

הוא מיושם לרוב מדינת ישראל

~~הוא מיושם לרוב מדינת ישראל~~
~~הוא מיושם לרוב מדינת ישראל~~

Reed - Solomon קוד : 1/2
 Reed - Miller קוד
 גילברט - ורשמן קוד
 וזנקרפט קוד

Reed - Solomon קוד

הוא קוד F קוד $n \leq q$ $[n, k, n-k+1]$ קוד

הוא קוד F^k : F^k הוא F k פעמים
 $(a_0, a_1, \dots, a_{k-1}) \in F^k \Leftrightarrow \sum_{i=0}^{k-1} a_i X^i$

$\{f(x) \mid f \in F \text{ ו-} k \geq \deg f\}$

$a_1, \dots, a_n \in F$ קוד n איברי F

$$\text{Enc}(F) = (f(a_1), \dots, f(a_n))$$

כיוון שהקוד F הוא קוד F $k-1$ פעמים
 הוא קוד F $k-1$ פעמים

הוא קוד F $k-1$ פעמים

הוא קוד F $k-1$ פעמים $(k-1) \geq 0$ $0 \neq$
 $n - (k-1) = n - k + 1$

$X - \alpha \mid f$ $f(\alpha) = 0$ $\alpha \in F$

Vandermonde

הוא קוד F $k-1$ פעמים

$$\begin{bmatrix} 1 & \alpha_1 & \dots & \alpha_1^{k-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{k-1} \end{bmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} f(\alpha_1) \\ \vdots \\ f(\alpha_n) \end{pmatrix}$$

הוא קוד F $k-1$ פעמים

$C^\perp \subseteq H$ $C^\perp = \{u \mid u \perp v \forall v \in C\}$

(byte)

$$F = GF(2^8)$$

data is bytes 256. with

$$[256, 240, 17]_{28}$$

מבוא : (מלאו את השאלות)

$$(\mathbb{F}_2 \text{ Ar 24}) \quad [2048, 1920, 17]_2$$

אם נניח שהמחיר של המוצר הוא 10 שקלים, אז:

Reed-Solomon $\rightarrow$ have no val elements in $11/2$ elements $\rightarrow 15$ for

[illegible][illegible][illegible]

ה' F_{28} . בעד 25 יום קריה י"ח אלול.

במה הקורא והסדרן מלווה נהיה? כי שאלה.

: Reed-Miller 12/p

[illegible]

$$f(x, y) = \sum_{i, j=0}^{\infty} a_{ij} x^i y^j$$

Fig. 10. New

$$\cdot (l+1)^2$$

$$\text{Enc}(F) = (F(\alpha, \beta))_{\alpha, \beta \in \mathbb{F}_q^2}$$

$$[n = 9^2, l = (l+1)^2, d = ?]_9$$

2/2

$$.9 = \sqrt{n}$$

20/01/21

$$\text{dist} = (q - l)^2$$

$$: \sim \sim \sim$$

$$f = \sum_{i=0}^l x_i' f_i(x)$$

Two more men (22)

2) ~~התא~~ $\frac{1}{2}$ ו $\frac{1}{2}$ כחלק

100% 100% 100% 100%

are 1 wa 5 e

משהו 100 מיליון ק"מ.

(total degree)

[illegible]

ההחלטה של הממשלה לא
לעצור את המגפה (לפי)

$$f \mapsto (f(z))_{z \in \overline{\mathbb{A}_q}^m}$$

$\therefore l < 9$ $\therefore$ $l \leq 8$

$$F = \sum_{\substack{d_1, \dots, d_m \\ d_i \geq 0 \\ \sum d_i \leq l}} \alpha_{d_1 d_2 \dots d_m} \cdot X_1^{d_1} \cdot \dots \cdot X_m^{d_m}$$

: 2/2/2

$$\binom{m+l}{m} = \text{מספר המילים } m \text{ בתור } m+l$$

$$n = q^m$$

$$\left(1 - \frac{l}{q}\right) \cdot q^m \leq \text{מרחק}$$

$$\frac{1}{q} = \text{מרחק המינימום}$$

$$(x_1-1) \cdot \dots \cdot (x_l-1)$$

$$\left[q^m, \binom{m+l}{m}, \left(1 - \frac{l}{q}\right) \cdot q^m \right]_q$$

$$l \approx \frac{\log k}{\log \log k}, m \approx \frac{\log k}{\log \log k}, q \approx \log k$$

$$\binom{m+l}{m} \approx \left(\frac{m+l}{m}\right)^m \approx \left(\frac{l}{m}\right)^m = k$$

$$q^m = k^2$$

$$\text{dist} = \left(1 - \frac{l}{q}\right) \cdot q^m = \left(1 - \frac{1}{\log k}\right) \cdot k^2 = (1 - o(1)) \cdot k^2$$

$$[n, \sqrt{n}, (1 - o(1)) \cdot n]_{O(\log k)} \approx [k^2, k, (1 - o(1)) \cdot k^2]_{\log k}$$

כל מה שאחר קוד שומר בעל הקאוד רגיל
 רק שומר אותן הבה שומר (בעל רגלי הקאוד)

מקרה ב- $q \geq l$: הנוסחה פשוטה במיוחד וניתן להשתמש בה

כל היות l , וישל שומר או מופיע $q-1$

מילוי קודק כל קודק

$n = q^m$ (מספר המילים) או k (מספר המילים)

$$0 \leq b < q-1, l = \alpha \cdot (q-1) + b, d = q^{m-\alpha} \cdot \left(1 - \frac{b}{q}\right)$$

$$\prod_{i=0}^{\alpha-1} (x_i - 0) \cdot \dots \cdot (x_i - (q-2)) \cdot [x_{\alpha} - 1] \cdot \dots \cdot [x_{\alpha} - b]$$

$k=?$

$$d = 2^{m-l}, k = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{l} \approx \binom{m}{l}, n = q^m, q = 2$$

$$RM(m, l) = [2^m, \binom{m}{l}, 2^{m-l}]_2$$

$$[n, \frac{1}{2}n, \sqrt{n}]_2, l = \frac{m}{2}$$

(ה- dist) - מרחק המינימום

BEC (בעל קוד) - מרחק המינימום, מרחק המינימום, מרחק המינימום

! 27~2/10 12/p

$$RM(m, 1) = [2^m, m+1, \frac{1}{2} \cdot 2^m]_2$$

ב קצת פרטנריות וסוף חצי קצת פרטנריות.
זה הכי טוב שאפשר כש- n , $\frac{n}{2}$ קבועים.

שאלה במה נחלק:

$A \cdot A^T = n \cdot I$ e $p \neq 1$ für $n \times n$ ist A ist

$\cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ - row 2/2 ✓

$$\therefore \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad - (1/2) \quad \checkmark$$

המרחק המינימלי בין קודים:

הקבוצה של קודים $C = \{C_i\}$, $C_i = [n_i, k_i, d_i]_q$, $n_i \rightarrow \infty$

$$R(C) = \liminf_{i \rightarrow \infty} \frac{k_i}{n_i}$$

$$\delta(C) = \liminf_{i \rightarrow \infty} \frac{d_i}{n_i}$$

הקבוצה של קודים

המרחק המינימלי

עבור קודים $R(C), \delta(C) > 0$ נקרא קודים אסימפטוטיים

כל קודים אסימפטוטיים מקיים $\delta \leq \frac{1}{2}$

Gilbert-Varshamov Lemma: $R + H(\delta) < 1$ $\Rightarrow \exists R, \delta$

יש קודים עם $R(C) \geq R, \delta(C) \geq \delta$

הוכחה של Gilbert: בנה מרחב $C_0 = \phi \subseteq \{0, 1\}^n$

בבסיס C_0 כל קודים שגודלם $\leq \delta n$ ונפרד, ולכן C_0 לא ריק

המרחב C_0 ונפרד δn כל קודים $\delta n \geq H(\delta) \cdot n$ נפרד

$$Vol(Ball(0, \delta n)) \geq 2^{H(\delta) \cdot n} \geq 2^{(H(\delta) + \epsilon) \cdot n}$$

$$Vol(Ball(0, \delta n)) \leq 2^{(H(\delta) + \epsilon) \cdot n}, n > n_0, n_0 \text{ ו- } \epsilon > 0$$

$$|C_0| \geq \frac{2^n}{2^{(H(\delta) + \epsilon) \cdot n}} = 2^{(1 - H(\delta) - \epsilon) \cdot n}$$

~~הוכחה של Gilbert~~

$$|R| \geq 1 - H(\delta) - \epsilon$$

בנקודה $\frac{1}{2} \delta n$ כל קודים $\frac{1}{2} \delta n$ נפרד $1 - H(\frac{1}{2} \delta)$

הוכחה של Varshamov: קודים $k \times n$ G מרחב G מרחב G

$$|C| = (1 - H(\delta) - \epsilon) \cdot n$$

כל קודים δn נפרד δn $dist$ כל קודים δn נפרד

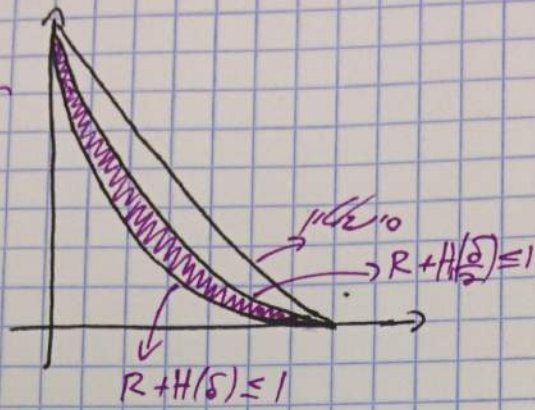
כל קודים δn נפרד δn $x \in \{0, 1\}^k$ נפרד

$$P(wt(x) \leq \delta n) \leq \frac{Vol(Ball(0, \delta n))}{2^n}$$

$$\binom{n}{\delta n} \cdot 2^{-\epsilon n} = \frac{2^k \cdot 2^{H(\delta + \epsilon) \cdot n}}{2^n}$$

ההסתברות $\geq$ כל קודים δn נפרד

در این شکل فرض می‌کنیم



فرض کنیم : فرض