Discrete Structures (Monsoon 2022)

Ashok Kumar Das

Associate Professor
IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

Coding Theory (Group Codes)

Error Detection

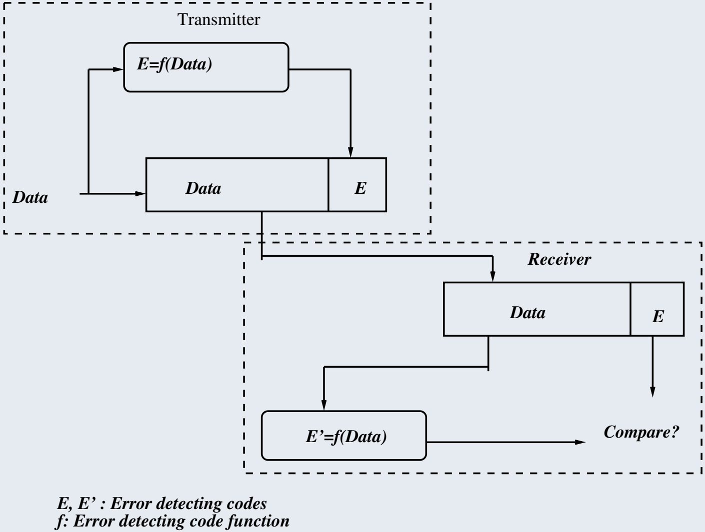


Figure: Error detection

Error Detection

- For a given frame of bits, additional bits that constitute an error-detecting code are added by the transmitter. This code is calculated as a function of the other transmitted bits.
- The receiver performs the same calculation and compares the two results. A detected error occurs if and only if there is a mismatch.

Group Codes

Definition

Let x and y be binary n-tuples, i.e., $x = \langle x_1, x_2, \ldots, x_n \rangle$ and $y = \langle y_1, y_2, \ldots, y_n \rangle$, where $x_i, y_i \in \{0, 1\}$. The Hamming distance between x and y denoted as $H(x, y)$ is the number of co-ordinates (components) in which they differ.

- Example: The Hamming distance between $\langle 1, 0, 1 \rangle$ and $\langle 1, 1, 0 \rangle$ is $H(\langle 1, 0, 1 \rangle, \langle 1, 1, 0 \rangle) = 2$.
- The Hamming distance between two n-tuples is equal to the number of independent single errors needed to change one n-tuple into the other.

Group Codes

Properties

- $H(x, y) \geq 0, \forall x, y \in C$, where C is the set of code words which are n-tuples $c_i = \langle c_{i,1}, c_{i,2}, \ldots, c_{i,n} \rangle$, $c_{i,j} \in \{0, 1\}$.
- $H(x, y) = 0$ if and only if $x = y$.
- $H(x, y) = H(y, x), \forall x, y \in C$.
- $H(x, z) \leq H(x, y) + H(y, z), \forall x, y, z \in C$.

Definition

The minimum distance (or minimum Hamming distance) of an n-coordinate code, C is $H_c = min_{c_i, c_j \in C} H(c_i, c_j)$.

Group Codes

Theorem

A code C can detect all combinations of d or fewer errors if and only if its minimum distance is at least $(d+1)$.
In other words,
C can detect $\leq d$ errors
if and only if
$H_c =$ *minimum distance of* $C = min_{c_i, c_j \in C} H(c_i, c_j) \geq (d+1)$.

Group Codes

Theorem

A code C can correct every combination of t or fewer errors if and only if its minimum distance is at least $(2t+1)$.

Proof. Let C be a code of n-tuple code words c_i, where $c_i = \langle c_{i,1}, c_{i,2}, \ldots, c_{i,n}\rangle$, $c_{i,j} \in \{0,1\}$.

The Hamming distance $H(x,y)$ between two n-tuple code words x and y, where $x, y \in C$, is $H(x,y) =$ number of coordinates in which they differ.

The minimum Hamming distance is given by $H_c = min_{c_i,c_j \in C} H(c_i, c_j)$.

$(\Rightarrow)$: Given C can correct $\leq t$ errors.

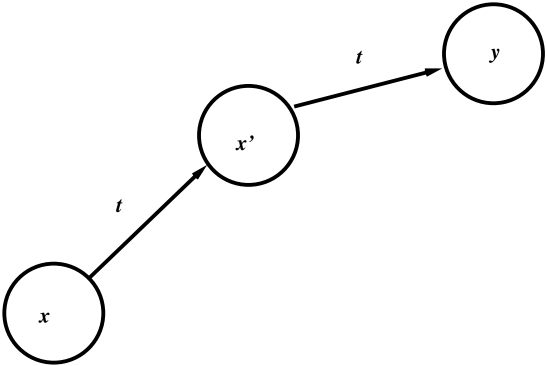
RTP: $H_c = 2t+1$, that is, $\forall x, y \in C, H(x,y) \geq (2t+1)$.

If possible, let $\exists x, y \in C$ such that $H(x,y) = 2t$.

Let $l_1, l_2, \ldots, l_{2t}$ be the coordinates (positions) where x and y differ.

Select $l_1, l_2, \ldots, l_t$ and change x to another n-tuple x' by changing x in these positions. Therefore, $H(x,x') = t$.

Proof (Continued . . .)



Group Codes

Proof (Continued ...) But, then from the property of Hamming distance, we have:

$$\begin{aligned} H(x,y) &\leq H(x,x') + H(x',y) \\ &= t + t \\ H(x,y) &\leq 2t. \end{aligned}$$

There exists some n-tuple x' that satisfies $H(x,x') = t$ and $H(x',y) \leq t$.
This is a contradiction. Hence, $H_c = 2t + 1$, that is, $\forall x, y \in C, H(x,y) \geq (2t+1)$.

Group Codes

Proof (Continued ...)

($\Leftarrow$) : Given $H_c = 2t + 1$, that is, $\forall x, y \in C$,

$$H(x, y) \geq 2t + 1. \quad (1)$$

Let x' be a received n-tuple that is corrupted by NOT more than t errors and x be a code word. x' has thus changed from x by t or fewer errors. Hence,

$$H(x, x') \leq t. \quad (2)$$

From the properties of Hamming distance, we have

$$\begin{aligned} H(x, y) &\leq H(x, x') + H(x', y) \\ H(x', y) &\geq H(x, y) - H(x, x') \\ &\geq t + 1, \text{ using Eqns. (1) and (2).} \end{aligned}$$

Therefore, every code word y is farther than x' than is x, and x can be correctly decoded. $\square$

Group Codes

Definition

A *group code* is a code from which n-tuple code words forms a group with respect to the operation $\oplus$ (modulo-2 or bitwise XOR), where $x \oplus y = \langle x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n \rangle$.

Definition

The weight of a code word x, denoted by $w(x)$, is the number of its coordinates (or components) that are 1s, that is, $w(x) =$ number of 1s in x.

Example: $w(\langle 1, 1, 1, 1 \rangle) = 4$
$w(\langle 1, 1, 0, 0 \rangle) = 2$.
We denote the n-tuple $\langle 0, 0, \ldots, 0 \rangle$ by 0.
Note that $w(x) = H(x, 0)$,
$H(x, y) = H(x \oplus y, 0) = w(x \oplus y)$.

Group Codes

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Lemma

The minimum distance of a group code, C is equal to the minimum weight of its non-zero code words.

Definition (Null Space)

Let H be an $r \times n$ binary matrix. Then the set of binary n-tuples x that satisfies $x.H^t = 0$ is called the *null space* of H, $N(H)$. In other words,

$$N(H) \;\; = \;\; \{x | x.H^t = 0, x \in C\},$$

where C is the group code and H^t the transposition of the matrix H.

Group Codes

Theorem

The null space $N(H)$ of an $r \times n$ binary matrix H is a group under $\oplus$, component-wise addition modulo-2 (XOR).

Proof. Let H be an $r \times n$ binary matrix (parity-check matrix) and C a group code of n-tuples code words. Then the *null space* of H, $N(H)$ is

$$N(H) \quad = \quad \{x | x.H^t = 0, x \in C\},$$

where C is the group code and H^t the transposition of the matrix H. RTP: $\langle N(H), \oplus \rangle$ is a group.

- Closure: Let $x, y \in N(H)$. Then, $x.H^t = 0$ and $y.H^t = 0$. Therefore, $x.H^t \oplus y.H^t = 0 \Rightarrow (x \oplus y).H^t = 0. \Rightarrow (x \oplus y) \in N(H)$. Hence, closure axiom holds.

Group Codes

Proof (Continued ...). .

- Associativity: Since $((x \oplus y) \oplus z).H^t = (x \oplus (y \oplus z)).H^t$, $\forall x, y, z \in N(H)$, we have $(x \oplus y) \oplus z = x \oplus (y \oplus z)$. Associativity under $\oplus$ holds.
- Existence of Identity: We have: $(0 \oplus x).H^t = (x \oplus 0).H^t = x.H^t$, $\forall x \in N(H)$. Thus, $0 \oplus x = x = x \oplus 0$, $\forall x \in N(H)$. This implies that $0 = \langle 0, 0, \ldots, 0 \rangle$ is the identity in $N(H)$.
- Existence of Inverse: It is noted that
  $(x \oplus x).H^t = 0.H^t = 0$
  $\Rightarrow x \oplus x = 0$, $\forall x \in N(H)$.
  It shows that every element $x \in N(H)$ is its own inverse.

As a result, $N(H)$ forms a group under $\oplus$. $\square$

Corollary

$\langle N(H), \oplus \rangle$ is an abelian (commutative) group.

Theorem

Let $c_1, c_2, \ldots, c_d$ be d distinct columns of the parity check $r \times n$ matrix H. Then the r-tuple sum $c_1 \oplus c_2 \oplus \cdots \oplus c_d$ is 0 if and only if the null space of H, $N(H)$ has a code word of weight d.

Theorem

H is a parity-check matrix for a code of minimum weight at least 3 if and only if
(i) no column of H is all 0s; and
(ii) no two columns are identical.
(iii) there exists three columns, whose sum is 0, that is, $\exists C_i, C_j, C_k$ such that $C_i \oplus C_j \oplus C_k = 0$.