Coding Theory: Finite Fields

$\mathbb{F}_q$ is a finite field with q elements.

For p a prime, the set of integers modulo p represented by $\{0, 1 \ldots, p-1\}$ is a finite field, denoted by $\mathbb{F}_p$.

Informally, that $\mathbb{F}_p$ is a field means that computations work as usual, namely we can add, subtract, multiply, in a commutative manner, and divide as long as it is not by 0.

Suppose there exists an element ω which is a zero of $X^2 + X + 1 \pmod 2$. Then $\omega \neq 0, 1$,

$$\omega^2 = \omega + 1 \pmod 2, \ \omega^3 = \omega(\omega + 1) = \omega^2 + \omega = 1 \pmod 2.$$

Suppose there exists an element ω which is a zero of $X^2 + X + 1 \pmod 2$. Then $\omega \neq 0, 1$,

$$\omega^2 = \omega + 1 \pmod 2, \ \omega^3 = \omega(\omega + 1) = \omega^2 + \omega = 1 \pmod 2.$$

$\mathbb{F}_4$

$+$	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	0	ω^2	ω
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\cdot$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

We want more alphabets than $\mathbb{F}_p$ and $\mathbb{F}_4$ ...

We want more alphabets than $\mathbb{F}_p$ and $\mathbb{F}_4$ ...

so we can build more codes, in particular MDS codes.

$\mathbb{F}_q[X]$

The set of polynomials in X with coefficients in $\mathbb{F}_q$.

- (Division Algorithm) Let $f(X), g(X) \in \mathbb{F}_q[X]$ with $g(X)$ non-zero. There exist unique polynomials $q(X), r(X)$ such that $f(X) = g(X)q(X) + r(X),\ \deg r(X) < \deg g(X),\ \text{ or } r(X) = 0.$

$\mathbb{F}_q[X]$

The set of polynomials in X with coefficients in $\mathbb{F}_q$.

- (Division Algorithm) Let $f(X), g(X) \in \mathbb{F}_q[X]$ with $g(X)$ non-zero. There exist unique polynomials $q(X), r(X)$ such that $f(X) = g(X)q(X) + r(X), \ \deg r(X) < \deg g(X), \ \text{ or } r(X) = 0$.
- (Greatest common divisor) If $f(X) = g(X)q(X) + r(X)$, then $\gcd(f(X), g(X)) = \gcd(g(X), r(X))$.

$\mathbb{F}_q[X]$

The set of polynomials in X with coefficients in $\mathbb{F}_q$.

- (Bezout identity) Let $f(X), g(X) \in \mathbb{F}_q[X]$ with $g(X)$ non-zero. There exist polynomials $a(X), b(X)$ such that $a(X)f(X) + b(X)g(X) = \gcd(f(X), g(X))$.

$\mathbb{F}_q[X]$

The set of polynomials in X with coefficients in $\mathbb{F}_q$.

- (Bezout identity) Let $f(X), g(X) \in \mathbb{F}_q[X]$ with $g(X)$ non-zero. There exist polynomials $a(X), b(X)$ such that $a(X)f(X) + b(X)g(X) = \gcd(f(X), g(X))$. Apply the

division algorithm iteratively: $f = gq_1 + r_1$, $g = r_1h_2 + r_2$, $r_1 = r_2h_3 + r_3, \ldots$,until $r_n = 0$, then $\gcd(f, g) = cr_{n-1}$, $c \in \mathbb{F}_q$.

Irreducible polynomial

A nonconstant polynomial $f(X) \in \mathbb{F}_q[X]$ is irreducible over $\mathbb{F}_q$ provided it does not factor into a product of two non-constant polynomials of smaller degree.

Recall:

If $f(X)$ has a factor of degree 1, that is $f(X) = (X - \alpha)g(X)$, then $f(\alpha) = 0$ and vice-versa.

Irreducible polynomial

A nonconstant polynomial $f(X) \in \mathbb{F}_q[X]$ is irreducible over $\mathbb{F}_q$ provided it does not factor into a product of two non-constant polynomials of smaller degree.

Recall:

If $f(X)$ has a factor of degree 1, that is $f(X) = (X - \alpha)g(X)$, then $f(\alpha) = 0$ and vice-versa.

If $f(X)$ has degree 2 or 3, then a factorization necessarily means a factor of degree 1, which is not the case if $f(X)$ has degree 4: it could be the product of two polynomials of degree 2.

Exercise. Are the following polynomials irreducible? (1) $X^2 + 1$ over $\mathbb{F}_2$ (2) $X^2 + 1$ over $\mathbb{F}_3$ (3) $X^4 - X + 1$ over $\mathbb{F}_3$

Exercise. Are the following polynomials irreducible? (1) $X^2 + 1$ over $\mathbb{F}_2$ (2) $X^2 + 1$ over $\mathbb{F}_3$ (3) $X^4 - X + 1$ over $\mathbb{F}_3$

(1) $X^2 + 1$ over $\mathbb{F}_2$ is not irreducible: indeed, $X^2 + 1 = (X + 1)^2$.

Exercise. Are the following polynomials irreducible? (1) $X^2 + 1$ over $\mathbb{F}_2$ (2) $X^2 + 1$ over $\mathbb{F}_3$ (3) $X^4 - X + 1$ over $\mathbb{F}_3$

(1) $X^2 + 1$ over $\mathbb{F}_2$ is not irreducible: indeed, $X^2 + 1 = (X + 1)^2$.

(2) $X^2 + 1$ over $\mathbb{F}_3$ is irreducible: $X^2 + 1$ evaluated in $X = 0$ is 1, evaluated in $X = 1$ is 2 and evaluated in 2 is $5 \equiv 2$.

Exercise. Are the following polynomials irreducible? (1) $X^2 + 1$ over $\mathbb{F}_2$ (2) $X^2 + 1$ over $\mathbb{F}_3$ (3) $X^4 - X + 1$ over $\mathbb{F}_3$

(1) $X^2 + 1$ over $\mathbb{F}_2$ is not irreducible: indeed, $X^2 + 1 = (X + 1)^2$.

(2) $X^2 + 1$ over $\mathbb{F}_3$ is irreducible: $X^2 + 1$ evaluated in $X = 0$ is 1, evaluated in $X = 1$ is 2 and evaluated in 2 is $5 \equiv 2$.

(3) $X^4 - X + 1$ over $\mathbb{F}_3$ is not irreducible: $X^4 - X + 1 \equiv X^4 + 2X + 1$ evaluated in $X = 2$ is 0.

$\mathbb{F}_q[X]/(p(X))$

The set of polynomials in X with coefficients in $\mathbb{F}_q$ modulo the polynomial $p(X)$.

It can be done with any $p(X)$, but we will consider the case where $p(X)$ is irreducible and monic (its leading coefficient is 1).

$\mathbb{F}_q[X]/(p(X))$

The set of polynomials in X with coefficients in $\mathbb{F}_q$ modulo the polynomial $p(X)$.

It can be done with any $p(X)$, but we will consider the case where $p(X)$ is irreducible and monic (its leading coefficient is 1).

$f(X)$ modulo $p(X)$ means that $f(X)$ is divided by $p(X)$: $f(X) = p(X)q(X) + r(X), \ \deg r(X) < \deg p(X), \ \text{ or } r(X) = 0$ (division algorithm) and we keep the remainder $r(X)$: $f(X) \equiv r(X) \mod p(X)$.

Exercise. Compute $\mathbb{F}_3[X]/(X^2+1)$.

Exercise. Compute $\mathbb{F}_3[X]/(X^2+1)$.

$\mathbb{F}_3[X] = \{f_0 + f_1X + f_2X^2 + \ldots, f_0, f_1, f_2 \ldots \in \mathbb{F}_3\}$

Modulo $p(X)$, any remainder must have a degree strictly less than that of $p(X) = X^2+1$, this means any remainder is of the form $r(X) = r_0 + r_1X$.

Thus $\mathbb{F}_3[X]/(X^2+1) = \{f_0 + f_1X,\ f_0, f_1 \in \mathbb{F}_3\}$.

Note that $p(X)$ is monic and irreducible, though we have not used this fact (yet).

$\mathbb{F}_q[X]/(p(X))$

For $f(X), g(X) \in \mathbb{F}_q[X]/(p(X))$, we have $f(X) + g(X) \in \mathbb{F}_q[X]/(p(X))$.

For $f(X), g(X) \in \mathbb{F}_q[X]/(p(X))$, we have $f(X)g(X) \in \mathbb{F}_q[X]/(p(X))$: indeed, compute $f(X)g(X)$, divide by $p(X)$ and take the remainder.

Exercise. In $\mathbb{F}_3[X]/(X^2+1)$, compute (1) the sum of $X+1$ and $2X+2$ and (2) the product of $X+1$ and $2X+2$.

Exercise. In $\mathbb{F}_3[X]/(X^2+1)$, compute (1) the sum of $X+1$ and $2X+2$ and (2) the product of $X+1$ and $2X+2$.

(1) $(X+1)+(2X+2)=3X+3\equiv 0$.

(2) $(X+1)(2X+2)=2X^2+2X+2X+2\equiv 2X^2+X+2$.
Next we reduce modulo X^2+1. We have
$2X^2+X+2=2(X^2+1)+X$, thus $(X+1)(2X+2)\equiv X$
in $\mathbb{F}_3[X]/(X^2+1)$.

Exercise. In $\mathbb{F}_3[X]/(X^2+1)$, compute (1) the sum of $X+1$ and $2X+2$ and (2) the product of $X+1$ and $2X+2$.

(1) $(X+1)+(2X+2) = 3X+3 \equiv 0$.

(2) $(X+1)(2X+2) = 2X^2+2X+2X+2 \equiv 2X^2+X+2$. Next we reduce modulo X^2+1. We have $2X^2+X+2 = 2(X^2+1)+X$, thus $(X+1)(2X+2) \equiv X$ in $\mathbb{F}_3[X]/(X^2+1)$.

We still have not used the fact that X^2+1 is irreducible.

Is $\mathbb{F}_q[X]/(p(X))$ a finite field?

Informally, a field means that computations work as usual, namely we can add, subtract, multiply, in a commutative manner, and divide as long as it is not by 0.

We can add. ✓

We can subtract. ✓

Is $\mathbb{F}_q[X]/(p(X))$ a finite field?

Informally, a field means that computations work as usual, namely we can add, subtract, multiply, in a commutative manner, and divide as long as it is not by 0.

We can add. ✓

We can subtract. ✓

We can multiply. ✓

Is $\mathbb{F}_q[X]/(p(X))$ a finite field?

Informally, a field means that computations work as usual, namely we can add, subtract, multiply, in a commutative manner, and divide as long as it is not by 0.

We can add. ✓

We can subtract. ✓

We can multiply. ✓

What about division?

Inverse in $\mathbb{F}_p$

For x a non-zero element in $\mathbb{F}_p$, its (multiplicative) inverse is the element in $\mathbb{F}_p$ denoted by x^{-1} which satisfies that $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

Inverse in $\mathbb{F}_q[X]/(p(X))$

For $f(X)$ a non-zero polynomial in $\mathbb{F}_q[X]$, its (multiplicative) inverse is the element in $\mathbb{F}_q[X]$ denoted by $f(X)^{-1}$ which satisfies that $f(X) \cdot f(X)^{-1} = f(X)^{-1} \cdot f(X) = 1$.

There exist polynomials $a(X), b(X)$ such that

$$a(X)f(X) + b(X)p(X) = \gcd(f(X), p(X))$$

There exist polynomials $a(X), b(X)$ such that

$$a(X)f(X) + b(X)p(X) = \gcd(f(X), p(X))$$

Since $p(X)$ is monic and irreducible, $\gcd(f(X), p(X)) = 1$ (if $f(X)$ is a multiple of $p(X)$, then $f(X) \equiv 0$).

There exist polynomials $a(X), b(X)$ such that

$$a(X)f(X) + b(X)p(X) = \gcd(f(X), p(X))$$

Since $p(X)$ is monic and irreducible, $\gcd(f(X), p(X)) = 1$ (if $f(X)$ is a multiple of $p(X)$, then $f(X) \equiv 0$). Thus, assuming $p(X)$ is irreducible, there exists $a(X)$ such that

$$a(X)f(X) \equiv 1$$

and $a(X) = f(X)^{-1}$.

Is $\mathbb{F}_q[X]/(p(X))$ a finite field?

If $p(X)$ is monic and irreducible, yes it is.

We can add. ✓

We can subtract. ✓

We can multiply. ✓

Is $\mathbb{F}_q[X]/(p(X))$ a finite field?

If $p(X)$ is monic and irreducible, yes it is.

We can add. ✓

We can subtract. ✓

We can multiply. ✓

We can divide since every non-zero polynomial is invertible. ✓

Exercise. (1) Find an irreducible polynomial $p(X)$ of degree 2 over $\mathbb{F}_2$, (2) compute the multiplication table of $\mathbb{F}_2[X]/(p(X))$, (3) compare with the multiplication table of $\mathbb{F}_4$.

Exercise. (1) Find an irreducible polynomial $p(X)$ of degree 2 over $\mathbb{F}_2$, (2) compute the multiplication table of $\mathbb{F}_2[X]/(p(X))$, (3) compare with the multiplication table of $\mathbb{F}_4$.

(1) We look for a polynomial $p(X) = p_0 + p_1 X + p_2 X^2$, with p_0, p_1, p_2 over $\mathbb{F}_2$. We need $p_2 = 1$ to have a degree of 2: $p(X) = p_0 + p_1 X + X^2$. Then we also need $p_0 = 1$, otherwise X can be factored out: $p(X) = 1 + p_1 X + X^2$. Finally we also need $p_1 = 1$, otherwise $X = 1$ is a root. This gives the polynomial $p(X) = X^2 + X + 1$.

Exercise. (1) Find an irreducible polynomial $p(X)$ of degree 2 over $\mathbb{F}_2$, (2) compute the multiplication table of $\mathbb{F}_2[X]/(p(X))$, (3) compare with the multiplication table of $\mathbb{F}_4$.

(2)

$\cdot$	0	1	X	$X^2 \equiv X+1$
0	0	0	0	0
1	0	1	X	X^2
X	0	X	X^2	1
X^2	0	X^2	1	X

$X^2 = (X^2+X+1)+X+1$
$X^3 =$
$(X+1)(X^2+X+1)+1$
$X^4 =$
$(X^2+X)(X^2+X+1)+X$

Exercise. (1) Find an irreducible polynomial $p(X)$ of degree 2 over $\mathbb{F}_2$, (2) compute the multiplication table of $\mathbb{F}_2[X]/(p(X))$, (3) compare with the multiplication table of $\mathbb{F}_4$.

(2)

$\cdot$	0	1	X	X^2
0	0	0	0	0
1	0	1	X	X^2
X	0	X	X^2	1
X^2	0	X^2	1	X

(3)

$\cdot$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

For $p(X)$ monic and irreducible
$\mathbb{F}_q[X]/(p(X)) \simeq \mathbb{F}_q[w]$ with $p(w) = 0$

Set $\deg(p) = n$, define a map $\phi :$ $\mathbb{F}_q[X]/(p(X)) \to \mathbb{F}_q[w]$, $f_0 + f_1 X + \ldots + f_{n-1} X^{n-1} \mapsto f_0 + f_1 w + \ldots + f_{n-1} w^{n-1}$

ϕ is an isomorphism:

$\phi(0) = 0$, $\phi(1) = 1$

$\phi(f + g) = \phi(f) + \phi(g)$

$\phi(fg) = \phi(f)\phi(g)$: this follows from the fact that for $f(X) = q(X)p(X) + r(X)$, $f(X) \equiv r(X) \iff f(w) = r(w)$.

For $p(X)$ monic and irreducible $\mathbb{F}_q[X]/(p(X)) \simeq \mathbb{F}_q[w]$ with $p(w) = 0$

Set $\deg(p) = n$, define a map ϕ : $\mathbb{F}_q[X]/(p(X)) \to \mathbb{F}_q[w]$, $f_0 + f_1 X + \ldots + f_{n-1} X^{n-1} \mapsto f_0 + f_1 w + \ldots + f_{n-1} w^{n-1}$

ϕ is an isomorphism:

- $\phi(0) = 0$, $\phi(1) = 1$
- $\phi(f + g) = \phi(f) + \phi(g)$
- $\phi(fg) = \phi(f)\phi(g)$: this follows from the fact that for $f(X) = q(X)p(X) + r(X)$, $f(X) \equiv r(X) \iff f(w) = r(w)$.
- Both sets have the same cardinality, namely q^n.
- The map is injective, thus bijective.

Recipe to construct $\mathbb{F}_q$

$q = p^n$

- Find a monic irreducible polynomial $p(X)$ of degree n over $\mathbb{F}_p$.
- Let w be a root of the polynomial $p(X)$. Then $\mathbb{F}_p[w]$ is the set $\{a_0 + a_1 w + \ldots + a_{n-1} w^{n-1},\ a_0, \ldots, a_{n-1} \in \mathbb{F}_p\}$, and w^n is given by $0 = p(w) = p_0 + p_1 w + \ldots + w^n \Rightarrow w^n = -p_0 - p_1 w - \ldots - p_{n-1} w^{n-1}$ (recall that $p(X)$ is monic).

Exercise. Construct $\mathbb{F}_9$, list its elements and give a multiplication table.

Exercise. Construct $\mathbb{F}_9$, list its elements and give a multiplication table.

(1) We already know that $p(X) = X^2 + 1$ over $\mathbb{F}_3$ is irreducible.

(2) Let w be a root of $p(X)$, that is $0 = p(w) = w^2 + 1 \Rightarrow w^2 = -1 = 2$. Then

$$\mathbb{F}_9 = \{0, 1, 2, w, w+1, w+2, 2w, 2w+1, 2w+2\}$$

(3)

$\cdot$	1	2	w	$w+1$	$w+2$	$2w$	$2w+1$	$2w+2$
1	1	2	w	$w+1$	$w+2$	$2w$	$2w+1$	$2w+2$
2	2	1	$2w$	$2w+2$	$2w+1$	w	$w+2$	$w+1$
w	w	$2w$	2	$2+w$	$2+2w$	1	$1+w$	$1+2w$
$w+1$	$w+1$	$2w+2$	$2+w$	$2w$	1	$1+2w$	2	w
$w+2$	$w+2$	$2w+1$	$2w+2$	1	w	$1+w$	$2w$	2
$2w$	$2w$	w	1	$1+2w$	$1+w$	2	$2+2w$	$2+w$
$2w+1$	$2w+1$	$w+2$	$1+w$	2	$2w$	$2+2w$	w	1
$2w+2$	$2w+2$	$w+1$	$1+2w$	w	2	$2+w$	1	$2w$

Irreducible polynomial

Construction of finite fields