof. Let

$$x, y \in \{e_1, e_2..., e_m, \bar{e}_1, \bar{e}_2, ..., \bar{e}_m\}$$

and let

$$\check{x}, \check{y} \in \{e_1, e_2..., e_m\}$$

where

$$\check{e}_i = \check{\bar{e}}_i = e_i$$

We show the existance of some j such that $p_j(x) = y$. Because $\{\check{p}_i\}$ is a maximal order fixed-point-free permutation group, it is transitive. Therefore there exists some $\check{p}_j \in \{\check{p}_i\}$ such that

$$\check{p}_j(\check{x}) = \check{y}$$

Let p_j be an automorphism with $\check{p}_j$ as its underlying permutation. Then, either

$$p_j(x) = y$$

in which case we are done, or

$$p_j(x) = \check{y}$$

But then

$$\bar{p}_j(x) = y$$

□

Since $\{p_i, \bar{p}_i\}$ is a transitive order 24 permutation group consisting of permutations of $\{e_1, e_2..., e_{12}, \bar{e}_1, \bar{e}_2, ..., \bar{e}_{12}\}$, it must be a fixed point free permutation group.

It now remains to comment on the relationship

$$e_{\bar{p}_n(m)} = \bar{e}_n e_m = (2e_n)e_m = e_n e_m + e_n e_m = 2e_{p_n(m)}$$

and similarly for $e_n \bar{e}_m$, which ensures multiplication distributes over addition.

13. Extended ternary Golay code results

Now we are ready to look for a multiplication on the ambient space of the extended ternary Golay code.

We use the following generator matrix for the extended Ternary Golay code:

$$\text{ter} = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 & 2 & 1 & 0 \end{array}\right]$$

However, we have seen this generator matrix used as well:

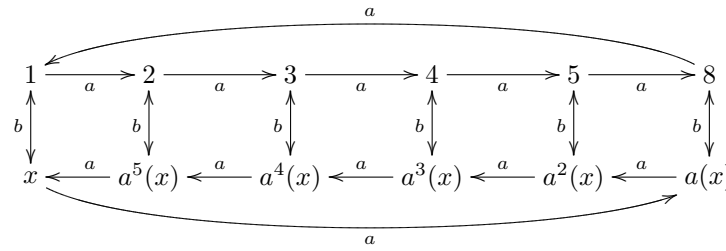
$$\text{ter'} = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{array}\right]$$

We prefer the former, since the sum of all rows is the word consisting of only 1's. The latter has a self transpose second block, however. Automorphisms are very similar in the two cases, simply multiply the point sent to seven, and the point seven is sent to by 2 to change between them.

The remainder of this text uses the generator matrix ter.

13.1. **Applying D_6.** Here is a diagram for D_6, building on

$$a = (1_2, 2, 3, 4_2, 5, 8_2)(6_2, 7_2, 9_2, 10, 12, 11)$$



Any choice for x will result in the same permutation group, since, if $b(1) = 6$ and $b'(1) = 7$, then

$$ab = b'$$

and so forth.

With $b(1) = x = 6$, we test if

$$\check{b} = (1, 6)(2, 11)(3, 12)(4, 10)(5, 9)(7, 8)$$

is the underlying permutation for some automorphism of ter. Indeed

$$b = (1_2, 6)(2, 11_2)(3, 12_2)(4, 10_2)(5, 9_2)(7, 8_2)$$

and its twin are automorphisms of ter.

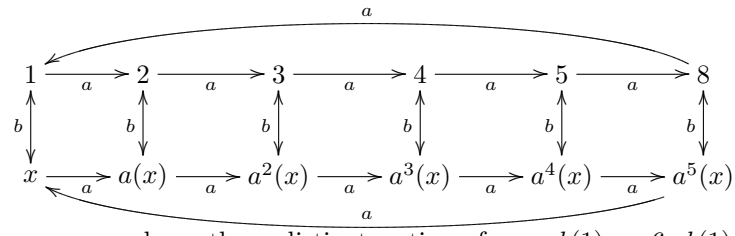
We use the unpacked permutations to do the right ideal test. Although $\|\hat{a}\| * \|\hat{b}\| = 48$, the equality $\hat{a}^6 = \hat{b}^2$ ensures the group $\langle \hat{a}, \hat{b} \rangle$ has order 24.

$$\begin{array}{ll}
p_1 = 1 & \bar{p}_1 = \hat{a}^6 \\
p_2 = \hat{a}^7 & \bar{p}_2 = \hat{a} \\
p_3 = \hat{a}^8 & \bar{p}_3 = \hat{a}^2 \\
p_4 = \hat{a}^9 & \bar{p}_4 = \hat{a}^3 \\
p_5 = \hat{a}^4 & \bar{p}_5 = \hat{a}^{10} \\
p_6 = \hat{a}^6\hat{b} & \bar{p}_6 = \hat{b} \\
p_7 = \hat{a}\hat{b} & \bar{p}_7 = \hat{a}^7 b \\
p_8 = \hat{a}^5 & \bar{p}_8 = \hat{a}^{11} \\
p_9 = \hat{a}^8\hat{b} & \bar{p}_9 = \hat{a}^2 b \\
p_{10} = \hat{a}^3 b & \bar{p}_{10} = \hat{a}^9 b \\
p_{11} = \hat{a}^5 b & \bar{p}_{11} = \hat{a}^{11} b \\
p_{12} = \hat{a}^4\hat{b} & \bar{p}_{12} = \hat{a}^{10} b
\end{array}$$

$$\begin{aligned}
\mathcal{S}(\hat{a}) &= \begin{pmatrix} 1 & 2 & ... & 2n \\ p_1(\bar{2}) & p_2(\bar{2}) & ... & \bar{p}_n(\bar{2}) \end{pmatrix} \\
&= (1_2, 8, 5_2, 4, 3, 2_2)(6_2, 7_2, 9_2, 10, 12, 11)
\end{aligned}$$

This is not an automorphism of ter.

13.2. **Applying $(\mathbb{Z})^6 \times (\mathbb{Z})^2$.** The diagram for this case looks a lot like the previous one



However, now we have three distinct options for x; $b(1) = 6$, $b(1) = 7$ and $b(1) = 9$, where only

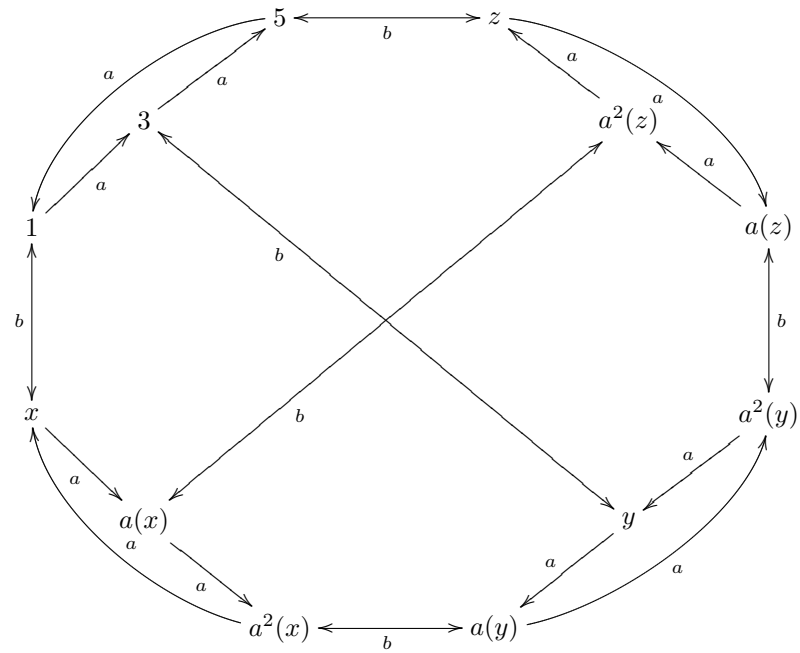
$$\check{b} = (1, 9)(2, 10)(3, 12)(4, 11)(5, 6)(7, 8)$$

is the underlying permutation of an automorphism, namely

$$b = (1, 9_2)(2_2, 10)(3, 12_2)(4_2, 11)(5_2, 6)(7, 8_2)$$

13.3. **Applying A_4.** We build the diagram for the case A_4, the alternating group on four elements, on the automorphism

$$a = (1_2, 3_2, 5_2)(2, 4_2, 8)(6, 9_2, 12)(7, 10, 11_2)$$



Here there are 9 options for x, followed by 6 for y and 3 for z. However, these options come in sets of three, that all generate the same group.

Listing only one of each such set, the following automorphisms all generate the desired group when combined with a, individually:

$$b = (1, 2_2)(3, 12_2)(4_2, 7)(5_2, 10)(6, 8_2)(9_2, 11)$$

$$c = (1_2, 4)(2, 12_2)(3, 9_2)(5, 10_2)(5, 11_2)(7, 8_2)$$

$$d = (1, 4_2)(2_2, 6)(3, 12_2)(5_2, 7)(8_2, 11)(9_2, 10)$$

$$e = (1_2, 8)(2, 10_2)(3, 6_2)(4_2, 9)(5_2, 11)(7, 12_2)$$
$$f = (1_2, 2)(3, 11_2)(4, 9_2)(5, 12_2)(6, 10_2)(7, 8_2)$$
$$g = (1_2, 4)(2_2, 10)(3_2, 7)(5, 9_2)(6_2, 8)(11, 12_2)$$
$$h = (1_2, 4)(2_2, 11)(3_2, 10)(5, 6_2)(7, 9_2)(8, 12_2)$$
$$i = (1, 8_2)(2, 12_2)(3_2, 7)(4_2, 10)(5, 6_2)(9, 11_2)$$

References

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

[2] MacWilliams, F. J., Sloane, N. J. A., *The theory of error-correcting codes. I*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–xv and 1–369.

[3] ———, *The theory of error-correcting codes. II*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–ix and 370–762.