Information Theory

Lecture 6

- **Block Codes and Finite Fields**
  - Codes: MWS1.1–MWS2.2, MWS5.1–2
    - codes, minimum distance, linear codes, G and H matrices, decoding, bounds,. . .
  - Finite fields: MWS3
    - groups, fields, the Galois field, polynomials,. . .

Block Channel Codes

- An (n, M) *block (channel) code* over a field $\mathrm{GF}(q)$ is a set

$$\mathcal{C} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M\}$$

  of *codewords*, with $\mathbf{x}_m \in \mathrm{GF}^n(q)$.
- $\mathrm{GF}(q) =$ "set of $q < \infty$ objects that can be added, subtracted, divided and multiplied to stay inside the set"
  - $\mathrm{GF}(2) = \{0, 1\}$ modulo 2
  - $\mathrm{GF}(p) = \{0, 1, \ldots, p-1\}$ modulo p, for a prime number p
  - $\mathrm{GF}(q)$ for a non-prime q; later. . .
- The *code* is now what we previously called the *codebook*; encoder α and decoder β not included in definition. . .

Some Fundamental Definitions

- *Hamming distance*: For $\mathbf{x}, \mathbf{y} \in \mathrm{GF}^n(q)$,

$$d(\mathbf{x}, \mathbf{y}) = \text{number of components where } \mathbf{x} \text{ and } \mathbf{y} \text{ differ}$$

- *Hamming weight*: For $\mathbf{x} \in \mathrm{GF}^n(q)$,

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$$

  where $\mathbf{0} = (0, 0, \dots, 0)$
- *Minimum distance* of a code $\mathcal{C}$:

$$d_{\text{min}} = d = \min \{ d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y};\ \mathbf{x}, \mathbf{y} \in \mathcal{C} \}$$

- A code $\mathcal{C}$ is *linear* if

  $\mathbf{x}, \mathbf{y} \in \mathcal{C} \implies \mathbf{x} + \mathbf{y} \in \mathcal{C}, \quad \mathbf{x} \in \mathcal{C}, \alpha \in \mathrm{GF}(q) \implies \alpha \cdot \mathbf{x} \in \mathcal{C}$

  where $+$ and $\cdot$ are addition and multiplication in GF(q)
- A linear code $\mathcal{C}$ forms a *linear vector space* $\subset \mathrm{GF}^n(q)$ of dimension $k < n$
- $\mathcal{C}$ linear $\implies$ exists a *basis* $\{\mathbf{g}_m\}_{m=1}^k$, $\mathbf{g}_m \in \mathcal{C}$, that spans $\mathcal{C}$, i.e.,

$$\mathbf{x} \in \mathcal{C} \iff \mathbf{x} = \sum_{m=1}^{k} u_m \mathbf{g}_m$$

  for some $\mathbf{u} = (u_1, \dots, u_k) \in \mathrm{GF}^k(q)$, and hence $M = |\mathcal{C}| = q^k$

- Let $\{\mathbf{g}_m\}_{m=1}^{k}$ define the rows of a $k \times n$ matrix $\mathbf{G}$ $\implies$

$$\mathbf{x} \in \mathcal{C} \iff \mathbf{x} = \mathbf{u}\mathbf{G}$$

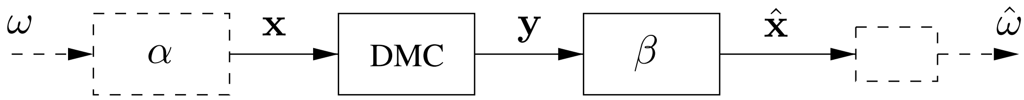
  for some $\mathbf{u} \in \mathrm{GF}^k(q)$.
- $\mathbf{G}$ is called a *generator matrix* for the code
- Any $\mathbf{G}$ with rows that form a *maximal set of linearly independent codewords* is a valid generator matrix $\implies$ a code $\mathcal{C}$ can have different $\mathbf{G}$'s
- An (n, M) linear code of dimension $k = \log_q M$ and with minimum distance d is called an $[n, k, d]$ code

- Let $r = n - k$ and let the rows of the $r \times n$ matrix $\mathbf{H}$ span

$$\mathcal{C}^{\perp} = \{\mathbf{v} : \mathbf{v} \cdot \mathbf{x} = 0, \ \ \forall \mathbf{x} \in \mathcal{C}\}, \quad \mathbf{v} \cdot \mathbf{x} = \sum_{m=1}^{n} v_m x_m \ \text{ in } \mathrm{GF}(q),$$

  that is, the *orthogonal complement* of $\mathcal{C}$ = *kernel* of $\mathbf{G}$. Any such $\mathbf{H}$ is called a *parity check* matrix for $\mathcal{C}$.
  - $\mathbf{G}\mathbf{H}^T = \mathbf{0} \quad (= \{0\}^{k \times r})$; $\quad \mathbf{x} \in \mathcal{C} \iff \mathbf{H}\mathbf{x}^T = \mathbf{0}^T$
  - $\mathbf{H}$ is a generator for the *dual code* $\mathcal{C}^{\perp}$
- $\mathcal{C}$ linear $\implies$ $d_{\text{min}} = \min_{\mathbf{x} \in \mathcal{C}} w(\mathbf{x})$ = minimal number of linearly dependent columns of $\mathbf{H}$

Coding over a DMC



- Information variable: $\omega \in \{1, \dots, M\}$ $(p(\omega) = 1/M)$
- Encoding: $\omega \to \mathbf{x}_\omega = \alpha(\omega) \in \mathcal{C}$
  - $\mathcal{C}$ linear with $M = q^k \implies$ any ω corresponds to some $\mathbf{u}_\omega \in \mathrm{GF}^k(q)$ and $\mathbf{x}_\omega = \mathbf{u}_\omega \mathbf{G}$
- A DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with $\mathcal{X} = \mathrm{GF}(q)$, used n times $\to \mathbf{y} \in \mathcal{Y}^n$
  - potentially $\mathcal{Y} \neq \mathcal{X}$, but we will assume $\mathcal{Y} = \mathcal{X} = \mathrm{GF}(q)$
- Decoding: $\hat{\mathbf{x}} = \beta(\mathbf{y}) \in \mathcal{C}$ $(\to \hat{\omega})$
- Probability of error: $P_e = \Pr(\hat{\mathbf{x}} \neq \mathbf{x})$

More about decoding

- $\mathbf{x}$ transmitted $\implies$ $\mathbf{y} = \mathbf{x} + \mathbf{e}$ where $\mathbf{e} = (e_1, \dots, e_n)$ is the *error vector* corresponding to $\mathbf{y}$
- The *nearest neighbor* (NN) decoder

$$\hat{\mathbf{x}} = \mathbf{x}' \quad \text{if} \quad \mathbf{x}' = \arg\min_{\mathbf{x} \in \mathcal{C}} d(\mathbf{y}, \mathbf{x})$$

  - Equiprobable ω and a symmetric DMC such that $\Pr(e_m = 0) = 1 - p > 1/2$ and $\Pr(e_m \neq 0) = p/(q-1)$,

    NN $\iff$ *maximum likelihood* $\iff$ minimum P_e
- With NN decoding, a code with $d_{\text{min}} = d$ can correct

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

errors; as long as $w(\mathbf{e}) \leq t$ the codeword $\mathbf{x}$ will *always* be recovered correctly from $\mathbf{y}$

- **Decoding of linear codes**
  - The *syndrome* $\mathbf{s}$ of an error vector $\mathbf{e}$,

$$\mathbf{s} = \mathbf{H}\mathbf{y}^T = \mathbf{H}\mathbf{e}^T$$

  - NN decoding for linear codes can be implemented using syndromes and the *standard array*. . .

Bounds

- *Hamming* (or sphere-packing): For a code with $t = \lfloor (d_{\text{min}} - 1)/2 \rfloor$,

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq M^{-1} q^n$$

  - equality $\Longrightarrow$ *perfect* code $\Longrightarrow$ can correct all $\mathbf{e}$ of weight $\leq t$ and no others
  - *Hamming codes* are perfect linear binary codes with $t = 1$
- *Gilbert–Varshamov*: There exists an $[n, k, d]$ code over $\mathrm{GF}(q)$ with $r = n - k \leq \rho$ and $d \geq \delta$ provided that

$$\sum_{i=0}^{\delta-2} \binom{n-1}{i} (q-1)^i < q^\rho$$

- *Singleton*: For any $[n, k, d]$ code,

$$r = n - k \geq d - 1$$

- $r = d - 1 \implies$ *maximum distance separable* (MDS)
- For MDS codes:
  - Any r columns in $\mathbf{H}$ are linearly independent
  - Any k columns in $\mathbf{G}$ are linearly independent

Some Additional Definitions

- Two codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathrm{GF}(q)$ are *equivalent* if there exist n permutations $\pi_1, \ldots, \pi_n$ of field elements and a permutation σ of coordinate positions such that

$$(x_1, \ldots, x_n) \in \mathcal{C} \implies \sigma\big\{(\pi_1(x_1), \ldots, \pi_n(x_n))\big\} \in \mathcal{D}$$

- In particular, swapping the same two coordinates in all codewords gives an equivalent code
- For a linear code, $(\mathbf{G}, \mathbf{H})$ can be manipulated (add, subtract, swap rows, swap columns) into an equivalent linear code in *systematic* or *standard form*

$$\mathbf{G}_{\text{sys}} = \big[\mathbf{I}_k \big| \mathbf{A}\big] \qquad \mathbf{H}_{\text{sys}} = \big[-\mathbf{A}^T \big| \mathbf{I}_r\big]$$

- For MDS codes: no swapping of columns needed

Groups

- A *group* is a set G with an associated operation $\cdot$ (often thought of as multiplication), subject to:
  - $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, x \in G$
  - There exists an element $1 \in G$ (the neutral or unity), such that $1 \cdot x = x \cdot 1 = x$ for all $x \in G$
  - For any $x \in G$ there exists an element $x^{-1} \in G$ (inverse), such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$
- If, in addition, it holds that $x \cdot y = y \cdot x$ for any $x, y \in G$ the group is called *commutative* or *Abelian*
- A finite group G is *cyclic of order r* if $G = \{1, x, x^2, \ldots, x^{r-1}\}$ ($x^2 = x \cdot x$ and so on). The element x is the *generator* of G.

Finite Fields

- The *Galois field* $\mathrm{GF}(q)$ of order q is a (the) set of $q < \infty$ objects for which the operations $+$ (addition) and $\cdot$ (multiplication) exist, such that for any $\alpha, \beta, \gamma \in \mathrm{GF}(q)$

$$\alpha + \beta = \beta + \alpha, \quad \alpha \cdot \beta = \beta \cdot \alpha$$
$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma, \quad \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$
$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

Furthermore, for any $\alpha \in \mathrm{GF}(q)$ the elements 0 (additive neutral), 1 (multiplicative neutral), $-\alpha$ (additive inverse) and α^{-1} (multiplicative inverse, for $\alpha \neq 0$) must exist, such that

$$0 + \alpha = \alpha, \quad (-\alpha) + \alpha = 0, \quad 0 \cdot \alpha = 0$$
$$1 \cdot \alpha = \alpha, \quad (\alpha^{-1}) \cdot \alpha = 1$$

- There is *only one* $\mathrm{GF}(q)$ in the sense that all finite fields of order q are *isomorphic*;
  - any two fields F and G of order q are essentially the same field, they differ only in the way elements are named
- As mentioned, for p a prime number
  - $\mathrm{GF}(p) =$ the integers $\{0, \dots, p-1\}$ modulo p

  for any non-prime integer q,
  - $\mathrm{GF}(q)$ is a finite field $\iff$ $q = p^m$ for some prime p and integer $m \geq 1$
  - $\mathrm{GF}(p^m)$, $m > 1$, can be constructed using an *irreducible polynomial* $\pi(x)$ of degree m over $\mathrm{GF}(p)$...

Polynomials

- A polynomial $g(x)$ of degree m over a finite field $\mathrm{GF}(q)$ has the form

$$g(x) = \alpha_m x^m + \alpha_{m-1} x^{m-1} + \cdots + \alpha_1 x + \alpha_0$$

  where $\alpha_l \in \mathrm{GF}(q),\ l = 0, \dots, m.$
  - When $q = p =$ *a prime* $\Rightarrow$ integer coefficients and operations coefficient-wise modulo p
  - $g(x)$ is *monic* if $\alpha_m = 1$
- A polynomial $\pi(x)$ over $\mathrm{GF}(p)$ is *irreducible* over $\mathrm{GF}(p)$ if $\pi(x)$ cannot be written as the product of two other polynomials over $\mathrm{GF}(p)$ (with degrees ≥ 1)

The Field GF(p^m)

- Let $\pi(x)$ be an irreducible degree-m polynomial over $\mathrm{GF}(p)$, with p a prime, then

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

"use the equation $\pi(x) = 0$ to reduce x^m to degree $< m$"

- *Modulo a polynomial*: Two polynomials $a(x)$ and $b(x)$ over $\mathrm{GF}(q)$ are equal modulo a polynomial $p(x)$ if

$$a(x) = q_1(x)p(x) + r(x), \quad b(x) = q_2(x)p(x) + r(x)$$