

Finite Fields and Double Error Correction

Hanwen Yao

Feb 20, 2025

Group and Field

A **group** is a set G with operation $*$, such that

- 1 Closure: $\forall a, b \in G, \quad a * b \in G$
- 2 Associativity: $\forall a, b, c \in G, \quad a * (b * c) = (a * b) * c$
- 3 Identity: $\exists e \in G$ such that $\forall a \in G, \quad a * e = e * a = a$
- 4 Inverse: $\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

A group is **abelian** if $\forall a, b \in G, \quad a * b = b * a$.

A **field** is a set \mathbb{F} with operations “+” and “.”, such that

- 1 \mathbb{F} is an Abelian group under “+”, with identity 0.
- 2 $\mathbb{F} \setminus \{0\}$ is an Abelian group under “.”, with identity 1.
- 3 Distributive law: $\forall a, b, c \in \mathbb{F}, \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Example of Fields:

- 1 \mathbb{R} = the set of real numbers with “+” and “.”

\mathbb{R} is an infinite field—these are not interesting because our alphabet is always finite.

(Also \mathbb{C} and \mathbb{Q})

- 2 $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ with “+” and “.” mod 7.

$$\begin{aligned}5 + 6 &\equiv 4 \pmod{7}, & 4 - 6 &\equiv 5 \pmod{7}, \\-6 &\equiv 1 \pmod{7} &\Rightarrow & 1 \text{ is the additive inverse of } 6 \\3 \cdot 5 &\equiv 1 \pmod{7} &\Rightarrow & 5 \text{ is the multiplicative inverse of } 3\end{aligned}$$

Note: working mod 7 is the same as standard math with $7 \equiv 0$

Theorem:

$\mathbb{Z}_q = \{0, 1, \dots, q-1\}$ with operations “+” and “·” mod q is a field if and only if $q = p$ is a prime.

Proof:

⇐ If q is not prime, then $ab = q$. Then a has no multiplicative inverse, otherwise

$$\begin{aligned} a \cdot x = 1 \pmod{q} &\Rightarrow a \cdot x = mq + 1 \\ &\Rightarrow 0 \equiv 1 \pmod{a} \quad (\text{contradiction}) \end{aligned}$$

⇒ If q is prime, we need to show:

- \mathbb{Z}_q is abelian under “+”
- $\mathbb{Z}_q \setminus \{0\}$ is abelian under “·”
- Distributive law holds

Easy to verify, except the existence of multiplicative inverse.

(Verify the other properties by yourself.)

Existence of the Inverse

Lemma:

For all $a, b \in \mathbb{Z}$, there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha a + \beta b = \gcd(a, b)$$

Proof:

Follows from the Euclidean algorithm. *(which we will study later)*

Now let $a \in \mathbb{Z}_p$, then

$$\gcd(a, p) = 1 \quad \Rightarrow \quad \exists \alpha, \beta \in \mathbb{Z} \text{ such that}$$

$$\begin{aligned} \alpha a + \beta p = 1 &\Rightarrow \alpha a \equiv 1 \pmod{p} \\ &\Rightarrow a^{-1} = \alpha \pmod{p} \end{aligned}$$

Example:

In \mathbb{Z}_7 , we have:

$$3 \cdot 5 - 2 \cdot 7 = 1 \quad \Rightarrow \quad 3 \cdot 5 \equiv 1 \pmod{7} \quad \Rightarrow \quad 3^{-1} = 5$$

\mathbb{Z}_p is called a prime field. Every finite field of prime order p is isomorphic to \mathbb{Z}_p .

Euclidean Algorithm

Lemma:

$$\gcd(a, b) = r_n$$

Proof:

For any nonzero integers a, b, q , and remainder r , where $a = bq + r$, we have:

$$\begin{aligned} \begin{cases} d|b \text{ and } d|r \Rightarrow d|a \\ d|a \text{ and } d|b \Rightarrow d|r \end{cases} &\Rightarrow \{d : d|a \text{ and } d|b\} = \{d : d|b \text{ and } d|r\} \\ &\Rightarrow \gcd(a, b) = \gcd(b, r) \end{aligned}$$

Hence,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n$$

Euclidean Algorithm Example

Given $a = 84$, $b = 54$,

$$84 = 1 \cdot 54 + 30$$

$$54 = 1 \cdot 30 + 24$$

$$30 = 1 \cdot 24 + 6$$

$$24 = 4 \cdot 6 + 0$$

$$\Rightarrow \gcd(84, 54) = 6$$

Then we can express $\gcd(84, 54)$ as a linear combination:

$$6 = 30 - 24$$

$$= 30 - (54 - 30)$$

$$= 2 \cdot 30 - 54$$

$$= 2 \cdot (84 - 54) - 54$$

$$= 2 \cdot 84 - 3 \cdot 54$$

The greatest common divisor (gcd) can be expressed as a linear combination of the original numbers.

Euclidean Algorithm Revisited

- **Input:** a, b ($a > b > 0$)
- **Initialization:**

$$\left. \begin{array}{l} r_{-1} = a, \quad r_0 = b \\ s_{-1} = 1, \quad s_0 = 0 \\ t_{-1} = 0, \quad t_0 = 1 \end{array} \right\} \text{ auxiliary variables}$$

- **Recursion:**

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ s_i &= s_{i-2} - q_i s_{i-1} \\ t_i &= t_{i-2} - q_i t_{i-1}, \end{aligned} \quad \text{where } q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor, \quad i = \{1, 2, 3, \dots\}$$

Claim: For all i , $r_i = s_i a + t_i b$ (proved by induction)

Therefore, $\gcd(a, b) = r_n = s_n a + t_n b$

So for all $a, b \in \mathbb{Z}$, there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha a + \beta b = \gcd(a, b)$$

Finite Fields

Theorem:

If \mathbb{F} is a finite field, then its order is $|\mathbb{F}| = p^m$ for some prime p and $m \geq 1$.

Proof:

We have $0, 1 \in \mathbb{F}$. Define:

$$u_0 = 0, \quad u_1 = 1, \quad u_n = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = u_{n-1} + 1 \in \mathbb{F}$$

Then:

$$u_m + u_n = \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} + \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = u_{n+m}$$

$$u_m \cdot u_n = \left(\underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} \right) \left(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \right) = u_{nm} \text{ (distributive law)}$$

Finite Fields

Proof (cont.):

Since \mathbb{F} is finite, assume the first repetition happens at u_p (we will prove p is prime later).

$$\underbrace{u_0, u_1, u_2, \dots, u_{p-1}}_{\text{all distinct}}, \quad u_p = u_k \quad \text{for some } 0 \leq k < p$$

Then,

$$u_{p-k} = u_p - u_k = 0 \quad \begin{array}{c} \Rightarrow \\ \uparrow \\ u_{p-k} \text{ is a repetition of } u_0 \end{array} \quad k = 0 \quad \Rightarrow \quad u_p = u_k = 0$$

Definition:

The **characteristic** of \mathbb{F} , $\text{char}(\mathbb{F})$, is defined as the least integer p such that

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0 \quad (\text{in } \mathbb{F})$$

Finite Fields

Proof (cont.):

Claim: $p = \text{char}(\mathbb{F})$ is a prime.

Assume $p = a \cdot b$, where $1 < a, b < p$. Then,

$$u_a \cdot u_b = u_p = 0 \quad \Rightarrow \quad u_a = 0 \text{ or } u_b = 0$$

This contradicts of the minimality of $p = \text{char}(\mathbb{F})$, so p must be prime.

Claim: $\mathbb{F}_p = \{u_0, u_1, \dots, u_{p-1}\}$ is a subfield of \mathbb{F} .

Define the mapping:

$$\varphi : \mathbb{F}_p \rightarrow \mathbb{Z}_p, \quad \varphi(u_i) = i$$

Verify: φ is an isomorphism (preserves 0, 1, addition, and multiplication).

$$\mathbb{Z}_p \text{ is a field} \Rightarrow \mathbb{F}_p \text{ is a field}$$

\mathbb{F}_p is called the prime subfield of \mathbb{F} .

Proof (cont.):

Claim: $|\mathbb{F}| = p^m$

If $\mathbb{F} = \mathbb{F}_p$, then $q = p$ and we are done. Otherwise, there exists $w_1 \in \mathbb{F} \setminus \mathbb{F}_p$. Define the set (not necessarily a subfield):

$$\mathbb{F}_p^2 = \{a_0 + a_1 w_1 : a_0, a_1 \in \mathbb{F}_p\} \subseteq \mathbb{F}$$

Then \mathbb{F}_p^2 has p^2 elements, since the uniqueness of this representation for the elements in \mathbb{F}_p^2 can be checked by:

$$a_0 + a_1 w_1 = b_0 + b_1 w_1 \quad \Rightarrow \quad w_1 = \frac{b_0 - a_0}{a_1 - b_1} \in \mathbb{F}_p$$

Hence, if $\mathbb{F} = \mathbb{F}_p^2$, then $q = p^2$. Otherwise, there exists $w_2 \in \mathbb{F} \setminus \mathbb{F}_p^2$. Define the set:

$$\mathbb{F}_p^3 = \{a_0 + a_1 w_1 + a_2 w_2 : a_0, a_1, a_2 \in \mathbb{F}_p\} \subseteq \mathbb{F}$$

with p^3 elements and so on.

Conclusions:

For any finite field $\text{GF}(q)$:

- 1 $q = p^m$ for a prime p .
- 2 $\text{GF}(q)$ contains a prime field $\mathbb{F}_q \cong \mathbb{Z}_p$.
- 3 $\text{GF}(q)$ may be regarded as a set of m -tuples over \mathbb{F}_p :

$$a_0 + a_1 w_1 + \cdots + a_{m-1} w_{m-1} \in \text{GF}(q) \quad \leftrightarrow \quad (a_0, a_1, \dots, a_{m-1})$$

$$b_0 + b_1 w_1 + \cdots + b_{m-1} w_{m-1} \in \text{GF}(q) \quad \leftrightarrow \quad (b_0, b_1, \dots, b_{m-1})$$

$$(a_0, \dots, a_{m-1}) + (b_0, \dots, b_{m-1}) = (a_0 + b_0, \dots, a_{m-1} + b_{m-1})$$

- 4 More precisely, $\text{GF}(q)$ can be regarded as a vector space of dimension m over \mathbb{F}_p .

Extension Field Construction

Let \mathbb{F} be a field. (Say $\mathbb{F} = \mathbb{F}_p$ is a prime field.)

- $\mathbb{F}[x] \triangleq$ the set of all polynomials over \mathbb{F} . ($\mathbb{F}[x]$ is a ring.)
- pick $g(x) \in \mathbb{F}[x]$ that is **monic** and **irreducible** with $\deg g(x) = m$.

Definitions

Monic: The coefficient of the leading term is 1.

Irreducible: A polynomial $g(x)$ is **reducible** if $g(x) = a(x)b(x)$ for some $a(x), b(x) \in \mathbb{F}[x]$ with $\deg a(x) > 0$ and $\deg b(x) > 0$. Otherwise $g(x)$ is called **irreducible**.

(An irreducible polynomial is analogous to a prime number in integers.)

Extension Field Construction

Definition:

$$\langle g(x) \rangle \triangleq \{f(x)g(x) : f(x) \in \mathbb{F}[x]\} \quad (\text{idea generated by } g(x))$$

$$\mathbb{F}[x]/\langle g(x) \rangle \triangleq \left\{ \begin{array}{l} \text{Set of all polynomials of degree } \leq m-1 \text{ in } \mathbb{F}[x], \\ \text{with operations " + " and " \cdot " modulo } g(x). \end{array} \right\}$$

Theorem:

$\mathbb{F}[x]/\langle g(x) \rangle$ is a field of order $|\mathbb{F}|^m$.

Proof:

All the properties of “+” and “·” are trivial to verify, except for the existence of inverses under “·”.

Note: polynomial math modulo a polynomial $g(x)$ is equivalent to standard polynomial math with $g(x) \equiv 0$.

Construction of Extension Fields

Lemma:

For all $a(x), b(x) \in \mathbb{F}[x]$, there exist $c(x), d(x) \in \mathbb{F}[x]$ such that:

$$c(x)a(x) + d(x)b(x) = \gcd(a(x), b(x))$$

Proof: Follows from the Euclidean algorithm applied to polynomials over $\mathbb{F}[x]$.

Therefore, for any $a(x) \in \mathbb{F}[x]/\langle g(x) \rangle$:

- $\gcd(g(x), a(x)) = 1$ (g monic and irreducible)
- $\Rightarrow \exists c(x), d(x)$ such that $c(x)a(x) + d(x)g(x) = 1$
- $\Rightarrow c(x)a(x) \equiv 1 \pmod{g(x)}$
- $\Rightarrow c(x)$ is the multiplicative inverse of $a(x)$

Construction of Extension Fields

Let \mathbb{F}_q be the finite field with q elements.

- $\mathbb{F}_q[x] \triangleq$ the set of all polynomials over \mathbb{F}_q .
- $g(x) \in \mathbb{F}_q[x]$ is **monic** and **irreducible**, with $\deg g(x) = m$.

Extension Field

$\mathbb{F}_q[x]/\langle g(x) \rangle$ is an **extension field** of \mathbb{F}_q .

Every polynomial in $\mathbb{F}_q[x]/\langle g(x) \rangle$ can be represented by an m -tuple over \mathbb{F}_q :

$$a(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_q[x]/\langle g(x) \rangle$$

\uparrow

$$(a_0, a_1, \dots, a_{m-1}) \in \mathbb{F}_q^m$$

So $|\mathbb{F}_q[x]/\langle g(x) \rangle| = p^m$

Example of Extension Fields

Example 1:

$$\mathbb{F}_2 = \{0, 1\}, \quad g(x) = 1 + x + x^4 \quad (\text{verify irreducibility})$$

$$a = x = 0 + x + 0x^2 + 0x^3 \in \mathbb{F}_2[x]/\langle g(x) \rangle \Rightarrow (0100)$$

$$b = 1 + x^3 = 1 + 0x + 0x^2 + x^3 \in \mathbb{F}_2[x]/\langle g(x) \rangle \Rightarrow (1001)$$

Then,

$$ab = x(1 + x^3) = x + x^4 \equiv 1 \pmod{g(x)} \Rightarrow (1000)$$

$$(0100) \cdot (1001) = (1000)$$

Construction of Extension Fields

Let \mathbb{F}_q be the field of order q , and $g(x)$ be a monic irreducible polynomial of degree m over \mathbb{F} . Then $\mathbb{F}[x]/\langle g(x) \rangle$ is a field of order q^m .

Since $\text{math mod } g(x)$ is the same as $g(x) \equiv 0$, we can represent the polynomial by replacing x with α , where α is a zero of $g(x)$.

$$\begin{aligned}1 + x + x^3 &\Rightarrow 1 + \alpha + \alpha^3 \\g(x) \equiv 0 &\Rightarrow g(\alpha) = 0\end{aligned}$$

In general, let α be a root of $g(x)$, then all roots of $g(x)$ are $\alpha^q, \alpha^{q^2}, \dots$. We can think of α as an arbitrary root because they are all equivalent.

Alternative Construction:

Take α as a root of $g(x)$. Let $\mathbb{F}(\alpha)$ be the smallest field such that $\mathbb{F} \subset \mathbb{F}(\alpha)$ and $\alpha \in \mathbb{F}(\alpha)$. By closure, we have:

$$1, \alpha, \alpha^2, \dots, \alpha^{m-1} \in \mathbb{F}(\alpha)$$

Construction of Extension Fields

- 1 $\mathbb{F}_q(\alpha)$ is a field of order q^m with operations defined by \mathbb{F}_q .
- 2 $\mathbb{F}_q(\alpha)$ is a set of m -tuples over \mathbb{F}_q . Specifically,

$$1 = \alpha^0 \leftrightarrow (100 \dots 0)$$

$$\alpha^1 \leftrightarrow (010 \dots 0)$$

$$\alpha^2 \leftrightarrow (001 \dots 0)$$

$$\vdots$$

$$\alpha^{m-1} \leftrightarrow (000 \dots 1)$$

More precisely, $\mathbb{F}_q(\alpha)$ is a vector space \mathbb{F}_q^m with $1, \alpha, \dots, \alpha^{m-1}$ forming a basis for $\mathbb{F}_q(\alpha)$ over \mathbb{F}_q .

- 3 $\mathbb{F}_q(\alpha) \cong \mathbb{F}_q[x]/\langle g(x) \rangle$.

Extension Fields: Summary

Let \mathbb{F}_q be a field of order q , and let

$$g(x) = x^m + g_{m-1}x^{m-1} + \cdots + g_1x + g_0$$

be monic and irreducible over \mathbb{F}_q . Then,

$$\mathbb{F}_q[x]/\langle g(x) \rangle \triangleq \left\{ \begin{array}{l} \text{Polynomials of degree } \leq m-1, \\ \text{with } + \text{ and } \cdot \text{ modulo } g(x). \end{array} \right\}$$

is a finite field of order q^m .

Alternatively, let α be a zero of $g(x)$, defined by

$$\alpha^m = -g_{m-1}\alpha^{m-1} + \cdots + g_1\alpha + g_0.$$

Define $\mathbb{F}_q(\alpha)$ as the smallest field containing both \mathbb{F}_q and α , then:

- 1 $\mathbb{F}_q(\alpha)$ is a vector space of dimension m over \mathbb{F}_q , with $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ forming a basis over \mathbb{F}_q .
- 2 $\mathbb{F}_q[x]/\langle g(x) \rangle \cong \mathbb{F}_q(\alpha)$.

Example of Extension Fields

Example 1 (Revisited):

$\mathbb{F} = \{0, 1\}$, $g(x) = x^4 + x + 1$, in $\mathbb{F}[x]/g(x)$:

$$(0100) \cdot (1001) = (1000).$$

Let α be a zero of $g(x)$, meaning:

$$\alpha^4 + \alpha + 1 = 0 \quad \Leftrightarrow \quad \alpha^4 = 1 + \alpha.$$

(Since $q = 2$, addition and subtraction are the same.)

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha + \alpha^2,$$

$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3.$$

Example of Extension Fields

Example 1 (cont.):

Here we list all elements in the field as powers of α (*This does not always happen.*):

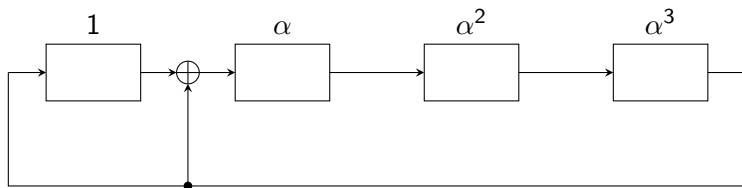
	α^0	α^1	α^2	α^3		α^0	α^1	α^2	α^3
0	0	0	0	0	α^7	1	1	0	1
1	1	0	0	0	α^8	1	0	1	0
α	0	1	0	0	α^9	0	1	0	1
α^2	0	0	1	0	α^{10}	1	1	1	0
α^3	0	0	0	1	α^{11}	0	1	1	1
α^4	1	1	0	0	α^{12}	1	1	1	1
α^5	0	1	1	0	α^{13}	1	0	1	1
α^6	0	0	1	1	α^{14}	1	0	0	1

Multiplying by α shifts the 1s, except at α^4 , where when 1 is shifted out, it returns as $1 + \alpha$.

Example of Extension Fields

Example 1 (cont.):

Multiplication by α in a linear feedback shift register (LFSR) circuit:



This circuit multiplies its contents by α at each clock pulse.

Example of Extension Fields

Example 1 (cont.):

For:

$$\alpha^5 = (0110), \quad \alpha^{12} = (1111)$$

Multiplication (from the table):

$$(0110) \cdot (1111) = \alpha^5 \cdot \alpha^{12} = \alpha^{17} = \alpha^{15} \cdot \alpha^2 = \alpha^2 = (0010)$$

Addition:

$$\begin{aligned} \alpha^5 + \alpha^{12} &= (\alpha + \alpha^2) + (1 + \alpha + \alpha^2 + \alpha^3) \\ &= 1 + \alpha^3 \end{aligned}$$

Binary Representation:

$$\begin{array}{r|cccc} & 0 & 1 & 1 & 0 \\ + & 1 & 1 & 1 & 1 \\ \hline & 1 & 0 & 0 & 1 \end{array}$$

Double-Error Correcting Codes

Try to construct a double-error correcting code.
Start with the $[15, 11, 3]$ Hamming code ($m = 4$):

$$H_m = [\mathbf{b}(1), \mathbf{b}(2), \dots, \mathbf{b}(15)] \triangleq [\underline{1}, \underline{2}, \dots, \underline{15}]$$

(Any number with an underline represents its binary representation.)

If $e = (0 \dots 0 \underset{\substack{\uparrow \\ i}}{1} 0 \dots 0)$, then:

$$s = H_m e^t = \mathbf{b}(i) \Rightarrow \text{error at position } i.$$

If $e = (0 \dots 0 \underset{\substack{\uparrow \\ i}}{1} 0 \dots 0 \underset{\substack{\uparrow \\ j}}{1} 0 \dots 0)$, then:

$$s = H_m e^t = \mathbf{b}(i) + \mathbf{b}(j).$$

We need one more equation to solve for i and j .

Double-Error Correcting Codes

Construct:

$$H'_m = \begin{bmatrix} \underline{1} & \underline{2} & \dots & \underline{15} \\ f(\underline{1}) & f(\underline{2}) & \dots & f(\underline{15}) \end{bmatrix}$$

then,

$$H'_m e^t = \begin{bmatrix} \underline{i} + \underline{j} \\ f(\underline{i}) + f(\underline{j}) \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$

$$\Rightarrow \begin{cases} \underline{i} + \underline{j} = s_1 \\ f(\underline{i}) + f(\underline{j}) = s_2 \end{cases}$$

Choice of f : Select f such that you can solve for $\underline{i}, \underline{j}$, given s_1, s_2 .

But how can we operate and solve equations over the set of 4-tuples?

Using Finite Fields!

Double-Error-Correcting Code

$$H = \begin{bmatrix} \underline{1} & \underline{2} & \cdots & \underline{15} \\ f(\underline{1}) & f(\underline{2}) & \cdots & f(\underline{15}) \end{bmatrix} \Rightarrow \begin{cases} \underline{i} + \underline{j} = s_1 \\ f(\underline{i}) + f(\underline{j}) = s_2 \end{cases}$$

Choice of $f(\cdot)$: Not linear! Note $f(\underline{i}) = (\underline{i})^2$ is linear in \mathbb{F}_2^4 , since

$$(\underline{i} + \underline{j})^2 = (\underline{i})^2 + (\underline{j})^2 + \cancel{2\underline{ij}} = (\underline{i})^2 + (\underline{j})^2.$$

We choose $f(\underline{j}) = (\underline{j})^3$, then if

$$e = (0 \dots 0 \underset{\substack{\uparrow \\ i}}{1} 0 \dots 0 \underset{\substack{\uparrow \\ j}}{1} 0 \dots 0),$$

we have

$$s = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = He^t = \begin{bmatrix} \underline{i} + \underline{j} \\ (\underline{i})^3 + (\underline{j})^3 \end{bmatrix}$$

Double-Error-Correcting Code

Solve \underline{i} and \underline{j} from s_1 and s_2 .

$$\begin{cases} \underline{i} + \underline{j} = s_1 \\ (\underline{i})^3 + (\underline{j})^3 = s_2 \end{cases} \Rightarrow \begin{cases} \underline{i} + \underline{j} = s_1 \\ \underline{i}\underline{j} = \frac{s_2}{s_1} - s_1^2 \end{cases}$$

Therefore, \underline{i} and \underline{j} are roots of

$$z^2 + s_1 z + \left(\frac{s_2}{s_1} + s_1^2 \right) = 0$$

If only one error occurs, then $s_2 = s_1^3$.

Double-Error-Correcting Code

Decoding Algorithm:

- 1 Compute $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = Hy^t (= He^t)$.
- 2 If $s_1 = s_2 = 0 \Rightarrow$ No errors, output y , ****exit****.
- 3 If $s_1^3 = s_2 \neq 0 \Rightarrow$ One error at location s_1 , correct, ****exit****.
- 4 If $s_1 \neq 0, s_2 \neq s_1^3 \Rightarrow$ Solve the quadratic equation:

$$z^2 + s_1 z + \left(\frac{s_2}{s_1} + s_1^2 \right) = 0$$

Correct two errors at the roots, ****exit****.

- 5 If $s_1 = 0, s_2 \neq 0$ or if the quadratic equation has no two distinct roots, \Rightarrow More than two errors, ****decoding failure****.

Double-Error-Correcting Code

Example: let $\alpha \in \mathbb{F}_2^4$ be the root of $g(x) = x^4 + x + 1$:

$$H = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{14} \\ \alpha^0 & \alpha^3 & \alpha^6 & \cdots & \alpha^{12} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots \\ 0 & 1 & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ 1 & 0 & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ 0 & 1 & \cdots \end{bmatrix} \quad (\alpha^i \text{ represents a binary 4-tuple})$$

Suppose two errors occur at positions 6 and 8, corresponding to columns:

$$\begin{bmatrix} \alpha^6 \\ \alpha^3 \end{bmatrix}, \quad \begin{bmatrix} \alpha^8 \\ \alpha^9 \end{bmatrix}$$
$$s = Hy^t = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$
$$\Rightarrow \begin{cases} s_1 = \alpha^6 + \alpha^8 = \alpha^{14} \\ s_2 = \alpha^3 + \alpha^9 = \alpha \end{cases}$$

Double-Error-Correcting Code

Example (cont.):

$$\begin{aligned}\frac{s_2}{s_1} + s_1^2 &= \frac{\alpha}{\alpha^{14}} + (\alpha^{14})^2 = \alpha^{-13} + \alpha^{28} \\ &= \alpha^2 + \alpha^{13} = \alpha^{14} \\ &\quad \uparrow \\ &\text{modulo } \alpha^{15}\end{aligned}$$

Solving the equation:

$$z^2 + \alpha^{14}z + \alpha^{14} = 0$$

How to solve this? Brute force—try all values in the finite field.

Roots: α^6 and α^8 .

Double-Error-Correcting Code

Example (cont.):

$$H = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{14} \\ \alpha^0 & \alpha^3 & \alpha^6 & \dots & \alpha^{12} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots \\ 0 & 1 & \dots \\ 0 & 0 & \dots \\ 0 & 0 & \dots \\ 1 & 0 & \dots \\ 0 & 0 & \dots \\ 0 & 0 & \dots \\ 0 & 1 & \dots \end{bmatrix}$$

Parameters of the Code

- $n = 15$
- $k \geq 15 - 2 \times 4 = 7$ (Some of the rows in H may be linearly dependent.)
- $d \geq 5$ (Can correct 2 errors.)

Actually: $(15, 7, 5)$

In general:

$$n = 2^m - 1,$$

$$k = 2^m - 1 - 2m,$$

$$d = 5.$$

Is it possible to generalize the construction so that we can correct t -errors?

YES! But we need more algebra.