9/17/2013

6.02 Recitation R4 (10 & 11 am)

## Linear Block Code (an example of algebraic block code)

- take the set of k-bit messages, $\{2^k\}$, and produce a set of $2^k$ CWs, each n bits long ($n \geq k$)
  - block: any long bit streams can be chopped up into k-bit blocks
  - linear: CWs are produced through linear transformation of the message bits
- notations: (n, k) or (n, k, d) where d = min HD of the block code
  - (n, 1, n) for repetition code
  - rate = k/n

## Binary Linear Codes (BLC)

- computation uses Boolean algebra, or arithmetic mod 2, or algebra in a Galois Field of order 2 (GF2, or $\mathbb{F}_2$)
- Galois is a 19th century mathematician in Finite Fields (died @ 21)
  - important for cryptography
- GF2 algebra

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

addition

| × | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

multiplication

| w | -w | $w^{-1}$ |
|---|---|---|
| 0 | 0 | - |
| 1 | 1 | 1 |

inverses

- Thm: a code is linear iff the sum of any two CWs is another CW
  - "all-0" CW is always in a linear code
- Thm: Define weight of a CW as the # of 1's in the word. Then min HD of a linear block code is equal to the weight of the non-zero CWs w/ the smallest weight.
- parity: define parity of bits $X_1, X_2, \cdots X_n$ as $(X_1 + X_2 + \cdots + X_n)$, where addition is performed mod 2 (XOR)
  - even parity: when sum is 0
  - odd parity: when sum is 1
- even parity code: for any message M, let $w = M \cdot \text{parity}(M)$ (· = concatenation)
  - parity(w) = 0
  - b/c # of 1's in each CW is even

(add a parity bit to each message)

---

[Example 5.14] Hat Game

- N people in room, each wearing a red or blue hat, standing in a line according to increasing height
- each person can see the hats of people in front, but not his/her own
- Each person gets to say "red" or "blue" about his/her own hat; → 1 pt if correct, 0 pt if wrong
- what's the protocol that will maximize score

Soln: (There are several, but here is one)

- assign red = 0, blue = 1
- start w/ tallest person, who computes the overall parity of all hats in front of him/her, shouts the number (i.e, color)
- next person computes the parity, and add to it the parity from the previous person, and shout the result
- let $p_k$ be the parity computed by the $k^{th}$ person, and $s_k$ be the shout by the $k^{th}$ person, then

$$s_k = p_{k-1} + p_k \qquad \text{where} \quad p_{k-1} = \sum_{i=1}^{k-1} s_i$$

[example]

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| parity | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| shout | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |

- only person who may be wrong is the 1st person ⇒ score = N or N−1

---

[Example 5.5] LBC (6.3) piecewise code

$$\begin{cases} p_1 = d_1 + d_2 \\ p_2 = d_2 + d_3 \\ p_3 = d_3 + d_1 \end{cases}$$

| $d_1$ | $d_2$ | $d_3$ | $p_1$ | $p_2$ | $p_3$ | weight | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | × | |
| 0 | 0 | 1 | 0 | 1 | 1 | 3 | ✓ |
| 0 | 1 | 0 | 1 | 1 | 0 | 3 | ✓ |
| 0 | 1 | 1 | 1 | 0 | 1 | 4 | |
| 1 | 0 | 0 | 1 | 0 | 1 | 3 | ✓ |
| 1 | 0 | 1 | 1 | 1 | 0 | 4 | |
| 1 | 1 | 0 | 0 | 1 | 1 | 4 | |
| 1 | 1 | 1 | 0 | 0 | 0 | 3 | ✓ |

a) rate = 3/6 = 1/2

b) # of 1's in a min-weight, non-zero CW: answer 3

c) min HD = 3 (from Thm 2 on page 2)

## Rectangular Parity SEC Code

- arrange k bits of message M into a rectangular array w/ r rows and c columns
- define $P_{\_row(i)}$ = parity of all bits in row i

$$R = \{P_{\_row(1)}, P_{\_row(2)}, \cdots, P_{\_row(r)}\}$$

- Similarly

$$C = \{P_{\_col(1)}, P_{\_col(2)}, \cdots P_{\_col(c)}\}$$

$\Big\}\ w = M \cdot R \cdot C$

- $n = rc + r + c$ rate $= rc/(rc+r+c)$

note: if there is a total parity for M, then $n = rc+r+c+1$

- <u>decoding process</u>: compute row and column parities at rcvr.

[Example, lecture 4, slide 16]

| | | | | |
|---|---|---|---|---|
| $D_1$ | $D_2$ | $D_3$ | $D_4$ | $P_1$ |
| $D_5$ | $D_6$ | $D_7$ | $D_8$ | $P_2$ |
| $D_9$ | $D_{10}$ | $D_{11}$ | $D_{12}$ | $P_3$ |
| $P_4$ | $P_5$ | $P_6$ | $P_7$ | $P$ |

} parity for rows

$P_4$ $P_5$ $P_6$ $P_7$: parity for columns

$P$: total parity (from M, excluding R & C)

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |

no error!

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 |

error in $D_1$

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |

error in $P_5$

| | | | | |
|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |

error in P

- assertion: Rectangular parity code is a SEC code
  - if $M_i$ and $M_j$ differ by one bit, then $W_i, W_j$ will differ by 3 bits (data bit, row and column bits) $\Rightarrow$ HD = 3
  - if $M_i$ and $M_j$ differ by 2 bits, then there are 3 possibilities:
    - differing bits are in the same row (2 data + 2 column bits), or
    - " " " column ( " " row " ), or
    - " " " different rows and columns (2 data, 2 row, 2 column bits) $\Rightarrow$ HD $\geq$ 4
  - if $M_i$ and $M_j$ differ by 3 or more bits, then HD $\geq$ 3
  - So HD $\geq$ 3 for rectangular parity code $\Rightarrow$ SEC code

---

How many parity bits are needed in an SEC code?

- rcvr needs to distinguish n+1 situations (ie, 0 to n single errors)
- n-k parity bits $\Rightarrow$ $2^{n-k}$ possible bit patterns

$$\boxed{n+1 \leq 2^{n-k}}$$

---

- Every linear code can be represented by an equivalent systematic form