

Hamming

...מקור המידע ...הודעת ...הודעה

$$Enc: \Sigma^k \rightarrow \Sigma^n$$

...הודעה ...הודעה

codeword \ block message, up n ... message length, ...

...הודעה ...הודעה

$$d = \min_{x \neq y} (dist(Enc(x), Enc(y))) = \#\{i \mid E(x)_i \neq E(y)_i\}$$

$$q = |\Sigma|$$

...הודעה ...הודעה

...הודעה ...הודעה

...הודעה

...הודעה ...הודעה

$$(dist(\eta_i) = wt(\eta) = e)$$

...הודעה ...הודעה

...הודעה

...הודעה ...הודעה

$$L \frac{d-1}{2}$$

$$\begin{matrix} n & = & 1/p \\ k & = & 1/p \\ d & = & 1/p \\ q & = & 1/p \end{matrix}$$

...הודעה ...הודעה

$(\Sigma \subseteq \mathbb{F}_2^n)$ $Enc(x) = x$, $n=k$: $d=1$

$\Sigma = \{0,1\}$: $d=2$

repetition code: $Enc(x) = (x, x)$, $n=2k$

$Enc(x) = (x_1, \dots, x_n, \sum_{i=1}^n x_i \text{ mod } 2)$

~~the code is not linear~~

$d=3$: $\Sigma = \{0,1\}$, $n=3k$

the code is linear : $\Sigma = \{0,1\}$, $n=3k$

$\Sigma = \{0,1\}$, $n=3k$, $d=3$

$(\mathbb{F}_2, +, \cdot)$, $\mathbb{F}_2 = \{0,1\}$, $x \in \mathbb{F}_2^k$, $y \in \mathbb{F}_2^n$, $n=3k$

$\Sigma = \{0,1\}$, $n=3k$, $d=3$

$C \subseteq \Sigma^n$, C is a linear code

$G_{n,k}$ is a $k \times n$ matrix , $Enc: \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n$, $Enc(x) = G_{n,k} \cdot x$

$Enc(x) = G_{n,k} \cdot x$, $x \in \mathbb{F}_2^k$

G is a $k \times n$ matrix

Enc is a linear map from $\mathbb{F}_2^k$ to $\mathbb{F}_2^n$

$\mathbb{F}_2^k$ is a vector space over $\mathbb{F}_2$

Generating Matrix - G is a $k \times n$ matrix

$C = \{w \mid H \cdot w = 0\}$, H is a $(n-k) \times n$ matrix , parity check matrix (PCM)

$C^\perp = \{v \mid v \cdot w = 0 \text{ for all } w \in C\}$, $C^\perp = C^\perp$, $\dim(C) = k$

$(u \cdot w) = 0$, $(v \cdot w) = 0$

$\dim(C) = k$

$C^\perp = \{v \mid v \cdot w_i = 0 \text{ for } i=1, \dots, k\}$, $\dim(C^\perp) = n-k$

$(v \cdot G = 0 \iff v \in C^\perp)$, $\dim(C^\perp) = n-k$

• $n \times n$ matrix $G = \begin{cases} \sum_{i=1}^n a_{ii} x_i = 0 \\ \sum_{i=1}^n a_{ik} x_i = 0 \end{cases}$ $G = [a_{ij}]$

• $C = \{x \mid Hx = 0\}$ $H = \begin{pmatrix} -v_1 \\ \vdots \\ -v_{n-k} \end{pmatrix}$ $C^\perp$ is $v_1, \dots, v_{n-k}$

? H is a matrix with rows $v_1, \dots, v_{n-k}$ and columns $x_1, \dots, x_n$

$\text{dist}(C) = \min_{\substack{x \neq 0 \\ x \in C}} \text{wt}(x) = \min_{\substack{x \neq 0 \\ x \in C}} \text{dist}(x, 0)$

$\text{dist}(x, y) = |\{i \mid x_i \neq y_i\}| = |\{i \mid x_i - y_i \neq 0\}| = \text{dist}(x - y, 0)$

if C is a code with distance d then C is a linear code with minimum distance d

• C is a linear code

• C is a linear code with minimum distance d then $\text{dist}(C) = d$

$GF(2) = \mathbb{F}_2 = \{0, 1\}$ is a field

• C is a linear code with minimum distance d then H is a matrix with rows $v_1, \dots, v_{n-k}$ and columns $x_1, \dots, x_n$

$H \cdot v = 0$ where $v \in C$

$\{0, 1\}^n$ is a vector space of dimension n over $GF(2)$

$[2^l - 1, 2^l - l - 1, 3]_2$ is a code with length $2^l - 1$, dimension $2^l - l - 1$, and minimum distance 3

(n, d) is a code with length n and minimum distance d

$2^k = 2^{2^l - l - 1}$ is a code with length 2^k and minimum distance 2^l

$n+1$ is a code with length $n+1$ and minimum distance $d+1$

if C is a code with length n and minimum distance d then C is a code with length $n+1$ and minimum distance $d+1$

(this is a recursive construction)

הקודקודים הם נקודות

אם $\frac{d-1}{2}$ אזי $\frac{d-1}{2}$ נקודות

הנקודות הן נקודות

$$(*) \cdot 2^k \cdot |Ball(0, \frac{d-1}{2})| \leq 2^n$$

הנקודות הן נקודות

$$\left[\begin{array}{l} 0 \leq R \leq 1, R = \frac{k}{n} \quad \text{: (rate) קצב הקידוד} \\ \delta = \frac{d}{n} \quad \text{: מרחק} \end{array} \right]$$

$$= 2^{R \cdot n} \cdot |Ball(0, \frac{\delta}{2} \cdot n)| \leq 2^n$$

$$= 2^{R \cdot n} \cdot 2^{H(\frac{\delta}{2}) \cdot n + o(n)} \leq 2^n$$

$\Downarrow$

$$\boxed{R + H(\frac{\delta}{2}) \leq 1}$$

נקודות סוליטיות (Singleton)

$$(\delta \leq 1 - R : \text{סוליטיות}) \quad d \leq n - k + 1$$

הקוד $[2k, k, d]_q$ הוא

הנקודות הן נקודות סוליטיות, כלומר נקודות

$n - k + 1$ נקודות הן נקודות סוליטיות, כלומר נקודות

הנקודות הן נקודות סוליטיות, כלומר נקודות

הנקודות הן נקודות סוליטיות, כלומר נקודות

$$|C| = |\Sigma|^k \quad \text{הנקודות הן נקודות סוליטיות}$$

הנקודות הן נקודות סוליטיות, כלומר נקודות

$$\text{dist}(x, y) \leq n - (k - 1) = n - k + 1$$

הנקודות הן נקודות סוליטיות (MDS)

maximum distance separation

$$\text{קוד } [n, k, n - k + 1]_q$$

הנקודות הן נקודות סוליטיות, כלומר נקודות

הנקודות הן נקודות סוליטיות, כלומר נקודות

הנקודות הן נקודות סוליטיות, כלומר נקודות

$$\begin{bmatrix} c_1 & \dots & c_{n-k} & c & c' & \dots \end{bmatrix}$$

הנקודות הן נקודות סוליטיות, כלומר נקודות

הנקודות הן נקודות סוליטיות, כלומר נקודות

בני-ש H תהיה PCM של MDS קוד!

(מרחב שדה מסומן F_2)

$$t = n-k \quad \begin{pmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{t+1} & \dots & \alpha_n^{t+1} \end{pmatrix}$$

כחל בלחץ הסטיות
(moment curve)

+ הצגת הסטיות הן מלכת, מלך-מלכת, מלך-מלכת, מלך-מלכת + מלכת מלכת
המלך של השדה לך מלכת מלכת.

מלכת מלכת: מלכת מלכת מלכת מלכת - מלכת, מלכת, מלכת, מלכת, מלכת, מלכת, מלכת, מלכת.

מלכת מלכת: $F_2(1)$ מלכת מלכת מלכת.

(2) R, Q, C

(3) P מלכת, $F_p = \{0, 1, \dots, p-1\}$ מלכת מלכת מלכת.

מלכת מלכת: מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת מלכת מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

$F_p \subseteq F$

מלכת מלכת: F_p מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

מלכת מלכת: $F_p = \{0, 1, x, x+1\}$ מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.

$$\begin{aligned} x+x &= x+1 \\ x \cdot (x+1) &= x \cdot x + x = 1 \\ (x^2+x+1) &= 0 \end{aligned}$$

מלכת מלכת: $\dim F/F_p = k$ מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת, מלכת מלכת.