III Finite Fields

Do motivation. Talk about looking for \( \cdot \), \( + \).

A. Basis

1. Definition

**Def:** A field is a set \( F \) of elements ("elements") and two operations \( + \) ("addition") and \( \cdot \) ("multiplication") such that:

- \( F, + \) is a **commutative group**:
  - \( \forall x, y \in F, x + y = y + x \) (commutativity)
  - \( \exists 0 \in F \) such that \( x + 0 = x \) (additive identity)
  - \( \exists -x \in F \) such that \( x + (-x) = 0 \) (additive inverse)

- \( F, \cdot \) is a **commutative group**:
  - \( \forall x, y \in F, x \cdot y = y \cdot x \) (commutativity)

2. \( (F, 0, 1) \) is a commutative group.

3. Distributive over +: \( x \cdot (y + z) = x \cdot y + x \cdot z \)
Examples

Infinite Fields

\[ \mathbb{R}, \mathbb{Q}, \mathbb{C} \]

Finite Fields

- arithmetic modulo a prime
- arithmetic modulo an irreducible polynomial with coefficients in a field

Example: \( GF(2) \)

\[ \begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array} \]

\[ \begin{array}{c|cc}
\cdot & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array} \]

Example: \( GF(p) \)

\( p \) a prime

\[ \begin{array}{c|cc}
\neq & 0, 1, \ldots, p-1 \\
+ & \text{modulo-}p \text{ addition} \\
\cdot & \text{modulo-}p \text{ multiplication} \\
\end{array} \]
Example (GF(4)?)

\[ 7 = \{0, 1, 2, 3\} \]

+ : mod 4 addition
\[ \vdots \]
\[ \vdots \]
\[ \vdots \]

\[ \text{\{\{7, +\\}\{a\}} \text{ a commutative group? Yes} \]

\[ \text{\{\{7-\{0\}\}} \text{ a commutative group? No} \]

\[ 2 \cdot 2 = 0 \notin \{\{7-\{0\}\} \]

But there does exist a field with 4 elements!

\[ \mathbb{F}_2 \text{ Finite Fields} \]

\[ \text{\{\{2\}} \text{ exist. } \text{Prop}\]s.

\[ \text{\{\{a\}} \text{ The characteristic (of a field) } \text{Prop}\]s.

\[ \text{\{\{2\}} \text{ Additive inverse.} \]

Consider a finite field GF(q)

\[ \text{\{\{3\}} \text{ an element "1" (the multiplicative identity).} \]

Form sums \[ \sum_{i=1}^{k} 1 \]

\[ 1, 1+1, 1+1+1, 1+1+1+1 \ldots \]

All of these must be in the field. Can they be distinct? No. The field is finite.
\[ \exists m, n \text{ s.t. } (n^m) \]

\[ \sum_{i=1}^{m} i = \sum_{i=1}^{n} i \]

\[ \Rightarrow \sum_{i=1}^{n-m} i = 0 \]

\[ \Rightarrow \sum_{i=1}^{m} i = 0 \]

\[ \lambda \text{ is the characteristic of the field.} \]

**Theorem.** The characteristic of a finite field is prime.

**Proof.**

Suppose \[ \lambda = km \quad (k \neq 1, m \neq 1) \]

\[ 0 = \sum_{i=1}^{km} i \]

\[ = \left( \sum_{i=1}^{k} i \right) \left( \sum_{i=1}^{m} i \right) \quad \text{(distributive law)} \]

\[ \Rightarrow \sum_{i=1}^{m} i = 0 \quad \text{or} \quad \sum_{i=1}^{k} i = 0 \quad \Rightarrow \text{contradiction} \]

\[ \Rightarrow \lambda \text{ must be prime.} \]
1. \( \lambda \) does not necessarily equal \( q \).

2. 
   \[ \lambda_1 + 1 + \lambda_2 + 1 + \lambda_3 + 1 + \cdots + \lambda_q = 0 \]
   are distinct elements in \( GF(q) \) that
   
   form a field \( GF(\lambda) \) (with \( \lambda_1 \) ñ of \( GF(q) \))
   (actually a subfield of \( GF(q) \))

3. \( q = 2^n \) for some \( n \) (not shown)

---

2. Let \( \beta \) be some non-zero element of \( GF(q) \).

   Consider
   
   \[ \beta, \beta^2, \beta^3, \beta^4, \ldots \]
   
   All of these are in the field, but they may not be distinct. No. The field is finite.

3. \( \beta \) is a primitive element

   \[ \beta^n = \beta^m \]

   \[ \Rightarrow \beta^{n-m} = 1 \] (by the multiplicative group properties)

   \[ \Rightarrow \beta^{n=1} = 1 \]
For each possible \( \beta \) in \( \mathbb{F}_p \), an integer \( k \) (which depends on \( \beta \)) is \( k \) \( \beta^k = 1 \)

\[ \beta, \beta^2, \beta^3, \ldots, \beta^{k-1}, \beta \beta^3, \ldots, \beta^{k-1} \ldots \]

\( k \) is called the **order** of \( \beta \) (\( \text{ord}(\beta) = k \))

**Notes:**

1. \( k \) does not necessarily equal \( q \).

2. \( \beta, \beta^2, \ldots, \beta^k = 1 \) are distinct elements in \( \mathbb{F}_p \) that form a cyclic group under the multiplication of \( \mathbb{F}_p \).

(A cyclic group is a group where all of the elements can be obtained by a power of one element)

**Theorem** Let \( \beta \) be a non-zero element of \( \mathbb{F}_p \). Then

\[ \beta^{q-1} = 1. \]

**Proof** Let \( \{0 \} = \{a_1, a_2, \ldots, a_{q-1} \} \)

Consider \( \beta \cdot a_1, \beta \cdot a_2, \ldots, \beta \cdot a_{q-1} \)

(non-zero and distinct)
all elements on $\mathbb{F}$ 

$$(\beta \cdot a_1 \cdot \beta \cdot a_2 \cdots \beta \cdot a_{q-1}) = a_1 \cdot a_2 \cdot a_3 \cdots a_{q-1}$$

$$\beta^{q-1} \cdot a_1 \cdot a_2 \cdots a_{q-1} = a_1 \cdot a_2 \cdot a_3 \cdots a_{q-1}$$

$$\beta^{q-1} = 1$$

\[ \square \]

\[ \text{Theorem} \]

Let $\beta$ be a non-zero element in $\mathbb{F}(q)$ 
and $k = \text{ord}(\beta)$

then $k$ divides $q-1$, $(q-1) \mod k = 0$.

\[ \text{Proof} \]

Suppose not. Then

$$q-1 = nk + r \quad 0 < r < k$$

$$1 = \beta^{q-1} = \beta^{nk+r} = (\beta^{n})^{k} \cdot \beta^{r} = \beta^{r}$$

\[ \text{contradiction (by definition of } k \text{) } \square \]

\[ \text{Def} \]

A non-zero element $\beta$ is said to be 
\text{primitive} if $\text{ord}(\beta) = q-1$.

(\text{Note that powers of a primitive } \beta \text{ generate} 
all of $\mathbb{F}(q)$)
III Finite Fields

A Bases

1. Definition

\[ F_2, +, \cdot \]

satisfy some properties:

1. \( \mathbb{F}_2, + \) a commutative group
2. \( \mathbb{F}_2, \cdot \) a commutative group
3. \( \cdot \) distributes over +

**GF(4) from \( x^2 + x + 1 \)**

<table>
<thead>
<tr>
<th>( \mathbb{F}_2^+ )</th>
<th>point</th>
<th>polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( 0 )</td>
<td>( 00 )</td>
</tr>
<tr>
<td>1</td>
<td>( \beta )</td>
<td>( 01 )</td>
</tr>
<tr>
<td>( \beta^2 )</td>
<td>( 2 )</td>
<td>( 11 )</td>
</tr>
</tbody>
</table>

\[
\begin{array}{c|ccc|cc|cccc}
+ & 0 & 1 & \beta & \beta^2 \\
\hline
0 & 0 & 1 & \beta & \beta^2 \\
1 & 1 & 0 & 3 & 2 \\
\beta & 2 & 3 & 0 & 1 \\
\beta^2 & 3 & 2 & 1 & 0
\end{array}
\]

\[
x (x-1) (x-\beta) (x-\beta^2) = x^4 - x^3 - \beta x^3 + \beta x^2 \\
(x^2 - x) (x^2 - \beta x - \beta^2 x + \beta^3) = -\beta^2 x^3 + \beta^3 x^2 + \beta x^2 - \beta x
\]
2 Properties

Characteristic number of 1's that sum to zero

\[ \lambda = 2 \implies 6 \phi(4) \]

\[ \Rightarrow \text{prime} \quad \checkmark \]

\[ \Rightarrow q = 2^n \quad \checkmark \]

3 Order

Smallest \( k \) s.t. \( \beta^k = 1 \)

\[
\begin{array}{c|c}
0 & \text{o-de-} \\
1 & 1 \\
\beta & 3 \\
\beta^2 & 3 \\
\end{array}
\]

Then \( \beta^{q-1} = 1 \quad \checkmark \checkmark \checkmark \)

\[ 1, \beta, \beta^2 \]

Then order divides \( q-1 \) \quad \checkmark

Then \( \text{primitive if } \text{ord}(\beta) = q-1 \)
**Operations in Binary Fields**

### Bases of Polys

We are interested in fields $GF(2^m)$. Let's work with $GF(2)$.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Consider a "polynomial" over $GF(2)$:

$$f(x) = f_0 + f_1 x + \ldots + f_n x^n$$  \quad $f_i \in \{0,1\}$

The degree of polynomial is largest $i$ s.t. $f_i = 1$.

Polynomials can be added and multiplied in the standard way.

**Example**

1. \((x^2 + x + 1) + (x^2 + 1) = x\)
2. \((x^2 + x + 1) \cdot (x^2 + 1) = x^4 + x^3 + x^2 + x + 1\)
Note that: polynomial addition and multiplication are commutative and associative, and
\[ a(x) \cdot [b(x) + c(x)] = [a(x) \cdot b(x)] + [a(x) \cdot c(x)] \]

We also want to divide polynomials:

**Example**
\[
\begin{align*}
\text{dividend} & = x^3 + x^2 \\
\text{divisor} & = x^3 + x + 1 \\
\hline
x^6 + x^5 + x^4 & \\
\underline{x^3 \cdot (x^3 + x + 1)} & \\
0 + x^4 + x^3 & \\
\underline{x^3 \cdot (x^3 + x + 1)} & \\
0 + x^3 + x^2 & \\
\underline{x^3 \cdot (x^3 + x + 1)} & \\
x^2 + x + 1 & \\
\end{align*}
\]

\[ \Rightarrow \quad f(x) + x^4 + x^5 + x^6 = (x^2 + x^2)(x^3 + x + 1) + (x^2 + x + 1) \]

In general,
\[ f(x) = \left( \frac{q(x)}{g(x)} \right) + r(x) \]
In field \( \mathbb{F}_2 \), \( f(a) = 0 \) implies \( f(x) \) is divisible by \( x - a \). This is still true.

**Example**

\[
f(x) = 1 + x^2 + x^3 + x^4
\]

\[
f(1) = 0
\]

\[
\begin{array}{c}
\phantom{1 + x} \\
\underline{1 + x + x^2 + x^3 + x^4}
\end{array}
\]

\[
\frac{x^3 + x + 1}{x + 1}\]

\[
\underline{x^4 + x^3 + x^2 + 1}
\]

\[
\frac{x^2 + x}{x^4 + x^3 + x^2 + 1}
\]

\[
\underline{x^2 + x + 1}
\]

\[
\frac{x + 1}{x^2 + x}
\]

\[
\boxed{1 + x^2 + x^3 + x^4 = (x + 1) (x^3 + x + 1)}
\]

An **irreducible polynomial** of degree \( n \) is said to be **irreducible** if it is not divisible by any polynomial of degree less than \( n \).

**Example** (Polynomials of degree 2)

\[
\begin{array}{c|c}
X^2 & X + 1 \\
X^2 + 1 & (X + 1)(X + 1) \\
X^2 + X & X(X + 1) \\
x^2 + x + 1 & \text{irreducible}
\end{array}
\]
Two Useful Properties

1. \( x^{2^{n}} - x = \prod_{\beta \in \text{GF}(2^{n})} (x - \beta) \)

2. If \( f(\beta) = 0 \), then \( f(\beta^{2^{k}}) = 0 \) for all \( k \geq 0 \).
Fact: An irreducible polynomial of degree \( n \) in \( \mathbb{F}_2 \) is said to be primitive if the smallest positive integer \( n \) for which \( x^n + 1 \) divides \( x^{2^n} - 1 \) is \( 2^n - 1 \).

For each \( \mathbb{F} \neq \mathbb{F}_2 \) (if it exists), the order of \( \mathbb{F} \) divides \( 2^n - 1 \) and \( 2^n - 1 \) is prime.
Construction of \( GF(2^n) \)

1. Construction

Start with elements 0 and 1. Add elements \( \alpha, \alpha^2, \alpha^3, \ldots \) and define "\( + \)" by:

\[ \alpha^i + \alpha^j = \alpha^{i+j} \]

Now suppose \( \alpha \) is a root of \( p(x) \), a primitive polynomial over \( GF(2) \). Then

\[ \alpha^{2^n-1} + 1 = 0 \quad \Rightarrow \quad \alpha^{2^n-1} = 1 \]

\[ \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^n-2}\} \]

(because primitive, it does not repeat sooner)

\( \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^n-2}\} \) forms a commutative group.

2. Associative
3. Identity
4. Inverse

Problem: How do we define "\( + \)"?

Idea: Let each element correspond to a polynomial over \( GF(2) \) of degree < \( n \) and add polynomials.

Problem: How do we get the polynomials?

Answer: \( \alpha^i \mod p(x) \)

(or \( r_i(x) \) from \( \alpha^i = q(x)p(x) + r_i(x) \))
Note that the remainder is a polynomial over \( \mathbb{F}_q \) of degree \( \leq n-1 \),
\[
0 + r_1 \alpha + r_2 \alpha^2 + \ldots + r_{n-1} \alpha^{n-1}
\]
of which there are \( 2^n \) (since we need)

**Fact:** The polynomials associated with \( \alpha^i, i = a, 0, 2, \ldots, 2^n - 2 \) are distinct.

**Proof:** Suppose not \( \exists j, k \ (k > j) \) s.t.
\[
\alpha^j \text{ and } p(\alpha) = \alpha^k \text{ and } p(\alpha)
\]

Then,
\[
\alpha^j + \alpha^k = (q_j(\alpha) + q_k(\alpha))p(\alpha) + r_j(\alpha) + r_k(\alpha)
\]
\[
= (q_j(\alpha) + q_k(\alpha))p(\alpha)
\]
\[
\implies p(\alpha) \text{ divides } \alpha^j + \alpha^k = \alpha^j (1 + \alpha^{k-j})
\]

Since \( \alpha \) and \( p(\alpha) \) have no common factors except 1 (they are relatively prime), \( p(\alpha) \) does not divide \( \alpha^j \),
\[
\implies p(\alpha) \text{ divides } (1 + \alpha^{k-j})
\]
\[
\implies \text{ contradiction. } \Box
\]
Thus, the $2^n$ polynomials are distinct. (and thus must cover all $2^n$ possible defining $\mathbf{Q} + \mathbf{Q}$ as the sum of the corresponding polynomials in $\mathbf{GF}(2)$, it can be shown that:

$[\mathbf{F}, +]$ is a commutative group.

Finally, the distributive property is easy to verify.

$\Rightarrow \mathbf{F}$ is a field with $2^n$ elements. $\mathbf{GF}(2^n)$.

**Examples:**

1. Build $\mathbf{GF}(16)$ from irreducible

\[ p(x) = x^4 + x^3 + x^2 + x + 1 \]
Midterm Avg: 83.5
High: 101 (2 proving)

II Channel Coding

2 Finite Fields

2. Minimal Polynomials

Recall: \( x^{2^n} - x = \prod_{\beta \in \mathbb{F}_{2^n}} (x - \beta) \)

2. \( f(p^{2^k}) = [f(p)]^{2^k} \) for all \( k \geq 0 \)

\[ \begin{align*}
\text{Def: The minimal polynomial } m_\beta(x) & \text{ is the (monic) polynomial of smallest degree for which } \beta \\
& \text{ is a root in } \mathbb{F}_{2^n}. \\
\text{Properties:} & \\
1. m_\beta(x) & \text{ is irreducible.} \\
2. f(\beta) = 0 & \Rightarrow m_\beta(x) \text{ divides } f(x) \\
3. m_\beta(x) & \text{ divides } x^{2^n} + x \\
& \text{(Think: } x^{14} + x) \\
4. \text{degree } m_\beta(x) & \leq n \\
& \text{(Think: } n = 4) \\
\end{align*} \]
5. The minimal polynomial of a primitive element $\alpha$ has degree $n$.

6. $B$ and $B^{\overline{n}}$ have the same minimal polynomial.

Define: A cyclotomic coset containing elements in the field with the same minimal polynomial.

(Normally, powers of $\alpha$ are noted.)

$c_0 = \{0\}$
$c_1 = \{1, 2, 4, 8\}$
$c_2 = \{3, 6, 12, 9\}$
$c_3 = \{5, 10\}$
$c_4 = \{7, 14, 13, 11\}$

\[
\frac{\text{min poly}}{X + 1} = m^{(0)}(x)
\]

\[
X^7 + X + 1 = m^{(1)}(x)
\]

\[
m^{(2)}(x)
\]

\[
m^{(3)}(x)
\]

\[
m^{(4)}(x)
\]

7. $\prod_{\sigma \in C_k} (x - \sigma) = m^{(k)}(x)$ — Beal's paradox.

\[
\prod_{\sigma \in C_k} (x - \sigma) = m^{(3)}(x) = X^2 + X + 1
\]

Two ways to calculate:

1. Direct calculation
2. Power argument

8. $x^{2^n} - x = \prod_{k} m^{(k)}(x)$

= product of allmonic polynomials that are irreducible and whose degree divides $n$. 

Finish Table

Trick 1: If $f(x)$ is primitive, so is $X^n f(x^{-1})$.

\[
X^4 + X + 1 \text{ primitive } \Rightarrow X^4 + X^3 + 1 \text{ primitive}
\]

\[
= X^4 + X^3 + 1 \text{ is somebody's polynomial}
\]
\( x^3 + x^3 + x + 1 = 0 \)

(continued)
\( x^7 + x^1 + x + 1 = 0 \checkmark \)

Fill in \( x^7, x^1, x^3, x^6 \)

Let polynomial: \( x^4 + x^3 + x^2 + x + 1 \)

(recall irreducible but not primitive)

\( x^3 + x^9 + x^6 + x^3 + 1 \)

\[ \begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{array} \]

Fill in \( x^3, x^6, x^1, x^9 \)

(put Hamming code on side board.)

2.3 Cyclic Codes

2.3.1 Introduction

Let a code vector \( \epsilon = (c_0, c_1, ..., c_{n-1}) \) have associated code polynomial

\( \epsilon(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} x^{n-1} \)

Suppose we cyclically shift \( \epsilon \) by \( i \) places to get

\( \epsilon^{(i)} = (c_{n-1}, c_{n-1+i}, ..., c_{i-1}, c_0, c_1, ..., c_{n-1-i}) \)
Can we find an easy way to get $\xi^{(i)}(x)$ from $\xi(x)$?

Consider

$$X^i \xi(x) = c_0 x^i + c_1 x^{i+1} + \ldots + c_{n-1} x^{n+i-1}$$

$$= c_{n-i} (x^{n+i}) + c_{n-i+1} x (x^{n+1}) + \ldots + c_{n-1} x^{i-1} x^{n-i+1} + c_{n-i} + c_{n-i+1} x + \ldots + c_{n-1} x^{n-1}$$

$$= q(x)(x^{n+1}) + \xi^{(i)}(x)$$

$$\Rightarrow \quad \xi^{(i)}(x) = X^i \xi(x) \mod (x^{n+1}) \quad \text{for } n=7$$

**Definition** An $(n,k)$ linear code is called a **cyclic code if** $X^i \xi(x) \mod (x^{n+1})$ is a codeword polynomial for all codeword polynomials $\xi(x)$.

**Example**

$$\xi(x) = x^3 + x^7 + x^8 \quad i = 4 \quad n = 7$$

$$\xi^{(1)}(x) = x^7 + x^8 + x^{10} \quad x^7 + 1 = 0 \quad x^2 = 1$$

$$= 1 + x + x^3$$

which is in the code.
III. Finite Fields

A. Basics
- definition
- characteristic - \( p = 2^k \)
- order - \( \text{ord}(\alpha) \) divides \( q - 1 \)

B. Polynomials

\[ \alpha^4 + \alpha + 1 \]

Suppose \( \alpha \) has order \( q \),
\[ \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \]

Find a polynomial \( \alpha^q = \alpha^{\alpha^{\alpha^4}} \)

\[ \text{check: } \alpha^{16} = 1 \]
Distributive Law:

First note that since $\omega^2$ equals its polynomial representation (given $F(\omega) = 0$), we can multiply polynomials (mod $p(x)$) instead of powers. Since polynomial multiplication is distributive, we are done.

Cenk's question: How about $GF(8)$?

<table>
<thead>
<tr>
<th>Powers</th>
<th>$\omega^2$</th>
<th>$\omega$</th>
<th>$1$</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-\infty$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>C</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>E</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>F</td>
</tr>
</tbody>
</table>

Consider:

\[ A \cdot (C + D) = A \cdot 1 = A \]

\[ A \cdot C + A \cdot D = 0 + E = B \]

(distributive does not work)
<table>
<thead>
<tr>
<th>Powers</th>
<th>$\omega^3$</th>
<th>$\omega^2$</th>
<th>$\omega$</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>-∞</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
\[\alpha^4 = \omega^3 + \omega^2 + \omega + 1\]
| 5      | 0          | 0          | 0        | 1 |
\[\alpha^5 = \alpha - \omega^4\]
| 6      | 0          | 0          | 0        | 1 |
\[\alpha^6 = \alpha^4 + \omega^3 + \omega^2 + \omega\]
| 7      | 0          | 0          | 0        | 1 |
\[\alpha^7 = (\omega^3 + \omega^2 + \omega + 1)\]
| 8      | Did not get| + (\omega^3 + \omega^2 + \omega) = 1 | field |

11. Why?

12. \[\frac{x + 1}{x^5 + x^4 + x^3 + x^2 + x + 1}\]

14. \[x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)\]

The polynomial is not primitive.
2. Minimal Polynomials

(a) Proposition

Recall that

\[ \beta^{q-1} = 1 \]

for any \( \beta \in \text{GF}(q) \)

\[ \Rightarrow \quad x^{q-1} - 1 = \prod_{\beta \in \text{GF}(q)} (x - \beta) \]
Fact Let $f(x)$ be a polynomial over $\mathbb{Gr}(2)$. Then

$$[f(x)]^2 = f(x^2)$$

Proof

$$f^2(x) = (f_0 + f_1 x + \ldots + f_n x^n)^2$$

$$= f_0^2 + (f_1 x + f_2 x^2 + \ldots + f_n x^n)^2$$

$$= f_0^2 + \sum_{i=0}^{n} (f_i x^i)^2$$

*USEFUL*

$$\Rightarrow f^2(x) = \sum_{i=0}^{n} f_i x^{2i} \quad f_i \in \{0,1\}$$

$$= f(x^2)$$


Theorem

Let $f(x)$ be a polynomial over $\mathbb{Gr}(2)$. If $\int(P) = 0$, $f(P^{2^q}) = 0$ for all $\mathbb{Z} = 0$.

Proof:

$$f(P^{2^q}) = [f(P)]^{2^q} = 0$$
Defn. The minimal polynomial $m_p(z)$ is the (monic) polynomial of smallest degree for which $z$ is a root.

Properties (a long list):

1. $m_p(z)$ is irreducible.

   **Proof**
   
   If $m(x) = m_1(x)m_2(x)$, then $m_1(z) = 0$ or $m_2(z) = 0 \Rightarrow m_1(x)$ or $m_2(x)$ would be the minimum polynomial.

2. Let $f(x)$ be any polynomial over $GF(2)$ s.t. $f(z) = 0$. Then $m_p(x)$ divides $f(x)$.

   **Proof**
   
   $f(x) = m_p(x)q(x) + r(x)$ (degree of $r(x)$ is degree of $m_p(x)$)

   $f(z) = 0 \Rightarrow r(z) = 0$

   $\Rightarrow r(x) = 0$ (or else $m_p(x)$ would not be minimal) because $r(z)$ would be $m_p(z)$. 


\[ m_p(x) \text{ divides } x^{2^n} + x \]

**Proof**

For any \( B \), \( B^{2^n} - B = 0 \).

4) degree \( m_p(x) \leq n \).

**Proof**

\( GF(2^n) \) forms an \( n \)-dimensional vector space over \( GF(2) \). Thus, any \( n+1 \) elements (e.g., \( B_0, B_1, \ldots, B^n \)) must be linearly dependent. Existence of such \( f_0, f_1, \ldots, f_n \) such that

\[ f_0 + f_1 B + \ldots + f_n B^n = 0 \]

5) (Recall a primitive element is one whose order \( = q = 2^n - 1 \))

The minimal polynomial of a primitive element of \( GF(2^n) \) has degree \( n \).

**Proof**

Let \( B \in GF(2^n) \) be primitive with minimal polynomial \( m_p(x) \) of degree \( d \). Can use this polynomial to generate field \( \{0, 1, B, B^2, \ldots\} \). Since \( B \) is primitive, I get at least \( 2^n \) elements \( \equiv d = n \).

(Fill in \( B \)'s minimal polynomial)
6. $B$ and $B^{2k}$ have the same minimal polynomial.

**Proof**

$$f(B) = 0 \iff f(B^{2k}) = 0$$

(Fill in $B^2, B^4, B^6, B^8, B^{10}, \ldots$)

Note around

Define a cyclotomic coset contains elements of the field with the same minimal polynomial (elements in the same cyclotomic coset are called conjugates.)

(Do cyclotomic cosets on side board)

Sometimes just powers of $\alpha$ are noted.

$$\begin{align*}
c_0 &= \{ 0 \} & \text{min poly} & \quad x + 1 = m^{(1)}(x) \\
c_1 &= \{ 1, 2, 4, 8 \} & x^4 + x + 1 = m^{(4)}(x) \\
c_2 &= \{ 3, 6, 12, 9 \} & m^{(2)}(x) \\
c_3 &= \{ 5, 10 \} & m^{(3)}(x) \\
c_4 &= \{ 7, 14, 13, 11 \} & m^{(5)}(x)
\end{align*}$$

7. $\prod_{\alpha \in c_k} (x - \alpha^i) = m^{(k)}(x)$

Note that this property helps us find minimal polynomials.