Feb 11

Reminders

- Log on to Autolab
- Email me if you want to sign up for proof reading of future lectures
- HW0 is out. Due 11.59pm ~~Wed~~ next week.
  - → ONLY submit Q1
  - → OPTIONAL
- General comment: Any proof technique is fine (as long as proof is correct of course!)
- Group composition due next Wed Feb 16

RECAP: 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) $\begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}$

$n=7$, $k=4$, $d=3$

→ Hamming bound: For any code with block length n, $q=2$, dim k & distance $=3$, $k \le n - \log_2(n+1)$

⇒ C_H is best for $n=7, d=3$.

Proof readers for today: Jonathan, Chitra Vardhini

Def Code of block length n, dimension k, distance d over alphabet Σ / alphabet size q will be denoted as an $(n,k,d)_\Sigma$ / $(n,k,d)_q$ code

⇒ C_H is $(7,4,3)_2$ - code

Generalized Hamming bound For any $(n,k,d)_q$ code,

$$k \le n - \log_q \left(\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right)$$

$\Rightarrow$ ($q=2$, $d=3$)

$$k \le n - \log_2 \left(\underbrace{\binom{n}{0}(2-1)^0}_{=1} + \underbrace{\binom{n}{1}(2-1)^1}_{=n} \right)$$

Reading Assignments: Sec 1.7

Linear codes

Q) How much space would you need to store an arbitrary $(n,k)_q$-code? / consider an arbitrary $(n,k,d)_q$ code / $(n,k)_q$ code

A: $q^k \cdot n$ symbols
(q^k → # codewords, n ↑ length of each codeword.)

TODAY! A general class of codes, linear codes, that can be represented in $\leq n^2$ symbols.

Def (Linear codes): Let q be a prime power ($q = p^s$, p → prime, $s \geq 1$ is an int), $C \subseteq$ "$\{0,\dots,q-1\}^n$" is a linear code if it is a linear subspace.

First: What set of "numbers" do we need? What operations do we want to support

Fields: $\mathbb{F} = (S, +, \cdot)$ → be able to add, subtract, multiply, divide

$a, b \in S$

$a+b \in S$, $a \cdot b \in S$, $a-b \in S$, $\frac{a}{b} \in S$

(→) Closure of $+, \cdot$ ⇒ $a, b \in S$, $a+b \in S$, $a \cdot b \in S$

(→) Associativity of $+, \cdot$ ⇒ $a, b, c \in S$ $a+(b+c) = (a+b)+c$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(→) Commutativity of $+, \cdot$ ⇒ $a, b \in S$ ⇒ $a+b = b+a$, $a \cdot b = b \cdot a$

(→) Distributivity ⇒ $a \cdot (b+c) = a \cdot b + a \cdot c$

(→) Identities: 0 for $+$, 1 for $\cdot$

$a+0 = a$ $\quad 1 \cdot a = a$

(→) 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 a field

$\mathbb{Q}$ is a field (set of rationals)

Finite fields

$|S|$ is finite
(overload $|\mathbb{F}|$ is finite)

THM 1: Any finite field has size p^s $\quad p \to$ prime, $s \geq 1$ int.

Ex: (1) field of size 2 $\to \mathbb{F}_2$ { GF(2) }
$(\{0,1\}, \oplus, \wedge)$

(2) field of size $p \to$ prime
$(\{0,1,\dots,p-1\}, +_{\bmod p}, \cdot_{\bmod p})$
$\to \quad -a \equiv p-a \qquad (a + (p-a)) \bmod p = p \bmod p = 0.$

THM 2: There is a unique finite field of size p^s (upto isomorphism)

$\Rightarrow$ q is a prime power

$\mathbb{F}_q$

Def (linear subspace) $S \subseteq \mathbb{F}_q^n$ is a linear subspace if

(i) $\forall\ \bar{x}, \bar{y} \in S$, $\bar{x} + \bar{y} \in S$
↖ component wise addition over $\mathbb{F}_q$

(ii) $\forall\ a \in \mathbb{F}_q$, $\bar{x} \in S$, $a \cdot \bar{x} \in S$
↖ mult each entry in $\bar{x}$ by a over $\mathbb{F}_q$