university of groningen

faculty of science and engineering

mathematics and applied mathematics

Determining the Normal Closure & Galois Group of some Field Extension over **F2** and Good Error Correcting Codes

Bachelor's Project Mathematics

April 2024

Student: H.S. Crane

First supervisor: Prof.dr. J. Top

Second assessor: Dr. P. Kılıçer

1 Introduction

In a paper [3] by Jaap Top, a certain tower of quadratic extensions of fields

$$\mathbb{F}_2(x) \subset K_1 \subset K_2 \subset K_3 \subset K_4$$

is constructed, with $\mathbb{F}_2(x)$ denoting the field of rational functions over the field $\mathbb{F}_2$ of cardinality 2, and such that $K_4 \supset K_1$ is a Galois extension with Galois group $\mathrm{Gal}(K_4/K_1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

A goal of the present thesis is to show that the total extension $K_4 \supset \mathbb{F}_2(x)$ is *not* Galois, and to describe the normal closure N of this extension and its Galois group over $\mathbb{F}_2(x)$. Moreover, we consider intermediate fields and we use examples of those for constructing error correcting codes, as explained, for example, in Chapter 2 of H. Stichtenoth's textbook [2] and in less detail at the end of this text.

2 Preliminaries

First we recall the explicit definition of the fields mentioned in Section 1 and we discuss the Galois group $\mathrm{Gal}(K_4/K_1)$.

The first extension is

$$\mathbb{F}_2(x) \subset K_1 = \mathbb{F}_2(x, y)$$

where y solves

$$T^2 + T = x^3 + x.$$

We claim that this extension has degree 2. This is equivalent to the statement that

$$T^2 + T + x^3 + x \in \mathbb{F}_2(x)[T]$$

is irreducible, i.e. has no zero in $\mathbb{F}_2(x)$.

To verify that indeed no such zero exists, note that it would look like some

$$\frac{f(x)}{g(x)} \text{ with } f, g \in \mathbf{F}_2[x] \text{ satisfying } \gcd(f, g) = 1.$$

Being a zero of $T^2 + T + x^3 + x$ implies

$$f(x)^2 = f(x)g(x) + (x^3 + x)g(x)^2,$$

hence

$$g(x)|f(x)^2.$$

Since

$$gcd(f, g) = 1,$$

this implies

$$g(x) = 1$$

leaving

$$f(x)^2 + f(x) = (x^3 + x).$$

Comparing degrees now shows that no such f exists. Hence the polynomial $T^2 + T + x^3 + x$ is irreducible in $\mathbb{F}_2(x)[T]$ and the degree of the extension $\mathbb{F}_2(x) \subset K_1 = \mathbb{F}_2(x, y)$ is therefore as claimed equal to 2.

(We have checked throughout this text the degrees of extensions like this by finding irreducibly of polynomials using Magma but I have also included a few examples like the above to show how this is done manually).

Now we add w_1, namely

$$K_1 = \mathbb{F}_2(x, y) \subset \mathbb{F}_2(x, y, w_1) = K_2$$

where w_1 solves

$$(x^7 + x + 1)(T^2 + T) = (x^5 + x)y + x^2 + x.$$

Again, this extension has degree 2 over $\mathbb{F}_2(x, y)$; in other words, the polynomial $T^2 + T +$ in $\mathbb{F}_2(x, y)[T]$ is irreducibe. This is checked, using the computer algebra system Magma (see [1]) as follows.

```
K0<x>:=FunctionField(GF(2));
P0<T>:=PolynomialRing(K0);
K1<y>:=ext<K0 | T^2+T+x^3+x>;
P1<T>:=PolynomialRing(K1);
IsIrreducible( T^2+T+((x^5+x)*y+x^2+x)/(x^7+x+1) );
```

We now present a direct proof of this irreducibility, without using Magma.

Write the given polynomial as

$$T^2 + T + r(x) + s(x)y$$

where $r(x) = \frac{x^2+x}{x^7+x+1}$ and $s(x) = \frac{x^5+x}{x^7+x+1}$. If it were reducible in $K_1[T] = \mathbb{F}_2(x, y)[T]$, it would have zeroes

$$\alpha, (\alpha + 1)$$

where

$$\alpha = a + by \in \mathbb{F}_2(x, y).$$

Comparing the constant term we see

$$r(x) + s(x)y = \alpha(\alpha + 1).$$

Since

$$\alpha(\alpha + 1) = (a + by)(a + by + 1) = a^2 + b^2y^2 + a + by$$

which, using

$$y^2 = x^3 + x + y$$

implies

$$\alpha(\alpha + 1) = a^2 + a + by + b^2(x^3 + x + y) = a^2 + a + b^2x^3 + b^2x + (b + b^2)y,$$

one concludes

$$s(x) = b + b^2.$$

We claim that no $b \in \mathbb{F}_2(x)$ exists satisfying $b^2 + b = s(x) := \frac{x^5+x}{x^7+x+1}$.

Firstly, note if $b \in \mathbb{F}_2(x)$ this means

$$b = \frac{f}{g} \qquad f, g \in \mathbb{F}_2[x], \quad gcd(f, g) = 1$$

$$\frac{f^2}{g^2} + \frac{f}{g} = \frac{x^5 + x}{x^7 + x + 1}$$

$$f^2(x^7 + x + 1) + fg(x^7 + x + 1) = g^2(x^5 + x)$$

which implies the following:

$$f|g^2(x^5 + x)$$

as $\gcd(f, g) = 1$ then

$$f|(x^5 + x)$$

and similarly,

$$g|(x^7 + x + 1)$$

but $x^7 + x + 1$ is irreducible so

$$g = x^7 + x + 1 \quad or \quad g = 1.$$

Case 1: $g = 1$

$$\frac{f^2}{g^2} + \frac{f}{g} = \frac{x^5 + x}{x^7 + x + 1}$$

$$f^2 + f = \frac{(x^5 + x)}{(x^7 + x + 1)}$$

which is clearly untrue as f is not a fraction and lies in $\mathbb{F}_2[x]$.

Next case: $g = (x^7 + x + 1)$

$$f^2 + f = (x^7 + x + 1)(x^5 + x)$$

as $(x^7 + x + 1)$ is irreducible

$$f|(x^5 + x)$$

but the f^2 term will never have degree 12 if $f|(x^5 + x)$ so this situation is also impossible proving the claim.

As a consequence, K_2 has degree $2 \cdot 2 = 4$ over $\mathbb{F}_2(x)$. The next step is

$$K_2 = \mathbb{F}_2(x, y, w_1) \subset \mathbb{F}_2(x, y, w_1.w_2) = K_3$$

where w_2 solves

$$(x^7 + x + 1)(T^2 + T) = (x^5 + x^4 + x^3 + x) \cdot y + x^6 + x^4.$$

The fact that $[K_3 : K_2] = 2$ is verified using Magma, see below.

```
K2<w1>:=ext<K1 | T^2+T+((x^5+x)*y+x^2+x)/(x^7+x+1) >;
P2<T>:=PolynomialRing(K2);
pol3:=T^2+T+((x^5+x^4+x^3+x)*y+x^6+x^5)/(x^7+x+1);
IsIrreducible(pol3);
K3<w2>:=ext<K2 | pol3>;
P3<T>:=PolynomialRing(K3);
pol4:=T^2+T+((x^6+x^5)*y+x^(10)+x^6+x^2+x)/(x^(14)+x^2+1);
IsIrreducible(pol4);
K4<w3>:=ext<K3 | pol4>;
```

The last few lines here verify that

$$K_3 = \mathbb{F}_2(x, y, w_1, w_2) \subset \mathbb{F}_2(x, y, w_1, w_2, w_3) = K_4$$

where w_3 solves

$$(x^{14} + x^2 + 1)(T^2 + T) = (x^6 + x^5)y + x^{10} + x^6 + x^2 + x,$$

defines a quadratic extension as well.

In total we now have a degree 16 extension over $\mathbb{F}_2(x)$ where all consecutive steps have degree 2:

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x,y) \subset \mathbb{F}_2(x,y,w_1) \subset \mathbb{F}_2(x,y,w_1,w_2) \subset \mathbb{F}_2(x,y,w_1,w_2,w_3).$$

Notice that over a field K of characteristic 2 a field extension by some α which has minimal polynomial

$$f := T^2 + T + a \in K[T],$$

one has $f(\alpha) = 0$ and also

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^2 + (\alpha+1)) + a \\ &= (\alpha^2 + 2\alpha + 1 + (\alpha+1)) + a \\ &= (\alpha^2 + 2\alpha + 2 + \alpha) + a \\ &= \alpha^2 + \alpha + a = 0. \end{aligned}$$

Hence $\alpha+1$ is the other root of the polynomial so all our quadratic extensions are normal. Moreover, the total extension is separable as each individual extension is the splitting field of a separable polynomial. The extension $K_4 \supset K_1 = \mathbb{F}_2(x,y)$ is Galois since it is the compositum of three separable quadratic extensions of $\mathbb{F}_2(x,y)$. Moreover

$$\mathrm{Gal}(K_4/K_1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

since any automorphism permutes each of the three sets $\{w_j, w_j+1\}$ and this can be done independently.

3 Are the given extensions $\mathbb{F}_2(x) \subset \mathbb{F}_2(x,y,w_i)$ normal and therefore Galois?

In this section we will discover that the aforementioned extensions are not normal. To show the extensions are not normal we will do the case for w_1 in detail. The others, we have checked using Magma are also not normal.

First we prove a small aside claim that possibly could be useful for further investigations into the subject. We claim:

$$\mathbb{F}_2(x,w_1) = \mathbb{F}_2(x,y,w_1).$$

This is easily shown. Rewrite

$$(x^7+x+1)(w_1^2+w_1) = (x^5+x)y + x^2 + x$$

in terms of y as

$$y = \frac{(x^7+x+1)(w_1^2+w_1)-(x^2+x)}{(x^5+x)} \in \mathbb{F}_2(x, w_1)$$

showing the inclusion

$$\mathbb{F}_2(x, y, w_1) \subset \mathbb{F}_2(x, w_1).$$

The reverse inclusion is trivial so indeed

$$\mathbb{F}_2(x, w_1) = \mathbb{F}_2(x, w_1, y).$$

Now let's see if adjoining a w_i to $\mathbb{F}_2(x)$ makes a normal extension. Again we will simply look at one case in detail then do the following similar cases using Magma.

Let's find the normal closure of $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1)$ or equivalently the normal closure of $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1)$. To do this we need all the roots of w_1's minimal polynomial over $\mathbb{F}_2(x)$. Note that one $\mathbb{F}_2(x)$ linear automorphism of $\mathbb{F}_2(x, y, w_1)$ can be constructed by extending the automorphism ϕ of extension $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y)$ that sends y to $y+1$. Then ϕ changes the minimal polynomial of w_1 over $\mathbb{F}_2(x, y)$ to a new polynomial. Explicitly, ϕ acts on our polynomial

$$(x^7+x+1)(T^2+T)+(x^5+x)y+x^2+x$$

changing it to

$$(x^7+x+1)(T^2+T)+(x^5+x)(y+1)+x^2+x.$$

Hence any extension of ϕ to the normal closure of $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1)$ needs to map w_1 to a zero of the latter polynomial. Using Magma, it turns out that this polynomial is irreducible, even over $K_4 = \mathbb{F}_2(x, w_1, w_2, w_3)$. So to obtain the normal closure, we need to adjoin the roots α and $\alpha+1$ of the latter polynomial to K_4. Then $w_1, w_1+1, \alpha, \alpha+1$ are the zeros of

$$(x^7+x+1)(T^2+T)+(x^5+x)y+x^2+x)((x^7+x+1)(T^2+T)+(x^5+x)(y+1)+x^2+x$$

$$=$$

$$(x^{14}+x^2+1)T^4+(x^1+x^{12}+x^8+x^6+x^5+x+1)T^2$$
$$+(x^{12}+x^8+x^6+x^5+x^2+x)T+x^{13}+x^{11}+x^7+x^6+x^5+x^4.$$

Similarly, using Magma we discover that taking further extensions including w_2 and w_3 and including the roots that we obtain again by using the automorphism that sends y to $y+1$ for each of the equations that w_2 w_3 solve call these roots α_2 and α_3 consecutively we get two further normal extensions of degree 4. So from our first normal extension

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1, \alpha_1)$$

we take two consecutive normal extensions one which is

$$\mathbb{F}_2(x, w_1, \alpha_1) \subset \mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2)$$

which is degree 4. Then,

$$\mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2) \subset \mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$$

which is also degree 4 i.e. adding in a w_i and α_i never gives us the other w_i's or α_i's . By using the tower law we see we have extensions of degrees 8, 4 and 4 so the total normal closure

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$$

has degree

$$8 \cdot 4 \cdot 4 = 128$$

For the Magma code below: Please be aware that doing the degree 128 extension will not run as it is too large. Instead you can look at individual extensions if you wish.

```
K0<x>:=FunctionField(GF(2));
P0<T>:=PolynomialRing(K0);
K1<y>:=ext<K0 | T^2+T+x^3+x>;
P1<T>:=PolynomialRing(K1);
IsIrreducible( T^2+T+((x^5+x)*y+x^2+x)/(x^7+x+1) );
Kw1<w1>:=ext<K1 | T^2+T+((x^5+x)*y+x^2+x)/(x^7+x+1) >;
P2<T>:=PolynomialRing(Kw1);
IsIrreducible( T^2+T+((x^5+x)*(y+1)+x^2+x)/(x^7+x+1) );
Ka1<a1>:=ext<Kw1 | T^2+T+((x^5+x)*(y+1)+x^2+x)/(x^7+x+1)>;
P3<T>:=PolynomialRing(Ka1);
pw2:=T^2+T+((x^5 +x^4+x^3+x)*y + x^6 + x^4)/(x^7 + x + 1));
IsIrreducible(pw2);
Kw2<w2>:=ext<Ka1 | pw2 >;
P4<T>:=PolynomialRing(Kw2);
pa2:=T^2+T+((x^5+x^4+x^3+x)*(y+1)+x^6+x^4)/(x^7+x+1));
```

```
IsIrreducible(pa2);
Ka2<a2>:=ext<Kw2 | pa2 >;
P5<T>:=PolynomialRing(Ka2);
pw3:=(x^(14)+x^2+1)*(T^2+T)+(x^6+x^5)*y+x^(10)+x^6+x^2+x;
IsIrreducible(pw3);
Kw3<w3>:=ext<Ka2 | pw3 >;
P6<T>:=PolynomialRing(Kw3);
pa3:=(x^(14)+x^2+1)*(T^2+T)+(x^6+x^5)*(y+1)+x^(10)+x^6+x^2+x;
IsIrreducible(pa3);
Ka3<a3>:=ext<Kw3 | pa3 >;
```

3.1 What is the Galois Group of our normal closure $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$

To find the Galois group, we first consider the smaller Galois extensions $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1, \alpha_1)$, $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_2, \alpha_2)$ and $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_3, \alpha_3)$ and their Galois groups . Magma tells us that these extensions all have Galois group equivalent to the dihedral group of 8 elements. Let's take a small detour to understand why this is true.

We restrict our attention to

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, w_1, \alpha)$$

as all other cases are analogous. We know that any automorphism permutes the roots $\alpha, \alpha+1, w_1, w_1+1$ of the minimal polynomial of w_1 over $\mathbb{F}_2(x)$, and is in fact determined by this. We now construct the possible automorphisms by considering the possible extensions of automorphisms on the intermediate field

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y) \subset \mathbb{F}_2(x, w_1, \alpha_1).$$

There are two automorphisms of the intermediate field, namely the identity and the automorphism that sends y to $y+1$.

Lets look a bit deeper at the two cases. First we take any of the automorphisms that fixes y. Since the minimal polynomials of w_1 and of α_1 over $\mathbb{F}_2(x, y)$ are the quadratic polynomials we saw earlier, the only possible extensions of the identity on y are the maps that send w_1 to either w_1 or w_1+1, and similarly α_1 to one of α_1, α_1+1. In total this gives 4 extensions of the identity.

Now consider possible extensions of an automorphism that sends y to $y+1$, hence that interchanges the minimal polynomials of w_1 and of α_1 over

$\mathbb{F}_2(x,y)$. Such an extension must send w_1 to α_1 or α_1+1 and similarly α_1 to one of w_1, w_1+1. This gives 4 posibilities. In total we have now described 8 possible automorphisms of $\mathbb{F}_2(x,w_1,\alpha_1)$ over $\mathbb{F}_2(x)$. As this number equals the degree of the field extension, each of the possibilities indeed occurs and we found the Galois group. Explicitly, consider τ given by

$$\tau\colon y\mapsto y+1 \text{ and } w_1\mapsto \alpha_1\mapsto w_1+1\mapsto \alpha_1+1.$$

It is easy to see that τ has order 4. This is our "rotation". Similarly, we can pick

$$\sigma\colon y\mapsto y \text{ and } w1\mapsto w_1+1 \text{ and } \alpha\mapsto\alpha.$$

This is our 'reflection'; it clearly has order two. It is easily verified that $\sigma\tau\sigma^{-1}=\tau^{-1}$, by checking what both maps do to the generators y, w_1, α_1. This shows that σ, τ generate the dihedral group of order 8. Any element of the Galois group then is some

$$\tau^n\cdot\sigma^m,\quad n\in\{0,1,2,3\},\quad m\in\{0,1\}.$$

We checked using Magma this is not just true for $\mathbb{F}_2(x,w_1,\alpha_1)$ but also for $\mathbb{F}_2(x,w_2,\alpha_2)$ and $\mathbb{F}_2(x,w_3,\alpha_3)$. With this knowledge we now take a look at the bigger Galois extension:

$$\mathbb{F}_2(x)\subset\mathbb{F}_2(x,w_1,\alpha_1,w_2,\alpha_2,w_3,\alpha_3).$$

Restricting elements in the big Galois group G to the subfields $\mathbb{F}_2(x,w_j,\alpha_j)$ (since these fields are Galois over $\mathbb{F}_2(x)$, restriction yields automorphisms of the smaller fields), I claim and will prove one obtains an injective homormorphism to $D_8\times D_8\times D_8$ which more importantly means for our group the following:

$$G:=\mathrm{Gal}(\mathbb{F}_2(x,w_1,\alpha_1,w_2,\alpha_2,w_3,\alpha_3)/\mathbb{F}_2(x))\subset D_8\times D_8\times D_8.$$

Let's see why the map given by these three restrictions is injective. It is given as

$$\phi\colon\sigma\mapsto(a_1,a_2,a_3)$$

where $\sigma\in\mathrm{Gal}(\mathbb{F}_2(x,w_1,\alpha_1,w_2,\alpha_2,w_3,\alpha_3)/\mathbb{F}_2(x))$ is mapped to the triple with $a_j=\sigma|_{\mathbb{F}_2(x,w_j,\alpha_j)}\in\mathrm{Gal}(\mathbb{F}_2(x,w_j,\alpha_j)/\mathbb{F}_2(x))\cong D_8$.

What is the kernel of ϕ. Well it must be maps σ that when restricted to each individual extension give the identity,

$$\phi(\sigma)=(Id,Id,Id).$$

This means therefore that our σ fixes each of $w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3$. Hence σ is the identity automorphism which means the kernel of the map ϕ is the identity and hence the map ϕ is injective.

To summarize: the injectivity of ϕ means the Galois group G of the big extension must be some subgroup of $D_8 \times D_8 \times D_8$. This subgroup has order 128 because the order equals the degree of the extension

$$\mathbb{F}_2(x, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3) \supset \mathbb{F}_2(x).$$

Note that $D_8 \times D_8 \times D_8$ has order $8^3 = 512$. The question is therefore: which subgroup is G? Well similarly to above we know some things about the automorphisms we are interested in: they are some extension of an automorphism of $\mathbb{F}_2(x, y)$ that fixes $\mathbb{F}_2(x)$. In other words, if $\phi(\sigma) = (a_1, a_2, a_3)$, then for each j we have $a_j|_{\mathbb{F}_2(x,y)} = \sigma|_{\mathbb{F}_2(x,y)}$. This rules out a number of the possible combinations in $D_8 \times D_8 \times D_8$.

More formally, create a further map:

$$\psi\colon D_8 \times D_8 \times D_8 \mapsto \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

given by restricting elements in $\mathrm{Gal}(\mathbb{F}_2(x, y, w_1, w_2, w_3, \alpha_1, \alpha_2, \alpha_3)/\mathbb{F}_2(x))$ to the subfield $\mathbb{F}_2(x, y)$ and observing that $\mathrm{Gal}(\mathbb{F}_2(x, y)/\mathbb{F}_2(x)) \cong \mathbb{Z}/2\mathbb{Z}$. The combinations which have image $(0, 0, 0)$ or $(1, 1, 1)$ form precisely the elements of the Galois Group we are interested in - note that there are $2 \cdot \#\mathrm{Ker}(\psi) = 2 \cdot 8^3/8 = 128$ such combinations. So

$$G = \psi^{-1}(\langle(1, 1, 1)\rangle) \subset D_8 \times D_8 \times D_8.$$

3.2 Note On Our Ability To Find Intermediate Fields Of The Normal Closure Using Magma

Now we know what the Galois Group is, another part of this project intended to use Magma to compute such things as the genus and the number of “degree 1 places” of the intermediate fields. Our use of Magma or possibly Magma itself struggles to compute inside the large extension of degree 128. The reader can note two things in case a follow up attempt is made:

1. We have asked the team at Magma and they ran my code on their version which allows a longer loading time (as opposed to the online version which is just 2 minutes then it cuts out.) The code could still not be executed this is not because there is an error rather the way Magma computes the field

extensions is not suitable to how I wrote out the code. Perhaps there is a more efficient way but for now we leave it as an open task.

2. Perhaps it will be useful for using Magma in an efficient way, to present the used extension of our base field in one go by adjoining a zero of an irreducible polynomial of degree 128 rather than in many consecutive steps of degree 2. In fact, we have

$$\mathbb{F}_2(x, y, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3) = \mathbb{F}_2(x, y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3).$$

I will now prove this. As the extension is Galois over $\mathbb{F}_2(x)$ we just need to show the element $(y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3)$ has orbit consisting of 128 elements under the action of the Galois group G. This is because such an element would NOT be fixed by any restriction of any map to a smaller Galois group of an intermediate field. Meaning, it lies in the largest field but not in any intermediate field so its minimal polynomial must have degree 128 the same degree as the largest extension. So it is at least isomorphic to the large field but as the element lies in the large field they must be the same and this element generates the extension therefore. To see why the element has orbit 128 consider a basis of

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$$

i.e.

$$1, y, w_1, y \cdot w_1, w_2, w_2 \cdot y, w_2 \cdot w_1, w_2 \cdot y \cdot w_1, w_3, w_3 \cdot y.w_3 \cdot w_1, w_3 \cdot w_2, w_3 \cdot y \cdot w_1, \cdots$$

(all products $y^{n_1} w_1^{n_2} w_2^{n_3} w_3^{n_4} \alpha_1^{n_5} \alpha_2^{n_6} \alpha_3^{n_7}$ with $n_1, \ldots, n_7 \in \{0, 1\}$).

Note that the Galois group H of

$$\mathbb{F}_2(x, y) \subset \mathbb{F}_2(x, y, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$$

is simply $(\mathbb{Z}/2\mathbb{Z})^6$. The elements of H just send each generator to itself $+1$ or leave it fixed independent of what is done to any other generator. We have $\#H = 64 = 2^6$. Now note our extension

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3)$$

has Galois group $H \cup H\tau$ where τ is determined by

$$\tau(y) = y + 1, \quad \tau(w_i) = a_i.$$

Now act with some element of $H \cup H\tau$ on $y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3$. Firstly, elements $h_1 \in H$ will send it to

$$y \cdot (w_1 + \zeta_1) \cdot (\alpha_1 + \zeta_2) \cdot (w_2 + \zeta_3) \cdot (\alpha_2 + \zeta_4) \cdot (w_3 + \zeta_5) \cdot (\alpha_3 + \zeta_6)$$

where $\zeta_1, \ldots, \zeta_6 \in \{0, 1\}$.

An element $h_2 \in H\tau$ sends $y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3$ to

$$(y + 1) \cdot (w_1 + \rho_1) \cdot (\alpha_1 + \rho_2) \cdot (w_2 + \rho_3) \cdot (\alpha_2 + \rho_4) \cdot (w_3 + \rho_5) \cdot (\alpha_3 + \rho_6)$$

with $\rho_1, \ldots, \rho_6 \in \{0, 1\}$. This describes in total $2^6 + 2^6 = 128$ distinct combinations of the given basis $y^{n_1} w_1^{n_2} w_2^{n_3} w_3^{n_4} \alpha_1^{n_5} \alpha_2^{n_6} \alpha_3^{n_7}$. The described orbit therefore indeed consists of 128 elements, proving our claim.

$y^{n_1} w_1^{n_2} w_2^{n_3} w_3^{n_4} \alpha_1^{n_5} \alpha_2^{n_6} \alpha_3^{n_7}$ Technical Aside Remark: After trying the above i.e. using an element of order 128 to generate the extension in one step on Magma we once again ran into the problem that it could not compute such a field extension of degree 128. I have personally contacted the Magma team and they tried something also for it to run for 1 hr without completing the task and they can use a faster version. There is almost certainly a way of doing this but as far as our time constraints permit we cannot figure it out so therefore we leave it as an open question for computing the places and genus of the bigger extension and from now on will focus our attention on the smaller extensions. We have shown it is possible for the reader to use the element $y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3$ in their attempt to analyse the big extension in Magma or some similar program but our attempt at this failed.

4 Which Extensions Can Magma Easily Handle And Do They Present Good Coding Opportunities

The reason we began this investigation was because it had been found already that an extension over $\mathbb{F}_2$ existed with 40 places of degree 1. Such a number of places made it nice for looking into to find error correcting codes. We therefore sort to analyse the normal closure of this extension in the hope that it would similarly bring useful codes. However, as we are having issues making Magma deal with such a large extension we instead look for suitable subextensions.

In this process we have found that each of $\mathbb{F}_2(x, y, w_1, \alpha_1)$, $\mathbb{F}_2(x, y, w_2, \alpha_2)$, $\mathbb{F}_2(x, y, w_3, \alpha_3)$, $\mathbb{F}_2(x, y, w_1, \alpha_2)$ has 20 places of degree 1 or equivalently 20 points on the corresponding curves with co-ordinates in $\mathbb{F}_2$. This also makes them somewhat useful for coding in this regard and more manageable to work with in Magma.

We present a few such codes. Some come close the limit in terms of possible dimension and minimal distance. We compared with the lists found on `http://www.codetables.de`. We also attach the Magma source code we used to describe these examples.

5 Results

Here are the parameters of four linear codes over $\mathbb{F}_2$ we found.

Code 1: Length $n = 20$, Dimension $k = 16$, Minimal distance 2. This is best possible for the given $[n, k]$. Example generated from the extension $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_1)$.

Code 2: Length $n = 20$, Dimension $k = 4$, Minimal distance 8. This is a little below the optimal minimal distance 10 for this $[n, k]$. Example generated from the extension $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_1)$.

Code 3: Length 20 Dimension 12 Distance 3 With Upper Bound On Distance 4 generated from extension $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_1)$.

Code 4: Length 20 Dimension 8 Distance 5 With Upper Bound On Distance 8 generated from extension $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, \alpha_2)$.

6 Codes

Here the Magma source code providing the binary linear codes we found, is given.

6.1 Code1

Length 20 Dimension 16 Distance 2

```
F2:=GF(2);
Kx<x>:=FunctionField(F2);
Px<T>:=PolynomialRing(Kx);
Kxy<y>:=ext< Kx | T^2+T+x^3+x>;
Pxy<T>:=PolynomialRing(Kxy);
```

```
pw:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*y + x^2 + x;
Kxyw<w>:=ext< Kxy | pw>;
Pxyw<T>:=PolynomialRing(Kxyw);
pa:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*(y+1) + x^2 + x;
Kxywa<a>:=ext< Kxyw | pa>;

P:=Places(Kxywa,1); n:=#P;
#Places(Kxywa,4);
D1:=Places(Kxywa,4)[1]; D2:=Places(Kxywa,4)[2];
D3:=Places(Kxywa,4)[3]; D4:=Places(Kxywa,4)[4];
V,g:=RiemannRochSpace(4*D3+ 4*D4 +3*D1);
d:=Dimension(V);
bas:=g(Basis(V));

CV:=[];
for i in [1..d] do
     vec:=[];
     for j in [1..n] do
          ev := Evaluate( bas[i], P[j]);
          Append(~vec, ev);
     end for;
     Append(~CV, vec);
end for;

C:=LinearCode<F2, n | CV>;
[Dimension(C), MinimumDistance(C)];
```

6.2 Code2

Length 20 Dimension 4 Distance 8

```
F2:=GF(2);
Kx<x>:=FunctionField(F2);
Px<T>:=PolynomialRing(Kx);
Kxy<y>:=ext< Kx | T^2+T+x^3+x>;
Pxy<T>:=PolynomialRing(Kxy);
pw:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*y + x^2 + x;
Kxyw<w>:=ext< Kxy | pw >;
Pxyw<T>:=PolynomialRing(Kxyw);
pa:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*(y+1) + x^2 + x;
Kxywa<a>:=ext< Kxyw | pa >;
```

```
P:=Places(Kxywa,1); n:=#P;
#Places(Kxywa,4);
D1:=Places(Kxywa,4)[1]; D2:=Places(Kxywa,4)[2];
D3:=Places(Kxywa,4)[3]; D4:=Places(Kxywa,4)[4];
V,g:=RiemannRochSpace(6*D3+ 2*D4);
d:=Dimension(V);
bas:=g(Basis(V));

CV:=[];
for i in [1..d] do
     vec:=[];
     for j in [1..n] do
          ev := Evaluate( bas[i], P[j]);
          Append(~vec, ev);
     end for;
     Append(~CV, vec);
end for;

C:=LinearCode<F2, n | CV>;
[Dimension(C), MinimumDistance(C)];
```

6.3 Code3

Length 20 Dimension 12 Distance 3

```
F2:=GF(2);
Kx<x>:=FunctionField(F2);
Px<T>:=PolynomialRing(Kx);
Kxy<y>:=ext< Kx | T^2+T+x^3+x>;
Pxy<T>:=PolynomialRing(Kxy);
pw:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*y + x^2 + x;
Kxyw<w>:=ext< Kxy | pw>;
Pxyw<T>:=PolynomialRing(Kxyw);
pa:=(x^7 + x + 1)*(T^2 + T) + (x^5 +x)*(y+1) + x^2 + x;
Kxywa<a>:=ext< Kxyw | pa >;

P:=Places(Kxywa,1); n:=#P;
#Places(Kxywa,4);
D1:=Places(Kxywa,4)[1]; D2:=Places(Kxywa,4)[2];
D3:=Places(Kxywa,4)[3]; D4:=Places(Kxywa,4)[4];
```

```
V,g:=RiemannRochSpace(9*D3 + D4);
d:=Dimension(V);
bas:=g(Basis(V));

CV:=[];
for i in [1..d] do
     vec:=[];
     for j in [1..n] do
          ev := Evaluate( bas[i], P[j]);
          Append(~vec, ev);
     end for;
     Append(~CV, vec);
end for;

C:=LinearCode<F2, n | CV>;
[Dimension(C), MinimumDistance(C)];
```

6.4 Code4

Length 20 Dimension 8 Distance 5

```
F2:=GF(2);
Kx<x>:=FunctionField(F2);
Px<T>:=PolynomialRing(Kx);
Kxy<y>:=ext< Kx | T^2+T+x^3+x>;
Pxy<T>:=PolynomialRing(Kxy);
pw:=(x^7 + x + 1)*(T^2 + T) + (x^5 + x)*y + x^2 + x;
Kxyw<w>:=ext< Kxy | pw>;
Pxyw<T>:=PolynomialRing(Kxyw);
pa2:=(x^7+x+1)*(T^2+T)+(x^5 + x^4 + x^3 +x)*(y+1) + x^6 + x^4;
Kxywa2<a2>:=ext< Kxyw | pa2 >;

P:=Places(Kxywa2,1); n:=#P;
#Places(Kxywa2,4);

D1:=Places(Kxywa2,4)[1]; D2:=Places(Kxywa2,4)[2];
D3:=Places(Kxywa2,4)[3]; D4:=Places(Kxywa2,4)[4];

V,g:=RiemannRochSpace(7*D3 +D4 +D1);
d:=Dimension(V);
bas:=g(Basis(V));
```

```
CV:=[];
for i in [1..d] do
     vec:=[];
     for j in [1..n] do
          ev := Evaluate( bas[i], P[j]);
          Append(~vec, ev);
     end for;
     Append(~CV, vec);
end for;

C:=LinearCode<F2, n | CV>;
[Dimension(C), MinimumDistance(C)];
```

7 Brief Discussion Of Coding Theory Used

The field extensions we are looking at correspond to some curve over $\mathbb{F}_2$. Such a curve has points where the co-ordinates lie in $\mathbb{F}_2$ to see this let's take a more basic example where it is easily seen where the co-ordinates lie in $\mathbb{F}_2$. (In reality for our big field extension we simply use Magma to calculate such points).

Take $\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y)$, remembering:

$$y^2 + y = x^3 + x.$$

In projective space where we replace x by x/z and y by y/z we get new equation which corresponds to a curve X:

$$y^2z + yz = x^3 + xz^2.$$

As we work over $\mathbb{F}_2$ it is extremely basic to see we can look for triplets (μ, ζ, ν) which solve the equation but whose values lie in $\mathbb{F}_2$.

Such triplets in this case are:

$$(0 : 1 : 0), (0 : 0 : 1), (0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 1).$$

For the curve X considered here, the points of X with coordinates in $\mathbb{F}_2$ form the set

$$X(\mathbb{F}_2) = \{(0 : 1 : 0), (0 : 0 : 1), (0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 1)\}.$$

It is useful to note for later that these 5 points on this curve correspond to the 5 "places" of degree 1 in our field $\mathbb{F}_2(x, y)$.

From these points a code can be constructed with length 5.

If one has forgotten: a binary code C of length n is defined as a nonempty subset of $\mathbb{F}_2^n$. The elements of C are called words and if

$$\forall v, w \in C \quad \text{also} \quad v + w \in C$$

then it is called a binary linear code.

So in general the aim of the game is to find some "nice" subsets of $\mathbb{F}_2^n$. For engineers "nice" means the dimension of the code which is just the dimension of the subspace in our case and the minimum distance between the vectors is high. Now there is a tradeoff between minimum distance and dimension. For example, to see this in the most basic case if one takes the subset which is just the entire space then clearly the dimension is n and the minimum distance is 1 as taking 2 distinct vectors they must differ in at least 1 place to be distinct therefore the minimum distance is 1.

In real life these codes are, for example, used in space. I send by code a vector or message in our subspace of $\mathbb{F}_2^n$ which you receive but because of physical effects the signal you receive is distorted. This will make the code word you receive different from what was sent. Now this is why we look for a high minimal distance. Say I receive a code with 2 errors in where instead of 1's there are 0's or vice versa. If my code has minimal distance 5, one can say with 100 percent certainty that the only possibility is that the code sent was the vector closest to the one received that actually lies in our subspace. However, if the code has 3 errors now there can be multiple closest options so you know that it must be this or that one but the exact precise code word is unknown. A code with minimum distance 1 is therefore in practical applications useless. Similarly a code with minimal distance 2 is not very useful.

Thus you can see the utility in finding a subspace with high minimal distance and also high dimension. The dimension means I can encode more information and the minimal distance means I can correct more errors. There is also a topic of efficiency: if the ratio k/n is large this means we aren't wasting much space i.e. most of the information we send is actually information useful to us or in mathematical terms: the dimension of our subspace is high in comparison to the larger space. If it were small this would mean we would have to send long messages to receive a small amount of information which obviously may not be optimal if encoding massive amounts of information.

The reason, then, algebraic curves are used for these error correcting codes is because there are known bounds for n, k and d and the ratios between them, for various ways of constructing codes from such a curve. This makes it somewhat easier to find good codes, as opposed to other methods for finding linear subspaces of $\mathbb{F}_2^n$.

As I mentioned earlier, the number of points on our curve corresponds to the dimension of $\mathbb{F}_2^n$ we use. So in our previous example there were 5 points so our code would be some subspace of $\mathbb{F}_2^5$ this is not immediately obvious why so I will attempt to make a small explanation. The main point to note is there exists a linear map between 2 vector spaces. The target space here is $\mathbb{F}_2^n$ and the vector space our map starts from, is the so-called Rieman-Roch Space $L(D)$. Here D is a formal finite sum of 'places', which corresponds to a formal finite sum of Galois-Orbits of points. As the map is linear the image is a subspace of $\mathbb{F}_2^n$ and this subspace we call our code. Again the reason why such a seemingly complex example is used is because there are guarantees or bounds for the values of n, k, d we will obtain which makes it easier to guess if we will obtain a nice code or not. The Rieman-Roch space to be precise is:

$L(D) = \{0-\text{function}\} \cup \{\text{all functions with zeroes and poles dictated by } D\}$.

For example,

$$L(3 * (0 : 1 : 0))$$

means include all functions with poles of order less than equal to 3 at (0:1:0) and no poles anywhere else.

If you see a negative, for example:

$$L(3 * (0 : 1 : 0) - 2 * (1 : 1 : 1))$$

it means take all functions with poles of order less than equal to 3 at (0:1:0) and no poles anywhere else & one zero at (1:1:1) of order less than equal to 2.

As I said previously there exists a linear map: evaluate the functions in our Rieman-Roch space at the points $p_1, \ldots, p_n$ of our curve,

$$L(D) \longrightarrow \mathbb{F}_2^n$$

$$f \in L(D) \mapsto (f(p_1), f(p_2)....f(p_n)) \in \mathbb{F}_2^n.$$

This is how one finds error correcting codes with good values for n, k, d and, indeed how we obtained the codes in this text.

7.1 Conclusion

In this report, we found the Normal Closure of our original field extension.

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, w_2, w_3)$$

and then studied this normal extension

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_1, w_2, w_3, \alpha_1, \alpha_2, \alpha_3)$$

. We proved the Galois Group is

$$\mathrm{Gal}(\mathbb{F}_2(x, y, w_1, w_2, w_3, \alpha_1, \alpha_2, \alpha_3)/\mathbb{F}_2(x)) \subset D_8 \times D_8 \times D_8$$

In particular, it is the subgroup which under the following map has image (0,0,0) , (1,1,1). I.e. when restricted to an element of the Galois group of $\mathbb{F}_2(x, y, w_1\alpha_1)/\mathbb{F}_2(x)$ or $\mathbb{F}_2(x, y, w_2\alpha_2)/\mathbb{F}_2(x)$ or $\mathbb{F}_2(x, y, w_3\alpha_3)/\mathbb{F}_2(x)$ must have the same action on y giving us the images mentioned in the following map:

$$D_8 \times D_8 \times D_8 \mapsto \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Where we recall that each of the smaller Galois group was isomorphic to D_8.

$$\mathrm{Gal}(\mathbb{F}_2(x)/\mathbb{F}_2(x, y, w_1, \alpha_1)) \cong D_8$$

We then encountered problems with running Magma in the hope of getting good error correcting codes for an extension of degree 128. In attempting to fix the issue we tried contacting Magma directly so we could use their superior verison of the product and we also proved the following:

$$\mathbb{F}_2(x, y, w_1, \alpha_1, w_2, \alpha_2, w_3, \alpha_3) = \mathbb{F}_2(x, y \cdot w_1 \cdot \alpha_1 \cdot w_2 \cdot \alpha_2 \cdot w_3 \cdot \alpha_3)$$

So that we could do the extension in one go rather than making multiple degree 2 extensions thinking this would ease the run time. Perhaps that equality will be useful in the future if the reader wishes to fix the issue.

Following this obstacle we switched our attention to more manageable normal sub extensions of degree 16 in Magma:

$$\mathbb{F}_2(x) \subset \mathbb{F}_2(x, y, w_i, \alpha_i)$$

Interestingly such extensions have 20 places of order 1 over $\mathbb{F}_2$ so we can make codes of length 20 with them. We found a number of codes with decent dimension and minimum distance and we have included such codes which can be easily adjusted in the attempt of finding better codes in the future in an attempt to make the project more complete. As a brief discussion I note that the process of finding codes once a Rieman Roch Space is determined is somewhat manual and involves lots of guessing it would be preferable I believe if one could iteratively change the Places , Poles and Zeroes in a way which all possibilities were seen this would simply produce the best codes and take less time.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[3] Jaap Top. Serre's genus fifty example. In *Arithmetic, geometry, cryptography and coding theory*, volume 770 of *Contemp. Math.*, pages 297–303. Amer. Math. Soc., Providence, RI, 2021.