

C suffered a burst error of length $6 = 3 \times 2$ which produced burst errors of length ≤ 2 in x, y & z . These were successfully corrected.

Notice the burst error here is like the "alternative" one in the handout. But the interleaved code & procedure, we have decoded successfully.

More finite fields

\mathbb{F}_q has $q - 1$ non-zero elements. With multiplication they form a group, \mathbb{F}_q^* .

The powers of one element form a group; sometimes all of \mathbb{F}_q^* , sometimes a smaller subgroup.

E.g. In \mathbb{F}_7 , the powers of 2 are 2,4,1

the powers of 3 are 3,2,6,4,5,1

Definition

If the powers of α make all of \mathbb{F}_q^* , α is a primitive element of \mathbb{F}_q .

So 3 is a primitive element of \mathbb{F}_7 , but 2 is not.

Recall

$F[x]$ is the set of polynomials in x with coefficients from F . We can add and multiply in $F[x]$

E.g. In $\mathbb{F}_3[x]$

$$(x + 1)(x + 1) = x^2 + 2x + 1$$

$$(x + 2)(x + 2) = x^2 + x + 1$$

$$(x + 1)(x + 2) = x^2 + 2$$

In $\mathbb{F}_2[x]$

$$(x + 1)(x + 1) = x^2 + 1$$

But most elements of $F[x]$ do not have multiplicative inverses $(x + 1) \cdot ? = 1$

So $F[x]$ is not a field, but it is a ring.

We made \mathbb{Z} into a finite field \mathbb{Z}_p , by identifying p with 0.

In \mathbb{Z}_p , the equivalence class a^- is really the set $\{a + kp \mid k \in \mathbb{Z}\}$. Similarly, in $F[x]$ we can identify a

polynomial $f(x)$ with zero, and get $\frac{F[x]}{(f(x))}$.

Then in $\frac{F[x]}{(f(x))}$, $g(x)^- = \left\{ g(x) + h(x) \cdot f(x) \mid h(x) \in F[x] \right\}$

Examples

In $\mathbb{F}_2[x]$ $f(x) = x^2 + x + 1$

In $\frac{\mathbb{F}_2[x]}{(f(x))}$, $(x^2 + x + 1)^- = 0$, so $(x^2)^- = -(x + 1)^- = (x + 1)^-$

This means we never need to write x^2

In fact, $\frac{\mathbb{F}_2[x]}{(f(x))} = \{0^-, 1^-, x^-, (x + 1)^-\}$

We write γ for x^- and have $\{0, 1, \gamma, \gamma + 1\} = \mathbb{F}_4$

$\gamma^2 = \gamma + 1$ gives arithmetic.
 \mathbb{F}_4

+	0	1	γ	$\gamma + 1$
0	0	1	γ	$\gamma + 1$
1	1	0	$\gamma + 1$	γ
γ	γ	$\gamma + 1$	0	1
$\gamma + 1$	$\gamma + 1$	γ	1	0

\mathbb{F}_4^*

*	1	γ	$\gamma + 1$
1	1	γ	$\gamma + 1$
γ	γ	$\gamma + 1$	1
$\gamma + 1$	$\gamma + 1$	1	γ

2) In $\mathbb{F}_3[x]$, let $f(x) = x^2 + 1$

In $\frac{\mathbb{F}_3[x]}{(f(x))}$, $(x^2 + 1)^{-} = 0^{-}$, $(x^2)^{-} = (-1)^{-} = 2^{-}$

Writing γ for x^{-} , $\frac{\mathbb{F}_3[x]}{(x^2 + 1)} = \{0, 1, 2, \gamma, \gamma + 1, \gamma + 2, 2\gamma, 2\gamma + 1, 2\gamma + 2\}$

This is \mathbb{F}_q

3) In $\mathbb{F}_2[x]$, let $f(x) = x^3 + x + 1$

In $\frac{\mathbb{F}_2[x]}{(x^3 + x + 1)}$, $(x^3)^{-} = (x + 1)^{-}$

So $\frac{\mathbb{F}_2[x]}{(x^3 + x + 1)} = \{0, 1, \gamma, \gamma + 1, \gamma^2, \gamma^2 + 1, \gamma^2 + \gamma, \gamma^2 + \gamma + 1\}$ This is \mathbb{F}_8

How do we choose $f(x)$?

i) If $q = p^r$, the $f(x) \in \mathbb{F}_p[x]$ and has degree r in \mathbb{F}_q

ii) Recall. \mathbb{Z}_n is a field if and only if n is prime (a field must not have zero divisors)

Similarly, to make \mathbb{F}_q we need an $f(x)$ which is irreducible in its prime field \mathbb{F}_p

iii) Choosing a different irreducible $f(x)$ (eg. $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$ for \mathbb{F}_9) makes the arithmetic look different but the two fields are isomorphic. Both are \mathbb{F}_9 .

Fact

\mathbb{F}_q always has a primitive element

E.g. 1) $\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}$ so $\gamma^2 = \gamma + 1$

γ^0	γ^1	γ^2	γ^3
1	γ	$\gamma + 1$	1

So γ is primitive

2) $\mathbb{F}_8 = \frac{\mathbb{F}_2[x]}{(x^3 + x + 1)}$ So $\gamma^3 = \gamma + 1$

γ^0	γ^1	γ^2	γ^3	γ^4	γ^5	γ^6	γ^7
1	γ	γ^2	$\gamma + 1$	$\gamma^2 + \gamma$	$\gamma^2 + \gamma + 1$	$\gamma^2 + 1$	1

$\mathbb{F}_9 = \frac{\mathbb{F}_3[x]}{(x^2 + 1)}, \gamma^2 = 2$

γ^0	γ^1	γ^2	γ^3	γ^4
1	γ	2	2γ	1

So γ is not primitive

i	0	1	2	3	4	5	6	7	8
$(\gamma + 1)^i$	1	$\gamma + 1$	2γ	$2\gamma + 1$	2	$2\gamma + 2$	γ	$\gamma + 2$	1

But $\gamma + 1$ is primitive in this field.

Usually we choose $f(x)$ so that γ is primitive

Eg. Take $\frac{\mathbb{F}_3[x]}{(x^2 + x + 2)}$ for \mathbb{F}_9 so $\gamma^2 = 2\gamma + 1$

i	0	1	2	3	4	5	6	7	8
γ^i	1	γ	$2\gamma + 1$	$2\gamma + 2$	2	2γ	$+ 2$	$\gamma + 1$	1

γ is primitive

These tables give us 2 ways to write most elements of \mathbb{F}_q ; one good for adding, one for multiplying.

Eg. In \mathbb{F}_8 as above, $\gamma^3 + \gamma^4 = (\gamma + 1) + (\gamma^2 + \gamma) = \gamma^2 + 1 = \gamma^6$

$(\gamma + 1)(\gamma^2 + \gamma + 1) = \gamma^3 \gamma^5 = \gamma^8 = \gamma^7 \gamma^1 = \gamma$

$(\gamma + 1)^{-1} = (\gamma^3)^{-1} = \gamma^4$ because $\gamma^3 \cdot \gamma^4 = \gamma^7 = 1$

Since $\gamma^7 = \gamma^0$, exponents work **mod** 7.
Similarly in \mathbb{F}_9 , the powers work **mod** 8.