29/7

Block code – Finite alphabet F

(n, M) block code $\rightarrow$ Subset $C \subseteq F^n$, $|C| = M$.

$n \rightarrow$ Code length, $C \rightarrow$ Codebook or code, elements called codewords.

$k \rightarrow \log_{|F|} M$ (dimension of code).

Rate $\rightarrow \frac{k}{n}$.

Error correction capability of code will depend on how 'far' or different codewords are from each other.

Hamming distance $\rightarrow$ $x, y \in F^n$. Hamming distance $d(x,y)$ is no. of positions in which x, y differ.

It is a valid distance metric since

① $d(x,y) \geq 0$. ② Symmetry: $d(x,y) = d(y,x)$

③ Δ-inequality: $d(x,y) \leq d(x,z) + d(z,y)$.

Minimum distance of C $\rightarrow$ $d(C) \triangleq \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} d(c_1, c_2)$

Will sometimes refer to code as (n, M, d)-code.

Eg → Repetition code $(3, 2, 3)$. $C = \{000, 111\}$

$d(C) = 3$

Eg - Simple parity check code $(3, 4, 2)$ code. $C = \{000, 011, 110, 101\}$

$d(C) = 2$

Error correction / detection, Erasure correction

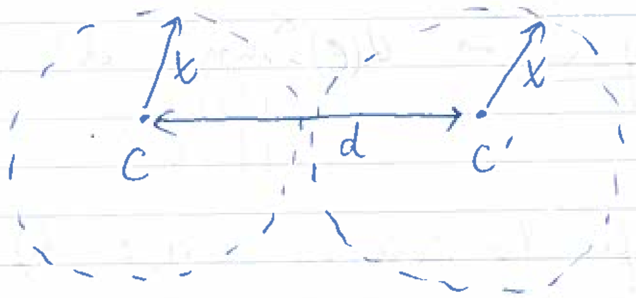
- An (n, M, d)-code can correct ~~upto~~ every error pattern with upto $\lfloor \frac{(d-1)}{2} \rfloor$ errors.

Pf → Consider the nearest-codeword decoder for which $D(y) = \min_{c \in C} d(y, c)$. Consider any received word y s.t. $d(y, c) \le \frac{d-1}{2}$. Assume to the contrary that c was transmitted & $c' \neq c$ s.t. $D(y) = c'$. Then

$$d(y, c') \le d(y, c) \le \frac{d-1}{2}.$$

$$\Rightarrow d(c, c') \le d(c, y) + d(c', y) \le d-1$$

Contradiction since min-distance $d(C) = d$.



For $t \le \lfloor \frac{d-1}{2} \rfloor$, spheres don't overlap

Eg → Repetition code, $(n, 2, n)$-code has $d(C) = n$ and can correct $\lfloor (n-1)/2 \rfloor$ errors

Eg → $(3, 4, 2)$ simple parity check code cannot correct all single errors

$C = \{000, 011, 101, 110\}$. If $y = 001$, c could be 000, 011 or 101

- An (n, M, d)-code can detect every error pattern of upto $d-1$ errors

Pf – Set $D(y) = \begin{cases} y & \text{if } y \in C \\ \text{error} & \text{if } y \notin C \end{cases}$

So detection fails only if error pattern converts true codeword c to another codeword c'.

Since $d(c, c') = d$, can detect upto $d-1$ errors.

Eg → Parity code $(3, 4, 2)$ could not correct all single errors, but can always detect a single error.

- Error Correction + Error detection

Consider an (n, M, d)-code s.t $\boxed{2t + l \leq d-1}$

- Then, if no. of errors is $\leq t$, errors will be recovered correctly

- If otherwise # errors is $\leq t+l$, then error can be detected.

Pf → Decoder $D(y) = \begin{cases} c & \text{if } \exists\, c \in C \text{ s.t } d(y,c) \leq t \\ \text{error} & \text{o.w.} \end{cases}$

Since $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, upto t errors can be corrected always

Now, say c is true codeword & y is received. $d(y, c) \leq t+l$

Error cannot be detected if y is contained in sphere of radius t around $c' \neq c \Rightarrow d(y, c') \leq t$. Then

$d(c, c') \leq d(y, c) + d(y, c') \leq t+l+t \leq d-1$. Contradiction

Erasure Correction

- (n, M, d) code can ~~correct~~ recover from upto $d-1$ erasures.

Pf → $D(y) = \begin{cases} c & \text{if } c \text{ is the unique codeword which agrees with } y \\ \text{error} & \text{o.w.} \end{cases}$

Since $d(c, c') \geq d$, there can be at most one c which agrees with received word y.

- ## Combined capability

- An (n, M, d) code. Consider a channel which causes errors and erasures.

Say ~~2t+l~~ $\boxed{2t + l + s \leq d-1}$. Then

a) If # errors (excluding erasures) $\leq t$, then all errors & erasures will be recovered correctly

b) Otherwise, if # errors $\leq t + l$, then error will be declared.

ALGEBRA DETOUR : GROUPS & FIELDS

Search for good codes cannot be done via exhaustive computation since the complexity is way too high

Structured search has been the basis of the design of codes and is based on algebraic frameworks like groups & fields.

GROUP — A set G along with an operation which acts on pairs of elements ($*$) with following properties:

1) Closure — $\forall\, a,b \in G,\quad a*b = c \in G$

2) Associativity — $a,b,c \in G \Rightarrow a*(b*c) = (a*b)*c$

3) Identity — $\exists$ an identity element e s.t $a*e = e*a = a$

4) Inverse — $\forall\, a \in G,\ \exists\, a' \in G$ s.t $a*a' = a'*a = e$.

In addition, if we have the following

5) Commutativity — $\forall\, a,b \in G \quad a*b = b*a,$

then its called an Abelian group. Order of g is no. of elements

Property 1 — In G, identity element is unique

Pf — By contradiction. Say $\exists$ identity elements e, e'.

Then, $e = e*e' = e'$. Contradiction.

Egs — Integers under addition, $\{0,1,2 \ldots n-1\}$ under mod-n addition

In particular $\{0,1\}$ with $+ \to$ mod-2 or $\oplus$ operation
$e = 0$

Let G be a group & H be a subset of G. Then H is called a subgroup of G is H is a group w.r.t $*$ restricted to H.

Verify

① H is closed under $*$ ① & ② imply $e \in H$.

② $\forall a \in H$, inverse $a' \in H$.

Eg $\Rightarrow$ Z under addition, $\rightarrow$ Subset of multiple of 3 is a subgroup.

<u>One construction of subgroup from a finite group G</u>

Take element $h \in G$. Consider h, $h*h$, $h*h*h$, - - -

Denote by h, h^2, h^3 - - .

Can't all be unique terms since G is finite. First element to be repeated will be equal to h itself since if two other i,j

$$h^i = h^j \Rightarrow \underbrace{h^{-1}}_{\text{inverse}} * h^i = h^{-1} * h^j \Rightarrow h^{i-1} = h^{j-1}.$$

Contradiction

Also if $h^j = h \Rightarrow h^{j-1} = e.$ Also called order of element h.

So subgroup $H = \{e, h, h^2, h^3 \ldots h^{j-1}\}$ is called cyclic subgroup and order of the group is # elements $= j$.

Note that it is closed & inverse of h^i is $h^{j-i} \in H$.

Defn - Let H be a subgroup of finite group G. Then an important notion is that of coset decomposition.

Say $H = \{h_1, h_2 - - h_n\}$ with $h_1 = e$

$h_1 = e \quad h_2 \quad h_3 \quad \ldots \quad h_n$

$g_2 * h_1 = g_2 \quad g_2 * h_2 \quad g_2 * h_3 \quad \ldots \quad g_2 * h_n$

$g_3 * h_1 = g_3 \quad g_3 * h_2 \quad g_3 * h_3 \quad \ldots \quad g_3 * h_n$

$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$

$g_m * h_1 = g_m \quad g_m * h_2 \quad g_m * h_3 \quad \ldots \quad g_m * h_n$

First row has elements of H. Choose any element of G not yet covered, call it g_2 and start second row with

$g_2 * h_1$, $g_2 * h_2$ -- and so on. Repeat the process

First element in each row is called coset leader and the row is called its coset. [Left coset here. If $h_i * g_2$, then right coset. Equal for abelian group]

We can show that this is a way to partition elements of G into such cosets. i.e. each element appears exactly once in the decomposition.

Claim – Each element in G appears exactly once in coset decomposition

Pf - Every element appears otherwise we can't stop.

If two elements in same row are equal, say $g_i * h_j = g_i * h_k$

Multiply by g_i^{-1} gives $h_j = h_k$.

Now say for $a > b$, $g_a * h_i = g_b * h_j$

Then $g_a * h_i * h_i^{-1} = g_b * h_j * h_i^{-1}$

$\Rightarrow g_a = g_b * h_j * h_i^{-1}$

But then g_a belongs to coset of g_b. Can't be coset leader.

Thus coset decomposition partitions element of G.

[Lagrange Thm] Corollary – (# elements in G) = n, Let H be a subgroup of G. of order m.

Then m divides n and the coset decomposition of G using H contains n/m rows.

Corollary – order of group G is divisible by order of any of its elements.

Eg – $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ $*$ = mod-9 addition

H = multiples of 3 → $\{0, 3, 6\}$ check is a subgroup

$n = 9$, $m = 3$

0	3	6
1	4	7
2	5	8

→ Coset decomposition.

Field — Use defn of group to define an algebraic structure which is closed under addition, subtraction, multiplication and division.

Defn → A field is a set F of elements with two operations defined: addition ($+$) and multiplication ($\cdot$) on pairs of elements, which satisfy the following conditions:

1. F is an abelian group under addition ($+$)
2. F is closed under multiplication ($\cdot$), set of non-zero elements forms an abelian group under ($\cdot$)
3. Distributive law holds → $a(b+c) = ab + ac \quad \forall a,b,c \in F$

Usually, the additive identity is denoted by 0 & multiplicative identity by 1.
Additive inverse of a by $-a$ & multiplicative inverse by a^{-1}
So by $a-b$, we mean $a+(-b)$ & by a/b, we mean $b^{-1}a$.
elements in field → order of field
element is finite → finite field

Basic Properties

Pf → $a = a\cdot 1 = a\cdot(1+0) = a + a\cdot 0$

1. $\forall a \in F, \; a\cdot 0 = 0\cdot a = 0$
2. $\forall a,b \in F/\{0\}, \; a\cdot b \neq 0$

(3) $a \cdot b = 0$ & $a \neq 0 \Rightarrow b = 0$

(4) $\forall a, b \in F$, $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

(5) $\forall a \neq 0$, $a \cdot b = a \cdot c \Rightarrow b = c$

Eg → (a) The smallest possible field has two elements.

In fact, it is $\{0, 1\}$ with mod-2 addition & multiplication

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

An important field which we will work with extensively

Denoted by Galois Field (2) or GF(2)

(b) There is GF(3) consisting of $\{0, 1, 2\}$ with mod-3 arithmetic

+	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

In fact, for any prime no. p, GF(p) exist with set $\{0, 1, 2 \ldots p-1\}$ under mod-p arithmetic.

(c) GF(4) exists → $\{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$\boxed{1+3=2, \quad 2\cdot 3 = 1}$

Not mod-4 arithmetic here. Defined differently, will cover later.

In fact, $GF(p^k)$ exists for each prime p, $k \geq 1$.

Mostly we will focus on $GF(2^k)$. There, one way of viewing addition is to consider elements as binary vectors of length k & performing component-wise mod-2 addition.

$$GF(4) = GF(2^2) \rightarrow \{\underset{\substack{\downarrow \\ 0}}{00}, \underset{\substack{\downarrow \\ 1}}{01}, \underset{\substack{\downarrow \\ 2}}{10}, \underset{\substack{\downarrow \\ 3}}{11}\}$$

$$1+3 = 2 \qquad \begin{array}{r} 01 \\ +\ 11 \\ \hline 10 \\ \downarrow \\ 2 \end{array} \qquad\qquad 2+1 = 3 \qquad \begin{array}{r} 10 \\ +\ 01 \\ \hline 11 \\ \downarrow \\ 3 \end{array}$$

We will define arithmetic of $GF(2^k)$ & their construction later when details are needed.

Vector spaces – Generalization of vector spaces over reals to finite fields.

Defn – Consider field F. Elements of F will be called 'scalars'. Set V is called a vector space & its elements called vectors if there is an operation 'vector addition' $(+)$ on element pairs and an operation 'scalar multiplication' $(\cdot)$ on an element from F and an element from V, which satisfy the following:

1. V is an abelian group under vector addition $(+)$

3. Distributive laws: $\forall\, v_1, v_2 \in V$ & $c \in F$,

$$c\cdot(v_1 + v_2) = c\cdot v_1 + c\cdot v_2$$

Also, $\forall\, v \in V,\ c_1, c_2 \in F$,

$$(c_1 + c_2)\cdot v = c_1\cdot v + c_2\cdot v$$

Note that $+$ denotes vector addition in V & field addition in F

4. Associative law – $\forall\, v \in V,\ c_1, c_2 \in F$,

$$(c_1 c_2)v = c_1(c_2 v)$$

5. Let 1 be the multiplicative identity in F. Then $1.v = v \ \forall v$

2. $\forall\, a \in F,\ v \in V,\ a.v \in V$

Denote additive identity of V by $\bar{0}$. Then, it follows that $0.v = \bar{0} \ \forall v \in V$.

Also ① $c.\bar{0} = \bar{0} \ \forall c \in F$, ② $(-c).v = c.(-v) = -(c.v)$ $\forall c \in F,\ v \in V$.

Eg1. Vector space over $GF(2)$

$$V = \{ (a_0, a_1, \dots a_{n-1}) : a_i \in GF(2) \}$$

n-tuples over $GF(2)$. $(+)$ on $V \rightarrow$ component-wise mod-2 addition.

$(\cdot)$ Scalar multiplication

$$c \cdot (a_0, a_1, \dots a_{n-1}) = (c \cdot a_0, c \cdot a_1, \dots c \cdot a_{n-1})$$

All properties satisfied.

Eg 2 - $V \rightarrow$ set of polynomials in x with coefficients from $GF(q)$

$F \rightarrow GF(q)$

vector addition $\rightarrow$ polynomial addition

Scalar multiplication $\rightarrow$ multiplication of $c \in F$ with polynomial

---

Defn - S be a non empty subset of vector space V over F.

Then S is a 'subspace' of V if

(1) $\forall u, v \in S$, $u + v \in S$

(2) $\forall a \in F$, $u \in S$, $a \cdot u \in S$

Then S is also a vector space over F.

Eg - $V \to$ all 5-tuples over $GF(2)$

$S - \{(00000), (00111), (11010), (11101)\}$

For $v_1, v_2 .. v_k \in V$ and $a_1, a_2 .. a_k \in F$,

$a_1 v_1 + a_2 v_2 - - + a_k v_k$ is called a linear combination of v_i's.

<u>Claim</u> $\to$ The set of all linear combinations of $v_1 - . v_k$ forms a subspace of V.

$v_1 ... v_k$ are said to be linearly dependent if $\exists$ $a_1 - - a_k$ (not all 0)

s.t $a_1 v_1 + a_2 v_2 - - - + a_k v_k = 0$.

If not, $v_1 - . v_k$ are linearly independent.

A set of vectors $v_1 - - v_k$ spans a vector space V if each vector in V is a linear combination of $v_1 .. v_k$. In any vector space V, $\exists$ at least one set B of linearly independent vectors which spans V. This is called ~~the~~ a basis & size of B is called dimension of the space.

Eg - V_n - set of n-tuples over $GF(2)$. $\{e_i\}_{i=1}^{n}$ s.t

$e_i \to$ only 1 in i^{th} position forms a basis.

Let $u = (u_0, u_1, \dots u_{n-1})$ & $v = (v_0, v_1, \dots v_{n-1})$ be two tuples in $V_n = \{(v_0, v_1, \dots v_{n-1}) : v_i \in F\}$ under component wise addition & componentwise scalar multiplication.

[Can represent any vector space as coefficient vectors $(a_0, a_1, \dots a_{n-1})$ of basis vectors.]

Then inner product (or dot product) of $u, v \in V_n$ is given by

$$u \cdot v = u_0 v_0 + u_1 v_1 + \dots + u_{n-1} v_{n-1}$$

① $u \cdot v = v \cdot u$, ② $u \cdot (v + w) = u \cdot v + u \cdot w$, ③ $(a u) \cdot v = a(u \cdot v)$

If $u \cdot v = 0$, u & v are said to be orthogonal. Curiously, a vector in $GF(q)$ can be orthogonal to itself.

<u>Claim</u> - Let V_n be vector space of n-tuples over a field F, and let W be a subspace. Then, the set of vectors orthogonal to W is itself a subspace, denoted by $W^\perp$ and is called the orthogonal complement / dual / null space of W

<u>Claim</u> - W is also the dual space of $W^\perp$.

<u>Claim</u> - Let W be a k-dimensional subspace of V_n. Then the dimension of $W^\perp = n-k$. $\dim(W) + \dim(W^\perp) = n$.

Eg V_3 over $GF(2)$. $S = \{(000), (101), (001), (100)\}$ is a subspace of dimension 2. $S^{\perp} = \{(010)\}$

$$\dim(S) + \dim(S^{\perp}) = 3$$

Matrices – $k \times n$ matrix M over $GF(q)$ has kn entries, each from $GF(q)$. Each row is an n-tuple and each column an k-tuple over $GF(q)$. Can think of matrix M as

$$\begin{bmatrix} m_0 \\ m_1 \\ \vdots \\ m_{k-1} \end{bmatrix}$$ collection of k n-tuples.

If the k rows are linearly independent, the q^k linear combinations form a subspace, called the row space of M.
Can perform elementary row operations (interchange rows or add rows) to convert M to M' without changing row space.

Eg
$$M = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$ over $GF(2)$

Adding 3^{rd} to 1^{st} row & interchanging 2^{nd} & 3^{rd} row, we get

$$M' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Let ω be the row space of G $(k \times n)$ over $GF(q)$ with linearly independent rows. Then $\dim(\omega) = k$. If $\omega^{\perp}$ is the dual space, $\dim(\omega^{\perp}) = n-k$. Let $h_0, h_2 \ldots h_{n-k-1}$ be $n-k$ linearly independent vectors in $\omega^{\perp}$. Form H s.t

$$H = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-k-1} \end{bmatrix}$$

with h_i's as rows. So row space of H is $\omega^{\perp}$. Thus, for each $g_i \in G$ and $h_j \in H$, $g_i \cdot h_j = 0$ (inner product)

Eg. Take $GF(2)$ & $G = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Then $H = G^{\perp} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

Each ~~g~~ row of G is orthogonal to each row of H.