Game of Minimum distance d

$\mathbb{Z}_2^n$

$\mathcal{C} \subseteq \mathbb{Z}_2^n$

$\mathcal{C} : (n, M, d) \qquad |\mathcal{C}| = M$

$d = \min$ Hamm. dist $\equiv d(\mathcal{C})$

$d_H(x,y) = w_H(x-y) = w_H(x+y)$

$\because x, y \in \mathbb{Z}_2^n$

$$d = \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} \{ d_H(x,y) \}$$

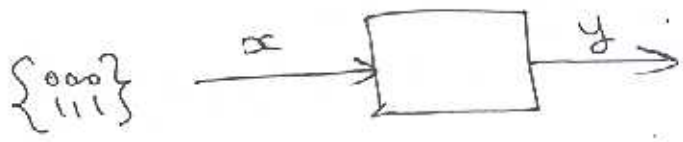
Example ① $\mathcal{C} = \{ \underbrace{00000}_{\bar{x}}, \underbrace{00111}_{\bar{y}}, \underbrace{11111}_{\bar{z}} \}$ (codewords)

$d(\bar{x},\bar{y}) = 3 \quad d(\bar{x},\bar{z}) = 5 \quad d(\bar{y},\bar{z}) = 2$

$\therefore$ $\mathcal{C}$ a binary $(5,3,2)$-code

Example ② $\mathcal{C} = \{ \underbrace{000000}_{\bar{x}}, \underbrace{000111}_{\bar{y}}, \underbrace{111222}_{\bar{z}} \}$ Ternary code $\subseteq \mathbb{Z}_3^6$

$\mathcal{C}$ ternary $(6,3,3)$-code



$d(y,000) =$
$d(y,111) =$

Def A code $\mathcal{C}$ is called s-error detecting if $(s(>0) \in \mathbb{Z})$

whenever a codeword incurs ≥ 1 but $\leq s$ errors the resulting word is not a codeword.

— A code $\mathcal{C}$ is exactly s-error detecting if it is s-error detecting but not $(s+1)$-error detecting

Example ① $\mathcal{C} = \{00000, 00111, 11111\}$ is 1-error detecting $\because$ changing any codeword in one position does not result in another codeword

$00000 \to 00111$ needs to change 3 bits $\quad 00111 \to 11111 \to 2$ bits

$00000 \to 11111$ 5 bits

In fact, $\mathcal{C}$ is exactly 1-error detecting
$\because$ $\mathcal{C}$ is not 2-error detecting

$$00111 \xrightarrow[\text{2 bits change}]{} 11111$$

Example ②

$$\mathcal{C} = \{000000, 000111, 111222\}$$

is 2-error detecting

$\because$ changing any codeword in 1 or 2 positions does not result in another codeword

$000000 \rightarrow 000111$ 3 changes
$000000 \rightarrow 111222$ 6 positions
$000111 \rightarrow 111222$ need 6 changes

$\mathcal{C}$ is exactly 2-error detecting
$\mathcal{C}$ is not 3-error detecting.

Theorem $\mathcal{C}$ is s-error detecting iff $d(\mathcal{C}) \geq s+1$

i.e. a code with dist. d is an exactly $(d-1)$ error detecty.

□ ($\Leftarrow$) Suppose $d(\mathcal{C}) \geq s+1$

If $\bar{x} \in \mathcal{C}$ & $\bar{y}$ s.t.

$$1 \leq d(\bar{x}, \bar{y}) \leq s < d(\mathcal{C})$$

($\because d \geq s+1$)
$\Rightarrow s \leq d-1 < d$

Then $\bar{y} \notin \mathcal{C}$ hence

$\mathcal{C}$ is s-error detecting.

($\Rightarrow$) On the other hand, if $d(\mathcal{C}) < s+1 \Rightarrow d \leq s$

$\Rightarrow \exists\ \bar{c}_1, \bar{c}_2 \in \mathcal{C}$ s.t. $1 \leq d(\bar{c}_1, \bar{c}_2) = d(\mathcal{C}) \leq s$

$\Rightarrow$ It is therefore possible that we begin with $\bar{c}_1$ & $d(\mathcal{C})$ errors (where $1 \leq d(\mathcal{C}) \leq s$) are incurred s.t. the resulting word is $\bar{c}_2$ another codeword in $\mathcal{C}$

Hence $\mathcal{C}$ is not s-error detecting. ▨

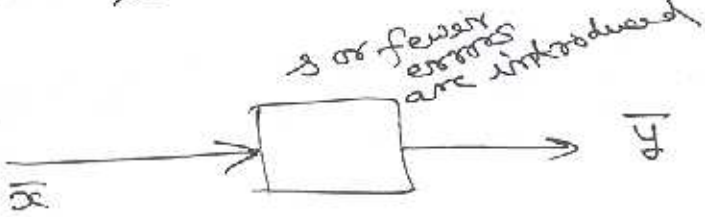
SC461. Lecture

— $\mathbb{Z}_2^n$ $\quad C \subseteq \mathbb{Z}_2^n$ $\quad C : \mathcal{S}(n, M, d)$

Lemma (1) C can detect up to s errors in any codeword if $d(C) \geq s+1$

□ $d(C) \geq s+1$

Suppose

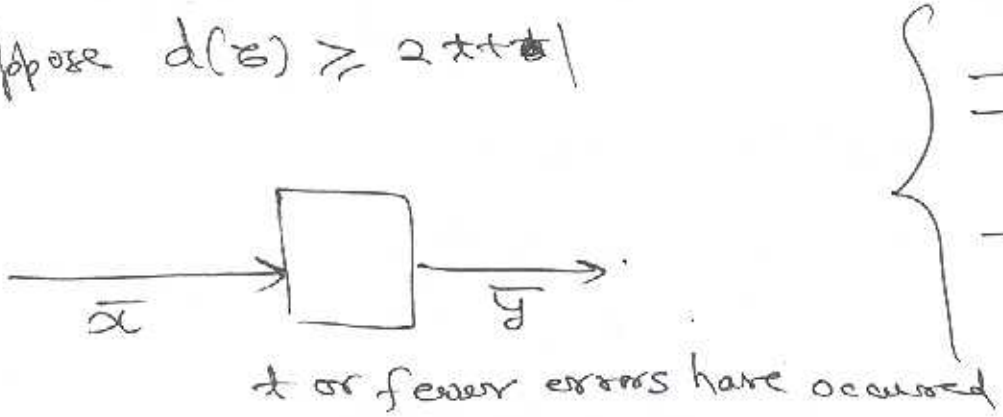


$d(\bar{x}, \bar{y}) \leq s$

$\Rightarrow$ errors can be detected

(2) A code C can correct up to t errors in any codeword if $d(C) \geq 2t+1$

□ Suppose $d(C) \geq 2t+1$



$d(\bar{x}, \bar{y}) \leq t$

then we claim $d(\bar{x}', \bar{y}) \geq t+1$

For otherwise $d(\bar{x}', \bar{y}) \leq t \Rightarrow$

$d(\bar{x}, \bar{x}') \leq d(\bar{x}, \bar{y}) + d(\bar{x}', \bar{y}) \leq t + t \leq 2t$

$\Rightarrow$ # to $d(C) \geq 2t+1$

$\therefore$ x is the nearest codeword to y

$\therefore$ we correct the errors.

Th. ~~def~~ $\mathcal{C}$ has min distance d then $\mathcal{C}$ can be used to correct $\lfloor \frac{d-1}{2} \rfloor$ errors & detect $d-1$ errors

① $d \geq s+1 \iff s \leq d-1$

② $d \geq 2t+1 \iff t \leq \frac{d-1}{2}$

$$S_r(\bar{u}) = \{ \bar{v} \in \mathbb{Z}_2^n \mid d(\bar{u}, \bar{v}) \leq r \}$$

$\mathcal{C}$ code (n, M, d)

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

$$S_t(\bar{c}) \cap S_t(\bar{c}') = \emptyset \qquad \bar{c}, \bar{c}' \in \mathcal{C}$$

$\bar{x} \in S_t(\bar{c}) \cap S_t(\bar{c}')$

$\Rightarrow$ $d(\bar{x}, \bar{c}) \leq t$

$d(\bar{x}, \bar{c}') \leq t$.

$\Rightarrow$ ~~$d(\bar{c}, \bar{x})$~~

$d(\bar{c}, \bar{c}') \leq d(\bar{c}, \bar{x}) + d(\bar{c}', \bar{x})$

$\leq 2t$

$\#$ $d(\mathcal{C}) \geq 2t+1$

Array Decoding — Slepian Method

Coset of a code $\quad \mathcal{C} : [n, k]_q$

$a \in \mathbb{F}_q^n \qquad a + \mathcal{C} = \{a + x \mid x \in \mathcal{C}\}$

① Every vector of $\mathbb{F}_q^n$ is contained in some coset of $\mathcal{C}$

□ Let $b \in \mathbb{F}_q^n \Rightarrow b \in b + \mathcal{C}$

~~② $\forall\ b \in \mathbb{F}_q^n \quad |b + \mathcal{C}| = |\mathcal{C}| = q^k$~~

~~□ By def, $b + \mathcal{C}$ has at most $|b + \mathcal{C}| \leq |\mathcal{C}| = q^k$ elements.~~

~~Since any two elements~~

② $b \in a + \mathcal{C} \Rightarrow \boxed{b + \mathcal{C} = a + \mathcal{C}}$ → $b + \mathcal{C} \subseteq a + \mathcal{C}$, $a + \mathcal{C} \subseteq b + \mathcal{C}$

□ $b \in a + \mathcal{C} \Rightarrow b = a + x$ for some $x \in \mathcal{C}$

Let $b + y \in b + \mathcal{C}$ for some $y \in \mathcal{C}$

$\Rightarrow b + y = (a + x) + y = a + (x + y) \in a + \mathcal{C}$

$\Rightarrow \boxed{b + \mathcal{C} \subseteq a + \mathcal{C}}$

$a + z \in a + \mathcal{C} \Rightarrow a + z = (b - x) + z$

$= b + (z - x) \in b + \mathcal{C}$

$\Rightarrow \boxed{a + \mathcal{C} \subseteq b + \mathcal{C}}$ Thus $\boxed{b + \mathcal{C} = a + \mathcal{C}}$

③ $|a + \mathcal{C}| = |\mathcal{C}| = q^k$

Consider the map ~~$x \to a + x$~~

$\theta : \mathcal{C} \to a + \mathcal{C}$

$\theta(x) = a + x \quad \forall x \in \mathcal{C}$

θ is 1-1 & onto $\Rightarrow |\mathcal{C}| = |a + \mathcal{C}| = q^k$

(4) Two cosets are either disjoint or coincide (partial overlap is impossible)

□ Suppose $a+\mathcal{C}$ and $b+\mathcal{C}$ overlap

$\Rightarrow z \in (a+\mathcal{C}) \cap (b+\mathcal{C})$

$\Rightarrow z = a+x = b+y$ for some $x, y \in \mathcal{C}$

$\Rightarrow b = a+(x-y) \in a+\mathcal{C}$

$\Rightarrow b \in a+\mathcal{C} \Rightarrow b+\mathcal{C} = a+\mathcal{C}$ ▨

Coset leader Codeword with min wt in a coset is called coset leader.

(5) $\mathbb{F}_2^n = (\bar{0}+\mathcal{C}) \cup (a_1+\mathcal{C}) \cup (a_2+\mathcal{C}) \cup \cdots \cup (a_t+\mathcal{C})$

disjoint cosets $\quad t = 2^{n-k}-1$

We usually take a_i as coset leaders.

Example $G = \begin{bmatrix} 1011 \\ 0101 \end{bmatrix}$ $\mathcal{C}: [4, 2]$

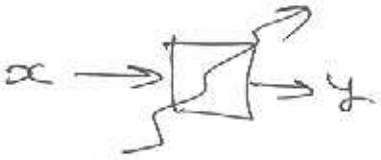
$\mathcal{C} = \{0000, 1011, 0101, 1110\}$

Array

Code words →				
0000	1011	0101	1110
1000	0011	1101	0110
0100	1111	0001	1010
0010	1001	0111	1100
↑			

Coset leaders

Syndrome Decoding



$$S(y) = Hy^t = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-k} \end{pmatrix}_{(n-k)\times 1}$$

① $S(y) = 0 \iff y$ is a codeword. $\in \mathcal{C}$

② Two vectors are in same coset of $\mathcal{C} \iff$ they have the same syndrome.

□ u, v are in the same coset

$\iff u - v \in \mathcal{C}$

$\iff u + \mathcal{C} = v + \mathcal{C}$

$\iff H(u-v)^t = 0$

$\iff Hu^t = Hv^t$

$\iff S(u) = S(v)$ ▨

③ There is 1-1 correspondence in cosets and syndrome.

Example $G = \begin{bmatrix} 1011 \\ 0101 \end{bmatrix}$ & $H = \begin{bmatrix} 1010 \\ 1101 \end{bmatrix}$

$\mathcal{C} : [4,2]$

message	00	10	01	11	Syndrome S of coset leaders
code	0000	1011	0101	1110	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
coset	1000	0011	1101	0110	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
coset	0100	1111	0001	1010	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
coset	0010	1001	0111	1100	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Coset leaders

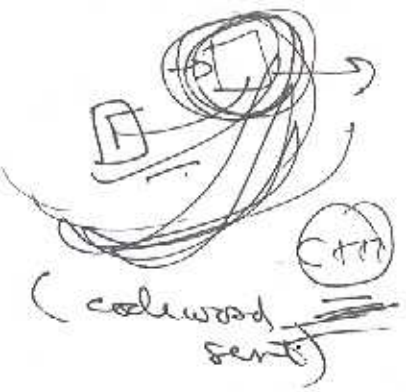
Decoding Recard. v^r $y = 1111$

$$S(1111) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$\Rightarrow$ $e = 0100$ (coset leader)

$\Rightarrow$ $x = 1111 - 0100 = 1011$ (codeword sent)

$\Rightarrow$ message $= ?$



For binary codes If $y = x + e \quad x \in \mathcal{C}$

$$S(y) = Hy^t = Hx^t + He^t = 0 + He^t$$
$$= He^t$$

$e = (00\cdots0\underset{a}{1}000\underset{b}{1}0\cdots0\underset{c}{1}00\cdots0)$

ORF

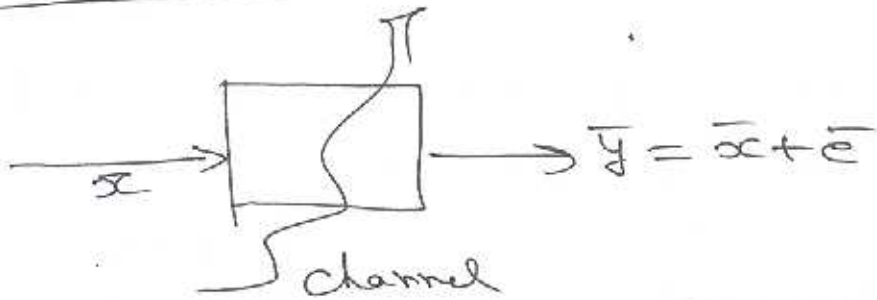
$$H = [H_1 | H_2 | \ldots | H_n]$$

$$S(y) = He^t = \sum_i e_i H_i = H_a + H_b + H_c$$

∴ For binary code, the syndrome is equal to the sum of the columns of H where the errors occured.

Natural Signal for

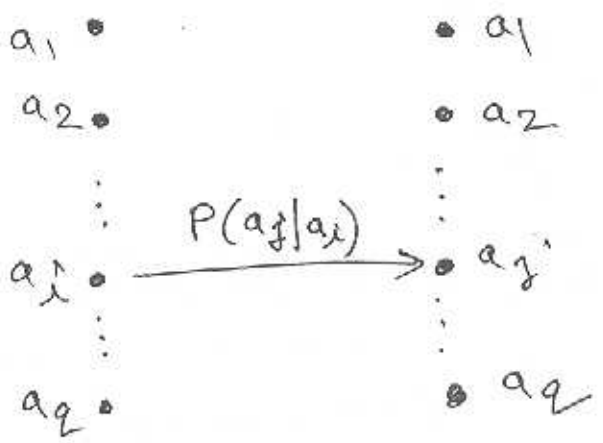
Probability of Error



Suppose Channel is binary symmetric channel (B.S.C)

Coding Theory Feb 2, 2010

Communication channel



— A communication channel consists of a finite channel alphabet $A = \{a_1, a_2, \ldots, a_q\}$ as well as a set of forward channel prob.s $P(a_j \text{ recv.} \mid a_i \text{ sent})$ satisfying

$$\sum_{j=1}^{q} P(a_j \text{ recv.} \mid a_i \text{ sent}) = 1 \qquad \forall\, i$$

(conditional prob. that a_j is recvd. given that a_i is sent)

— A comm. channel is said to be memoryless if the outcome of any one transmission is indep. of the outcome of the previous transmissions i.s.

$$P(\bar{x} \text{ recvd.} \mid \bar{c} \text{ sent}) = \prod_{i=1}^{n} P(x_i \text{ recvd.} \mid c_i \text{ sent})$$

$\bar{x} = x_1 x_2 \ldots x_n$
$\bar{c} = c_1 c_2 \ldots c_n$

— A q-ary symmetric channel is a memoryless channel which has a channel alphabet size q s.t.

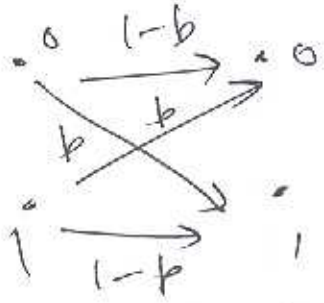
(1) Each symbol transmitted has the same prob. $p (< \frac{1}{2})$ of being received in error

(2) If a symbol is recvd. in error then each of $q-1$ possible errors is equally likely.

— For BSC

$P(1 \text{ rcvd} \mid 0 \text{ sent}) = P(0 \text{ rcvd} \mid 1 \text{ sent}) = p$ = crossover prob.

$P(0 \text{ rcvd} \mid 0 \text{ sent}) = P(1 \text{ rcvd} \mid 1 \text{ sent}) = 1-p$



General decoding Rule — Maximum likelihood decoding

$\mathcal{C}$ codewords $\quad \bar{c} \in \mathcal{C}$ is sent

& $\bar{x}$ is rcvd.

— Compute fwd. channel prob. $P(\bar{x} \text{ rcvd} \mid \bar{c} \text{ sent})$

$\forall$ codewords $\bar{c} \in \mathcal{C}$

— The MLD rule will conclude that $\bar{c}_x$ is the most likely codeword transmitted if $\bar{c}_x$ maximizes fwd channel prob. (~~fcp~~ FCP) i.e.

$$P(\bar{x} \text{ rcvd} \mid \bar{c}_x \text{ sent}) = \max_{\bar{c} \in \mathcal{C}} P(\bar{x} \text{ rcvd} \mid \bar{c} \text{ sent})$$

MLD ⟶ CMLD (Complete)

After receiving $\bar{x}$ find the most likely codeword transmitted. If there are more than one such codeword select one of them arbitrarily.

~~IMLD~~ IMLD (Incomplete)

request a retransmission if more than one most likely codeword is there.

— Suppose codewords from a code $\mathcal{C}$ are being sent over a BSC with crossover prob. p ($< \frac{1}{2}$) error rate

$$P(\bar{x} \text{ rcvd} \mid \bar{c} \text{ sent}) = p^e (1-p)^{n-e}$$

e = # of places $\bar{x}$ & $\bar{c}$ differ

If $p < \frac{1}{2} \Rightarrow 1-p > p$ ∴ prob will be large for larger values of $n-e$ i.e. for smaller values of e ∴ prob can be maximized by choosing a codeword ② $\bar{c}$ for which e is as small as poss

Theorem For a BSC with crossover prob. p ($p < \frac{1}{2}$) the MLD rule is same as the nearest nbd. decoding rule.

□

$$d(\bar{x}, \bar{c}) = i \iff P(\bar{x} \text{ recd} \mid \bar{c} \text{ sent}) = p^i (1-p)^{n-i}$$

$\because p < \frac{1}{2}$

$$\Rightarrow p^0(1-p)^n > p^1(1-p)^{n-1} > p^2(1-p)^{n-2} > \cdots > p^n(1-p)^0$$

By MLD rule decodes $\bar{x}$ to $\bar{c} \in C$ s.t. $P(\bar{x} \text{ recd} \mid c \text{ sent})$ is largest

i.e. s.t. $d(\bar{x}, \bar{c})$ is the smallest

$\therefore$ **MLD $\iff$ NND** □

$\{ x^{(1)}, x^{(2)}, \ldots, x^{(M)} \}$ used with equal prob.

$\in C$

$$P_{err} = \frac{1}{M} \sum_{i=1}^{M} \text{Prob}\{\text{decoder output} \neq x^{(i)} \mid x^{(i)} \text{ was sent}\}$$

Avg.

For decoding with std. array

$$P_{err} = \text{Prob}\{\bar{e} \neq \text{coset leader}\}$$

Suppose there are α_i coset leaders of wt. i. Then

$$P_{err} = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i} \quad (3)$$

word error rate

decoder output the wrong codeword

— If $d(C) = 2t+1$ or $2t+2$

then it can correct t errors.

∴ every vr of wt. $\leq t$ is a coset leader.

i.e. $\alpha_i = \binom{n}{i}$ for $0 \leq i \leq t$

for $i > t$ very difficult to compute α_i

Perfect codes If $\alpha_i = 0$ for $i > t = \left\lfloor \frac{d-1}{2} \right\rfloor$

code is perfect.

Quasi-perfect codes If $\alpha_i = 0$ for $i > t+1$

code is called quasi perfect

Sphere-packing Bound Hamming bound

— A t-error correcting binary code of length n containing M codewords must satisfy

$$M \left(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right) \leq 2^n$$

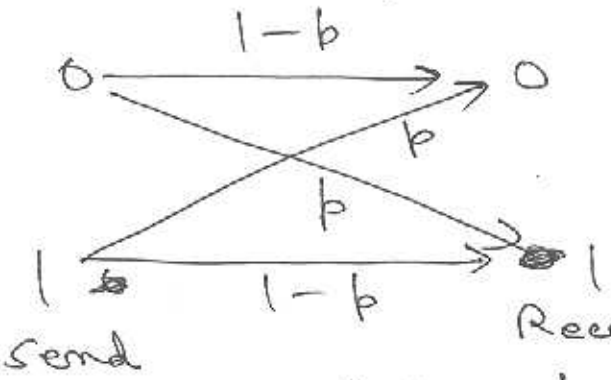
for a code over GF(q)

$$M \left(1 + (q-1)\binom{n}{1} + \cdots + (q-1)^t \binom{n}{t}\right) \leq q^n$$

□ ∵ $|S_t(\bar{c})| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}$ vectors.

$$S_t(\bar{c}) = \{ \bar{x} \mid d(\bar{x}, \bar{c}) \leq t \}$$

BSC



Memory less channel

error prob. $= p$ $\quad$ In gen., $0 \le p \le \frac{1}{2}$

$$\text{Prob}\{\bar{e} = 00000\} = (1-p)^5$$
$$\text{Prob}\{\bar{e} = 01000\} = p(1-p)^4$$
$$\text{Prob}\{\bar{e} = 10010\} = p^2(1-p^3)$$

In gen. if $\bar{e}$ is some fixed vr of wt. a

$$\text{Prob}\{\bar{e} = \bar{e}\} = p^a (1-p)^{n-a}$$

$P(1 \text{ rec.} \mid 0 \text{ sent}) = P(0 \text{ recv.} \mid 1 \text{ sent}) = p$

$P(0 \text{ rec.} \mid 0 \text{ sent}) = P(1 \text{ recv.} \mid 1 \text{ sent}) = 1-p$

Example $\quad C = \{000, 111\}$ $\quad$ cross over prob. $= p = .05$

recv. $= 110$

$$P(110 \text{ recv.} \mid 000 \text{ sent}) = P(1 \text{ recv.} \mid 0 \text{ sent})^2 \times P(0 \text{ recv.} \mid 0 \text{ sent})$$
$$= (.05)^2 (0.95) = 0.00285$$

$$P(110 \text{ recv.} \mid 111 \text{ sent}) = 0.04515 > P(110 \mid 000)$$

$\therefore$ 111 is more likely to be codeword sent

March 12, 2010 Weight Enumerators

MacWilliams Identity

$\mathcal{C}: [n, k]_2$ linear code

Weight Enumerator is a poly.

$$W_{\mathcal{C}}(z) = \sum_{i=0}^{n} A_i z^i$$

$$= A_0 + A_1 z + A_2 z^2 + \cdots + A_n z^n.$$

A_i = # of codewords of wt. i in $\mathcal{C}$

$$W_{\mathcal{C}}(z) = \sum_{\bar{x} \in \mathcal{C}} z^{wt(\bar{x})}$$

Ex. ①

$$\mathcal{C} = \{000, 011, 101, 110\}$$

$$\mathcal{C}^\perp = \{000, 111\}$$

$$W_{\mathcal{C}}(z) = 1 + 3z^2$$

$$W_{\mathcal{C}^\perp}(z) = 1 + z^3$$

②

$$\mathcal{C} = \{00, 11\} \text{ self dual}$$

$$W_{\mathcal{C}}(z) = W_{\mathcal{C}^\perp}(z) = 1 + z^2$$

For binary codes

Lemma ① $\mathcal{C}: [n, k]_2$ code $y \in \mathbb{F}_2^n$ s.t. (fixed y) $y \notin \mathcal{C}^\perp$

then $\bar{x} \cdot \bar{y} = 0$ and 1 equally often as $\bar{x}$ runs over the codewords of $\mathcal{C}$.

□ $A = \{\bar{x} \in \mathcal{C} \mid \bar{x} \cdot \bar{y} = 0\}$

$B = \{\bar{x} \in \mathcal{C} \mid \bar{x} \cdot \bar{y} = 1\}$

Claim $|A| = |B|$

Let $\bar{u} \in \mathcal{C}$ s.t. $\bar{u} \cdot \bar{y} = 1$ ($\bar{u}$ exists since $\bar{y} \notin \mathcal{C}^\perp$)

$\bar{u} + A = \{\bar{u} + \bar{x} \mid \bar{x} \in A\}$

then $\bar{u} + A \subseteq B$

For if $\bar{x} \in A \Rightarrow (\bar{u} + \bar{x}) \cdot \bar{y}$

$= \bar{u} \cdot \bar{y} + \bar{x} \cdot \bar{y}$

$= 1 + 0 = 1$

$\Rightarrow \bar{u} + A \subseteq B$ ✓

Similarly $\bar{u} + B \subseteq A$

$\Rightarrow |A| = |\bar{u} + A| \leq |B| = |\bar{u} + B| \leq |A|$

$\Rightarrow |A| = |B|$ ▨

Lemma ② $\mathcal{C} : [n, k]_2$ code & $\bar{y} \in \mathbb{F}_2^n$

then

$$\sum_{\bar{x} \in \mathcal{C}} (-1)^{\bar{x} \cdot \bar{y}} = \begin{cases} 2^k & \text{if } \bar{y} \in \mathcal{C}^\perp \\ 0 & \text{if } \bar{y} \notin \mathcal{C}^\perp \end{cases}$$

□ If $\bar{y} \in \mathcal{C}^\perp$ then $\bar{x} \cdot \bar{y} = 0 \ \forall \bar{x} \in \mathcal{C}$

& so $\sum_{\bar{x} \in \mathcal{C}} (-1)^{\bar{x} \cdot \bar{y}} = |\mathcal{C}| \cdot 1 = 2^k$ ✓

If $\bar{y} \notin \mathcal{C}^\perp$ then by Lemma 1 as $\bar{x}$ runs over all codewords of $\mathcal{C}$ $(-1)^{\bar{x} \cdot \bar{y}} = 1$ & -1 equally often

$\Rightarrow \sum_{\bar{x} \in \mathcal{C}} (-1)^{\bar{x} \cdot \bar{y}} = 0$

Lemma ③ Let $\bar{x} \in \mathbb{F}_2^n$ (fixed $\bar{x}$) then z indeterminate

$$\sum_{\bar{y} \in \mathbb{F}_2^n}{}' z^{wt(\bar{y})} (-1)^{\bar{x}\cdot\bar{y}} = (1-z)^{wt(\bar{x})} (1+z)^{n-wt(\bar{x})}$$

□ L.H.S. $= \sum_{y_1=0}^{1}{}' \sum_{y_2=0}^{1}{}' \cdots \sum_{y_n=0}^{1}{}' z^{y_1+y_2+\cdots+y_n} (-1)^{x_1y_1+x_2y_2+\cdots+x_ny_n}$

$$= \sum_{y_1=0}^{1}{}' \cdots \sum_{y_n=0}^{1}{}' \left(\prod_{i=1}^{n} z^{y_i} (-1)^{x_i y_i} \right)$$

$$= \prod_{i=1}^{n} \left(\sum_{j=0}^{1}{}' z^j (-1)^{j x_i} \right)$$

$$= (1-z)^{wt(\bar{x})} (1+z)^{n-wt(\bar{x})}$$

$\because \sum_{j=0}^{1}{}' z^j (-1)^{jx_i} = \begin{cases} 1+z & \text{if } x_i = 0 \\ 1-z & \text{if } x_i = 1 \end{cases}$

▨

Th. Macwilliams Identity for binary linear codes

$$W_{\mathcal{C}^\perp}(z) = \frac{1}{2^k} (1+z)^n \, W_{\mathcal{C}}\left(\frac{1-z}{1+z}\right).$$

□ Express $f(z)$ in 2 ways

$$f(z) = \sum_{\bar{x} \in \mathcal{C}} \left(\sum_{\bar{y} \in \mathbb{F}_2^n}{}' (-1)^{\bar{x}\cdot\bar{y}} z^{wt(\bar{y})} \right)$$

Using L-3.

$$f(z) = \sum_{\bar{x} \in \mathcal{C}} (1-z)^{wt(\bar{x})} (1+z)^{n-wt(\bar{x})}$$

$$= (1+z)^n \sum_{\bar{x} \in C} \left(\frac{1-z}{1+z}\right)^{wt(\bar{x})}$$

$$= (1+z)^n W_C\left(\frac{1-z}{1+z}\right)$$

On the other hand reversing the order of summation

$$f(z) = \sum_{\bar{y} \in \mathbb{F}_2^n} z^{wt(\bar{y})} \left(\sum_{\bar{x} \in C} (-1)^{\bar{x} \cdot \bar{y}} \right)$$

$$= \sum_{\bar{y} \in C^\perp} z^{wt(\bar{y})} \, 2^k \quad \text{(by Lemma-3)}$$

$$= 2^k W_{C^\perp}(z)$$

On general

Th. $C : [n,k]_q$ code $C^\perp [n, n-k]_q$

$$W_{C^\perp}(z) = \frac{1}{q^k}\left[1+(q-1)z\right]^n W_C\left(\frac{1-z}{1+(q-1)z}\right)$$

For binary case,

$$W_C(z) = \frac{1}{2^{n-k}}(1+z)^n W_{C^\perp}\left(\frac{1-z}{1+z}\right)$$

Ex-1

$$W_C(z) = 1+3z^2$$

$$W_{C^\perp}(z) = \frac{1}{4}(1+z)^3 W_C\left(\frac{1-z}{1+z}\right)$$

$$= \frac{1}{4}\left[(1+z)^3 + 3(1-z)^2(1+z)\right]$$

$$= 1+z^3$$

Wed. Interclass

Ex-2 . .

For binary Golay code $\mathcal{G}_{24}$.

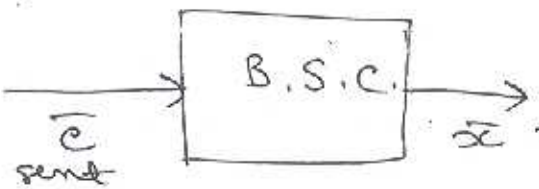
$$W_{\mathcal{G}_{24}}(z) = 1 + 759 z^8 + 2576 z^{12} + 759 z^{16} + z^{24}$$

Bounds on Codes

Feb 3, 2010

① **Sphere packing Bound**

Trade off between decoded bit error prob. and rate of the



The Capacity of the channel is defined as the max. rate at which communication is possible with arb. small Symbol error rate (P_{symb}).

Symbol Error Rate (Even if decoder outputs the wrong codeword it is possible that some of the message symbols are correct ∴ we define symbol error rate)

$\mathcal{C}$: $(n, M, d)_q$ code

$$\text{Rate}(\mathcal{C}) = \frac{\log_q M}{n}$$

For linear code $M = q^K$ $\mathcal{C}$ is K-dimnl

$$\text{Rate } \mathcal{C} = \frac{K}{n} = \text{ratio of } \#\frac{\text{of message symbol}}{\text{total } \# \text{ of message symbol sent}}$$

∴ Good code will have high rate

$\left\{ x^{(i)} = x_1^{(i)} \cdots x_n^{(i)} \right\}_{i=1,2,\ldots,M}$

First K symbols $x_1^{(i)} \ldots x_K^{(i)}$ are information symbols

Let $\hat{x} = \hat{x}_1 \ldots \hat{x}_n$ be the decoder output

P_{symb} (symbol error rate)

$=$ Avg. prob. that an information symbol is in error after decoding

$$P_{symb} = \frac{1}{KM} \sum_{j=1}^{K} \sum_{i=1}^{M} \text{Prob}\left\{ \hat{x}_j \neq x_j^{(i)} \,\middle|\, x^{(i)} \text{ was sent} \right\}$$

$$\frac{1}{K} P_{err} \leq P_{symb} \leq P_{err}$$

P_{symb} ↓ Symbol error rate

P_{err} ↓ word error rate

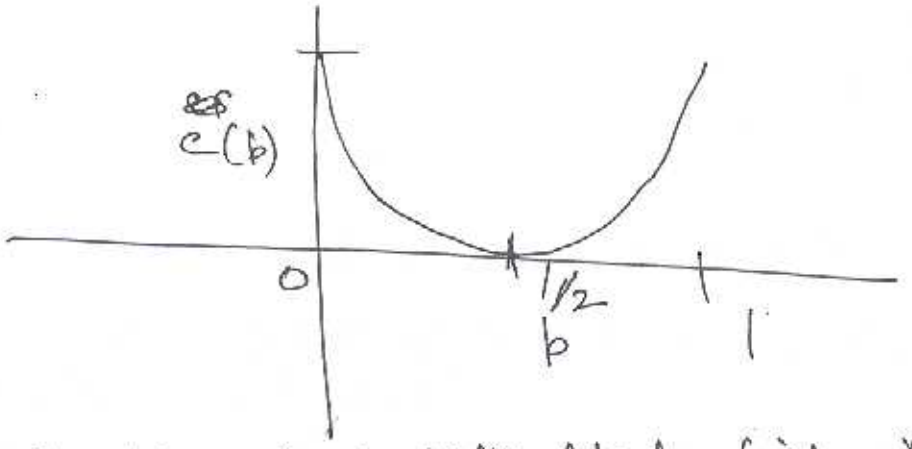
B.S.C. with crossover prob. p

$C(p) = 1 - H_2(p) \rightarrow$ binary Entropy fn.

$C(p) = 1 + p \log_2 p + (1-p) \log_2 (1-p)$

Shannon's Theorem

For any $\epsilon > 0$, if Rate $(C) < C(p)$ & n is suff. large then $\exists$ $[n, k]$ binary code of rate $k/n \geq R$ with error prob. $P_{err} < \epsilon$



Capacity of a B.S.C.

— In practice it is difficult to find P_{err} & P_{symb}

∴ People use Hamming distance as to measure how good is the code

MAIN CODING THEORY PROBLEM

Find codes with large rate R (for efficiency) & large d (to correct many errors)

Given alphabet A of size q ($q>1$)
& given values of n & d

let
$$A_q(n,d) = \max\{M \mid \exists \text{ an } (n,M,d) \text{ code over } A\}$$

— A code is called optimal if $|C| = A_q(n,d)$

~~Singleton~~.

— If H is the p.c.m of a code of length n, the code has min distance d iff every $d-1$ columns of H are l.i. & some d columns are l.d.

Singleton Bound C : $[n,k,d]$ code then
$$n-k \geq d-1$$
or
$$d \leq n-k+1$$

□ $H_{n-k \times n}$ $\quad rank(H) = n-k$
$= \max.$ no. of l.i. columns

$\therefore \quad d-1 \leq n-k$

or $\boxed{d \leq n-k+1}$

MDS code Codes for which $d = n-k+1$ called Maximum distance separable codes (MDS).

Plotkin Bound

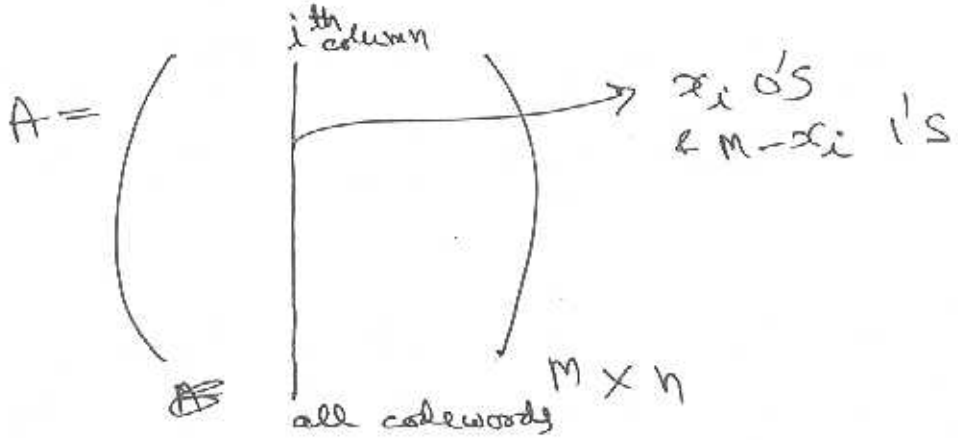
For any (n,M,d) code C for which $n < 2d$ we have
$$M \leq 2\left\lfloor \frac{d}{2d-n} \right\rfloor$$

□
$$\sum_{u \in C} \sum_{v \in C} dist(u,v)$$

① $\because$ $dist(u,v) \geq d$ $\therefore$ if $u \neq v$

$$Sum \geq M(M-1)\,d$$

②



$\therefore$ i^{th} column contributes $2x_i(M - x_i)$ to the sum

0 1
1 0

$$Sum = \sum_{i=1}^{n} 2x_i(M - x_i)$$

When this sum is maximum?

Case ① M is even then it is max. when $x_i = \frac{M}{2}$

& $Sum \leq \frac{1}{2} n M^2$ $\quad \sum_{i=1}^{n} 2 \cdot \frac{M}{2} \cdot \frac{M}{2}$

$\therefore$ $M(M-1)\,d \leq \frac{1}{2} n M^2$

or $M \leq \frac{2d}{2d-n}$

$\because$ M is even

$$\Rightarrow M \leq 2\left\lfloor \frac{d}{2d-n} \right\rfloor$$

Case ② M is odd $\quad Sum \leq n\,\frac{(M^2-1)}{2}$

$$\therefore M \leq \frac{n}{2d-n} = \frac{2d}{2d-n} - 1$$

$$\Rightarrow M \leq \left\lfloor \frac{2d}{2d-n} \right\rfloor - 1 \leq 2\left\lfloor \frac{d}{2d-n} \right\rfloor$$

$\because$ $\lfloor 2x \rfloor \leq 2\lfloor x \rfloor + 1$

Hadamard Matrix

$H = (\pm 1)_{n \times n}$ s.t. $HH^t = nI$

$\langle R_i, R_j \rangle = 0$ $(\because H^{-1} = (\frac{1}{n})H^t \Rightarrow H^t H = nI)$

$\therefore \langle c_i, c_j \rangle = 0$

— Normalized Hadamard Matrix $R_1 = (11\cdots1)$, $c_1 = (11\cdots1)$

$n=1$ $H_1 = (1)$ $\quad n=2$ $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$n=4$ $H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

Theorem If a Hadamard matrix H of order n exists then $n = 1, 2$ or $n \equiv 0 \pmod 4$ i.e. $n = 4K$

□ W.L.O.G. Suppose H is normalized. Suppose $n \geq 3$ $(n \geq 3)$

R_1 1 1 1 ⋯ 1 | 1 1 ⋯ 1 | 1 1 ⋯ 1 | 1 1 ⋯ 1

R_2 1 1 ⋯ 1 | 1 1 ⋯ 1 | − − ⋯ − | − − ⋯ −

R_3 1 1 ⋯ 1 | − − ⋯ − | 1 1 ⋯ 1 | − − ⋯ −

i j k l

$\because$ Rows are orthogonal $\Rightarrow$

$$\left.\begin{aligned} i + j - k - l &= 0 \\ i - j + k - l &= 0 \\ i - j - k + l &= 0 \end{aligned}\right\} \Rightarrow i = j = k = l \Rightarrow n = 4i$$

a multiple of 4

Conjecture Hadamard matrix exist whenever order is a multiple of 4 (No proof is known yet).

Construction (1) (Sylvester) If H_n is a Hadamard matrix of order n then $H_{2n} = H_n \otimes H_2 = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$ (of order 2n)

$\therefore$ if u start with $H_1 = (1)$ this gives $H_2, H_4, H_8, \ldots$

$\therefore$ Hadamard matrix of all orders which are powers of 2.

Quadratic residues

$p \neq 2$ prime

— Non zero squares mod p i.e. the numbers

$1^2, 2^2, 3^2, \ldots \pmod p$ called the q.r. mod p

$\because (p-a)^2 \equiv (-a)^2 \equiv a^2 \pmod p$

We consider $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod p$

$p = 11$

$1^2 = 1 \quad 2^2 = 4, \; 3^2 = 9, \; 4^2 = 16 = 5$

$5^2 = 25 \equiv 3$

$\therefore$ Q.R. $= \{1, 3, 4, 5, 9\}$

Q.N.R. $= \{2, 6, 7, 8, 10\}$

$A \equiv B \pmod c$
$\Rightarrow c \mid A-B$
or $A-B$ is $\times$ of c.

Properties

(1) q.r. $\times$ q.r. $=$ q.r.
q.n.r $\times$ q.n.r $=$ q.r
q.r $\times$ q.n.r $=$ q.n.r

(2) If $p = 4k+1$ then -1 is a q.r. mod p
if $p = 4k+3$ then -1 is a q.n.r. mod p

(3) $p \neq 2$ prime $\quad \chi \rightarrow$ Legendre symbol

$\chi(i) = 0$ if i is a multiple of p

$\chi(i) = 1$ if the remainder when $i \pmod p$ is q.r.

$= -1$ if $i \pmod p$ is q.n.r.

Jacobsthal matrix

$Q = (q_{ij})_{p \times p}$ $\quad q_{ij} = \chi(j-i)$

$p = 7$

$$Q = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{bmatrix} \end{array}$$

$n = p+1 \equiv 0 \pmod 4$

$q_{ij} = \chi(j-i) = \chi(-1)\chi(i-j) = -q_{ij}$

$$H = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1}^t & Q - I \end{pmatrix}$$

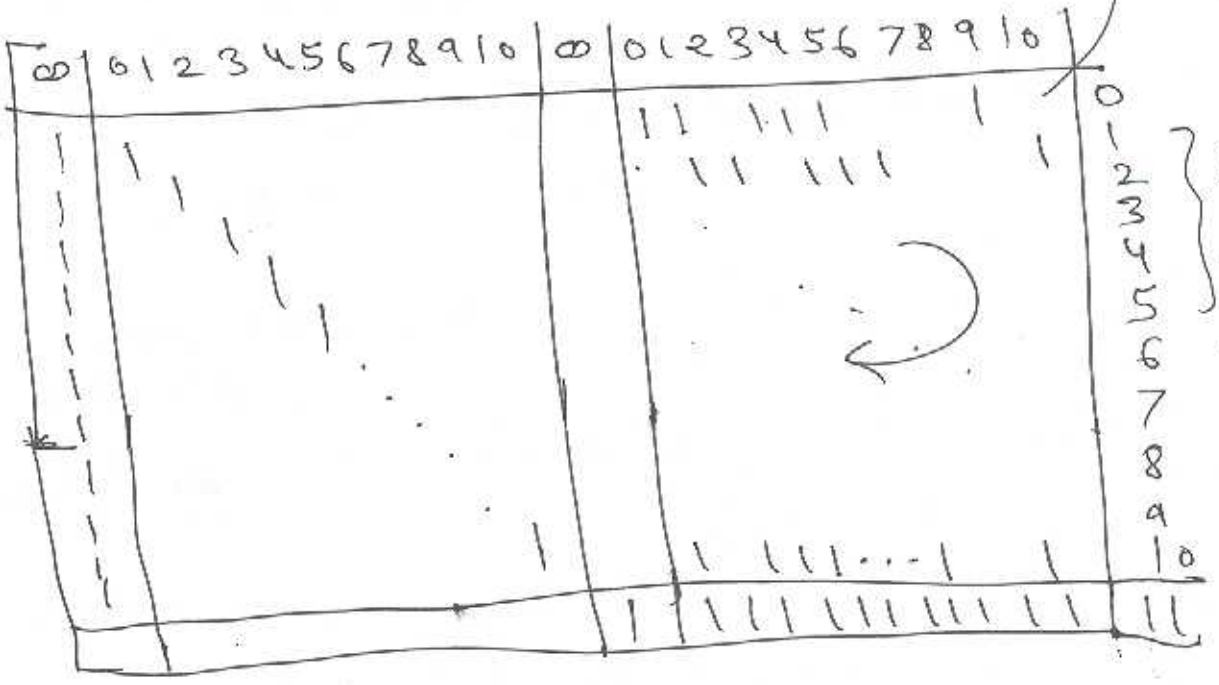
$HH^t = (p+1) I_p$

normalized Hadamard matrix

Paley type Hadamard matrix

Extended Golay Code : $[24, 12]$

$G =$



Lemma (1) G_{24} is self dual: $G_{24} = G_{24}^{\perp}$

(Voyager 1 & 2 spacecraft 1977 used Golay code)

(2) Wt. of every codeword of Golay code is multiple of 4

~~(3) $d = 8$ (∵ there is no codeword of wt. 4~~

(3) G_{24} contains all one vector $\bar{1} = 111\ldots1$

(4) If $\bar{c} = (L|R) = (a_0 a_0 a_1 \ldots a_{10} | b_0 b_0 b_1 \ldots b_{10}) \in G_{24}$

$\Rightarrow \hat{\bar{c}} = (L'|R') = (b_0 b_0 b_1 \ldots b_{10} | a_0 a_0 a_1 \ldots a_{10})$ also $\in G_{24}$

Thus

(5) If $\bar{c} = (L|R) \in G_{24}$ s.t. $wt(L) = i$, $wt(R) = j$

$\Rightarrow \exists\ (L'|R') \in G_{24}$ s.t. $wt(L') = j$ & $wt(R') = i$

∵ Possible wts are $x \not\equiv 4$

$\Rightarrow$ They are $0, 4, 8, 12, 16, 20, 24$

If $\bar{u} \in G_{24}$ s.t. $wt(u) = 20$ then $wt(\bar{u}+\bar{1}) = 4$

(6) There is no codeword of wt. 2 ($\Leftrightarrow$ no codeword of wt. 2 or 4)

□ for any $(L|R) \in G_{24}$ $wt(L) \equiv wt(R) \equiv 0 \pmod 2$

Now a codeword of wt. 4 can occur in one of the two ways

(i) $wt(L) = 0$, $wt(R) = 4$ ↗ This is not possible

OR (ii) $wt(L) = 2$, $wt(R) = 2$

$\Rightarrow$ Possible wts are 0, 8, 12, 16, 24

A_i = # of words of wt. i

$\Rightarrow$ $A_0 = A_{24} = 1$ $\quad A_8 = A_{16}$

i:	0	8	12	16	24
A_i:	1	759	2576	759	1

min dis $d = 8$ $\Rightarrow$ 3 error correcting

perfect

Binary Golay code

G_{23} = 12 x 23 matrix

$G_{23} = (I_{12} | \hat{A})$ $\quad \hat{G} = (I_{12} | \hat{A})$ 12×11

by deleting last column

$G_{23}: [23, 12, 7]$; Binary Golay code

i	0	7	8	11	12	15	16	23
A_i	1	253	506	1288	1288	506	253	1

Ternary Golay code Extended

$G_{12} = (I_6 | B)$

$B = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$ 6×6

C_{12}: $[12, 6, 6]_3$

C_{11}: $[11, 6, 5]_3 \rightarrow$ Perfect code Puncture in last coordinate.

— Web * Takes n, k, d

— Hadamard Matrices

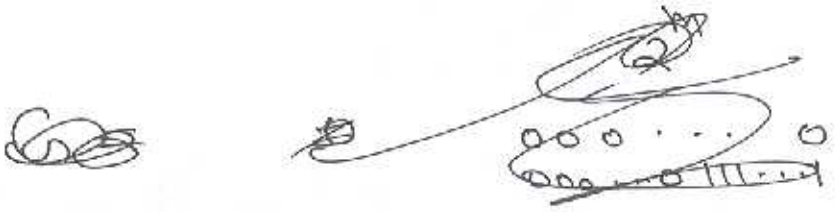
—.

Reed Muller Code

$0 \le r \le m$

$RM(r,m) : [2^m, k, d]_2$

$= \{$ Set of all vectors $\bar{f}$ where $f(v_1, v_2, \ldots, v_m)$ is a Boolean fn. (a poly of deg $\le r\}$



$G(r,m)$ =

1111 111	$\bar{1}$	deg 0
00 . . . 0 111 . . . 1	v_m	
0 . . . 011 . . . 1 000 . . . 0111 . . . 1	v_{m-1}	deg 1
0101010 . . . 0101010	v_1	
	$v_1 v_2$	
	$v_1 v_3$	deg 2
	⋮	
		deg r

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$$

$$RM(1,3) = \{a_0 \bar{1} + a_1 \bar{v_1} + a_2 \bar{v_2} + a_3 \bar{v_3} \mid a_i \in \{0 \text{ or } 1\}\}$$

Theorem

$$R(r+1, m+1) = \{(u \mid u+v) \mid u \in R(r+1, m),\ v \in R(r, m)\}$$

$$G(r+1, m+1) = \begin{pmatrix} G(r+1, m) & G(r+1, m) \\ 0 & G(r, m) \end{pmatrix}$$

Theorem $\quad d(R(r,m)) = 2^{m-r}$

Theorem $\quad RM(m-r-1, m) = R(r,m)^{\perp} \quad 0 \le r \le m-1$

Codes over $\mathbb{Z}_4$:

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\mathbb{Z}_4^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{Z}_4\}$ Module

$\mathcal{C} \subseteq \mathbb{Z}_4^n$ (subset)

$\mathcal{C} \leq \mathbb{Z}_4^n$ submodule

$\mathcal{C} : [n, k, d_H, d_L]_2$ $\quad |\mathcal{C}| = 2^k = 4^{k_0} \cdot 2^{k_1}$

$k = 2k_0 + k_1$

$$G = \begin{bmatrix} I_{k_0} & A & B_1 + 2B_2 \\ 0 & 2I_{k_1} & 2C \end{bmatrix}$$

A, B_1, B_2, C are binary matrices

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix} \quad \& \quad G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 2 \\ 0 & 2 & 0 & 2 \end{bmatrix}$$

2 codes

Lee wt.

$w_L(0) = 0$
$w_L(1) = 1$
$w_L(2) = 2$
$w_L(3) = 1$

$\bar{x} \in \mathbb{Z}_4^n \qquad w_L(\bar{x}) = \sum_{i=1}^{n} w_L(x_i)$

Lee distance

$d_L(\bar{x}, \bar{y}) = w_L(\bar{x} - \bar{y})$

Gray Map

$$\mathbb{Z}_4 \to \mathbb{Z}_2^2$$

$0 \to 00$
$1 \to 01$
$2 \to 11$
$3 \to 10$

$\phi : (\mathbb{Z}_4^n, \text{Lee distance}) \longmapsto ((GF(2))^{2n}, \text{Hamm. dist.})$
isometry.

Inner ×:

$$\bar{x} \cdot \bar{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \pmod 4$$

$$\mathcal{C}^{\perp} = \{ \bar{x} \in \mathbb{Z}_4^n \mid \bar{x} \cdot \bar{c} = 0 \ \forall \ \bar{c} \in \mathcal{C} \}$$

– self orthogonal $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ & self dual $\mathcal{C} = \mathcal{C}^{\perp}$

$$G^{\perp} = \begin{bmatrix} -(B_1 + 2B_2)^t - C^t A^t & C^t & I_{n-k_0-k_1} \\ 2A^t & 2I_{k_1} & 0 \end{bmatrix}$$

Basic L.A. over $\mathbb{Z}_4$

$$g(x) = x^3 + x + 1 \mid x^7 - 1$$

Lift $g(x) \longrightarrow G(x) = x^3 + 3x^2 + 2x + 3 \mid x^7 - 1$ over $\mathbb{Z}_4$

$G(x) \bmod 2 \to g(x)$

Add zero dok symbol

∞ 0 1 2 3 4 5 6

$$\begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}$$

Octacode

$$G = \begin{bmatrix} 1000 & 3121 \\ 0100 & 1231 \\ 0010 & 3332 \\ 0001 & 2311 \end{bmatrix}$$

self dual

$O_8 : [8, 8, 4, 6]$ $\quad |O_8| = 4^4$

$d_H \quad d_L$

$d_L = 6$

$$G = \begin{bmatrix} 2000 & 1311 \\ 2011 & 2231 \\ 0101 & 2301 \\ 1111 & 1111 \end{bmatrix}$$

$A(16, 6) \leq 2^8 = 256$

$(16, 256, 6)$ N.R. code

$P(m) : (2^m, 2^{(2^m - 2m)}, 6)$

$K(m) : \left(2^m, 2^{2m}, 2^{m-1} - 2^{\frac{(m-2)}{2}}\right)$

$m \geq 4$ mercen

For $m = 4$

$P(4) = K(4) =$ N. Robinson code

$|P(m)| \cdot |K(m)| = 2^{2m}$

Residue code

$$\mathcal{C}^{(1)} = \{\mathcal{C} \pmod 2\}$$

$$\mathcal{C}^{(2)} = \left\{ \frac{\bar{c}}{2} : \bar{c} \in \mathcal{C} \;\&\; c_i \equiv 0 \pmod 2 \;\forall i \right\}$$

$$G^{(1)} = [I_{k_0} \; A \; B_1]$$

$$G^{(2)} = \begin{bmatrix} I_{k_0} & A & B_1 \\ 0 & I_{k_1} & C \end{bmatrix}$$

More is diff.
Europhys Letter 86 (2009) 27003

— Betweenness metric

— geodesic

— Assortativity Newman 2002

— multiple metrics in networks. Europhysics letters 86 (2009)

New growth in — ~~Complex~~ assing graphs

Cyclic Codes

Feb 23, 2010

Def: A code $\mathcal{C}$ is called cyclic if

(i) $\mathcal{C}$ is a linear code

(ii) Any cyclic shift of codeword is also a codeword.

$$c_0 c_1 \dots c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1} c_0 c_1 \dots c_{n-2} \in \mathcal{C}$$

Ex: ① $\{000, 101, 011, 110\}$ cyclic

② $\{0000, 1001, 0110, 1111\}$ is not cyclic

$\sim \{0000, 1010, 0101, 1111\}$ interchanging 3rd & 4th coord.

③ $\{11111\} \subset \mathbb{F}_2^5$ not cyclic code

④ $\{0112, 2011, 1201, 1120\} \subset \mathbb{F}_3^4$ not cyclic code

⑤ $\{\bar{0}\}$, $\{\lambda \cdot \bar{1} \mid \lambda \in \mathbb{F}_2\}$ & $\mathbb{F}_2^n$

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

cyclicity reduces to $c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}$

$x \cdot c(x) \in \mathcal{C}$ iff $x^n = 1$

$$\mathbb{F}_q[x] = \{ f_0 + f_1 x + f_2 x^2 + \dots + f_m x^m \}$$
$$\forall\, f_i \in \mathbb{F}_q$$

Set of all polynomials over $\mathbb{F}$ of deg m

Polynomial Ring

- added
- subtracted
- multiplied

- This is not a field (why?) poly.s of deg $\neq 0$ do not have multiplicative inverse.

Division Algo for Poly.

$\forall$ pair of polys $a(x) \& b(x) \neq 0$ in $\mathbb{F}_q[x]$

$\exists$! pair of polys $q(x)$ (quotient) & $r(x)$ (remainder) s.t.

$$a(x) = q(x)\, b(x) + r(x)$$

where $\deg r(x) < \deg b(x)$

Ex. in $\mathbb{F}_2[x]$ $\qquad \mathbb{Z}_2[x]$

$$\begin{array}{r|l} & x+1 \\ \hline x^2+x+1 & x^3 + x + 1 \\ & x^3 + x^2 + x \\ \hline & x^2 + 1 \\ & x^2 + x + 1 \\ \hline & x \end{array}$$

Def: (Ideal) $\quad R \to$ Ring

$I \subseteq R$ called Ideal if $I \neq \phi$

(1) $a+b$ & $a-b \in I$ $\forall$ $a, b \in I$

(2) $r \cdot a \in I$ $\forall$ $r \in R$ & $a \in I$

Ex. $\mathcal{C} = \{000, 110, 101, 011\}$

$\pi: \mathbb{F}_2^{\,n} \longmapsto \mathbb{F}_2[x]/(x^n-1) = R_n$ (Poly. ring mod. x^n-1)

$(c_0 c_1 \cdots c_{n-1}) \longmapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

$I = \{0, 1+x, 1+x^2, x+x^2\} \subset \mathbb{F}_2[x]/x^3-1$ ideal

Ex. $\mathbb{Z}$ (Ring) $\quad 2\mathbb{Z}$ ~~ideal~~ ideal in $\mathbb{Z}$.

Ex-3 $\mathbb{F}_2[x]$ for a given poly $f(x) \neq 0$ all the polys divisible by $f(x)$ form an ideal.

Ex-4 : $\mathbb{F}_2[x]/(x^n-1)$ if $g(x) \mid x^n-1$ all the polys divisible by $g(x)$ form an ideal.

Def: R ring, I Ideal — I → Principal Ideal (P.I.) if $\exists$ an element $g \in I$ s.t. $I = \langle g \rangle$

$\langle g \rangle := \{gr \mid r \in R\}$

$g \to$ generator of I or I is gen. by g.

- Ring R is called PIR (Principal Ideal Ring) if every ideal of R is principal.
- Generators of P.I. may not be 1.

Ex.. $R_3 = \mathbb{F}_2[x]/(x^3-1)$ $I = \{0, 1+x, x+x^2, 1+x^2\}$ ↓ P.I. gen by $(1+x)$

$I = \langle 1+x \rangle$

$0 \cdot (1+x) = 1+x^3 = 0 = (1+x+x^2)\cdot(1+x)$

$1 \cdot (1+x) = 1+x = (x+x^2)(1+x)$

$x \cdot (1+x) = x+x^2 = (1+x^2)(1+x)$

$x^2(1+x) = 1+x^2 = (1+x)(1+x)$

Th. The rings $\mathbb{Z}$, $\mathbb{F}_2[x]$ & $\mathbb{F}_2[x]/(x^n-1)$ are all P.I.R.

Th. The ring $\mathbb{F}_2[x]/f(x)$ is a field $\iff$ $f(x)$ is irreducible in $\mathbb{F}_2[x]$.

($\mathbb{Z}_m$ is a field $\iff$ m is prime)

Th. A code $\mathcal{C}$ in R_n is cyclic code iff @ $\mathcal{C}$ satisfies the following

(i) $a(x), b(x) \in \mathcal{C} \Rightarrow a(x)+b(x) \in \mathcal{C}$

(ii) $a(x) \in \mathcal{C}$ & $r(x) \in R_n \Rightarrow r(x)\, a(x) \in \mathcal{C}$
(closed under × w.r.t. any element of R_n)

Def $f(x) \in R_n$ $\quad \langle f(x) \rangle = \{ r(x) f(x) \mid r(x) \in R_n \}$
Cyclic code gen. by $f(x)$

Ex. $R_3 = \mathbb{F}_2[x]/(x^3-1)$

$\mathcal{C} = \langle 1+x^2 \rangle$ Multiply $1+x^2$ by each of elements of R_3 mod x^3-1 producing only 4 distinct codes

$\{0, 1+x, 1+x^2, x+x^2\}$

Th. $\mathcal{C}$ $(\neq 0)$ cyclic code in R_n. Then

(1) $\exists$ a ! monic poly $g(x)$ of smallest deg in $\mathcal{C}$

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

(3) $g(x)$ is a factor of x^n-1

□ (1) Suppose $g(x)$ & $h(x)$ (both monic poly in $\mathcal{C}$ of smallest deg)
$\Rightarrow g(x)-h(x) \in \mathcal{C}$ ← has smaller deg. #

(2) Suppose $a(x) \in \mathcal{C}$ s.t. $a(x) = q(x)\, g(x) + r(x)$
$\Rightarrow r(x) = a(x) - q(x) g(x) \in \mathcal{C}$
Contradiction — $\deg r(x) < \deg g(x)$
(4) $\Rightarrow \deg r(x) =$ smallest deg $g(x)$ is of

(iii) By div. algo

$$x^n - 1 = q(x)\, g(x) + r(x), \quad \deg r(x) < \deg g(x)$$

$$\Rightarrow r(x) \equiv -q(x)\, g(x) \pmod{x^n - 1}$$

$$\Rightarrow r(x) \in \langle g(x) \rangle$$

By minimality of deg $g(x)$ we must have $r(x) = 0$.

$$\Rightarrow g(x) \mid x^n - 1$$ ▨

$g(x) \rightarrow$ gen. poly of cyclic code

(iv) If $g(x) = g_0 + g_1 x + \cdots + g_r x^r$

then $\mathcal{C}$ is gen. by (as a subspace of $\mathbb{F}_2^n$) the rows of gen. matrix

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{r-1} & g_r & & & \\ & & & & & & & & \\ 0 & \cdots & 0 & & & g_0 & \cdots & & g_r \end{bmatrix}$$

Ex. $x^3 - 1 = (x+1)(x^2+x+1)$

irr. poly. irr. poly.

All binary cyclic codes of length 3

Gen. Poly.	Code in R_3	Code in $\mathbb{F}_2^3$
1	all of R_3	all of $\mathbb{F}_2^3$
$x+1$	$\{0, 1+x, x+x^2, 1+x^2\}$	$\{000, 110, 011, 101\}$
x^2+x+1	$\{0, 1+x+x^2\}$	$\{000, 111\}$
$x^3-1=0$	$\{0\}$	$\{000\}$

$\mathcal{C}$ cyclic $[n, k]$ code with gen. poly $g(x)$

$g(x) \mid x^n - 1 \Rightarrow x^n - 1 = g(x) h(x)$

for some poly $h(x)$ ↓ check poly.

$\because g(x)$ is monic $\Rightarrow h(x)$ is monic

$g(x)$ has deg $n-k \Rightarrow h(x)$ has deg. k.

Ex. $x^6 - 1 = (1+x)^2 (1+x+x^2)^2$ Binary cyclic ~~Code~~

n	Factorization of $x^n - 1$	No. of cyclic codes
1	$1+x$	2
2	$(1+x)^2$	3
3	$(1+x)(1+x+x^2)$	4
4	$(1+x)^4$	5
5	$(1+x)(1+x+x^2+x^3+x^4)$	4
6	$(1+x)^2(1+x+x^2)^2$	9
7	$(1+x)(1+x^2+x^3)(1+x+x^3)$	8
8	$(1+x)^8$	9
9	$(1+x)(1+x+x^2)(1+x^3+x^6)$	8
10	$(1+x)^2(1+x+x^2+x^3+x^4)^2$	9

Cyclic Codes

Feb 24, 2010

How many cyclic codes of length n?

– Let $x^n-1 \in \mathbb{F}_q[x]$ s.t. $x^n-1 = \prod_{i=1}^{r} p_i(x)^{e_i}$

$p_i(x)$ distinct monic irr. polys & $e_i \geq 1$
$1 \leq i \leq r$

then there are $\prod_{i=1}^{r}(e_i+1)$ cyclic codes of length n over $\mathbb{F}_q$.

Ex. ① $x^7-1 = (1+x)(1+x^2+x^3)(1+x+x^3) \in \mathbb{F}_2[x]$

There are only 2 binary $[7,3]$-cyclic codes:

$\langle (1+x)(1+x^2+x^3) \rangle = \{ 0000000, 1110100, 0111010, 0011101, 1001110, 0100111, 1010011, 1101001 \}$

&

$\langle (1+x)(1+x+x^3) \rangle = \{ 0000000, 1011100, 0101110, 0010111, 1001011, 1100101, 1110010, 0111001 \}$

Ex-2 $x^7-1 = (2+x)(1+x+x^2+x^3+x^4+x^5+x^6) \in \mathbb{F}_3[x]$

We do not have any ternary $[7,2]$ cyclic codes.

Th. Let $g(x)$ gen. poly of an ideal of $\mathbb{F}_2[x]/\langle x^n-1 \rangle$ then the corresponding cyclic code has dim k if the deg $g(x)$ is $n-k$

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

$\leq n-1 \quad \leq k-1 \quad \leq n-k$

$c(x) = m(x)\, g(x)$

$(c_0+c_1x+\cdots+c_{n-1}x^{n-1}) = (m_0+m_1x+\cdots+m_{k-1}x^{k-1})(g_0+g_1x+\cdots+g_{n-k}x^{n-k})$

☐ Consider the set

$$S := \{ g(x)\, c(x) \mid c(x) \in \mathbb{F}_q[x]/(x^n-1),\ \deg(c(x)) \le k-1 \}$$

$|S| = ?$ ∵ For two polys $c_1(x) \neq c_2(x)$

s.t. $\deg(c_1(x)) \le k-1$, $\deg(c_2(x)) \le k-1$

$$g(x)c_1(x) \not\equiv g(x)c_2(x) \pmod{x^n-1}$$

$$|S| = q^k$$

$$\therefore S \subseteq \langle g(x) \rangle$$

On the other hand

for any codeword $g(x)\,a(x)$ with $a(x) \in \mathbb{F}_q[x]/(x^n-1)$

$$a(x)g(x) = u(x)\cdot(x^n-1) + v(x)$$

$$\deg(v(x)) < n$$

$$\Rightarrow v(x) = a(x)g(x) - u(x)(x^n-1)$$

$$\Rightarrow g(x) \mid v(x)$$

$\Rightarrow$ write $v(x) = g(x)\,b(x)$ for some poly $b(x)$

then $\deg(b(x)) < k$

$\therefore v(x) \in S$ (∵ cyclic code has dim k)

$$\Rightarrow \langle g(x) \rangle \subseteq S \Rightarrow S = \langle g(x) \rangle$$

$\Rightarrow |\mathcal{C}| = q^k \Rightarrow \dim \mathcal{C} = k$

$$g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$$

$$C = \langle g(x) \rangle \qquad \deg(g(x)) = n-k$$

$$G = \begin{bmatrix} g(x) \\ x\,g(x) \\ \vdots \\ x^{k-1} g(x) \end{bmatrix} = \begin{bmatrix} g_0 \cdots g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & \\ & & & \\ 0 & 0 & \cdots & g_0\ g_1 \cdots g_{n-k} \end{bmatrix}$$

is gen. matrix of C.

Ex. $[7,4]_2$ cyclic code $C = \langle 1 + x^2 + x^3 \rangle$

$$G = \begin{bmatrix} g(x) \\ x\,g(x) \\ x^2 g(x) \\ x^3 g(x) \end{bmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Th. Let C_1 & C_2 be cyclic codes over $\mathbb{F}_2$ with gen. poly $g_1(x)$ & $g_2(x)$. Then

$C_1 \subseteq C_2$ iff $g_2(x) \mid g_1(x)$

Th. The dual code of a cyclic code is cyclic.

Cyclic codes

Feb 26, 2010

$\mathcal{C}$ is a cyclic code with gen. poly $g(x)$

$[n, k]$

$$g(x) \mid x^n - 1$$

$$x^n - 1 = g(x)\, h(x)$$

↳ check poly.

$$\deg g(x) = n - k \qquad \therefore \deg h(x) = k$$

$$\langle h(x) \rangle = \mathcal{C}' \quad \text{but } \mathcal{C}' \neq \mathcal{C}^{\perp} = \langle g(x) \rangle^{\perp}$$

may not be

Th. $\mathcal{C} \leq R_n$ & chk poly. $= h(x)$

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

then $c(x)$ of R_n is a codeword of $\mathcal{C}$ iff $c(x) \cdot h(x) = 0$

an element

Note in R_n, $g(x)\, h(x) = x^n - 1 = 0$

□

$c(x) \in \mathcal{C} \Rightarrow c(x) = a(x)\, g(x)$ for some $a(x) \in R_n$

$\Rightarrow c(x) \cdot h(x) = a(x) \cdot g(x)\, h(x) = 0$

On the other hand if $c(x) \cdot h(x) = 0$ By div. algo

$$c(x) = q(x)\, g(x) + r(x) \qquad \deg r(x) < n - k$$

Thus $c(x)\, h(x) = 0 \Rightarrow r(x) \cdot h(x) = 0$

$\Rightarrow r(x)\, h(x) \equiv 0 \pmod{x^n - 1}$

But $\deg (r(x)\, h(x)) < n - k + k = n$

$\therefore r(x) h(x) = 0$ in $\mathbb{F}_2[x]$

$\Rightarrow r(x) = 0$

$\Rightarrow c(x) = q(x)\, g(x) \in \mathcal{C}$ ▨

Note: $\dim \langle h(x) \rangle = n-k = \dim(\mathcal{C}^\perp)$

but $\langle h(x) \rangle \neq \langle g(x) \rangle^\perp$ need not be

Th. $\mathcal{C} = \langle g(x) \rangle$ $[n, k]$ chk poly $h(x)$

$h(x) = h_0 + h_1 x + \cdots + h_k x^k$

then, (i) p.c.m. for $\mathcal{C}$ is

$$H = \begin{bmatrix} h_k & h_{k-1} \cdots h_0 & 0 & 0 \cdots 0 \\ 0 & h_k \cdots & h_0 \cdots & 0 \\ & & & \\ 0 & 0 \cdots & h_k h_{k-1} \cdots & h_0 \end{bmatrix}$$

$= \begin{pmatrix} h_R(x) \\ x\, h_R(x) \\ \vdots \\ x^{n-k-1} h_R(x) \end{pmatrix}$

(ii) $\mathcal{C}^\perp = \langle h^*(x) \rangle$ Reciprocal poly.

$h^*(x) = h_k + h_{k-1} x + \cdots + h_0 x^k$

□ (1) $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ is a codeword iff $c(x) h(x) = 0$ ($\because h(x)$ is of deg k)

$\Rightarrow$ coeff of $x^k, x^{k+1}, \ldots, x^{n-1}$ must be zero

i.e.,

$$c_0 h_k + c_1 h_{k-1} + \cdots + c_k h_0 = 0$$
$$c_1 h_k + c_2 h_{k-1} + \cdots + c_{k+1} h_0 = 0$$
$$\vdots$$
$$c_{n-k-1} h_k + \cdots + c_{n-1} h_0 = 0$$

$\Rightarrow$ Any codeword $c_0 c_1 \ldots c_{n-1}$ of $\mathcal{C}$ is $\perp$ to the v^r $h_k h_{k-1} \ldots h_0 0 0 \ldots 0$ and to its cyclic shifts.

∴ Rows of H (in Th.) are all codewords of $\mathcal{C}^\perp$

∴ $h(x)$ is monic of deg K ∴ $h_K = 1$

⇒ Rows of H are l.i.

# of rows of H $= n-k = \dim \mathcal{C}^\perp$

⇒ H is gen. matrix of $\mathcal{C}^\perp$ i.e. p.c.m. of $\mathcal{C}$.

(2) Claim $h^*(x) = x^K h(x^{-1}) \mid x^n - 1$

Now $h(x^{-1})\, g(x^{-1}) = (x^{-1})^n - 1$

$\Rightarrow \underbrace{x^K h(x^{-1})}_{h^*(x)}\, x^{n-K} g(x^{-1}) = x^n (x^{-n} - 1) = 1 - x^n$

$\Rightarrow h^*(x) \mid x^n - 1$

$\Rightarrow \langle h^*(x) \rangle$ is a cyclic code with gen. matrix H

$\Rightarrow \langle h^*(x) \rangle = \mathcal{C}^\perp$

Ex. $\mathcal{C} : [7,4]$ $g(x) = 1 + x^2 + x^3$

$h(x) = x^7 - 1 \,/\, g(x) = 1 + x^2 + x^3 + x^4$

$h^*(x) = 1 + x + x^2 + x^4$

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$ p.c.m of $\mathcal{C}$.

Ex. $x^{23} - 1 = (x-1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$

$(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$

$= (x-1)\, g_1(x)\, g_2(x)$

$\mathcal{C}_1 = \langle g_1(x) \rangle$ $\mathcal{C}_2 = \langle g_2(x) \rangle$ $\mathcal{C}_2 \sim \mathcal{C}_1$

$[23, 12]$ binary Golay code

(3) $g_1(x) + g_2(x)$ are reciprocals of each other

Systematic cyclic code

Decoding of cyclic codes

March 9 2016

Let $H = (I_{n-k} | A)$ p.c.m. of a q-ary cyclic code $\mathcal{C} = \langle g(x) \rangle$ then syndrome of $\overline{w} \in \mathbb{F}_q^n = \big(w(x) \pmod{g(x)}\big)$

□ Let $a_i(x)$ is the poly. of deg $\leq n-k-1$ for the i^{th} column of A

$$\Rightarrow A = (a_0(x), a_1(x), \dots, a_{k-1}(x))$$

but $G = (-A^T | I_k)$ is a gen. matrix for $\mathcal{C}$

$\Rightarrow$ $x^{n-k+i} - a_i(x)$ is a codeword of $\mathcal{C}$.

$$\Rightarrow x^{n-k+i} - a_i(x) = q_i(x)\, g(x) \qquad q_i(x) \in \mathbb{F}_q[x]/(x^q)$$

$$\Rightarrow a_i(x) = x^{n-k+i} - q_i(x)\, g(x)$$

$$w(x) = w_0 + w_1 x + \dots + w_{n-1} x^{n-1}$$

$$s = Hy^T = \qquad s(w) = Hw^T$$

$$s(x) = w_0 + w_1 x + \dots + w_{n-k-1} x^{n-k-1} + w_{n-k} a_0(x) + \dots + w_{n-1} a_{k-1}(x)$$

$$= \sum_{i=0}^{n-k-1} w_i x^i + \sum_{j=0}^{k-1} w_{n-k+j} \left(x^{n-k+j} - q_j(x)\, g(x) \right)$$

$$= \sum_{i=0}^{n-1} w_i x^i - \left(\sum_{j=0}^{k-1} w_{n-k+j} q_j(x) \right) g(x)$$

$$\equiv w(x) \pmod{g(x)}.$$

Example $[7,4,3]_2$ Hamming code $\qquad g(x) = 1 + x^2 + x^3$

$H = (I_3 | A)$, $\quad A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$ $\qquad w = 0110110$

$s = 010$

$$w(x) = x + x^2 + x^4 + x^5 = x + x^2 g(x)$$

$$\Rightarrow w(x) \pmod{g(x)} = x$$

$w(x) - s(x) \in \mathcal{C}$ is a codeword.

Theorem $C = \langle g(x) \rangle$ if $w(x) \to$ received word

remainder $s(x)$ of $w(x)$ by mod $g(x)$ has wt. $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$

then $s(x)$ is the error pattern of $w(x)$ i.e.,

$w(x)$ is decoded to $w(x) - s(x)$ by $M(s)$.

Finite Fields

March 15, 2010

$\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\}$, $i = \sqrt{-1}$

$\uparrow$ $x^2+1=0$, $i^2+1=0$

$\mathbb{R}$

$GF(4) = \{a+\alpha b \mid a, b \in \mathbb{Z}_2\}$

$\uparrow$ $x^2+x+1=0$, $\alpha^2+\alpha+1=0$

$\mathbb{Z}_2$

$GF(2) = \{0, 1, \alpha_2, \ldots, \alpha_{2-2}\}$

0: additive identity; 1: $\times$ identity

$2 = p^m$ $\quad GF(2) = \mathbb{Z}_p$ $\quad 2 = p$

Properties of finite fields $\quad \beta (\neq 0) \in GF(2)$

— The order of β is the smallest +ve integer m s.t.

$$\beta^m = 1$$

— A poly. is irreducible if $\neq f(x)\, g(x)$ lesser deg $\forall g$

— If $t = \text{ord}(\beta)$ then $t \mid (2-1)$

— In any $GF(2)$ there are one or more elements of order $2-1$ called primitive elements.

Ex $GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$1^1 = 1$ $\quad \text{ord}(1) = 1$

$2^2 = 2$ $\quad 2^2 = 4$ $\quad 2^3 = 3$ $\quad 2^4 = 1$ $\quad \text{ord}(2) = 4$

$3^1 = 3$ $\quad 3^2 = 4$ $\quad 3^3 = 2$ $\quad 3^4 = 1$ $\quad \text{ord}(3) = 4$

$4^1 = 4$ $\quad 4^2 = 1$ $\quad \text{ord}(4) = 2$

$\therefore$ 2 & 3 are primitive elements

— The # of elements of order t is given by Euler's totient fn. $\phi(t)$

$\phi(10) = 4$ — 1, 2, 3, 4, 5, 6, 7, 8, 9 — 1, 3, 7, 9 are relprime

$\phi(p) = p-1$

$\phi(37) = 36$ $\quad \phi(1) = 1$

— $\phi(x) = x \prod_{p \mid x} \left(1 - \frac{1}{p}\right)$

p prime

$\phi(6) = \phi(2 \cdot 3) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2$

$\phi(63) = 36$ $\quad \phi(15) = 8$

— The # of elements in $GF(q)$ of order x is $\phi(x)$

Ex. $GF(16) = GF(2^4)$ — $\alpha, \alpha^2, \alpha^4$ are primitive element

$\Pi(x) = 1 + x + x^4$ — α^3 & α^5 are not.

— A poly having primitive element as a zero is called primitive poly.

Ex. $x^4 + x^3 + x^2 + x + 1$ is irr. & gen. $GF(16)$ but not a primitive poly.

— $F_q^* = GF(q)^*$ is a cyclic multiplicative gp. of order $p^m - 1$ or $q - 1$

Th. Every element $\beta \in F_q$ of order p^m satisfies the identity $\beta^{p^m} = \beta$ or β is a root of the eqn $x^{p^m} = x$

$\Rightarrow x^{p^m} - x = \prod_{\beta \in F_q} (x - \beta)$ — (2)

— In GF(q) there are exactly $\phi(q-1)$ primitive elements.

— A primitive element α is an element of order $q-1$
i.e., $\alpha^{q-1} = 1$

$\Rightarrow 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$ are must be non zero elements of GF(q)

Ex: GF(5) $= \mathbb{Z}_5$ $\quad q-1 = 4$
non zero elem = {1, 2, 3, 4}

— A finite field exist for all prime powers $GF(p^m)$

— If α is p.e. so is α^{-1}.

— If $p(x)$ is primitive so is $p^*(x) = x^m p(x^{-1})$.

— No. of primitive poly of deg m $= \phi(q-1)/m$.

Minimal polys

— FLT. $\Rightarrow$ $\beta (\neq 0) \in GF(q)$ $\beta^q - \beta = 0$
or β is root of $x^q - x = 0$. $\rightarrow$ poly has roots over & is monic GF(p)
but β may satisfy a lower deg poly.

Def: The minimal poly over GF(p) of β is the lowest deg monic poly $M(x)$ s.t. $M(\beta) = 0$

Ex In GF(16)

Elements	Minimal polys
0	x
1	$x+1$
α	x^4+x+1
α^2	x^4+x^3+1
α^3	$x^4+x^3+x^2+x+1$
α^5	x^2+x+1

Properties of minimal poly $M(x)$ ← min poly of $\beta \in GF(2)$

(M1) $M(x)$ is irreducible

□ If $M(x) = M_1(x) M_2(x)$ · $\deg M_i > 0$

then $M(\beta) = M_1(\beta) M_2(\beta) = 0 \Rightarrow$ either $M_1(\beta) = 0$ or $M_2(\beta) = 0$

Contradicting the fact that $M(x)$ is the lowest deg poly with β as a root. ▨

(M2) If $f(x)$ is any poly. (coff in $GF(p)$) s.t. $f(\beta) = 0$ then $M(x) \mid f(x)$

□ By div. alg. $f(x) = M(x)\, q(x) + r(x)$

Put $x = \beta \Rightarrow 0 = 0 + r(\beta)$ (deg $r(x) <$ deg $M(x)$)

#

(M3) $M(x) \mid x^{p^m} - x$ or $M(x) \mid x^{2^m} - x$

□ from M_2 & FLT

(M4) deg $M(x) \leq m$

□ $GF(2)$ or $GF(p^m)$ is a v.s. of dim m over $GF(p)$

$\therefore$ Any $m+1$ elements such as

$1, \beta, \ldots, \beta^m$ are l.d.

$\Rightarrow \exists\ a_i \in GF(p)$ not all zero s.t.

$\sum_{i=0}^{m} a_i \beta^i = 0 \Rightarrow \sum_{i=0}^{m} a_i x^i$ is a poly of deg $\leq m$ having β as a root $\therefore$ deg $(M(x)) \leq m$.

(M5) The minimal poly of a p.e. of $GF(q)$ has deg m. (Such a poly is called a p.p.)

□ β p.e. of $GF(q)$ with m.p. $M(x)$ of deg d

$\therefore$ $M(x)$ will give field of order p^d but $\notin$ contain β

$\Rightarrow$ case of $GF(p^m)$ $\therefore$ $d \geq m$

$\Rightarrow d = m$. (but $d \leq m$ by M4)

(M6) β & β^p have same m.polys.

$\Rightarrow$ In h over $GF(2^m)$ β & β^2 have same m.p.

□ By example

Let $\beta \in GF(2^4)$ has m.p. x^4+x^3+1

then $(\beta^2)^4 + (\beta^2)^3 + 1 = (\beta^4+\beta^3+1)^2 = 0$

$\Rightarrow$ m.p. of $\beta^2 \mid x^4+x^3+1$ But $(\beta^2)^8 = \beta$

$\Rightarrow$ we can use same argument to show that

m.p. of $\beta \mid$ m.p of β^2 $\Rightarrow$ They are same. ▨

β & β^2 are conjugates Powers of α form into

Cyclotomic cosets

Let $p(x)$ be a minimal poly of $\alpha \in GF(q)$

$\Rightarrow p(\alpha) = 0$ Other roots of $p(x)$

Conjugates of α : $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots \alpha^{q^{d-1}}\}$

Conjugacy class of α w.r.t. $GF(q)$

GF(8)

$q=2 \quad m=3$

x^3+x+1

Conjugacy class	order	minimal poly
$\{0\}$	—	x
$\{1\}$	1	$x+1$
Same order. $\{\alpha, \alpha^2, \alpha^4\}$	7	$(x+\alpha)(x+\alpha^2)(x+\alpha^4) = x^3+x+1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	7	$(x+\alpha^3)(x+\alpha^6)(x+\alpha^5) = x^3+x^2+1$

$$(x+1)(x^3+x+1)(x^3+x^2+1) = x^7+1$$

mod 7

$C_0 = \{0\}$

$C_1 = \{1,2,4\}$

$C_3 = \{3,6,5\}$

$\pi(x) = x^3+x+1$

$000 = 0$
$100 = 1$
$010 = \alpha$
$001 = \alpha^2$
$110 = \alpha^3$
$011 = \alpha^4$
$111 = \alpha^5$
$101 = \alpha^6$
$(\alpha^7 = 1)$

Ver 1.0

α and $\beta = \nu^3$ both have minimal poly x^3+x+1

$\alpha \longleftrightarrow \nu^3$ is an isomorphism

$\pi(x) = x^3+x^2+1$

$000 = 0$
$100 = 1$
$010 = \nu$
$001 = \nu^2$
$101 = \nu^3$
$111 = \nu^4$
$110 = \nu^5$
$011 = \nu^6$
$(\nu^7 = 1)$

Ver 2.0

$1+\alpha^2 = \alpha^6$

$\updownarrow$

$1+(\nu^3)^2 = (\nu^3)^6$

Do it for GF(16)

~~x^4+x^3+1~~

x^4+x+1

$< \infty$ fields

March 19, 2010

— All finite fields of order p^m are isomorphic

— For any prime p & integer $m \geq 1$ there is a field of order p^m ; $GF(p^m)$ & it is unique.

— ① $GF(p^r) \supset GF(p^s)$ iff $s \mid r$

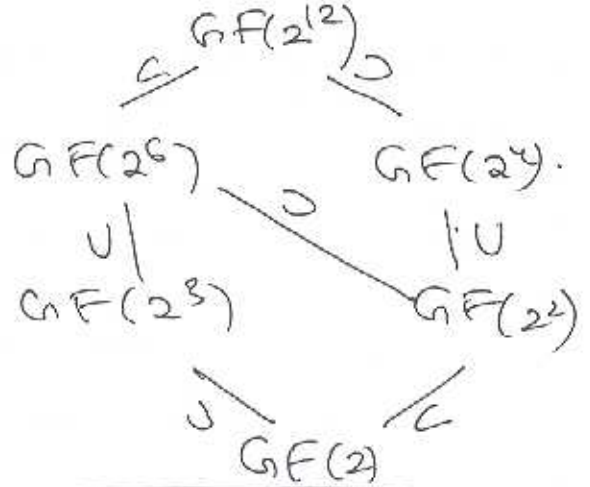
② If $\beta \in GF(p^r)$ then $\beta \in GF(p^s)$ iff $\beta^{p^s} = \beta$

In any field if $\beta^2 = \beta$ then $\beta = 0$ or 1

Lemma: If n, r, s are integers with $n \geq 2$, $r \geq 1$, $s \geq 1$ then $n^s - 1 \mid n^r - 1$ iff $s \mid r$

— In any field $x^s - 1 \mid x^r - 1$ iff $s \mid r$

① ② q.e.d. $\{x^r - 1, x^s - 1\} = x^d - 1$ where $d = \gcd\{r, s\}$



Subfields of $GF(2^{12})$

How to find irreducible polys

① $x^{p^m} - x$ = Product of all monic polys irr. over $GF(p)$ whose deg $\mid m$.

② For any field $GF(q)$, q = prime power

$x^{q^m} - x$ = Product of all monic polys irr. over $GF(q)$ whose deg $\mid m$.

Ex. $2=2$ irr. poly of deg 1

$m=1$ ↙ ↘

$x^2+x = x(x+1)$

min poly of 0 & 1 in GF(2) x & $x+1$

$m=2$

$x^{2^2}+x = x^4+x = x(x+1)(x^2+x+1)$

one irr. poly of deg 2

GF(2^2)

Element	Minimal poly
0	x
1	$M^{(0)}(x) = x+1$
α, α^2	$M^{(1)}(x) = M^{(2)}(x) = x^2+x+1$

$(x+\alpha)(x+\alpha^2)$

$x^2+\alpha^3 x+\alpha x+\alpha^3$

x^2+x+1 ✓

$m=3$

GF(2^3)

$x^{2^3}+x = x^8+x = x(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$

$= x(x+1)(x^3+x+1)(x^3+x^2+1)$

Two irr. poly of deg 3, x^3+x+1 & x^3+x^2+1 (Reciprocal polys.)

$\alpha^3+\alpha+1=0$.

Element	Minimal poly
0	x
1	$M^{(0)}(x) = x+1$
$\alpha, \alpha^2, \alpha^4$	$M^{(1)}(x) = M^{(2)}(x) = M^{(4)}(x)$
	$= (x+\alpha)(x+\alpha^2)(x+\alpha^4)$
	$= x^3+x+1$
$\alpha^3, \alpha^6, \alpha^5$	$M^{(3)}(x) = M^{(6)}(x) = M^{(5)}(x)$
	$= M^{(-1)}(x)$
	$= (x+\alpha^3)(x+\alpha^6)(x+\alpha^5) = x^3+x^2+1$

$m=4$

Cyclotomic cosets

March 16, 2010

The partition of powers of α by the conjugacy classes is called the set of cyclotomic cosets.

$GF(8)$: $\{0\}, \{1,2,4\}, \{3,6,5\}$

$GF(16)$: $\{0\}, \{1,2,4,8\}, \{3,6,12,9\}, \{5,10\}, \{7,14,13,11\}$

$GF(32)$: $\{0\}, \{1,2,4,8,16\}, \{3,6,12,24,17\}, \{5,10,20,9,18\}, \{7,14,28,25,19\}, \{11,22,13,26,21\}, \{15,30,29,27,25\}$

Set $\mathbb{Z}_{p^m-1}$ • $\times$ by p divides $\mathbb{Z}_{p^m-1}$ into cosets

The cyclotomic coset containing s consists of

$$\{s, ps, p^2s, p^3s, \ldots, p^{m_s-1}s\}$$

where m_s is smallest +ve integer

s.t. $p^{m_s} \cdot s \equiv s \bmod (p^m-1)$

mod 15 $\quad p = 2$

$C_0 = \{0\}$

$C_1 = \{1,2,4,8\}$

$C_3 = \{3,6,12,9\}$

$C_5 = \{5,10\}$

$C_7 = \{7,14,13,11\}$

$s \rightarrow$ coset representative mod $p^m - 1$.

Def: of $M^{(i)}(x)$.

$M^{(i)}(x) :=$ minimal poly of $\alpha^i \in GF(p^m)$.

By (M_6) $\quad M^{(pi)}(x) = M^{(i)}(x)$

— if $i \in C_s$ (cyclotomic coset contains s}
then in $GF(p^m)$

$$\prod_{j \in C_s} (x - \alpha^j) \;\Big|\; M^{(i)}(x)$$

(M_7) $\quad M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j)$

$\Rightarrow$

$$x^{p^m - 1} - 1 = \prod_{s} M^{(s)}(x)$$

s runs through coset reps mod $p^m - 1$.

$(Th-1)$ $x^q - x$ = Product of all monic irr. polys whose deg(m, over $GF(p)$
$(q = p^m)$

$(Th-2)$ For any f.f. $GF(q)$, $q = p^s$
$x^{q^m} - x$ = product of all monic poly irr. over $GF(q)$
whose deg $| m$.

BCH Codes

April 4, 2010

- Start with cyclic Hamming Codes:

$g(x)$ prim. poly of deg m over $GF(2)$

$GF(2)[x]/g(x)$ field of order 2^m

— α root of $g(x)$ then $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \end{bmatrix}$$

$m \times (2^m - 1)$

Use $(2^m - 1)$ non zero elements (m-tuples)

$\mathcal{C}$ with p.c.m. H is Hamming code

Ex. $m = 4$, $n = 15$

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & 14 & 15 \end{bmatrix}$$

Ex. $g(x) = x^3 + x + 1 \rightarrow GF(2)[x]/(g(x))$ is $GF(8)$

$\{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1\}$

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$1 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6$

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} = [P^t \mid I]$$

Add 4 more rows

$$H' = \begin{bmatrix} 1 & 2 & 3 & 4 & \cdots & 15 \\ f(1) & f(2) & f(3) & \cdots & & f(15) \end{bmatrix}$$

How to choose $f(i)$

BCH codes

April 7, 2010

Let $\alpha \in \mathbb{F}_{q^m}$ (primi.) $\quad M^{(i)}(x)$ = min poly of α^i w.r.t. $\mathbb{F}_q$

— A (primitive) BCH code over $\mathbb{F}_q$ of length $n = q^m - 1$ with designed distance δ $(2 \le \delta \le n)$ q-ary cyclic code gen. by $g(x) = \text{lcm}\{M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta-2)}(x)\}$ for some a

— narrow sense BCH code if $a = 1$

$$g(x) = \prod_{x \in S} (x - \alpha^x), \quad S = C_1 \cup C_2 \cup \dots \cup C_{\delta-1}$$

$$C_x = \{x q^k \bmod n \mid 0 \le k < m\}$$

q-ary cyclotomic cosets of x mod n

$BCH(n, q; \delta)$

— Parameters: $n = q^m - 1$

Th: The dim. of a q-ary BCH code of $n = q^m - 1$ gen.

① by $g(x) := \text{lcm}(M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta-2)}(x))$ is independent of α.

② $\dim = k \ge q^m - 1 - m(\delta - 1)$

□ $C_i = \{x q^k \bmod n \mid x = i\}$ = cyclotomic coset of q mod $q^m - 1$ containing i

$$S = \bigcup_{i=a}^{a+\delta-2} C_i$$

$$g(x) = \text{lcm}\left(\prod_{i \in C_a} (x - \alpha^i), \prod_{i \in C_{a+1}} (x - \alpha^i), \dots, \prod_{i \in C_{a+\delta-2}} (x - \alpha^i)\right)$$

$$= \prod_{i \in S} (x - \alpha^i)$$

$\Rightarrow \dim = n - \deg g(x) = q^m - 1 - |S|$

(ii) $k = 2^m - 1 - |S| = 2^m - 1 - \left| \bigcup_{i=a}^{q+\delta-2} C_i \right|$

$\geq 2^m - 1 - \sum_{i=a}^{q+\delta-2} |C_i|$

$\geq 2^m - 1 - \sum_{i=a}^{q+\delta-2} m = 2^m - 1 - m(\delta-1)$

$\therefore$ dim $\geq 2^m - 1 - m(\delta-1)$.

(Note $|C_i| \leq m$)

$2^m \equiv 1 \pmod{2^m-1}$

$|C_i| = m$ if $\gcd(i, 2^m-1) = 1$

Ex. 2 mod 15

(i) $C_2 = \{1,2,4,8\}$ $C_3 = \{3,6,12,9\}$

$\delta = 3$ $n = 15$

dim = binary $15 - |C_2 \cup C_3| = 15 - 8 = 7$

$g(x) = \text{lcm}\{M^{(2)}(x), M^{(3)}(x)\}$

dim $\Rightarrow$

(ii) 3 mod 26

$C_1 = C_3 = \{1,3,9\}$, $C_2 = \{2,6,18\}$

$C_4 = \{4,12,10\}$

dim ternary BCH code of $n = 26$ & des. distance $\delta = 5$

$g(x) = \text{lcm}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x))$

ie $26 - |C_1 \cup C_2 \cup C_3 \cup C_4| = 26 - 9 = 17$

$\therefore$ dim bigger than lower bound.

Ex. For $t \geq 1$, t & $2t$ $\in$ same cyclotomic coset of 2 mod $2^m - 1$.

$\Rightarrow M^{(t)}(x) = M^{(2t)}(x)$

$\text{lcm}(M^{(1)}(x), \ldots, M^{(2t-1)}(x), M^{(2t)}(x)) = \text{lcm}(M^{(1)}(x), \ldots, M^{(2t)}(x))$

⇒ narrow sense binary BCH code of $n = 2^m - 1$ with $\delta = 2t+1$

same as " " " $n = 2^m - 1$ & $\delta = 2t$.

Th. A narrow-sense q-ary BCH code of $n = q^m - 1$ with desg. dist. δ has

$$\text{dim} = q^m - 1 - m(\delta - 1) \quad \text{if } q \neq 2 \text{ &}$$

$$\gcd(q^m - 1, e) = 1 \quad \forall\ 1 \leq e \leq \delta - 1$$

□ Note $\text{dim} = q^m - 1 - \left| \bigcup_{i=1}^{\delta-1} c_i \right|$

∴ if we prove that $|c_i| = m \quad \forall\ 1 \leq i \leq \delta - 1$

& $c_i \cap c_j = \phi \quad 1 \leq i < j \leq \delta - 1$

Two c_i's & c_j's are either disjoint or equal

Claim For any integer $1 \leq t \leq m-1$ $\quad i \neq q^t \cdot i \pmod{q^m - 1}$ for $1 \leq i \leq \delta - 1$

Th. A narrow sense binary BCH code of $n = 2^m - 1$ & desg. dist $\delta = 2t+1$ has $\text{dim} \geq n - m\frac{(\delta-1)}{2}$

□ ∵ c_{2i} & c_i are same

$$k = 2^m - 1 - \left| \bigcup_{i=1}^{2t} c_i \right|$$

$$= 2^m - 1 - \left| \bigcup_{i=1}^{t} c_{2i-1} \right| \geq 2^m - 1 - \sum_{i=1}^{t} |c_{2i-1}|$$

$$\geq 2^m - 1 - tm$$

$$= 2^m - 1 - m\frac{(\delta-1)}{2}$$

Lemma Let $\mathcal{C}$ be a q-ary cyclic code of length n, gen. poly $g(x)$. Suppose $\alpha_1, \alpha_2, \dots, \alpha_r$ are all the roots of $g(x)$ & $g(x)$ has no multiple roots. Then an element $c(x) \in \mathbb{F}_q[x]/(x^n-1)$ is a codeword of $\mathcal{C}$ iff $c(\alpha_i) = 0 \quad \forall\ 1 \le i \le r$.

Th. A BCH code with designed distance δ has min dist $\ge \delta$.

$\square$ $\alpha \in \mathbb{F}_{q^m}$ (primi.) $\quad \mathcal{C}$ = BCH code with

$$g(x) = \text{lcm}\{m^{(a)}(x), \dots, m^{(a+\delta-2)}(x)\}$$

Clearly $\alpha^a, \alpha^{a+1}, \dots, \alpha^{a+\delta-2}$ are roots of $g(x)$

Suppose $d < \delta \Rightarrow \exists$ a nonzero codeword

$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ s.t.

$wt(c(x)) = d < \delta$

$$\Rightarrow \quad c(\alpha^i) = 0 \quad \forall\ i = a, \dots, a+\delta-2$$

$$\Rightarrow \begin{pmatrix} 1 & \alpha^a & (\alpha^a)^2 & \cdots & (\alpha^a)^{n-1} \\ 1 & \alpha^{a+1} & (\alpha^{a+1})^2 & \cdots & (\alpha^{a+1})^{n-1} \\ \vdots & & & & \\ 1 & \alpha^{a+\delta-2} & (\alpha^{a+\delta-2})^2 & \cdots & (\alpha^{a+\delta-2})^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0$$

Suppose support of $c(x)$ is $R = \{i_1, \dots, i_d\}$

$c_j \neq 0$ iff $j \in R$

$$\begin{pmatrix} (\alpha^a)^{i_1} & (\alpha^a)^{i_2} & \cdots & (\alpha^a)^{i_d} \\ (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ \vdots & \vdots & & \vdots \\ (\alpha^{a+\delta-2})^{i_1} & & \cdots & (\alpha^{a+\delta-2})^{i_d} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ c_{i_3} \\ \vdots \\ c_{i_d} \end{pmatrix} = \bar{0}$$

$\because$ $d \le \delta - 1$ (choose first d eqns of the above syst.

$$\begin{pmatrix} (\alpha^a)^{i_1} & (\alpha^a)^{i_2} & \cdots & (\alpha^a)^{i_d} \\ (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ \vdots & & & \vdots \\ (\alpha^{a+d-1})^{i_1} & \cdots & & (\alpha^{a+d-1})^{i_d} \end{pmatrix} \begin{pmatrix} c_{i_1} \\ c_{i_2} \\ \vdots \\ c_{i_d} \end{pmatrix} = 0$$

$$\det = \prod_{j=1}^{d} (\alpha^a)^{i_j} \prod_{k>l} (\alpha^{i_k} - \alpha^{i_l}) \neq 0$$

$$\Rightarrow (c_{i_1} \cdots c_{i_d}) = (0\,0\,0 \cdots 0) \quad \#.$$

Let $m=1 \Rightarrow$ BCH code has $n = q-1$
& $m^{(i)}(x) = x - \alpha^i$ $\alpha \to$ prim. elem. of $\mathbb{F}_q$

$\therefore$ for $\delta \le q-1$

$$g(x) = \text{lcm}\left(x-\alpha^a, x-\alpha^{a+1}, \ldots, x-\alpha^{a+\delta-2}\right)$$

$$\Leftarrow g(x) = (x-\alpha^a)(x-\alpha^{a+1}) \cdots (x-\alpha^{a+\delta-2})$$

$\therefore$ **q-ary Reed Solomon code** $n = q-1$

$a \ge 0$ & $2 \le \delta \le q-1$

Reed Solomon Codes

March 22, 2010

(1960)

$GF(q)$

$(m_0, m_1, \ldots, m_{k-2}, m_{k-1}) \in (GF(q))^k$

$$P(x) = m_0 + m_1 x + m_2 x^2 + \cdots + m_{k-2} x^{k-2} + m_{k-1} x^{k-1}$$

$$\bar{c} \in RS \quad \bar{c} = (c_0, c_1, \ldots, c_{q-1}) = [P(0), P(\alpha), P(\alpha^2), \ldots, P(\alpha^{q-1})] \quad \text{---} (1)$$

$$C_{RS} = \{ \bar{c} = (c_0, c_1, \ldots, c_{q-1}) = (P(0), P(\alpha), \ldots, P(\alpha^{q-1})) \mid m_i \in GF(q) \}$$

$\Rightarrow |C_{RS}| = q^k$

Claim (1) C_{RS} are linear codes.

(2) $\dim C_{RS} = k$ ($\because$ C_{RS} is k-dimensional VS over $GF(q)$)

(3) $n = q \Rightarrow [q, k, \overset{d}{?}]_q$

(2)

$$\begin{aligned}
P(0) &= m_0 \\
P(\alpha) &= m_0 + m_1 \alpha + m_2 \alpha^2 + \cdots + m_{k-1} \alpha^{k-1} \\
P(\alpha^2) &= m_0 + m_1 \alpha^2 + m_2 \alpha^4 + \cdots + m_{k-1} \alpha^{2(k-1)} \\
&\vdots \\
P(\alpha^{q-1}) &= m_0 + m_1 \alpha^{q-1} + m_2 \alpha^{2(q-1)} + \cdots + m_{k-1} \alpha^{(k-1)(q-1)}
\end{aligned}$$

Any k of these expressions can be used to construct a syst. of k eqns in k variables.

$\Rightarrow$ first k will give

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{k-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(k-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(k-1)(k-1)} \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ \vdots \\ m_{k-1} \end{bmatrix} = \begin{bmatrix} P(0) \\ P(\alpha) \\ P(\alpha^2) \\ \vdots \\ P(\alpha^{k-1}) \end{bmatrix} \quad (3)$$

$$A \bar{m} = \bar{P}$$

$\rightarrow$ non singular matrix (Vandermonde matrix)

$\Rightarrow$ This system has a unique soln.

~~Error Co~~

Error Correction

Suppose that t of the codeword coordinates are corrupted.

$\Rightarrow$ Corresponding expressions in (2) are incorrect

$\Rightarrow$ would lead to incorrect soln if used in (3)

— Assuming that we do not know where are the errors we might construct all possible distinct systems of K expressions from the set of expression in (2).

— There are $\binom{q}{K}$ such systems, and $\binom{t+K-1}{K}$ of which give incorrect information symbols. If we use majority opinion among the solns to all possible linear systems we will get correct information as long as $\binom{t+K-1}{K} < \binom{q-t}{K} \iff t+K-1 < q-t$

$\iff 2t < q-K+1 \Rightarrow t = \left\lfloor \frac{q-K+1}{2} \right\rfloor$

it will correct t errors. MDS code : $[q, K,$

New construction of cyclic code

- $m(x) = m_0 + m_1 x + \cdots + m_{K-1} x^{K-1}$

$c(x) = m(x)\, g(x) = \langle g(x) \rangle$

where $g(x) = \prod_{j=1}^{2t} (x - \beta^j)$

$n = q-1 \qquad K = q-2t-1$

Applications

1. Digital Audio Disk (CIRC code)
2. Deep space Communication
3. Systems with feedback
4. Spread-Spectrum Systems (GSM & FH(SS))
5. Computer Memory
6. VLSI Codec
7. frequency Hop Communication

Decoding

1. Berlekamp–Massey algorithm
2.

$f_1(x)$ & $f_2(x) \in \mathbb{F}_2[x]$ $(\neq 0)$

(1) $\text{lcm}(f_1, f_2)$ = monic poly. of lowest deg. which is multiple of both f_1 & f_2.

(2) $\text{lcm}(f_1, f_2, \ldots, f_t)$ = similar def.

(3) $\text{lcm}(f_1, f_2, f_3) = \text{lcm}(\text{lcm}(f_1, f_2), f_3)$

(4) $\text{lcm}(f_1, f_2, \ldots, f_t) = \text{lcm}(\text{lcm}(f_1, \ldots, f_{t-1}), f_t)$

(5) If $f_1, \ldots, f_t \in \mathbb{F}_2[x]$ s.t.

$$f_1(x) = a_1 \cdot p_1(x)^{e_{1,1}} \cdots p_n(x)^{e_{1,n}}$$
$$\vdots$$
$$f_t(x) = a_t \cdot p_1(x)^{e_{t,1}} \cdots p_n(x)^{e_{t,n}}$$

$a_1, \ldots, a_t \in \mathbb{F}_2^*$, $e_{i,j} \geq 0$ & $p_i(x)$ are distinct monic irr. polys over $\mathbb{F}_2$ then

$$\text{lcm}(f_1, \ldots, f_t) = p_1(x)^{\max(e_{1,1}, \ldots, e_{t,1})} \cdots p_n(x)^{\max(e_{1,n}, \ldots, e_{t,n})}$$

(6) $f(x), f_1, \ldots f_t \in \mathbb{F}_2[x]$ If $f(x)$ is divisible by every f_i then $f(x) \equiv 0 \left(\text{lcm}(f_1, \ldots f_t)\right)$

Th. $\alpha \in \mathbb{F}_{2^m}$ (primitive element) $M^{(i)}(x)$ = min poly of α^i w.r.t. $\mathbb{F}_2$

Each root β of $M^{(i)}(x)$ is an element of $\mathbb{F}_{2^m}$

$\Rightarrow \beta^{2^m - 1} = 1$ i.e. $x - \beta \mid x^{2^m - 1} - 1$

$M^{(i)}(x)$ has no multiple roots

$\Rightarrow M^{(i)}(x) \mid x^{2^m - 1} - 1$

$\Rightarrow$ For a subset I of $\mathbb{Z}_{2^m - 1}$, $\text{lcm}\left(M^{(i)}(x)\right)_{i \in I} \mid x^{2^m - 1} - 1$.

Convolutional Codes

April 9, 2010

Peter Elias 1955

Forney

McEliece

Turbo codes

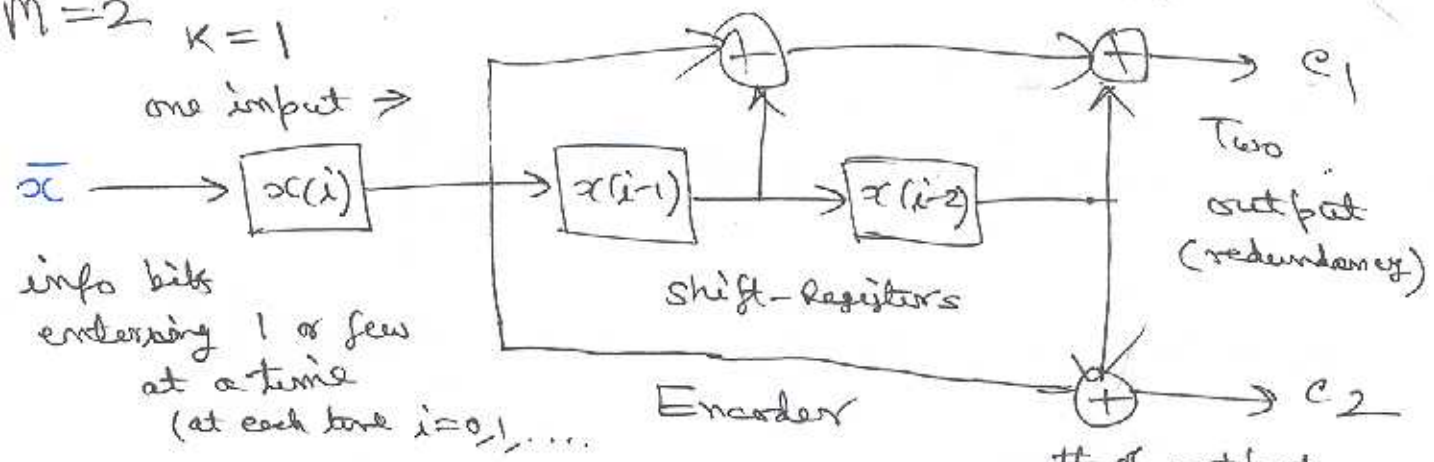
Algebra + Finite-State-machine

DEEP SPACE COMMUNICATIONS

Memory

$M = 2$ $K = 1$

one input →



info bits entering 1 or few at a time (at each time $i = 0, 1, \ldots$

# of outputs $\geq$ # of inputs

$$c_1(i) = x(i) + x(i-1) + x(i-2)$$

$$c_2(i) = x(i) + x(i-2)$$

Sequential decoding algo. were known till 1960's for spacecraft transmission

1967 Viterbi Algo. for AWGN

Optimal] A seq. formed by F.S.M & corrupted by an independent random noise seq. has the properties of a Markov seq.

Input stream of bits entering

$x(0)\, x(1)\, x(2) \ldots\ldots x(i) \ldots\ldots$

of | Input Stream | $= L$

$$\bar{x} = \sum_{i=0}^{L-1} x(i) D^i \in \mathbb{F}_2[D]$$

Out puts

At time 0; $c_1(0)$ $c_2(0)$

At time 1 $c_1(1)$ $c_2(1)$ ...

$D \rightarrow$ Delay operation $\left\{ \begin{array}{l} \text{Set of all polynomials} \\ \text{in variable } D \end{array} \right.$ $=$ Integral Domain

$$\mathbb{F}_2(D) = \left\{ \left. \frac{p(D)}{q(D)} \right| p, q \in \mathbb{F}_2[D],\ q(D) \neq 0 \right\}$$

Rational field

All rational fns.

$|\mathbb{F}_2(D)| = \infty$

(n, k) convolutional code C is a K-dimensional $\leq \mathbb{F}_2(D)^n$

$|C| = \infty$ (infinite no. of codewords)

Rate of $C = \frac{k}{n}$

$\bar{c} = (c_1, c_2, \ldots, c_n)$ $\quad \bar{x} G = \bar{c}$ (1)

Gen. Matrix

$$G = [g_{ij}]_{k \times n} \quad g_{ij} \in \mathbb{F}_2(D)$$

whose rows forms a basis for G

— Any x by non zero member of $\mathbb{F}_2(D)$ is also a gen. matrix

Ex-1 $C_1 : (2,1)$

$$G_1 = \begin{bmatrix} 1+D+D^2 & 1+D^2 \end{bmatrix}$$

$$G_1 \sim G_1' = \begin{bmatrix} 1+D^3 & 1+D+D^2+D^3 \end{bmatrix}$$

$$= (1+D) \times G_1$$

Ex-2 $C_2 : (4,2)$

$$G_2 = \begin{bmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D & D & 1 \end{bmatrix}$$

$$G_2 \sim G_2' = \begin{bmatrix} 1 & D & 1+D & 0 \\ 0 & 1+D & D & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+D & D & 1 \end{bmatrix}$$

$$G_2''' = \begin{bmatrix} 1+D & 0 & 1 & D \\ D & 1+D+D^2 & D^2 & 1 \end{bmatrix}$$

Ex-1 Input $11011 \Rightarrow \bar{x} = 1 + D + D^3 + D^5$

(⇒ 1 enters at 0, 1, 3, 5 times & 0 at 2 & 4)

$\bar{x} G_1 = (c_1, c_2)$

$c_1 = (1+D+D^3+D^5)(1+D+D^2)$

$c_1 = 1 + D^4 + D^6 + D^7 \Rightarrow c_1 = 10001011$

& $c_2 = (1+D+D^3+D^5)(1+D^2)$

$= 1 + D + D^2 + D^7 \quad c_2 = 11100001$

⇒ ∴ Output = 11 01 01 00 10 00 10 11 ← c_1, c_2 } Interleaved

(Exercise) ~~Suppose~~ Encode $(11010, 10111)$ using the $(4,2)$ c.code $\mathcal{C}_2$ by $G_2 = \begin{bmatrix} 1 & 1+D+D^2 & 1+D^2 & 1+D \\ 0 & 1+D & D & 1 \end{bmatrix}$

xG_2

$= (1101, 01101, 10111, 0)$ ∵ length is different. Pad with 0's.

$(11010000, 01101000, 10111000, 00000000)$

∴ Interleave will give

$10101100001101010011000000000$

$c_1(i) = x_1(i)$

$c_2(i) = x_1(i) + x_1(i-1) + x_1(i-2) + x_2(i) + x_2(i-1)$

$c_3(i) = x_1(i) + x_1(i-2) + x_2(i-1)$

$c_4(i) = x_1(i) + x_1(i-1) + x_2(i)$

$M = 2$

State Diagrams

Trellis Diagrams

A directed edge from vertex $(x(i-1), \ldots, x(i-M))$ to vertex $(x(i), x(i-1), \ldots, x(i-M+1))$

if input is 0 ⟶ is solid if $x(i) = 0$

" " 1 ⟶ & dashed if $x(i) = 1$

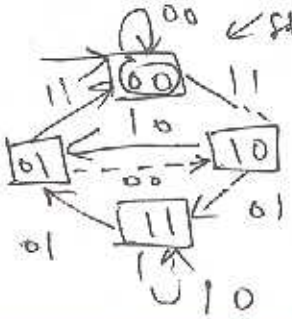
If the shift-register at time i contains $x(i), x(i-1), \ldots, x(i-M)$ then the encoder is in the state $(x(i-1), \ldots, x(i-M))$

M = memory of the encoder

and is labeled $(c_1(i), \ldots, c_n(i))$

Example if 101 to be encoded into 111000101111

After 3 inputs take two zero inputs



Trellis diagram = state diagram at different time $i = 0, 1, 2, \ldots$

state $a = 00$ $b = 01$ $c = 10$ & $d = 11$

Encoding is done by tracing left-to-Right through the trellis beginning at state a (& ending at the zero state a)

Ex. let state $s \in \{a, b, c, d\}$ at time i is denoted by s_i

then encoding of $|011|$ is done by the path

$a_0 c_1 b_2 c_3 d_4 b_5 a_6$ (by following dashed, then solid, then 2 dashed & finally 2 solid edges)

input 2 additional 0's to reach state a

$\Rightarrow$ $|011| \rightarrow 11|00|00|01|11$

(writing labels on the edges of the path)

Exercise erode

$|001|$

0011

Truncated trellis

Portion of the trellis that starts at $i = 0$ & ends at time $L + M$

M = memory.

The Viterbi Algorithm

Suppose the message

$$x(i) = (x_1(i), \ldots, x_k(i))$$

for $i = 0, 1, \ldots, L-1$

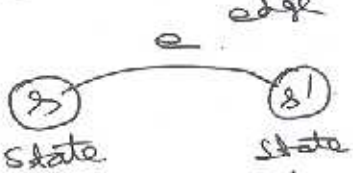
is encoded using the gen. matrix G to produce a codeword $c(i) = (c_1(i), \ldots, c_n(i))$ for $i = 0, 1, \ldots, L+M-1$

& assume

$$y(i) = (y_1(i), \ldots, y_n(i)) \text{ for } i = 0, 1, \ldots, L+M-1$$

is recvd.

Let



— wt. (edge) = d(edge label of e, Hamming portion $y(i-1)$ of the recvd VR at time $i-1$)

— The wt. of a Path P through the trellis is $\sum_{\text{edges} \in \text{Path}}$ wt(edges)

— Zero state a at time 0 is denoted by a_0.

— Suppose P is a path in the trellis starting at a_0 & ending at time i in state s

— We call such a path survivor at time i starting if its wt. is smallest among all paths from a_0 & ending at time i in state s.

Put

— $S(s,i) = \{$ Collection of all survivor paths starting at a_0 & ending at s at time i $\}$

— If P is a path starting at a_0 & ending at time I define $\bar{c}_p$ codeword associated with P where

— $c_p(i)$ is the label of the edge in P from state at time i to state at time $i+1$ for $0 \le i < I$

— $\bar{x}_p$ = message associated with P where

— $x_p(i)$ is the input identified by the type of the edge in P from state at time i to state at time $i+1$ for $0 \le i < \min\{I, L\}$

Viterbi Decoding Algo

Step I: Draw the L truncated trellis for G & replace the edge labels by edge wts.

$a \to$ zero state

Step II Compute $S(s,1)$ $\forall$ states s using the trellis of step I

Step III Repeat the following for $i = 2, 3, \ldots, L+M$ using the trellis of step I. Assuming $S(s, i-1)$ has been computed $\forall$ state s, compute $S(s,i)$ $\forall$ s as follows:

— For each state s' & each edge e from s' to s form the path P made from P' followed by e where $P' \in S(s', i-1)$. Install P in $S(s,i)$ if it has smallest wt among all such paths.

Step (4) A nearest nbr. to y is any c_p for $p \in S(a, L+M)$ obtained from the message given by x_p.

Ex. Recvd. vr $y = 11\,01\,11\,01\,10\,11\,00\,01\,01\,11$

for C_1 two bits are read at each clock cycle

$a = 00 \quad b = 01 \quad c = 10 \quad d = 11$

Let — state s at time i is denoted by s_i

$\Rightarrow$ zero state at time 0 is a_0

Step II $S(a,1) = \{a_0 a_1\}$

$S(b,1) = \phi$

$S(c,1) = \{a_0 c_1\}$ & $S(d,1) = \phi$

Compute $S(s,2)$ $S(a,2) = \{a_0 a_1 a_2\}$

$S(b,2) = \{a_0 c_1 b_2\}$

$S(c,2) = \{a_0 a_1 c_2\}$ $S(d,2) = \{a_0 c_1 d_2\}$

$S(a,3) = \{a_0 c_1 b_2 a_3\}$

...

$S(a,8)$ contains the path $p = a_0 c_1 d_2 d_3 b_4 c_5 d_6 b_7 a_8$ of wt. 2

$\therefore$ codeword

trace p $c_p = 11\,01\,10\,00\,01\,01\,11$

message: 111011

Free distance $f(D) \in \mathbb{F}_2(D)$

Ex. $f(D) = h(D)/g(D) = \sum_{i \geq a} f_i D^i$

$wt(1+D+D^2) = 3$

$wt\left(\frac{1+D}{1+D^3}\right) = \infty$

$u(D) \in \mathbb{F}_2(D)^n$

$wt(\bar{u}(D)) = \sum_{i=1}^{n} wt(u_i(D))$

$d_{free}^{(n,k)} = wt(u(D) - v(D))$

$a \in \mathbb{Z} \quad f_i \in \mathbb{F}_2$

$g(0) \neq 0$

$wt(f(D))$ = # of non-zero coeff in series expn

LDPC Codes

April 20, 2010

Tanner graph of a code

$C = [n, k, d]_2$

b. Graphical realizations of codes

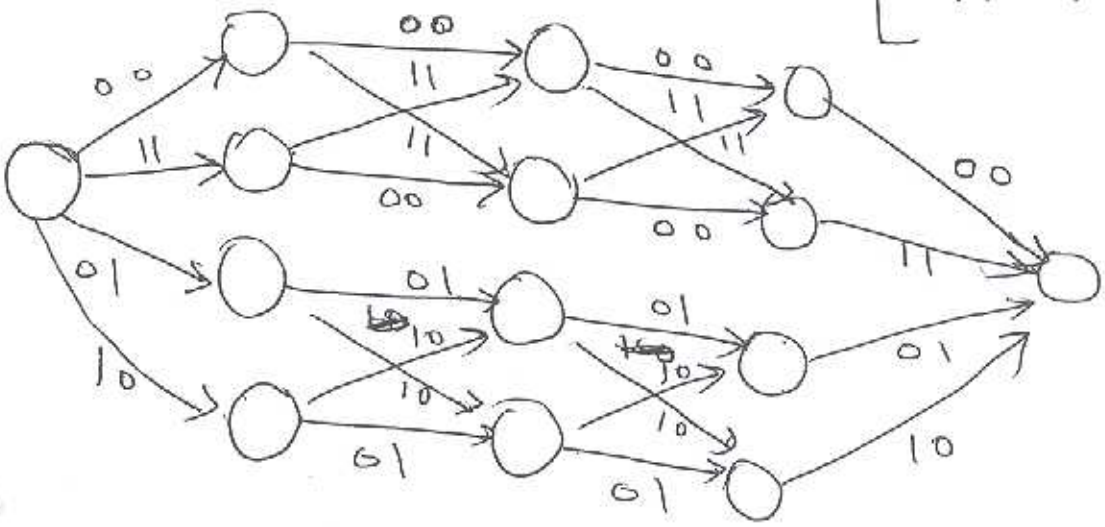
Trellis — p.c. (Tanner graph) — p.c.m. — Generator realization

Trellis representations of binary linear block codes

Ex. (8,4,4) RM code $G =$

$$\begin{bmatrix} 11110000 \\ 10101010 \\ 11001100 \\ 11111111 \end{bmatrix}$$

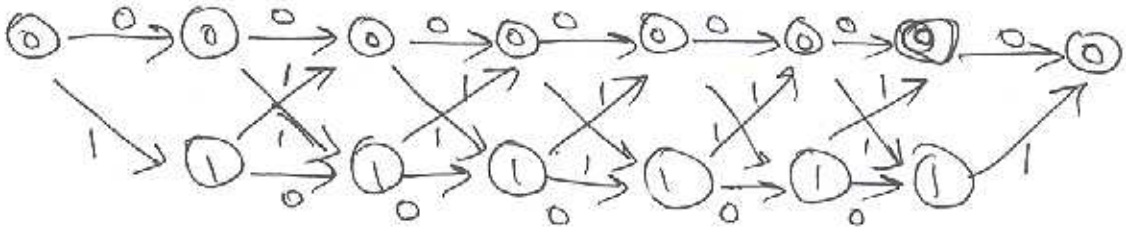
RM(1, 3)



4 states
00
01
10
11

Ex-2 (7,6,2) single p.c. code

2 state trellis



⟹ Any binary linear block code can be decoded using Trellis-based (Viterbi algo) decoding method for ML decoding.

Ex-3 $G = [1111\,0000]$ $[8,1,4]_2$