Information Theory

Lecture 7

- Finite fields continued: MWS4.1–MWS4.5 (MWS4.6–8)
  - the field GF(p^m),. . .
- **Cyclic Codes**
  - Intro. to cyclic codes: MWS7 (not MWS7.7)

The Field GF(p^m)

- $\pi(x)$ irreducible degree-m over $\mathrm{GF}(p)$, p a prime,

  $\mathrm{GF}(p^m) =$ all polynomials over $\mathrm{GF}(p)$ of degree $\leq m - 1$, with calculations modulo p and $\pi(x)$

  - modulo $\pi(x) \leftrightarrow$ use $\pi(x) = 0$ to reduce x^m to degree $< m$
  - without loss of generality, $\pi(x)$ can be assumed *monic*
- The prime number p is called the *characteristic* of $\mathrm{GF}(p^m)$; smallest p such that $\sum_{i=1}^{p} 1 = 0$
- $\mathrm{GF}(p^m)$ is a linear vector space of dimension m over $\mathrm{GF}(p)$
- For $s < r$, $\mathrm{GF}(p^s) \subset \mathrm{GF}(p^r) \iff s|r$
- For $\beta \in \mathrm{GF}(p^r)$, $\beta \in \mathrm{GF}(p^s) \iff \beta^{p^s} = \beta$

The Cyclic Group $G = \mathrm{GF}(p^m) \setminus \{0\}$

- For any $\beta \in \mathrm{GF}(p^m)$, the smallest $r > 0$ such that $\beta^r = 1$ is called the *order* of β.
- The elements in $G = \mathrm{GF}(p^m) \setminus \{0\}$ form a *cyclic group*;
  - There exists an element $\alpha \in \mathrm{GF}(p^m)$ of order $r = p^m - 1$ that generates all the non-zero elements of $\mathrm{GF}(p^m)$, that is

$$G = \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$$

- Any such α is called a *primitive element*

$\Longrightarrow$ *Fermat's theorem*: Any $\beta \in \mathrm{GF}(q)$ satisfies $\beta^q = \beta$, that is

$$x^q - x = \prod_{\beta \in \mathrm{GF}(q)} (x - \beta) = x \prod_{i=1}^{r-1} (x - \alpha^i)$$

Polynomial Factorizations

- For $\beta \in \mathrm{GF}(p^m)$ the *minimal polynomial* of β is the lowest degree monic polynomial $m(x)$ over $\mathrm{GF}(p)$ with β as a root
- $m(x)$ is irreducible, has degree $s \leq m$ such that $s|m$, and roots

$$\beta, \beta^p, \beta^{2p}, \ldots, \beta^{(s-1)p}$$

  called *conjugates*
- If $f(\beta) = 0$ for $f(x) \neq m(x)$ over $\mathrm{GF}(p)$, then $m(x)|f(x)$;

$$f(\beta) = 0 \implies f(\beta^p) = 0$$

- The minimal polynomial of a primitive element in $\mathrm{GF}(p^m)$ has degree m, and is called a *primitive polynomial*

- A field has at least one primitive element.
  - When generating $\mathrm{GF}(p^m)$ using $\pi(x)$ with roots $\alpha, \alpha^p, \ldots, \alpha^{(m-1)p}$, the element α is primitive in $\mathrm{GF}(p^m)$; this is our "standard" primitive element, henceforth denoted α
- Let $m^{(i)}(x)$ be the minimal polynomial of $\alpha^i \in \mathrm{GF}(q)$, then

$$x^{q-1} - 1 = \prod_t m^{(t)}(x)$$

  over all $t \in \{1, 2, \ldots, q-1\}$ that give different $m^{(t)}(x)$'s
- An independent statement is: *$x^{p^m} - x =$ product of all monic irreducible polynomials over GF(p) with degrees that divide m* $\implies$ help to identify the $m^{(i)}(x)$'s
- $m^{(i)}(x)$ of degree $s \implies m^{(-i)}(x) = x^s \, m^{(i)}(x^{-1})$

Cyclic Codes

- $\mathcal{C}$ over $\mathrm{GF}(q)$ is *cyclic* $\iff$ $\mathcal{C}$ is linear and

$$(c_0, \ldots, c_{n-1}) \in \mathcal{C} \implies (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$$

- For a cyclic code $\mathcal{C}$, let $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ correspond to a *codeword polynomial* $c(x)$ over $\mathrm{GF}(q)$, such that

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$$

- A *cyclic shift* $\leftrightarrow$ multiplication with x modulo $x^n - 1$

- Let $\mathcal{R}_n =$ "the set of all polynomials over GF(q) that are equal modulo $x^n - 1$" (a *ring* of dimension n)
- Given $g(x) \in \mathcal{R}_n$, let

$$\langle g(x) \rangle = \{c(x) : c(x) = u(x)g(x), \text{ over all } u(x) \in \mathcal{R}_n\}$$

- A *cyclic code* of length n with *generator polynomial* $g(x) \in \mathcal{R}_n$ is then formally defined as

$$\mathcal{C} = \langle g(x) \rangle$$

The Generator Polynomial $g(x)$

- For $\mathcal{C} = \langle g(x) \rangle$,
  - $g(x)$ is the unique monic polynomial in $\mathcal{C}$ of minimal degree r
  - the dimension of $\mathcal{C}$ is $k = n - r$
  - $g(x) | x^n - 1$
  - any $u(x)$ over $\mathrm{GF}(q)$ of degree $< n - r$ corresponds uniquely to a $c(x) \in \mathcal{C}$ via $c(x) = u(x)g(x)$ over $\mathrm{GF}(q)$
- k *message symbols* $(u_0, \dots, u_{k-1})$, $u_l \in \mathrm{GF}(q)$, give a codeword $c(x)$ as

$$c(x) = u(x)g(x), \; u(x) = u_0 + u_1 x + \dots + u_{k-1} x^{k-1}$$

  - C.f., $\mathbf{c} \in \mathbf{C} \iff \mathbf{c} = \mathbf{u}\mathbf{G}$

The Parity Check Polynomial $h(x)$

- The polynomial
$$h(x) = \frac{x^n - 1}{g(x)}$$
is the *parity check polynomial* of the cyclic code $\langle g(x) \rangle$ of length n
  - $g(x)h(x) = 0$, and $c(x) \in \langle g(x) \rangle \iff c(x)h(x) = 0$ in $\mathcal{R}_n$; c.f.,
$$\mathbf{G}\mathbf{H}^T = \mathbf{0} \text{ and, } \mathbf{c} \in \mathcal{C} \iff \mathbf{c}\mathbf{H}^T = \mathbf{0}$$
  - $h(x)$ has degree $k =$ dimension of $\langle g(x) \rangle$

$\mathbf{G}$ and $\mathbf{H}$ matrices

- For a cyclic code with
$$g(x) = g_r x^r + g_{r-1} x^{r-1} + \cdots + g_0$$
$$h(x) = h_k x^k + h_{k-1} x^{k-1} + \cdots + h_0$$
we get $\mathbf{G}$ and $\mathbf{H}$ in *cyclic form* as
$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ & & & & \cdots & & & \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$
$$\mathbf{H} = \begin{bmatrix} 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 & 0 \\ & & & & \cdots & & & \\ h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Why Polynomials?

- Encoding and decoding circuitry based on simple logical operations straightforward to derive...
- Construct and analyze (cyclic) codes based on finite field theory and polynomial factorizations

Factors of $x^n - 1$

- Cyclic code over $\mathrm{GF}(q)$: $g(x)h(x) = x^n - 1 = \prod\{$ irreducible factors $\}$ $\Longrightarrow$ code can be constructed based on the factors
- Assume (always) n and q relatively prime (no common factors) $\Longrightarrow$ exists a smallest m such that $n | q^m - 1$
- The n zeros of $x^n - 1 \in \mathrm{GF}(q^m)$ and no smaller field,

$$x^n - 1 = \prod_{i=1}^{n} (x - \alpha_i)$$

  for some $\{\alpha_1, \ldots, \alpha_n\} \subset \mathrm{GF}(q^m)$ with the α_i's distinct
  - The nth *roots of unity*; $\mathrm{GF}(q^m)$ is the *splitting field* of $x^n - 1$

- The roots $\{\alpha_1, \ldots, \alpha_n\}$ form a cyclic group $\subset \mathrm{GF}(q^m)$, that is, there is an $\alpha \in \mathrm{GF}(q^m)$, the *primitive* nth root of unity, such that

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$$

  - $n = q^m - 1 \iff \alpha$ is a primitive element in $\mathrm{GF}(q^m)$
- Assume α a primitive nth root of unity $\in \mathrm{GF}(q^m)$ where m is the smallest integer such that $n | q^m - 1$,
  $p^{(i)}(x) =$ minimal polynomial of $\alpha^i \in \mathrm{GF}(q^m) \implies$

$$x^n - 1 = \prod_j p^{(j)}(x)$$

  over all $j \in \{0, \ldots, n-1\}$ that give different $p^{(j)}(x)$'s

- Given a factorization

$$x^n - 1 = \prod_j p^{(j)}(x)$$

  some of the $p^{(j)}(x)$'s can form $g(x)$ and the others $h(x)$;
- The zeros of a code,
  - let $\mathcal{C} = \langle g(x) \rangle$ of length n, and let $K = \{k : p^{(k)}(x) | g(x)\}$, then $\{\alpha^k : k \in K\}$ are called the *zeros of the code*;
    - i.e., all roots of $g(x)$
  - α^i for $i \notin K$ $(i \leq n-1)$ are the *nonzeros* (all roots of $h(x)$)
    - the nonzeros of $\mathcal{C}$ are the zeros of $\mathcal{C}^\perp$ and vice versa