4. Brief Review of Finite Fields

Fields

- A *field* is a set $\mathbb{F}$ with two operations, $+$ (addition) and $\cdot$ (multiplication), satisfying the following properties:
  - *Associativity*: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
  - *Commutativity*: $a + b = b + a$ and $a \cdot b = b \cdot a$.
  - *Identities*: there exist two unique elements, $0, 1 \in \mathbb{F}$, $0 \neq 1$, such that $\forall a \in \mathbb{F}$, $a + 0 = a$ and $a \cdot 1 = a$.
  - *Additive inverses*: $\forall a \in \mathbb{F},\ \exists b \in \mathbb{F}$ such that $a + b = 0$ (b is denoted $-a$).
  - *Multiplicative inverses*: $\forall a \in \mathbb{F} \setminus \{0\},\ \exists b \in \mathbb{F}$ such that $a \cdot b = 1$ (b is denoted a^{-1}).
  - *Distributivity* of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- Other properties, such as $a \cdot 0 = 0$ or $a \cdot b = 0 \implies a = 0$ or $b = 0$ follow easily from the defining ones.
- A field has an *additive group* $\mathbb{F}^+$, and a *multiplicative group* $\mathbb{F}^*$ (with underlying set $\mathbb{F} \setminus \{0\}$). Both groups are *abelian* (commutative).
- A *finite field* (or *Galois field*) is a field with a *finite* underlying set: $|\mathbb{F}| = q,\ \ q \geq 2$. We denote such a field $\mathbb{F}_q$, or $\mathrm{GF}(q)$

  (for the time being, this may be an *abuse of notation*, since there may be different fields of size q).

Fields: Examples

- Well known infinite fields: the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, the complexes $\mathbb{C}$.
- Well known *non-fields*: the integers $\mathbb{Z}$, the naturals $\mathbb{N}$.
  - The integers $\mathbb{Z}$ form a *commutative ring* (all the properties hold except for multiplicative inverses).
- Given a field $\mathbb{F}$ and an indeterminate symbol x, the field $\mathbb{F}(x)$ of all *rational functions* $f(x)/g(x)$, where $f(x), g(x)$ are polynomials over $\mathbb{F}$, $g(x) \neq 0$, $\gcd(f(x), g(x)) = 1$. This field is always infinite.
- Examples of finite fields:
  - Smallest: $\mathbb{F}_2 = \{0,1\}$ with $+ = \text{XOR}$ (addition modulo 2), $\cdot = \text{AND}$.
  - Next smallest: $\mathbb{F}_3 = \{0, 1, 2\}$ with operations modulo 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

  - $\mathbb{F}_4$:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

not integers modulo 4

Finite Field Basics

- For a prime p, let $\mathbb{F}_p$ denote the ring of integers mod p, with underlying set $\{0, 1, \ldots, p-1\}$.
- **Claim:** $\mathbb{F}_p$ is a *finite field*.
  - For every integer $a \in \{1, 2, \ldots, p-1\}$, we have $\gcd(a, p) = 1$. By *Euclid's extended algorithm*, there exist integers s, t such that $s \cdot a + t \cdot p = 1$. The integer s, taken modulo p, is the multiplicative inverse of a in the field $\mathbb{F}_p$.
- **Refresher:** Euclid's $\gcd$ algorithm.
  - To compute $\gcd(a, b)$, $a, b \in \mathbb{N}$, we start with $r_{-1} = a$, $r_0 = b$, and compute a sequence of *remainders* $r_1, r_2, \ldots, r_m$, where for $i \geq 1$,

$$r_i = r_{i-2} - q_i r_{i-1}, \quad q_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor, \ 0 \leq r_i < r_{i-1}$$

    q_i, r_i are the quotient and remainder (resp.) of the integer division of r_{i-2} by r_{i-1}.
  - The sequence $r_1, r_2, \ldots$ is non-negative and *strictly decreasing*, so it must reach zero. Say, $r_m = 0$. Then $r_{m-1} = \gcd(a, b)$.
  - The *extended Euclidean algorithm* also keeps track of auxiliary sequences of integers $s_1, s_2, \ldots$ and $t_1, t_2, \ldots$ such that

$$s_i a + t_i b = r_i, \quad i \geq 1 \, .$$

Finite Field Basics

- **Example:** Inverse of 16 modulo 41, start with $r_{-1} = 41$, $r_0 = 16$:

i	r_i	$=$	r_{i-2}	$-$	$q_i \cdot r_{i-1}$	$=$	$s_i \cdot a$	$+$	$t_i \cdot b$
1	9	$=$	41	$-$	$2 \cdot 16$	$=$	$1 \cdot 41$	$-$	$2 \cdot 16$
2	7	$=$	16	$-$	$1 \cdot 9$	$=$	$-1 \cdot 41$	$+$	$3 \cdot 16$
3	2	$=$	9	$-$	$1 \cdot 7$	$=$	$2 \cdot 41$	$-$	$5 \cdot 16$
4	1	$=$	7	$-$	$3 \cdot 2$	$=$	$-7 \cdot 41$	$+$	$18 \cdot 16$

$\Rightarrow \quad 18 \cdot 16 \equiv 1 \bmod 41 \qquad \Rightarrow \quad 18 = 16^{-1}$ in $\mathbb{F}_{41}$.

Finite Field Basics

- *Order of a finite group*: number of elements in the group. The additive group of $\mathbb{F}_q$ has order $|\mathbb{F}_q| = q$, the multiplicative group order $|\mathbb{F}^*| = q - 1$.
- *Order of an element $a \in \mathbb{F}_q$*:
  - *Additive*: least positive integer k such that
    $$\underbrace{a + a + \cdots + a}_{k} = 0\,.$$
  - *Multiplicative* (for $a \neq 0$): least positive integer m such that $a^m = 1$.
- *Lagrange's theorem for finite groups*: If G is a finite group, and H is a subgroup of G, then $|H|$ divides $|G|$. It follows that the order of any $g \in G$ divides $|G|$.

Proposition

Let $a \in \mathbb{F}_q$. Then, $q \times a \triangleq \underbrace{a + a + \cdots + a}_{q} = 0$ and $a^q = a$.

Proof. By Lagrange's theorem, the additive order of a divides q, and the multiplicative order divides $q - 1$. Therefore $q \times a = 0$ and $a^{q-1} = 1$ for $a \neq 0$. Together with $0^q = 0$, we get $a^q = a$ for all a in $\mathbb{F}_q$. $\square$

Field Characteristic

Let $\mathbb{F}$ be a field, and let 1 be the identity in $\mathbb{F}^*$. The *characteristic* $\text{char}(\mathbb{F})$ of $\mathbb{F}$ is the least positive integer c, *if any*, such that

$$c \times 1 = \underbrace{1 + 1 + 1 + \cdots + 1}_{c} = 0\,.$$

If c exists, it is the additive order of 1 in $\mathbb{F}$. If no such integer exists, we define $\text{char}(\mathbb{F}){=}0$.

- If $c = \text{char}(\mathbb{F}) > 0$, then for any $\alpha \in \mathbb{F}$, $c \times \alpha = 0$.
- For a finite field $\mathbb{F}$, we always have $\text{char}(\mathbb{F}) > 0$.
- **Examples:** $\text{char}(\mathbb{F}_7) = 7$, $\text{char}(\mathbb{F}_4) = 2$, $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$.
- An infinite field can have a positive characteristic. For example, $\mathbb{F}_2(x)$ is infinite, with $\text{char}(\mathbb{F}_2(x)) = 2$.

Field Characteristic

Proposition

If $\mathrm{char}(\mathbb{F}) > 0$ *then it is a prime* p*.* $\mathbb{F}$ *then contains a sub-field isomorphic to* $\mathbb{F}_p$*.*

Proof. Assume $p = \mathrm{char}(\mathbb{F}) > 0$, and p factors as $p = ab$ with $1 < a \leq b < p$. Then, $0 = p \times 1 = (a \times 1) \cdot (b \times 1)$, which implies that either $a \times 1 = 0$ or $b \times 1 = 0$, contradicting the minimality of p. The subset $\{0, 1, 1{+}1, \ldots, \underbrace{1 + 1 + \cdots + 1}_{p-1}\} \subseteq \mathbb{F}$ is isomorphic to $\mathbb{F}_p$. $\square$

Proposition

Let $\mathbb{F}$ *be a finite field, let* $a, b \in \mathbb{F}$*, and let* $p = \mathrm{char}(\mathbb{F})$*. Then* $(a + b)^p = a^p + b^p$*.*

Proof. The binomial coefficient $\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{1\cdot 2\cdots(i-1)i}$ is a multiple of p for $0 < i < p$. $\square$

Polynomials

- For a field $\mathbb{F}$ and indeterminate x,
  - $\mathbb{F}[x]$: ring of polynomials in x, with coefficients in $\mathbb{F}$. This is an *Euclidean ring*: degree, divisibility, division with reminder, GCD, etc. are well defined and "behave" as we're used to over $\mathbb{R}$.
  - The *extended Euclidean algorithm* can be applied to elements of $\mathbb{F}[x]$, and for $a, b \in \mathbb{F}[x]$, not both zero, we have polynomials $s(x), t(x)$ such that

$$s(x) \cdot a(x) + t(x) \cdot b(x) = \gcd(a(x), b(x))$$

- $P(x) \in \mathbb{F}[x]$ is called *irreducible* if

$$\deg(P(x)){>}0 \text{ and } P(x){=}a(x)b(x) \implies \deg(a(x)){=}0 \text{ or } \deg(b(x)){=}0$$

  - **Example:** $x^2 + 1$ is irreducible over $\mathbb{R}$.
  - **Example:** irreducibles over $\mathbb{F}_2$

    degree 1: $x,\ x{+}1$ degree 3: $x^3{+}x{+}1,\ x^3{+}x^2{+}1$
    degree 2: $x^2{+}x{+}1$ degree 4: $x^4{+}x{+}1,\ x^4{+}x^3{+}1,\ x^4{+}x^3{+}x^2{+}x{+}1$
  - $\mathbb{F}[x]$ is a *unique factorization domain* (factorization into irreducible polynomials is unique up to permutation and scalar multiples).

Arithmetic Modulo an Irreducible Polynomial

- Let $\mathbb{F}$ be a field and $P(x)$ an *irreducible* polynomial of degree $h \geq 1$.
- The ring of residue classes of $\mathbb{F}[x]$ modulo $P(x)$ is denoted $\mathbb{F}[x]/\langle P(x)\rangle$.
  - Let $\mathbb{F}[x]_n =$ set of polynomials of degree $< n$ in x over $\mathbb{F}$.
  - $\mathbb{F}[x]/\langle P(x)\rangle$ can be represented by $\mathbb{F}[x]_h$ with arithmetic mod $P(x)$.

Theorem

$\mathbb{F}[x]/\langle P(x)\rangle$ *is a field.*

- This theorem, and the one saying $\mathbb{F}_p$ is a field (p prime), are special cases of the same theorem on Euclidean rings.
- As with integers, inverses are found found using the Euclidean algorithm: $\gcd(a(x), P(x)) = 1 \implies$
  $\exists\, s(x), t(x)$: $s(x)a(x) + t(x)P(x) = 1 \implies$
  $s(x)$ is a multiplicative inverse of $a(x)$ in $\mathbb{F}[x]/\langle P(x)\rangle$.

Arithmetic Modulo an Irreducible Polynomial

Example: Inverse of x^2 modulo x^3+x+1 over $\mathbb{F}_2$ (recall that $z=-z$).

$r_i(x) =$	$r_{i-2}(x)$	$+\, q_i(x)\cdot r_{i-1}(x) =$	$t_i(x)\cdot P(x)$	$+s_i(x)\cdot a(x)$
$x{+}1 =$	$x^3{+}x{+}1$	$+x\cdot x^2 =$	$1\cdot(x^3{+}x{+}1)$	$+x\cdot(x^2)$
$x =$	x^2	$+x\cdot(x{+}1) =$	$x\cdot(x^3{+}x{+}1)$	$+(x^2{+}1)\cdot(x^2)$
$1 =$	$(x{+}1)$	$+1\cdot x =$	$(x{+}1)\cdot(x^3{+}x{+}1)$	$+(x^2{+}x{+}1)\cdot(x^2)$

$\Rightarrow \quad x^2{+}x{+}1 = (x^2)^{-1}$ in $\mathbb{F}_2[x]/\langle x^3{+}x{+}1\rangle$

Sub-fields and Extension Fields

- Let $\mathbb{K}$ be a field, and let $\mathbb{F}$ be a subset of $\mathbb{K}$, such that $\mathbb{F}$ is a field under the operations of $\mathbb{K}$. Then,
  - $\mathbb{F}$ is a *sub-field* of $\mathbb{K}$, and $\mathbb{K}$ is an *extension field* of $\mathbb{F}$.
- $\mathbb{K}$ is a vector space over $\mathbb{F}$ ($\forall \alpha, \beta \in \mathbb{K}, a, b \in \mathbb{F}$: $a\alpha + b\beta \in \mathbb{K}$). The dimension $[\mathbb{K} : \mathbb{F}]$ of this vector space is referred to as the *extension degree* of $\mathbb{K}$ over $\mathbb{F}$.
  - If $[\mathbb{K} : \mathbb{F}]$ is finite, $\mathbb{K}$ is called a *finite extension* of $\mathbb{F}$. A finite extension is not necessarily a finite field: $\mathbb{C}$ is a finite extension of $\mathbb{R}$.
  - $\mathbb{F}[x]/\langle P(x)\rangle$ is an extension of degree h of $\mathbb{F}$, where $h = \deg(P)$.
  - If $|\mathbb{F}| = q$, then $|\mathbb{F}_q[x]/\langle P(x)\rangle| = q^h$.
  - If $|\mathbb{F}| = q$, and $\mathrm{char}(\mathbb{F}) = p$, then $q = p^m$ for some integer $m \geq 1$.
- We can also create an extension field by *adjoining* to $\mathbb{F}$ a root α of an irreducible polynomial over $\mathbb{F}$. This *algebraic* extension is denoted $\mathbb{F}(\alpha)$.
  - Examples:
    - $\mathbb{C} = \mathbb{R}(i)$ (using the rule $i^2 = -1$).
    - $\mathbb{Q}(\sqrt{2})$, typical elements are of the form $a + b\sqrt{2},\ a, b \in \mathbb{Q}$, and we use the rule $(\sqrt{2})^2 = 2$.
    - $F_2(\alpha)$, where α is a root of $x^3 + x + 1 \in \mathbb{F}_2[x]$. Rule: $\alpha^3 = \alpha{+}1$.
  - The two ways of creating extensions are *equivalent*.

Finite Field Example (a)

$\mathbb{F} = \mathbb{F}_2,\ P(x) = x^3 + x + 1$. Let $[f(x)]$ represent the residue class $\{g(x) \in \mathbb{F}_2[x] \,:\, g(x) \equiv f(x) \pmod{P(x)}\}$.

Elements of $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle P(x) \rangle$ and their inverses

element	*inverse*
0	–
1	1
$[x]$	$[x^2+1]$
$[x+1]$	$[x^2+x]$
$[x^2]$	$[x^2+x+1]$
$[x^2+1]$	$[x]$
$[x^2+x]$	$[x+1]$
$[x^2+x+1]$	$[x^2]$

Examples:

- $[x] \cdot [x^2+1] = [x^3+x] = 1$
- $[x] \cdot [x^2+x] = [x^3+x^2] = [x^2+x+1]$
- $[x^2+1] \cdot [x^2] = [x^4+x^2]$
  $= [x^2+x+x^2] = [x]$

Facts (for general $\mathbb{F}$ and $P(x)$):

- *The element* $[x] \in \mathbb{F}[x]/\langle P(x) \rangle$ *is a root of* $P(x)$.
- Denote $\alpha = [x]$. Then, $\mathbb{F}[x]/\langle P(x) \rangle$ is isomorphic to $\mathbb{F}(\alpha)$.
- If $\deg(P(x)) = h$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{h-1}\}$ is a basis of $\mathbb{F}(\alpha)$ over $\mathbb{F}$.

Finite Field Example (b)

$\mathbb{F} = \mathbb{F}_2,\ P(x) = x^3 + x + 1$. Let $[f(x)]$ represent the residue class $\{g(x) \in \mathbb{F}_2[x] \ :\ g(x) \equiv f(x) \pmod{P(x)}\}$.

Elements of $\mathbb{F}_8 = \mathbb{F}(\alpha)$ and their inverses

element	*inverse*
0	–
1	1
α	α^2+1
$\alpha+1$	$\alpha^2+\alpha$
α^2	$\alpha^2+\alpha+1$
α^2+1	α
$\alpha^2+\alpha$	$\alpha+1$
$\alpha^2+\alpha+1$	α^2

Examples (rule: $\alpha^3 = \alpha + 1$):

- $\alpha \cdot (\alpha^2+1) = \alpha^3 + \alpha = 1$
- $\alpha \cdot (\alpha^2+\alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
- $\alpha^2 + 1 \cdot \alpha^2 = \alpha^4 + \alpha^2$
  $= \alpha^2 + \alpha + \alpha^2 = \alpha$

Facts (for general $\mathbb{F}$ and irreducible $P(x)$):

- The element $[x] \in \mathbb{F}[x]/\langle P(x)\rangle$ is a root of $P(x)$.
- Denote $\alpha = [x]$. Then, $\mathbb{F}[x]/\langle P(x)\rangle$ is isomorphic to $\mathbb{F}(\alpha)$.
- If $\deg(P(x)) = h$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{h-1}\}$ is a basis of $\mathbb{F}(\alpha)$ over $\mathbb{F}$.

Roots of Polynomials

Proposition

A polynomial of degree $n \geq 0$ over a field $\mathbb{F}$ has at most n roots in any extension of $\mathbb{F}$.

Proposition

Let $\mathbb{F}$ be a finite field. Then, $x^{|\mathbb{F}|} - x = \prod_{\beta \in \mathbb{F}} (x - \beta)$.

Proposition

Let $\mathbb{F} = \mathbb{F}_q$, let $P(x)$ be an irreducible polynomial of degree h over $\mathbb{F}$. Let α be a root of $P(x)$. Then, $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{h-1}}$ are also roots of $P(x)$.

Proof. Recall that $a^q = a$ for all $a \in \mathbb{F}$. Thus,
$0 = P(\alpha)^q = \left(\sum_{i=0}^{h} P_i \alpha^i\right)^q = \sum_{i=0}^{h} P_i^q \alpha^{iq} = \sum_{i=0}^{h} P_i \cdot (\alpha^q)^i = P(\alpha^q)$. $\square$

Roots of Polynomial

Proposition

Let $\mathbb{F} = \mathbb{F}_q$, let $P(x)$ be an irreducible polynomial of degree h over $\mathbb{F}$. Let α be a root of $P(x)$. Then, $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{h-1}}$ are also roots of $P(x)$.

- $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{h-1}}\}$ is the set of *all* roots of P; therefore, $P(x) = \prod_{i=0}^{h-1}(x - \alpha^{q^i})$.
- $\varphi : x \mapsto x^q$ is called a *Frobenius* mapping. $\{\varphi^i\}_{i=0}^{h-1}$ are *automorphisms* of $\mathbb{F}(\alpha)$ that fix $\mathbb{F}$. They form the *Galois group* of $[\mathbb{F}(\alpha) : \mathbb{F}]$.
- $\mathbb{F}(\alpha)$ is the *splitting field* of $P(x)$.
- $P(x)$ is the *minimal polynomial* of α.

Primitive Elements

Theorem

Let $\mathbb{F}$ be a finite field. Then, $\mathbb{F}^*$ is a cyclic group.

- Recall: $\mathbb{F}^*$ is a cyclic group if there is an element $\alpha \in \mathbb{F}^*$ such that

$$\mathbb{F}^* = \{\, \alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{|\mathbb{F}^*|-1} \,\}.$$

  - Such α is called a *generator* of the cyclic group. In our case, where $\mathbb{F}^*$ is the multiplicative group of the finite field $\mathbb{F}$, we call α a *primitive* element of $\mathbb{F}$.
  - The theorem says that *every finite field has a primitive element*.
  - Let $\mathcal{O}(\beta)$ denote the multiplicative *order* of $\beta \in \mathbb{F}^*$. If $|\mathbb{F}| = q$, then $\mathcal{O}(\beta) \,|\, (q-1)$, and, for a primitive element α, $\mathcal{O}(\alpha) = q-1$.
  - If $\beta = \alpha^k$ then $\mathcal{O}(\beta) = (q-1)/\gcd(q-1,k)$
    $\implies$ if $\gcd(q-1,k) = 1$, β is also primitive.
- Let $P(x)$ be an irreducible polynomial of degree h over $\mathbb{F}$, and α a root of $P(x)$. $P(x)$ is called a *primitive polynomial* if α is a primitive element of $\mathbb{F}(\alpha)$.
  - A primitive polynomial is irreducible.

Minimal polynomial

- Let $\mathbb{F}$ be a finite field, $|\mathbb{F}| = q$, and let $\mathbb{K}$ be an extension of finite degree h of $\mathbb{F}$, $|\mathbb{K}| = q^h$.
- Let $\beta \in \mathbb{K}$. The *minimal polynomial* of β with respect to $\mathbb{F}$ is the *monic* polynomial $M_\beta(x) \in \mathbb{F}[x]$ of *least degree* such that $M_\beta(\beta) = 0$.
  (*Monic* polynomial = polynomial with leading coefficient equal to 1.)
  - Why does such a polynomial exist? Recall that $x^{q^h} - x = \prod_{\gamma \in \mathbb{K}} (x - \gamma)$.
    In particular, β is a root of $x^{q^h} - x \implies \beta$ is a root of a monic polynomial of degree q^h in $\mathbb{F}[x] \implies$ there must be a monic polynomial of least degree in $\mathbb{F}[x]$ that β is a root of.
- $M_\beta(x)$ is *irreducible* in $\mathbb{F}[x]$.
- The degree of $M_\beta(x)$ is the least integer ℓ such that $\beta^{q^\ell} = \beta$.
  The integer ℓ satisfies $\ell | h$.
- $\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{\ell-1}}$ are *all the roots* of $M_\beta(x)$,

$$M_\beta(x) = \prod_{i=0}^{\ell-1} (x - \beta^{q^i}) \, .$$

Characterization of Finite Fields

Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$.

- $q = p^n$ for some prime p and integer $n \geq 1$.
  - p is the characteristic of F.
- Let $Q(x) = x^{q^h} - x$, $h \geq 1$. There is an extension Φ of $\mathbb{F}$ that contains all the roots of $Q(x)$ (its *splitting field*), and all the roots are distinct.
- The set of roots of $Q(x)$ in Φ forms an extension field $\mathbb{K}$ of $\mathbb{F}$, with $[\mathbb{K} : \mathbb{F}] = h$.
  (It will turn out that, in fact, Φ is unique, and $\Phi = \mathbb{K}$).

> *There is a finite field of size q for all q of the form $q = p^n$, p prime, $n \geq 1$. All finite fields of size q are isomorphic.*

The *unique* (up to isomorphism) field of size $q = p^n$ is denoted $\mathbb{F}_q$ or $\mathrm{GF}(q)$.

- There are irreducible polynomials and primitive polynomials of any degree ≥ 1 over $\mathbb{F}_q$.

Finite Fields: Summary

- There is a *unique* finite field $\mathbb{F}_q$, of size q, for each q of the form $q = p^m$, where p is prime and $m \geq 1$.
- When p is prime, $\mathbb{F}_p$ can be represented as the integers $\{0, 1, \ldots, p-1\}$ with arithmetic modulo p.
- When $q = p^m$, $m>1$, $\mathbb{F}_q$ can be represented as $\mathbb{F}_p[x]_m$ (polynomials of degree $<m$ in $\mathbb{F}_p[x]$) with arithmetic modulo an irreducible polynomial $P(x)$ of degree m over $\mathbb{F}_p$: $\mathbb{F}_q \sim \mathbb{F}_p[x]/\langle P(x) \rangle$
  - $\mathbb{F}_q$ is an *extension* of degree m of $\mathbb{F}_p$
  - here, p can be a prime or itself a power of a prime
  - $P(x)$ has a root α in $\mathbb{F}_q$, $\alpha \sim [x] \in \mathbb{F}_p[x]_m$
  - $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$ are *all* the roots of $P(x)$; all are in $\mathbb{F}_q$
  - $\alpha^0, \alpha^1, \ldots, \alpha^{m-1}$ is a *basis* of $\mathbb{F}_q$ over $\mathbb{F}_p$.
  - *All* irreducible polynomials of degree m over $\mathbb{F}_p$ have *all* their roots in $\mathbb{F}_q$
- Every finite field $\mathbb{F}_q$ has a *primitive* element α: $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$
  - the minimal polynomial $P(x)$ of a primitive element α is a *primitive polynomial*
  - every primitive polynomial is irreducible, but *not every irreducible is primitive*

Finite Field Example: GF(16)

α is a root of $P(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ (primitive). Rule: $\alpha^4 = \alpha + 1$.

i	α^i	*binary in base* $1,\alpha,\alpha^2,\alpha^3$	*minimal polynomial*
–	0	0 0 0 0	x
0	1	1 0 0 0	$x+1$
1	α	0 1 0 0	x^4+x+1
2	α^2	0 0 1 0	x^4+x+1
3	α^3	0 0 0 1	$x^4+x^3+x^2+x+1$
4	$\alpha+1$	1 1 0 0	x^4+x+1
5	$\alpha^2+\alpha$	0 1 1 0	x^2+x+1
6	$\alpha^3+\alpha^2$	0 0 1 1	$x^4+x^3+x^2+x+1$
7	$\alpha^3+\alpha+1$	1 1 0 1	x^4+x^3+1
8	α^2+1	1 0 1 0	x^4+x+1
9	$\alpha^3+\alpha$	0 1 0 1	$x^4+x^3+x^2+x+1$
10	$\alpha^2+\alpha+1$	1 1 1 0	x^2+x+1
11	$\alpha^3+\alpha^2+\alpha$	0 1 1 1	x^4+x^3+1
12	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1	$x^4+x^3+x^2+x+1$
13	$\alpha^3+\alpha^2+1$	1 0 1 1	x^4+x^3+1
14	α^3+1	1 0 0 1	x^4+x^3+1

If $\beta = \alpha^i$, $0 \le i \le (q-2)$, we say that i is the *discrete logarithm* of β to base α.

For $\mathrm{GF}(q)$, we operate on logarithms modulo $(q-1)$.

Examples:

- $(\alpha^2+\alpha)\cdot(\alpha^3+\alpha^2) = \alpha^5 \cdot \alpha^6 = \alpha^{11} = \alpha^3+\alpha^2+\alpha$
- $(\alpha^3+\alpha+1)^{-1} = \alpha^{-7} = \alpha^8 = \alpha^2+1$
- $\log_\alpha(\alpha^3+\alpha^2+1) = 13$

Finite Field Example: GF(16)

α is a root of $P(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ (primitive). Rule: $\alpha^4 = \alpha + 1$.

i	α^i	*binary in base* $1, \alpha, \alpha^2, \alpha^3$	*minimal polynomial*
–	0	0 0 0 0	x
0	1	1 0 0 0	$x+1$
1	α	0 1 0 0	x^4+x+1
2	α^2	0 0 1 0	x^4+x+1
3	α^3	0 0 0 1	$x^4+x^3+x^2+x+1$
4	$\alpha+1$	1 1 0 0	x^4+x+1
5	$\alpha^2+\alpha$	0 1 1 0	x^2+x+1
6	$\alpha^3+\alpha^2$	0 0 1 1	$x^4+x^3+x^2+x+1$
7	$\alpha^3+\alpha+1$	1 1 0 1	x^4+x^3+1
8	α^2+1	1 0 1 0	x^4+x+1
9	$\alpha^3+\alpha$	0 1 0 1	$x^4+x^3+x^2+x+1$
10	$\alpha^2+\alpha+1$	1 1 1 0	x^2+x+1
11	$\alpha^3+\alpha^2+\alpha$	0 1 1 1	x^4+x^3+1
12	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1	$x^4+x^3+x^2+x+1$
13	$\alpha^3+\alpha^2+1$	1 0 1 1	x^4+x^3+1
14	α^3+1	1 0 0 1	x^4+x^3+1

- Take $\beta = \alpha^5$.
  $\beta + \beta^2 = 0110 + 1110 = 1000 = 1$
  $\beta * \beta^2 = \alpha^{15} = 1$
- $\{0, 1, \beta, \beta^2\} = \mathbb{F}_2(\beta) \simeq \mathbb{F}_4$
- β is a root of $x^2 + x + 1$

Field inclusions

We saw

$$\begin{array}{c} \mathbb{F}_{2^4} \\ \bigcup \\ \mathbb{F}_{2^2} \\ \bigcup \\ \mathbb{F}_2 \end{array}$$

In general, for $k < n$,

$$\begin{array}{c} \mathbb{F}_{q^n} \\ \bigcup \\ \mathbb{F}_{q^k} \\ \bigcup \\ \mathbb{F}_q \end{array} \quad \Leftrightarrow \quad k|n$$

$n = rs$, $(r, s) = 1$,

$$\begin{array}{ccc} & \mathbb{F}_{q^{rs}} & \\ & \bigcup & \\ / & & \backslash \\ \mathbb{F}_{q^r} & & \mathbb{F}_{q^s} \\ \backslash & & / \\ & \bigcup & \\ & \mathbb{F}_q & \end{array}$$

Example

$$\begin{array}{ccc} & \mathbb{F}_{2^6} & \\ & \bigcup & \\ / & & \backslash \\ \mathbb{F}_{2^2} & & \mathbb{F}_{2^3} \\ \backslash & & / \\ & \bigcup & \\ & \mathbb{F}_2 & \end{array}$$

Application: Double-Error Correcting Codes

- The PCM of the $[2^m-1, 2^m-1-m, 3]$ binary Hamming code is $H_m = [\ \mathbf{h}_1\ \mathbf{h}_2\ \ldots\ \mathbf{h}_{2^m-1}\ ]$, where the $\mathbf{h}_i$ are all the nonzero m-tuples over $\mathbb{F}_2$. This can be reinterpreted as

$$H_m = (\ \alpha_1\ \alpha_2\ \ldots\ \alpha_{2^m-1}\ )\ ,$$

where α_j ranges over all the nonzero elements of $\mathbb{F}_{2^m}$.

- **Example:** $m{=}4$, α a root of $P(x){=}x^4+x+1$. Take $\alpha_j = \alpha^{j-1}$, and

$$H_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} .$$

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

- A vector $\mathbf{c} = (c_1\ c_2\ \ldots\ c_n)$ is a codeword of $\mathcal{H}_m$ iff

$$H_m\mathbf{c}^T = \sum_{j=1}^{n} c_j\alpha_j = 0.$$

- If there is exactly one error, we receive $\mathbf{y} = \mathbf{c} + \mathbf{e}_i$ where $\mathbf{e}_i = [0^{i-1}\,1\,0^{n-i}]$. The syndrome is

$$s = H_m\mathbf{y}^T = \underbrace{H_m\mathbf{c}^T}_{0} + H_m\mathbf{e}_i^T = \alpha_i.$$

The syndrome gives us the error location directly (i such that $s = \alpha_i$).

Application: Double-Error Correcting Codes

What if there are two errors? Then, we get $\mathbf{e} = \mathbf{e}_i + \mathbf{e}_j$, and

$$s = \alpha_i + \alpha_j, \text{ for some } i, j, \quad 1 \le i < j \le n,$$

which is insufficient to solve for α_i, α_j. *We need more equations ...*

Consider the PCM

$$\hat{H}_m = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{2^m-1} \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_{2^m-1}^3 \end{pmatrix} .$$

Syndromes are of the form

$$\mathbf{s} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \hat{H}_m \mathbf{y}^T = \hat{H}_m \mathbf{e}^T .$$

Assume that the number of errors is at most 2.

- Case 1: $\mathbf{e} = 0$ (no errors). Then, $s_1 = s_3 = 0$.
- Case 2: $\mathbf{e} = \mathbf{e}_i$ for some i, $1 \le i \le n$ (one error). Then,

$$\begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \hat{H}_m \mathbf{e}^T = \begin{pmatrix} \alpha_i \\ \alpha_i^3 \end{pmatrix} ;$$

  namely, $s_3 = s_1^3 \ne 0$, and the error location is the index i such that $s_1 = \alpha_i$.

Application: Double-Error Correcting Codes

- Case 3: $\mathbf{e} = \mathbf{e}_i + \mathbf{e}_j$ for some $i, j,\ \ 1 \leq i < j \leq n$ (two errors).

$$\begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \hat{H}_m \mathbf{e}^T = \begin{pmatrix} \alpha_i + \alpha_j \\ \alpha_i^3 + \alpha_j^3 \end{pmatrix} .$$

Since $s_1 = \alpha_i + \alpha_j \neq 0$, we can write

$$\frac{s_3}{s_1} = \frac{\alpha_i^3 + \alpha_j^3}{\alpha_i + \alpha_j} = \alpha_i^2 + \alpha_i\alpha_j + \alpha_j^2 .$$

Also,

$$s_1^2 = (\alpha_i + \alpha_j)^2 = \alpha_i^2 + \alpha_j^2 .$$

We add the two equations, and recall the definition of s_1 to obtain

$$\frac{s_3}{s_1} + s_1^2 = \alpha_i\alpha_j \qquad (\star)$$

$$s_1 = \alpha_i + \alpha_j \qquad (\star\star)$$

Notice that $(\star)$ and $\alpha_i\alpha_j \neq 0 \implies s_3 \neq s_1^3$, separating Case 3 from Cases 1–2.

Application: Double-Error Correcting Codes

- Case 3 (cont.):

$$\frac{s_3}{s_1} + s_1^2 = \alpha_i \alpha_j \qquad (\star)$$

$$s_1 = \alpha_i + \alpha_j \qquad (\star\star)$$

It follows from $(\star)$ and $(\star\star)$ that α_i and α_j are the roots of the following quadratic equation in x over $\mathbb{F}_{2^m}$:

$$x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2 \right) = 0 \; .$$

s_1 and s_3 are fully known to the decoder (computed from the received word $\mathbf{y}$), and therefore so are the coefficients of the quadratic equation.

Assuming we know how to solve a quadratic equation, we have a decoding algorithm for up to two errors.

Two-error correcting BCH code.

Solving a quadratic equation

We want to find the two roots of the quadratic equation

$$\Lambda(x) \triangleq x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2\right) = 0$$

over $\mathbb{F}_{2^m}$.

- What *doesn't* work: $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (in characteristic 2).
- Exhaustive search:

  for ℓ in $[1, 2, \ldots, n]$:
      evaluate $\lambda = \Lambda(\alpha_\ell)$
      if $\lambda == 0$:
          flip bit ℓ

  - Requires n evaluations of a quadratic function, time complexity is *linear in* n.
  - Works also in te case of one error!
- There are ways to solve the equation explicitly, without search. However, search is good enough for us here!

Example: Double-Error Correcting Code

- As before, $\mathbb{F} = \mathbb{F}_{16}$, and α is a root of $P(x) = x^4 + x + 1$.

$$\hat{H}_4 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

and, in binary form,

$$\hat{H}_4 = \left(\begin{array}{ccccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

For this code, we know

- $k \geq 15 - 8 = 7$ (in fact, the dimension is exactly 7)
- $d \geq 5$ (in fact, $d = 5$)
- $[n, k, d] = [15, 7, 5]$

Variations on the Double-error Correcting Code

- Add an overall parity bit

$$\hat{H}_4 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & 0 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

  For this code, we know

  - $n = 16$
  - $k = 7$ (same number of words)
  - $d = 6$
  - corrects 2 errors, detects 3

- Expurgate words of odd weight

$$\bar{H}_4 = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

  - $n = 15,\ k = 6,\ d = 6$: corrects 2 errors, detects 3