

-4 fze-

— 48C 11-25-26 (3)

11/5/2020

[illegible]
$$H(\delta) \cdot n < t \quad \text{and} \quad \delta \text{ is } \text{CRC}$$

$$\begin{pmatrix} n \\ \leq n \end{pmatrix} = \begin{pmatrix} n \\ \leq d \end{pmatrix} < \infty \quad V_1, \dots, V_{\begin{pmatrix} n \\ \leq d \end{pmatrix}}$$

dist → fn של קו $\rho = \sqrt{v_i - \frac{1}{T}}$ זחל'ה של

$$2^{(1-R) \cdot n} = t \quad \text{ערפול, נרמל}$$

[illegible]

1. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 2. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 3. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 4. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 5. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 6. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 7. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 8. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 9. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ
 10. $V_1 = 10$ מ"מ, $V_2 = 20$ מ"מ, $V_3 = 30$ מ"מ

הכוח W (Work)

$k = \frac{n}{2}$, n - even
 $\mathbb{F}_2$ הוא $k \times k$ ~~matrix~~ M over $\mathbb{F}_2$. $GF(2^k) = \mathbb{F}_{2^k}$ is a field

$T_\alpha: x \mapsto \alpha \cdot x$ is a linear map $\alpha \in \mathbb{F}_{2^k}$
 $T_\alpha: \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$ (is $k \times k$ matrix) over $\mathbb{F}_2$

$\mathbb{F}_2$ has $k \times k$ (is $k \times k$ matrix) M_α over $\mathbb{F}_2$ (matrix)
 $\{0,1\}^k$ is V_α , $V_\alpha = \{x, \alpha \cdot x \mid x \in \mathbb{F}_{2^k}\}$ is a subspace, $\alpha \in \mathbb{F}_{2^k}$

$$V_\alpha = \left\{ \begin{pmatrix} I_{k \times k} \\ M_\alpha \end{pmatrix} \cdot \vec{x} \mid x \in \{0,1\}^k \right\}$$

$\vec{v} \in V_\alpha \cap V_\beta$ is a vector in the intersection

$$\vec{v} = (x, \alpha x) \text{ for some } x$$

$$\vec{v} = (y, \beta y) \text{ for some } y$$

$$\vec{v} = \vec{0} \iff x = y = 0 \iff \alpha x = \beta y, \alpha \neq \beta$$

over $\mathbb{F}_2$, $t = 2^{(n-k)/2}$, n is even, $2^k = 2^{\frac{1}{2}n} = t$
 is a subspace, $\text{dist}(\vec{v}, \vec{0}) = t$

$$\begin{aligned} \text{dist}(\vec{v}, \vec{0}) &= t \\ H(\vec{v}) &= \frac{1}{2} \\ \delta &= H(\frac{1}{2}) \end{aligned}$$

Rate = $\frac{1}{2}$? $(x, \alpha x, \beta x)$ is a vector
 Rate $\leq \frac{1}{2}$? $(x, \alpha x)$ is a vector

is a vector, $\vec{v} = (x, \alpha x, \beta x)$ is a vector
 is a vector, $\vec{v} = (x, \alpha x, \beta x)$ is a vector

פערמאט קאז'ס :

* הוספת הית' סטיות :

אם C הוא $[d, k, n]_q$ קוד, ו- $d-1$ אינו שלילי, אז C הוא קוד פארקליט, ומוסיף את הית' סטיות

$$C^\perp = \{ (v, \sum v_i x_i) \mid v \in C \}$$

קוד קוד $[n+1, k, d+1]_q$ ("הוספת הית' סטיות")

* ניקח C אם C הוא $[d, k, n]_q$ קוד, אז

יש לנו קוד $C^\perp$ $[n+1, k, d+1]_q$ קוד, $C^\perp$ ("הוספת הית' סטיות")

$$v = (v_1, \dots, v_n)$$

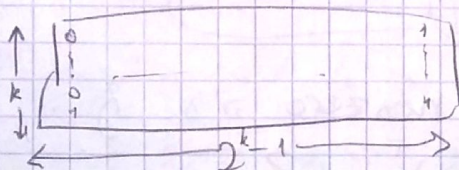
(כאן v_i הוא האיבר v_i ב- C)

הסבר: C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$. נבדוק את זה.

(יש הוכחה גם אם C אינו קוד, אבל זה לא נכנס אליו)

עכשיו: C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

הוכחה: קוד C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.



יש לנו C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

הוכחה: קוד C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

הוכחה: קוד C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

הוכחה: קוד C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

* Direct Product: $C = C_1 \otimes C_2$

יש לנו קוד C הוא קוד $[d, k, n]_q$

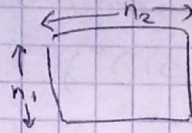
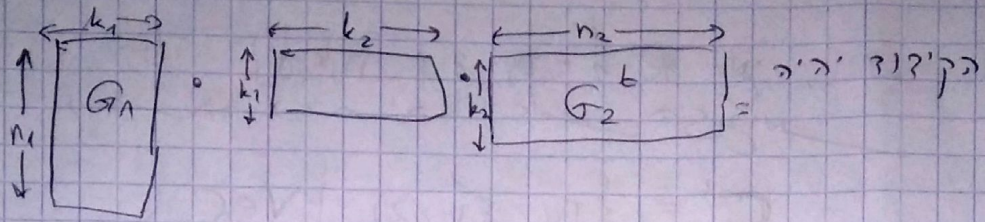
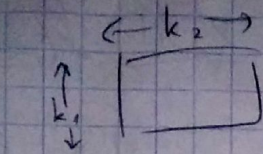
$$C = C_1 \otimes C_2$$

הוכחה: קוד C הוא קוד $[d, k, n]_q$ אז C הוא קוד $[d, k, n]_q$ ו- $C^\perp$ הוא קוד $[n+1, k, d+1]_q$.

$C_1 = [d_1, k_1, n_1]_q$ קוד

$C_2 = [d_2, k_2, n_2]_q$ קוד

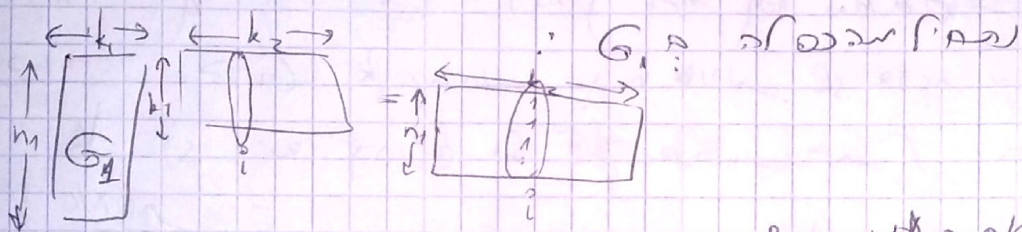
סעיף 3: נחשב את המרחק בין G_1 ו- G_2



(כיוון ש- $G = G_1 \otimes G_2$)

המרחק בין G_1 ו- G_2 הוא k_1

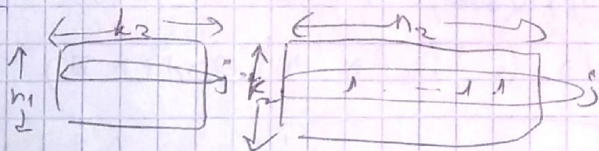
ואם d_1 אז d_2



אם המרחק בין G_1 ו- G_2 הוא k_1 non-zero

הוא לא אפס ואם d_1 אז d_2 non-zero

(כיוון ש- G_2^t)

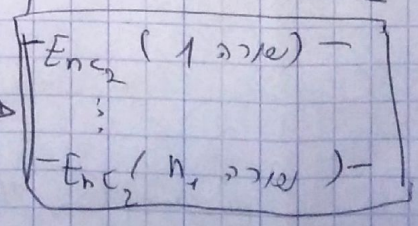
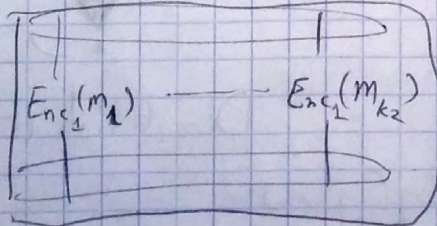
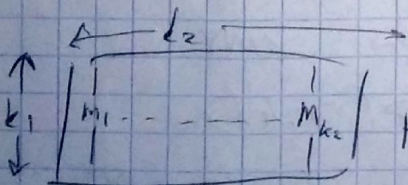


אם המרחק בין G_1 ו- G_2 הוא k_1 non-zero

אם המרחק בין G_1 ו- G_2 הוא k_1 non-zero

$dist = d_1 \cdot d_2$

הערה: המרחק בין קווי G_1 ו- G_2 הוא k_1



(ולכן אם המרחק בין G_1 ו- G_2 הוא k_1 non-zero)

Concert. 22222 (*)

מחזורי חיים

$(v_1, \dots, v_n) \in \mathbb{F}_q^n$
 $(\underbrace{v_1}_{\in \mathbb{F}_2}, \dots, \underbrace{v_n}_{\in \mathbb{F}_2}) \in \mathbb{F}_2^{l \cdot n}$

$\Rightarrow [l \cdot n, l \cdot k, n - k + 1]$

[illegible]

7310ND 7321

$$(s, \sqrt{3} \cdot n^2) \quad \text{Exp} - [m, k, d]_{n=0}^{\infty} - C_0 \cdot n^d$$

$$(\cdot, \cdot)_{N(\mathcal{N})} \text{ auf } [n_2, \underline{l}, \underline{d_2}]_{\underline{q_2}} - \underline{G_2} \text{ :}$$

eg. $\{n_1, n_2, k_1, d_1, d_2\}_2$, $C = C_1 \circ C_2$ zip and

דאס איז q_2 פאר k_1 און C_1 איז פאר k_2 .
 און k_1 איז פאר q_2 (און C_2 איז פאר q_1).
 און C_1 איז פאר q_1 און C_2 איז פאר q_2 .
 און q_1 איז פאר C_1 און q_2 איז פאר C_2 .
 און C_1 איז פאר q_1 און C_2 איז פאר q_2 .

$$g_1 = g_2 \mapsto (g_2)^2 \text{ and } g_1 \mapsto g_2 \text{ and } g_2 \mapsto g_1$$

התחלתי לכתוב את המכתב הזה

$$F_{nc}(0) = 0$$

$$\{C_2, \dots, C_n\}$$

הערה: נראה שהקוד C_2 יכול להיות באורך $n-k$ במקום $n-k+1$.
~~אבל~~ C_2 עדיף להיות באורך $n-k+1$ במקום $n-k$.

RS = Hadamard על $\mathbb{F}_2$

$$RS: [n, k, n-k+1]$$

$$Had: [n-1, \log n, \frac{n}{2}]_2 \quad q=n=2^{\log n}$$

$$\approx [n^2, k \log n, \frac{1}{2} n \log n]$$

$$R = \frac{k \cdot \log n}{n \cdot n}$$

$$\delta = \frac{1}{2} \frac{n-k}{n}$$

$$R = \frac{1}{2} \frac{\log n}{n} - k = \frac{n}{2}$$

שיעור הנדסה

$$\delta = \frac{1}{4}$$

למשל: המרחק בין הקודים $[22, 2, 2]_2$ הוא 20.

$$d = (22) \cdot H\left(\frac{1}{2}\right)$$

$$= 8 \cdot 22$$

נראה כי הקודים $[2n \log n, k \log n, \delta \cdot 2n \log n \cdot (n-k+1)]_2$ הם קודים RS.

$$[2n \log n, k \log n, \delta \cdot 2n \log n \cdot (n-k+1)]_2 \leftarrow \begin{cases} RS[n, k, n-k+1]_{2^{\log n}} \\ W: [2 \log n, \log n, \delta \cdot 2 \log n]_2 \end{cases}$$

$$R = \frac{1}{2} \cdot \frac{k}{n}$$

$$\text{distance} = \delta \cdot \frac{n-k+1}{n}$$

כדי שיהיה קוד RS, צריך שיהיה $k \leq n$ ו- $\delta \leq \frac{1}{2}$.
 נראה ש- $R \rightarrow \frac{1}{2}$ ו- $\delta \rightarrow \frac{1}{2}$.

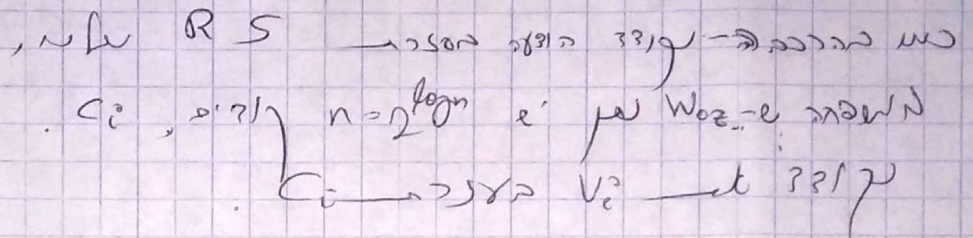
$$R = \frac{1}{4}, \quad k = \frac{n}{2}$$

$$\delta = \frac{1}{2} H\left(\frac{1}{2}\right)$$

הערה: במקרה של $poly(n)$ קודים, נראה ש- W הוא קוד RS.



2. $\frac{1}{2}$ and 3 are

$$[2n \log n, R_1 n \log n, (1-R_1-\varepsilon)n \log n]_2 \quad \text{if } n \geq n_2$$


על המבחן, ש/ח, חתום, PS, ע' ב' ב'

[illegible]
$$d\epsilon \leq \frac{1}{2} \frac{dV_i}{V_i}$$