

סימון: יהי \mathbb{F} שדה ויהיו $m, n \in \mathbb{N}_+$ אזי $\mathbb{F}^{m \times n} = M_{m \times n}(\mathbb{F})$

מרחק האמינג: תהא X קבוצה אזי נגדיר $\Delta : X^n \times X^n \rightarrow \mathbb{N}$ כך $\Delta(x, y) = |\{i \in [n] \mid x_i \neq y_i\}|$

טענה: תהא X קבוצה אזי Δ משרה את נורמת ℓ_0

משקל האמינג: יהי \mathbb{F} שדה אזי נגדיר $w : \mathbb{F}^n \rightarrow \mathbb{N}$ כך $w(x) = \Delta(x, 0)$

קוד לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ אזי $\mathcal{C} \subseteq [q]^m$

גודל האלפבית בקוד לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי q

גודל הבלוק בקוד לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי m

מרחק בקוד לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי $d[\mathcal{C}] = \min_{x \neq y} \Delta(x, y)$

מימד/קצב בקוד לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי $r[\mathcal{C}] = \log_q |\mathcal{C}|$

סימון: יהיו $q, m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי $[m, r[\mathcal{C}], d[\mathcal{C}], q]$ לתיקון שגיאות.

טענה: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות יהי $w \in \mathcal{C}$ ויהי $w' \in [q]^m$ באשר $\Delta(w, w') \leq d - 1$ אזי $w' \notin \mathcal{C}$

טענה: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות יהי $w \in \mathcal{C}$ ויהי $w' \in [q]^m$ באשר $\Delta(w, w') \leq \lfloor \frac{d-1}{2} \rfloor$ אזי $\arg \min_{v \in \mathcal{C}} \Delta(v, w') = w$

משפט חסם הסינגלטון: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות אזי $r \leq m - d + 1$

קוד חזרות: יהיו $q, m, k \in \mathbb{N}_+$ אזי $\mathcal{C}_{k\text{-rep}} = \{w \in [q]^{mk} \mid \forall i \in [mk]. w_i = w_{i \bmod m}\}$

טענה: יהיו $q, m, k \in \mathbb{N}_+$ אזי $\mathcal{C}_{k\text{-rep}}$ הינו קוד $[mk, m, k, q]$ לתיקון שגיאות.

קוד שאריות: יהיו $q, m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}} = \{w \in [q]^{m+1} \mid w_{m+1} = (\sum_{i=1}^m w_i \bmod q)\}$

טענה: יהיו $q, m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}}$ הינו קוד $[m+1, m, 2, q]$ לתיקון שגיאות.

קוד האמינג: יהי $m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hamming}} = \left\{ x \in \mathbb{F}_2^{2^m-1} \mid \forall i \in [m]. \left(\bigoplus_{k \in \binom{[2^m-1]}{i}} x_k = 0 \right) \right\}$

טענה: יהי $m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hamming}}$ הינו קוד $[2^m - 1, 2^m - m - 1, 3, 2]$ לתיקון שגיאות.

טענה: יהיו $m, r, d, q \in \mathbb{N}_+$ עבורם קיים קוד $[m, r, d, q]$ לתיקון שגיאות אזי קיים $d' \geq d$ עבורו קיים קוד

$[m \lceil \log(q) \rceil, r \log(q), d', 2]$ לתיקון שגיאות.

טענה: יהיו $m, r, d, q \in \mathbb{N}_+$ עבורם קיים קוד $[m, r, d, q]$ לתיקון שגיאות ויהי $\ell \in \mathbb{N}_+$ אזי קיים קוד $[\ell m, \ell r, d, q]$ לתיקון שגיאות.

טענה: יהי $d \in \mathbb{N}_{\text{odd}}$ ויהיו $m, r \in \mathbb{N}_+$ עבורם קיים קוד $[m, r, d, 2]$ לתיקון שגיאות אזי קיים קוד $[m+1, r, d+1, 2]$ לתיקון שגיאות.

משפט האמינג: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq q^m \cdot \left(\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{m}{i} \cdot (q-1)^i \right)^{-1}$

למה פלוטקין: יהיו $d, q, m \in \mathbb{N}_+$ באשר $d \geq \left(1 - \frac{1}{q}\right)m$ ויהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq \frac{d}{d + \frac{m}{q} - m}$

טענה: יהיו $d, m \in \mathbb{N}_+$ באשר $d \leq \frac{m}{2}$ ויהי \mathcal{C} קוד $[m, r, d, 2]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq d \cdot 2^{m-2d+2}$

קוד לינארי לתיקון שגיאות: יהיו $q, m \in \mathbb{N}_+$ באשר \mathbb{F}_q שדה אזי קוד לתיקון שגיאות $\mathcal{C} \subseteq \mathbb{F}_q^m$ המקיים כי \mathcal{C} מרחב וקטורי.

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $\dim(\mathcal{C}) = r$

מטריצה יוצרת: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות ויהי $b_1 \dots b_r \in \mathcal{C}$ בסיס אזי נגדיר $M_C \in \mathbb{F}_q^{m \times r}$ כך $C_i(M_C) = b_i$

לכל $i \in [r]$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $\mathcal{C} = \{M_C \cdot v \mid v \in \mathbb{F}_q^r\}$

מערכת משוואות לינאריות: יהי \mathbb{F} שדה יהיו $m, n \in \mathbb{N}_+$ תהא $M \in \mathbb{F}^{m \times n}$ ויהי $t \in \mathbb{F}^m$ אזי (M, t, \mathbb{F})

ערך של מערכת משוואות לינאריות: תהא (M, t, \mathbb{F}) מערכת משוואות לינאריות אזי $\text{Val}((M, t, \mathbb{F})) = \min_{x \in \mathbb{F}^n} \left(\frac{1}{m} \cdot \Delta(Mx, t) \right)$

בעיית חיפוש הוקטור הקרוב ביותר: תהא (M, t, \mathbb{F}) מערכת משוואות לינאריות ויהי $\varepsilon > 0$ אזי $\text{CVP-code-search}((M, t, \mathbb{F}), \varepsilon) = v$

באשר $\|Mv - t\|_0 \leq \varepsilon$

בעיית הוקטור הקרוב ביותר: $\text{CVP-code} = \{((M, t, \mathbb{F}), \varepsilon) \mid \text{Val}((M, t, \mathbb{F})) \leq \varepsilon\}$

טענה: יהיו $q, m, k \in \mathbb{N}_+$ אזי $\mathcal{C}_{k\text{-rep}}$ קוד לינארי לתיקון שגיאות.

מסקנה: יהיו $q, m, k \in \mathbb{N}_+$ אזי $M_{\mathcal{C}_{k\text{-rep}}} = \begin{pmatrix} I_m \\ \vdots \\ I_m \end{pmatrix}$

טענה: יהיו $q, m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}}$ קוד לינארי לתיקון שגיאות.

מסקנה: יהיו $q, m \in \mathbb{N}_+$ אזי $M_{\mathcal{C}_{\text{parity}}} = \begin{pmatrix} I_m \\ \mathbf{1}^T \end{pmatrix} = \begin{pmatrix} I_m \\ \mathbf{1}^T \end{pmatrix}^T$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $d = \min_{v \in \mathcal{C}} \Delta(v, 0)$

בעיית הוקטור הקצר ביותר: $\text{SVP-code} = \{((M, 0, \mathbb{F}), \varepsilon) \mid \exists v \neq 0. \|Mv\|_0 \leq \varepsilon\}$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי קיים קוד לינארי $[m, r, d, q]$ לתיקון שגיאות \mathcal{D} עבורו קיימת $A \in \mathbb{F}_q^{(m-r) \times r}$ המקיימת $M_{\mathcal{D}} = \begin{pmatrix} I_r \\ A \end{pmatrix}$.

סימון: יהי \mathbb{F} שדה יהיו $m, n \in \mathbb{N}_+$ ותהא $M \in \mathbb{F}^{m \times n}$ אזי $R(M) = \{R_i(M) \mid i \in [m]\}$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי

• לכל $V \subseteq \mathcal{C}$ באשר $\dim(V) = r - 1$ מתקיים $|R(M_{\mathcal{C}}) \cap V| \leq m - d$

• קיים $V \subseteq \mathcal{C}$ המקיים $\dim(V) = r - 1$ וכן $|R(M_{\mathcal{C}}) \cap V| = m - d$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי קיים $d' \geq \left\lceil \frac{d}{q} \right\rceil$ עבורו קיים קוד לינארי $[m - d, r - 1, d', q]$ לתיקון שגיאות.

משפט גרייסמור: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $m \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil$

למה: יהי $q \in \mathbb{N}_+$ באשר \mathbb{F}_q שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $x \in \mathbb{F}_q^r \setminus \{0\}$ אזי לכל מתקיים $b \in \mathbb{F}_q^m$ $\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}}(Mx = b) = \frac{1}{q^m}$

סימון: יהי $q \in \mathbb{N}_+$ באשר \mathbb{F}_q שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $M \in \mathbb{F}_q^{m \times r}$ אזי $\mathcal{C}_M = \{M \cdot v \mid v \in \mathbb{F}_q^r\}$

משפט: יהי $q \in \mathbb{N}_+$ באשר \mathbb{F}_q שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $\delta \in (0, 1)$ אזי

$$\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}} \left(d[\mathcal{C}_M] \leq (1 - \delta) \left(m - \frac{m}{q} \right) \right) \leq |\mathcal{C}_M| \cdot \exp \left(-\frac{\delta^2}{2} \left(m - \frac{m}{q} \right) \right)$$

קוד לינארי \mathcal{C}_M

הקוד הדואלי: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $\mathcal{C}^\vee = \{w \in [q]^m \mid \forall c \in \mathcal{C}. \langle w, c \rangle = 0\}$

טענה: יהי \mathcal{C} קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי קיים $d' \in \mathbb{N}_+$ עבורו \mathcal{C}^\vee הינו קוד לינארי $[m, m - r, d', q]$ לתיקון שגיאות.

מטריצת בדיקת שאריות: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי $H_{\mathcal{C}} = M_{\mathcal{C}^\vee}$

טענה: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי $\mathcal{C} = \ker(H_{\mathcal{C}}^T)$

קוד מקסימלי לתיקון שגיאות: קוד $[m, r, d, q]$ לתיקון שגיאות המקיים $d = m - r + 1$

טענה: יהי $q \in \mathbb{N}_+$ באשר \mathbb{F}_q שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $M \in \mathbb{F}_q^{m \times r}$ אזי \mathcal{C}_M קוד לינארי מקסימלי לתיקון שגיאות) \iff (לכל $A \in \mathcal{P}_r(R(M))$ מתקיים כי A בת"ל).

טענה: יהי \mathcal{C} קוד לינארי מקסימלי לתיקון שגיאות אזי \mathcal{C}^\vee הינו קוד לינארי מקסימלי לתיקון שגיאות.

משפט גילברט-וורשאמוב: יהיו $d, m \in \mathbb{N}_+$ באשר $d \leq m$ ויהי $q \in \mathbb{P}$ אזי קיים קוד לינארי $[m, k, d, q]$ לתיקון שגיאות \mathcal{C} המקיים $|\mathcal{C}| \geq q^m \cdot \left(\sum_{i=0}^{d-1} \binom{m-1}{i} \cdot (q-1)^i \right)^{-1}$

למה: יהי $d \in \mathbb{N}_{\geq 2}$ יהיו $k, m \in \mathbb{N}_+$ באשר $k \leq m$ ויהי $q \in \mathbb{P}$ עבורו $\sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k}$ אזי קיים $H \in \mathbb{F}_q^{m \times (m-k)}$ עבורו לכל $A \in \mathcal{P}_{d-1}(R(M))$ מתקיים כי A בת"ל.

משפט גילברט-וורשאמוב: יהי $d \in \mathbb{N}_{\geq 2}$ יהיו $k, m \in \mathbb{N}_+$ באשר $k \leq m$ ויהי $q \in \mathbb{P}$ עבורו $\sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k}$ אזי קיים קוד לינארי $[m, k, d, q]$ לתיקון שגיאות \mathcal{C} המקיים $|\mathcal{C}| \geq q^m \cdot \left(1 + \sum_{i=0}^{d-2} \binom{m-1}{i} \cdot (q-1)^i \right)^{-1}$

סכימת חלוקת סוד מושלמת: תהייה X, Y קבוצות יהי $n \in \mathbb{N}_+$ ויהי $k \in [n]$ אזי $f: X \rightarrow Y^n$ עבורה

• קיימת $g: Y^k \rightarrow X$ עבורה לכל $s \in X$ ולכל $p_1, \dots, p_k \in [n]$ מתקיים $g(f(s)_{p_1}, \dots, f(s)_{p_k}) = s$

• לא קיימת $g: Y^{k-1} \rightarrow X$ עבורה לכל $s \in X$ ולכל $p_1, \dots, p_{k-1} \in [n]$ מתקיים $g(f(s)_{p_1}, \dots, f(s)_{p_{k-1}}) = s$

טענה: יהיו $\ell, k \in \mathbb{N}_+$ באשר $\ell \leq k$ יהי \mathbb{F} שדה סופי באשר $|\mathbb{F}| \geq k$ יהיו $x_1 \dots x_\ell \in \mathbb{F}$ שונים ונגדיר $\varphi: \mathbb{F}_{\leq k-1}[x] \rightarrow \mathbb{F}^\ell$ כך $\varphi(p) = (p(x_i))_{i=1}^\ell$

• אם $\ell = k$ אז φ איזומורפיזם וכן φ, φ^{-1} חשיבות בזמן פולינומי.

• אם $\ell < k$ אז לכל $y \in \mathbb{F}^\ell$ מתקיים כי $\varphi^{-1}(y)$ מרחב אפני ממימד $k - \ell$.

סכימת שמיר: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $n \in \mathbb{N}_+$ באשר $n < q$ ויהי $k \in [n]$ אזי נגדיר $f: \mathbb{F}_q \times (\mathbb{F}_q \setminus \{0\})^{k-1} \rightarrow (\mathbb{F}_q^2)^n$ כך $f(s, a) = \left((s_i, s + \sum_{j=1}^{k-1} a_j s_i^j) \right)_{i=1}^n$ באשר $s_1 \dots s_n \in \mathbb{F}_q \setminus \{0\}$ שונים.

מסקנה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $n \in \mathbb{N}_+$ באשר $n < q$ ויהי $k \in [n]$ אזי סכימת שמיר הינה סכימת חלוקת סוד מושלמת.

קוד ריד-סולומון: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $m \in [q]$ ויהי $r \in [m]$ אזי $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ שונים אזי

$$RS_q[m, r] = \left\{ (f(\alpha_i))_{i=1}^m \mid f \in (\mathbb{F}_q)_{\leq r-1}[x] \right\}$$

הערה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $r \in [q]$ אזי $RS_q[q, r] \simeq (\mathbb{F}_q)_{\leq r-1}[x]$

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $m \in [q]$ ויהי $r \in [m]$ אזי $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ הינו קוד לינארי מקסימלי $[m, r, m - r + 1, q]$ לתיקון שגיאות.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה יהי $m \in [q]$ ויהי $r \in [m]$ אזי $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ אזי $(M_{RS_q[m, r]})_{i,j} = \alpha_i^{j-1}$ לכל $(i, j) \in [m] \times [r]$

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהי $i \in \{0, \dots, q-2\}$ אזי $\sum_{x \in \mathbb{F}_q} x^i = 0$

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהי $r \in [q]$ אזי $\text{RS}_q[q, r]^\vee = \text{RS}_q[q, q - r]$.

אלגוריתם ברלקמפ-וולץ: ...

קוד ריד-מילר: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r \in \mathbb{N}_+$ אזי $\text{RM}_q[m, r] = \left\{ (f(\alpha))_{\alpha \in \mathbb{F}_q^m} \mid f \in (\mathbb{F}_q)_{\leq r}[x_1, \dots, x_m] \right\}$.

הערה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r \in \mathbb{N}_+$ אזי $\text{RM}_q[m, r] \simeq (\mathbb{F}_q)_{\leq r}[x_1, \dots, x_m]$.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r \in \mathbb{N}_+$ אזי קיימים $r, d \in \mathbb{N}_+$ עבורם $\text{RM}_q[m, r]$ הינו קוד לינארי $[q^m, r, d, q]$ לתיקון שגיאות.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r \in \mathbb{N}_+$ באשר $r < q$ אזי $r \cdot [\text{RM}_q[m, r]] = \binom{m+r}{r}$.

טענה: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r \in \mathbb{N}_+$ באשר $r < q$ אזי $d \cdot [\text{RM}_q[m, r]] \geq (q - r) q^{m-1}$.

טענה: יהיו $m, r \in \mathbb{N}_+$ אזי $r \cdot [\text{RM}_2[m, r]] = \sum_{i=0}^r \binom{m}{i}$.

משפט: יהי $q \in \mathbb{N}$ באשר \mathbb{F}_q שדה ויהיו $m, r, a, b \in \mathbb{N}_+$ באשר $r = a(q - 1) + b$ חלוקה עם שארית אזי

$$d \cdot [\text{RM}_q[m, r]] \geq (q - b) q^{m-a-1}.$$

טענה: יהיו $m, r \in \mathbb{N}_+$ אזי $\text{RM}_2[m, r]^\vee = \text{RM}_2[m, m - r - 1]$.

טענה: יהיו $m, r \in \mathbb{N}_{\geq 2}$ אזי $\text{RM}_2[m, r] = \{(u, u + v) \mid (u \in \text{RM}_2[m - 1, r]) \wedge (v \in \text{RM}_2[m - 1, r - 1])\}$.

שרשור קודים לתיקון שגיאות: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות יהי \mathcal{C}' קוד $[m', \log_{q'}(q), d', q']$ לתיקון שגיאות ותהא $\rho : [q] \rightarrow \mathcal{C}'$ הפיכה אזי $\mathcal{C} \circ \mathcal{C}' = \{(\rho(w_i))_{i=1}^m \mid w \in \mathcal{C}\}$.

טענה: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות ויהי \mathcal{C}' קוד $[m', \log_{q'}(q), d', q']$ לתיקון שגיאות אזי $\mathcal{C} \circ \mathcal{C}'$ הינו קוד $[m \cdot m', r \cdot \log_{q'}(q), d \cdot d', q']$ לתיקון שגיאות.

הערה: יהי \mathcal{C} קוד $[m, r, d, q]$ לתיקון שגיאות יהי \mathcal{C}' קוד $[m', \log_{q'}(q), d', q']$ לתיקון שגיאות ותהא $\rho : [q] \rightarrow \mathcal{C}'$ הפיכה אזי $\mathcal{C} \circ \mathcal{C}' \simeq \left\{ h : [m] \times [m'] \rightarrow [q] \mid \exists w \in \mathcal{C}. h(i, j) = (\rho(w_i))_j \right\}$.

הגדרה: יהי $n \in \mathbb{N}$ ותהא $S \subseteq [n]$ אזי נגדיר $\chi_S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ כך $\chi_S(x) = \sum_{i \in S} x_i$.

קוד אדמר: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hadamard}} = \left\{ (\chi_S(x))_{x \in \mathbb{F}_2^n} \mid S \subseteq [n] \right\}$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hadamard}}$ הינו קוד לינארי $[2^n, n, 2^{n-1}, 2]$ לתיקון שגיאות.

הערה: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hadamard}} \simeq \left\{ \chi_S \mid S \subseteq [n] \right\}$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hamming}} = \left\{ (\chi_S(x))_{x \in \mathbb{F}_2^n \setminus \{0\}} \mid S \subseteq [n] \right\}$.

קוד דיקטטורות: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Dic}} = \left\{ (\chi_{\{i\}}(x))_{x \in \mathbb{F}_2^n} \mid i \in [n] \right\}$.

טענה: יהי $n \in \mathbb{N}_+$ אזי \mathcal{C}_{Dic} הינו קוד $[2^n, \log_2(n), 2^{n-1}, 2]$ לתיקון שגיאות.

הערה: יהי $n \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Dic}} \simeq \left\{ \chi_{\{i\}} \mid i \in [n] \right\}$.

כדור: תהא X קבוצה יהי $r \in \mathbb{R}_+$ ויהי $x \in X$ אזי $B_r(x) = \{y \in X \mid \Delta(x, y) \leq r\}$.

קוד לתיקון שגיאות רשימתי: יהיו $r, \ell \in \mathbb{N}_+$ אזי קוד $[m, k, d, q]$ לתיקון שגיאות \mathcal{C} עבורו לכל $w \in [q]^m$ מתקיים $|B_r(w) \cap \mathcal{C}| \leq \ell$.

סימון: יהיו $r, \ell \in \mathbb{N}_+$ ויהי \mathcal{C} קוד $[m, k, d, q]$ לתיקון שגיאות רשימתי (r, ℓ) אזי \mathcal{C} הינו קוד (m, k, r, ℓ, q) לתיקון שגיאות רשימתי.

טענה: יהי \mathcal{C} קוד $[m, k, d, q]$ לתיקון שגיאות אזי \mathcal{C} הינו קוד $(m, k, \frac{d}{2}, 1, q)$ לתיקון שגיאות רשימתי.

אלגוריתם סודן: ...

הגדרה: יהי \mathbb{F} שדה ויהי $n \in \mathbb{N}_+$ אזי נגדיר $\vec{1} \in \mathbb{F}^n$ כך $\vec{1}_i = 1$ לכל $i \in [n]$.

בעיית החתך המקסימלי: $\text{MaxCut} = \left\{ \left\langle (M, \vec{1}, \mathbb{F}_2), \varepsilon \right\rangle \mid (\forall i (w(R_i(M)) = 2)) \wedge \left(\text{Val} \left((M, \vec{1}, \mathbb{F}) \right) \leq \varepsilon \right) \right\}$.

טענה: קיים $\varepsilon \in (0, 1)$ עבורו $\text{GAP}_{[\varepsilon, 1-\varepsilon]} \text{MaxCut}$ הינה Promise- \mathcal{NP} -קשה.

מסקנה: קיים $\varepsilon \in (0, 1)$ עבורו $\text{CVP-code}_\varepsilon$ הינה \mathcal{NP} -קשה.

מסקנה: קיים $\varepsilon \in (0, 1)$ עבורו $\text{CVP-code-search}_\varepsilon$ הינה \mathcal{NP} -קשה.

טענה: קיימים $\varepsilon, \delta \in (0, 1)$ עבורם $\text{GAP}_{[1-\varepsilon, 1-(1+\delta)\varepsilon]} \text{MaxCut}$ הינה Promise- \mathcal{NP} -קשה.

בעיית המרווח לוקטור הקרוב ביותר: יהיו $a, b \in [0, 1]$ אזי $\text{GAP}_{[a, b]} \text{CVP-code} = \text{GAP}_{[a, b]} \text{Val}$.

מסקנה: יהי $\varepsilon > 0$ אזי קיים שדה סופי \mathbb{F} עבורו $\text{GAP}_{[\varepsilon, 1-\varepsilon]} \text{CVP-code}_\mathbb{F}$ הינה Promise- \mathcal{NP} -קשה.

מסקנה: אם קיים אלגוריתם פולינומי A אשר מהווה $\frac{1-\varepsilon}{\varepsilon}$ -קירוב לבעיית CVP-code-search אז $\mathcal{P} = \mathcal{NP}$.

מטריצת משחק: יהי \mathbb{F} שדה אזי $M \in \mathbb{F}^{n \times m}$ עבורה לכל $i \in [n]$ מתקיים $w(R_i(M)) = 2$ וכן קיים $j \in [m]$ עבורו $(M)_{i, j} = 1$.

$$R_i(M) \cdot \vec{1} = 0.$$

הגדרה: יהי \mathbb{F} שדה תהא $M \in \mathbb{F}^{n \times m}$ מטריצת משחק ויהי $t \in \mathbb{F}^m$ אזי $\text{Val}_{1 \leftrightarrow 1}((M, t, \mathbb{F})) = \text{Val}((M, t, \mathbb{F}))$.

בעיית המשחקים אחד על אחד: יהיו $a, b \in [0, 1]$ אזי $\text{PCP}_{1 \leftrightarrow 1}[a, b] = \text{GAP}_{[a, b]} \text{Val}_{1 \leftrightarrow 1}$.

בעיית המשחקים היחודיים: יהי $\varepsilon > 0$ אזי $\text{UG}(\varepsilon) = \text{PCP}_{1 \leftrightarrow 1}[\varepsilon, 1 - \varepsilon]$.

השערת המשחקים היחודיים: יהי $\varepsilon > 0$ אזי $\text{UG}(\varepsilon)$ הינה Promise- \mathcal{NP} -קשה. השערה פתוחה

הגדרה: יהי \mathbb{F} שדה יהי $m \in \mathbb{N}_+$ ויהיו $v, u \in \mathbb{F}^m$ אזי $\text{Interpol}(u, v) = \{t \in \mathbb{F}^m \mid \forall i \in [m]. t_i \in \{u_i, v_i\}\}$

הגדרה: יהי \mathbb{F} שדה תהא $M \in \mathbb{F}^{n \times m}$ מטריצת משחק ויהיו $u, v \in \mathbb{F}^m$

$$\text{Val}_{2 \rightarrow 1}((M, \{u, v\}, \mathbb{F})) = \min_{t \in \text{Interpol}(u, v)} \text{Val}((M, t, \mathbb{F}))$$

בעיית המשחקים שניים על אחד: יהיו $a, b \in [0, 1]$ אזי $\text{PCP}_{2 \rightarrow 1}[a, b] = \text{GAP}_{[a, b]} \text{Val}_{2 \rightarrow 1}$

משפט חות-מינזר-ספרא: יהי $\varepsilon > 0$ אזי $\text{PCP}_{2 \rightarrow 1}[\varepsilon, 1 - \varepsilon]$ הינה Promise- \mathcal{NP} -קשה. לא הוכח בקורס

הגדרה: יהי $\varepsilon > 0$ אזי $\frac{1}{2} \text{UG}(\varepsilon) = \text{PCP}_{1 \leftrightarrow 1}[\frac{1}{2}, 1 - \varepsilon]$

מסקנה: יהי $\varepsilon > 0$ אזי $\frac{1}{2} \text{UG}(\varepsilon)$ הינה Promise- \mathcal{NP} -קשה.

בעיית כפל מטריצות: יהי \mathbb{F} שדה יהיו $k, m, n \in \mathbb{N}_+$ תהא $A \in \mathbb{F}^{k \times m}$ ותהא $B \in \mathbb{F}^{m \times n}$ אזי $\text{MatMul}(\mathbb{F}, A, B) = AB$

אלגוריתם כפל מטריצות נאיבי: יהי \mathbb{F} שדה יהיו $k, m, n \in \mathbb{N}_+$ תהא $A \in \mathbb{F}^{k \times m}$ ותהא $B \in \mathbb{F}^{m \times n}$ אזי ...

טענה: יהי \mathbb{F} שדה יהיו $k, m, n \in \mathbb{N}_+$ תהא $A \in \mathbb{F}^{k \times m}$ ותהא $B \in \mathbb{F}^{m \times n}$ אזי סיבוכיות הריצה של NaiveMatMul הינה $\Theta(kmn)$.

אלגוריתם קרסובנה: יהי $n \in \mathbb{N}$ ויהיו $a, b \in \{0, 1\}^n$

Function KaratsubaMult(a, b):

```

if  $n = 1$  then return  $a_1 \cdot b_1$ 
 $\alpha \leftarrow (a_1 \dots a_{\frac{n}{2}}); \quad \beta \leftarrow (a_{\frac{n}{2}+1} \dots a_n)$ 
 $\gamma \leftarrow (b_1 \dots b_{\frac{n}{2}}); \quad \delta \leftarrow (b_{\frac{n}{2}+1} \dots b_n)$ 
 $A \leftarrow \text{KaratsubaMult}(\alpha, \gamma)$ 
 $B \leftarrow \text{KaratsubaMult}(\beta, \delta)$ 
 $C \leftarrow \text{KaratsubaMult}(\alpha + \beta, \gamma + \delta)$ 
return  $B \cdot 2^n + (C - B - A) \cdot 2^{\frac{n}{2}} + A$ 

```

טענה: יהיו $a, b \in \mathbb{N}$ אזי $(\text{KaratsubaMult}((a)_2, (b)_2))_{10} = ab$

טענה: סיבוכיות הריצה של KaratsubaMult הינה $\mathcal{O}(n^{\log_2(3)})$.

אלגוריתם סטרסן: יהי \mathbb{F} שדה יהי $n \in \mathbb{N}$ ותהיינה $A, B \in \mathbb{F}^{2^n \times 2^n}$ אזי ...

טענה: יהי \mathbb{F} שדה יהי $n \in \mathbb{N}$ ותהיינה $A, B \in \mathbb{F}^{2^n \times 2^n}$ אזי $\text{StrassenMatMul}(\mathbb{F}, A, B) = AB$

טענה: סיבוכיות הריצה של StrassenMatMul הינה $\mathcal{O}(m^{\log_2(7)})$.

בעיית היפוך מטריצה: יהי \mathbb{F} שדה יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{F}^{n \times n}$ הפיכה אזי $\text{MatInv}(\mathbb{F}, A) = A^{-1}$

משפט: תהא $T: \mathbb{N} \rightarrow \mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T) \iff (בעיית MatInv חשיבה בזמן T).

בעיית הדטרמיננטה: יהי \mathbb{F} שדה יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{F}^{n \times n}$ הפיכה אזי $\text{MatDet}(\mathbb{F}, A) = \det(A)$

משפט: תהא $T: \mathbb{N} \rightarrow \mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T) \iff (בעיית MatDet חשיבה בזמן T).

בעיית פירוק LU: ...

משפט: תהא $T: \mathbb{N} \rightarrow \mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T) \iff (בעיית Mat-LU חשיבה בזמן T).

בעיית פתרון מערכת משוואות לינארית: ...

משפט: תהא $T: \mathbb{N} \rightarrow \mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T) \iff (בעיית MatEqSol חשיבה בזמן T).

סריג: יהי \mathbb{F} שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ יהיו $n, k \in \mathbb{N}_+$ ותהא $M \in \mathbb{F}^{n \times k}$ אזי $\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M] = \{M \cdot x \mid x \in \mathcal{F}^k\}$

מימד של סריג: יהי \mathbb{F} שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג יהיו $n, k \in \mathbb{N}_+$ ותהא $M \in \mathbb{F}^{n \times k}$ מדרגה k אזי $\dim(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]) = k$

בסיס של סריג: יהי \mathbb{F} שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג יהיו $n, k \in \mathbb{N}_+$ ותהא $M \in \mathbb{F}^{n \times k}$ מדרגה k אזי $\text{basis}(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]) = M$

סימון: יהיו $n, k \in \mathbb{N}_+$ ותהא $M \in \mathbb{R}^{n \times k}$ מדרגה k אזי $\mathcal{L}[M] = \mathcal{L}_{\mathbb{R}|\mathbb{Z}}[M]$

סריג אבסטרקטי: יהיו $k, n \in \mathbb{N}_+$ ותהא $\mathcal{L} \subseteq \mathbb{R}^n$ אזי (\mathcal{L}, k) באשר

• לכל $x, y \in \mathcal{L}$ מתקיים $x - y \in \mathcal{L}$

• $\max\{|V| \mid (V \subseteq \mathcal{L}) \wedge (\mathbb{Z} \text{ מעל } V)\} = k$

• קיים $r > 0$ המקיים $B_r(0) \cap \mathcal{L} = \{0\}$

מימד של סריג אבסטרקטי: יהיו $k, n \in \mathbb{N}_+$ ותהא $\mathcal{L} \subseteq \mathbb{R}^n$ באשר (\mathcal{L}, k) סריג אבסטרקטי אזי $\dim(\mathcal{L}, k) = k$

הערה: יהי (\mathcal{L}, k) סריג אבסטרקטי אזי נסמן $\mathcal{L} = (\mathcal{L}, k)$

למה: יהי \mathcal{L} סריג אבסטרקטי אזי קיים $v \in \mathcal{L} \setminus \{0\}$ עבורו לכל $u \in \mathcal{L} \setminus \{0\}$ מתקיים $\|v\| \leq \|u\|$.

משפט: יהיו $k, n \in \mathbb{N}_+$ ותהא $\mathcal{L} \subseteq \mathbb{R}^n$ אזי (\mathcal{L}, k) הינו סריג אבסטרקטי \iff (קיימת $M \in \mathbb{R}^{n \times k}$ מדרגה k עבורה $\mathcal{L} = \mathcal{L}[M]$).

טענה: יהי $n \in \mathbb{N}_+$ ותהיינה $A, B \in \mathbb{R}^{n \times n}$ מדרגה מלאה אזי $(\mathcal{L}[A] = \mathcal{L}[B]) \iff (\exists U \in \text{GL}_n(\mathbb{Z}) : A = BU)$.

טרנספורמציות אלמנטריות: