February 12, 2019

Reminders:

(◦) Register on piazza
(◦) Log on to Autolab
(◦) HW 0 out this Th (HW 0 is <u>optional</u> and will <u>not</u> be graded)

all HW 1-3 out in subsequent weeks.

RECAP: $(n, k, d)_q$ code

block length, dimension, distance, alphabet size

Big Q: Given a distance d, what is the largest rate for a code with distance d?

→ Hamming code: $C_H: (x_1\ x_2\ x_3\ x_4) \cdot \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}$ $(7,4,3)_2$-code

→ $d(C_H) = \min\limits_{\bar{c} \neq 0 \in C_H} wt(c)$ Hamming wt $= |\{i \mid c_i \neq 0\}|$

→ Hamming bound: For any $(n,k,3)_2$ code, $k \le n - \log_2(n+1)$

Volunteer for proof reading?

Linear codes

Q: How much space do we need to represent an $(n,k,d)_q$ code?

A: In general nothing better an nq^k symbols. ~~for~~ k.

TODAY: A general class of codes that needs $O(n^2)$ symbols.

Def (Linear codes) Let q be a prime power ($q = p^s$: p is prime, $s \ge 1$ is an int) $C \subseteq \{0, 1, \dots, q-1\}^n$ is a linear code if it is a linear subspace. A linear $(n,k,d)_q$ code is ALWAYS referred to as $[n,k,d]_q$ code.

First: What set of "numbers"? What arithmetic operations?

Fields: $\mathbb{F} = (S, +, \cdot) \rightarrow$ can add, subtract, multiply, divide 2 elements from S & stay in S.

→ Closure of $+, \cdot$
→ Associativity of $+, \cdot$
→ Commutativity of $+, \cdot$

→ Distributivity : $a \cdot (b+c) = a \cdot b + b \cdot c$
→ Identities : 0 for +, 1 for $\cdot$ $[0, 1 \in S]$
→ Inverses : $\forall a \in S, \exists -a \in S$ s.t $a + (-a) = 0$
$\forall a \in S \setminus \{0\}, \exists a^{-1} \in S$ s.t $a \cdot (a^{-1}) = 1$

Ex: $\mathbb{R}$ is a field, $\mathbb{Z}$ is not
$\mathbb{Q}$ ———

Finite fields $|S|$: finite

THM 1: Any finite field $\mathbb{F}$ has size $|\mathbb{F}| = p^s$ (p → prime, s int ≥ 1)

Ex: $(\{0,1\}, \oplus, \wedge)$ ← finite field of size 2
$(\{0, .., p-1\}, +_{\text{mod } p}, \cdot_{\text{mod } p})$ ← finite field of size p.
(p → prime)

THM 2: There is a unique finite field for each prime power (up to isomorphism)
$\Longrightarrow$ $\mathbb{F}_q$ for prime power q

Linear subspaces $S \subseteq \mathbb{F}_q^n$ is a linear subspace if
(1) $\forall \bar{x}, \bar{y} \in S$, $\bar{x} + \bar{y} \in S$
(2) $\forall a \in \mathbb{F}_q, \bar{x} \in S$; $a \cdot \bar{x} \in S$ $\Rightarrow$ $\bar{0} \in S$

Ex 1: Subspace of $\mathbb{F}_5^3$:
$S_1 = \{(0,0,0), (1,1,1), (2,2,2), (3,3,3), (4,4,4)\}$ (1,1,2)
→ (1) $(1,1,1) + (2,2,2) = (3,3,3) \in S_1$
(2) $2 \cdot (4,4,4) = (8,8,8) \bmod 5 = (3,3,3) \in S_1$

Ex 2: subspace of $\mathbb{F}_3^3$:
$S_2 = \{(0,0,0), \cancel{(1,1,1)}, \cancel{(2,2,2)}$ $(1,0,1), (2,0,2),$
$(0,1,1), (0,2,2), (1,1,2), (2,2,1), (1,2,0), (2,1,0)\}$

Def (span) $B = \{ \bar{u}_1, \dots, u_\ell \}$, its span

$$\mathrm{span}(B) = \{ \sum_{i=1}^{\ell} a_i u_\ell \mid a_i \in \mathbb{F}_q \} \subseteq \mathbb{F}_q^n$$

Ex: Over $\mathbb{F}_5$: $S_1 = \mathrm{span}\{(1,1,1)\}$

Def (linear independence) $\{\bar{u}_1, \dots, u_k\} \subseteq \mathbb{F}_q^n$ are linearly independent if $\forall\ i \in [k]$

$$\bar{u}_i \notin \mathrm{span}(\{\bar{u}_1, \dots, \bar{u}_{i-1}, \bar{u}_{i+1}, \dots, \bar{u}_k\})$$

Ex: Over $\mathbb{F}_3$ $(1,0,1)$ & $(0,1,1)$ are lin indep.

Def (rank): Rank of a matrix $M \in \mathbb{F}^{k \times k}$ is the largest # of linearly independent rows (or columns)

$M \in \mathbb{F}_q^{k \times n}$ is full rank if it has rank $\min(k,n)$

E.g: $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ is full rank over $\mathbb{F}_3$

THM: $S \subseteq \mathbb{F}_q^n$ be a linear subspace $\Rightarrow$

(i) $|S| = q^k$ $0 \le k \le n$ integer (k: dimension of S)

(ii) $\exists\ \bar{u}_1, \dots, \bar{u}_k$ lin. independent (basis of S) s.t $\forall\ \bar{x} \in S$,

$$\bar{x} = a_1\bar{u}_1 + a_2\bar{u}_2 + \dots + a_k\bar{u}_k \ ;\ a_i \in \mathbb{F}_q$$

$$= \bar{x} = (a_1\ a_2\ \dots\ a_k) \underbrace{\begin{pmatrix} \leftarrow \bar{u}_1 \rightarrow \\ \leftarrow \bar{u}_2 \rightarrow \\ \vdots \\ \leftarrow u_k \rightarrow \end{pmatrix}}_{\text{full rank } (k \le n)}$$

$\mathbb{F}_q^{k \times n} \ni G$ a generator matrix.

(iii) $\exists$ a full rank $(n-k) \times n$ matrix H s.t $\forall\ \bar{x} \in S$

$$H x^T = \bar{0} \in \mathbb{F}_q^{n-k}$$

(iv) G & H are orthogonal: $G \cdot H^T = 0$

S_1 : $G_1 = (1\ 1\ 1)$ $\quad H_1 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 2 & 1 \end{pmatrix}$ over $\mathbb{F}_5$

S_2 : $G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ $\quad H_2 = (1\ 1\ 2)$ over $\mathbb{F}_3$

Lemma: G is gen matrix for $S_1 \subseteq \mathbb{F}_q^n$, H is parity check matrix for $S_2 \subseteq \mathbb{F}_q^n$ s.t $GH^T = 0 \Rightarrow S_1 = S_2$

Properties of linear codes:

$[7,4,3]_2$ Hamming code over $\mathbb{F}_2$

$$G_{Ham} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H_{Ham} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Prop 1: Any $[n,k]_q$ code can be represented with $\min(kn, (n-k)n)$ symbols from $\mathbb{F}_q$

Prop 2: Any $[n,k]_q$ code has $O(kn)$ operations over $\mathbb{F}_q$ encoding

Prop 3: ———— $O((n-k)n)$ ———— error detection.

Lemma: For any $[n,k,d]_q$ code $\mathcal{C}$

$$d = \min_{\substack{\bar{c} \neq 0 \\ \in \mathcal{C}}} wt(\bar{c})$$

Pf: $\leq$: Let $\bar{c}' = \arg\min_{\substack{\bar{c} \neq 0 \\ \bar{c} \in \mathcal{C}}} wt(c)$

$$\Rightarrow d \leq \Delta(\bar{0}, \bar{c}') =$$

$\geq$: Let $\bar{c}_1 \neq \bar{c}_2 \in \mathcal{C}$ s.t $\Delta(\bar{c}_1, \bar{c}_2) = d$

$$\Rightarrow d = \Delta(\bar{c}_1, \bar{c}_2) = wt(\bar{c}_1 - \bar{c}_2) \geq$$

Claim: $\bar{c}_1 - \bar{c}_2 \in \mathcal{C}$

Pf: By scalar mult prop of linear subspace $-\bar{c}_2 = (-1)\cdot\bar{c}_2 \in \mathcal{C}$

— additive ⟵ $\bar{c}_1 + (-\bar{c}_2) \in \mathcal{C}$

$= \bar{c}_1 - \bar{c}_2$