

Review Week 05

2022-10-24

ANNOUNCEMENT: CAREERS FAIR
Wed. 26 Oct

Reminder: coursework 1 TOMORROW Tuesday 25-Oct 11am *

Weight enumerator and $P_{\text{undetected}}$

Recall the code with standard array

weight: 0	3	2	2	3	3	4	2	3
00000	10011	01001	00110	11010	10101	01111	11100	
10000	00011	11001	10110	01010	00101	11111	01100	
01000	11011	00001	01110	10010	11101	00111	10100	
00100	10111	01101	00010	11110	10001	01011	11000	

• Assuming BSC(p), calculate $P_{\text{undetected}}$

• Decide if C offers a significant improvement in error detection compared to sending unencoded messages.

Recall the definition of the weight enumerator

(polynomial, each monomial has total degree n)

$$W_C(x, y) = \sum_{\underline{v} \in C} x^{n-w(\underline{v})} y^{w(\underline{v})} = A_0 x^n + A_1 x^{n-1} y + \dots + A_n y^n$$

where $A_i = \# \{ \underline{v} \in C : w(\underline{v}) = i \}$

$$A_i \in \mathbb{Z}_{\geq 0}, i = 0, 1, \dots, n; A_0 = 1$$

In the above example, $W_C(x, y) = x^5 + 2x^3y^2 + 4x^2y^3 + xy^4$

$$P_{\text{undetected}}(C) = W_C(1-p, p) - (1-p)^n$$

1 0 0 1 1 prob = $p^3(1-p)^2$ contain p^2 $P_{\text{undetected}} \approx 2p^2$

The inner product. The dual code

$$\mathbb{F}_3^4$$

$$1102 \cdot 2201 = 2+2+0+2=0$$

- The inner product $\underline{x} \cdot \underline{y}$ of vectors $\underline{x}, \underline{y} \in \mathbb{F}_q^n$ is defined as $\underline{x} \cdot \underline{y} = \sum_{i=1}^n x_i y_i$. $1102 \cdot 1102 = 0$
- If $C \subseteq \mathbb{F}_q^n$ is a linear code, the dual code C^\perp is $\{\underline{v} \in \mathbb{F}_q^n : \underline{v} \cdot \underline{c} = 0 \text{ for all } \underline{c} \in C\}$ (that is: C^\perp consists of all vectors orthogonal to C).

$$\text{Rep}(3, \mathbb{F}_2)^\perp = \{000, 111\}^\perp$$

$$\underline{v} \cdot 000 = 0 \quad \forall \underline{v} \in \mathbb{F}_2^3$$

$$\underline{v} \cdot 111 = 0 \Leftrightarrow \underline{v} \in E_3$$

$$\text{Rep}(3, \mathbb{F}_2)^\perp = E_3$$

- Result from the lectures: $\dim C^\perp = n - k$ where $k = \dim C$.

The check matrix H . The syndrome of a vector. The use of H for error detection

"parity check"

- A generator matrix H for C^\perp is called a check matrix for C .
- Fix H . Given a vector $\underline{y} \in \mathbb{F}_q^n$, the vector $S(\underline{y}) = \underline{y}H^T$ of size $n - k$ is the syndrome of \underline{y} . By the same theorem, $C = \{\underline{c} \in \mathbb{F}_q^n : S(\underline{c}) = \underline{0}\}$.

- This allows the receiver to detect errors.

The use of H for error correction - syndrome decoding.

$$S(\underline{y}) = \underline{y}H^T$$

- A2. Let C be the binary linear code with parity check matrix $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$.
- Construct a table of syndromes for C .
 - Use your table of syndromes to decode the received vectors 11110 and 10011.

$$\begin{bmatrix} 00000 \\ 00000 \\ 00000 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 000 \end{bmatrix}$$

a
(coset leader)

$S(\underline{a})$

$8 = 2^3$
rows

$$S(\underline{y}) = S(\underline{z}) \Leftrightarrow \text{coset}(\underline{y}) = \text{coset}(\underline{z})$$

Look for a vector of least weight whose syndrome is not yet in the table

$$\text{DECODE}(11110) = 11100$$

$$S(11110) = 100 \Rightarrow \underline{a} = 00010$$

00000

00001

00010

00100

01000

10000

~~00011~~

01010

00110

000

101

100

011

010

001

~~001~~

110

111