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

מרחק האמינג: תהא X קבוצה אזי נגדיר $\Delta:X^{n}\times X^{n}\to\mathbb{N}$ כך $\Delta\left(x,y\right)=\left|\left\{ i\in\left[m\right]\mid x_{i}\neq y_{i}\right\} \right|$.

טענה: תהא X קבוצה אזי Δ משרה את נורמת ℓ_{0}.

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

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

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

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

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

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

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

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

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

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

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

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

קוד שארית: יהיו $q,m\in\mathbb{N}_{+}$ אזי $\mathcal{C}_{\text{parity}}=\left\{ w\in\left[q\right]^{m+1}\,\middle|\,w_{m+1}=\left(\sum_{i=1}^{n}w_{i}\mod q\right)\right\}$.

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

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

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

טענה: יהיו $m,r,d,q\in\mathbb{N}_{+}$ עבורם קיים קוד $\left[m,r,d,q\right]$ לתיקון שגיאות אזי קיים $d'\geq d$ עבורו קיים קוד $\left[m\left\lceil \log\left(q\right)\right\rceil ,r\log\left(q\right),d',2\right]$ לתיקון שגיאות.

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

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

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

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

טענה: יהיו $d,m\in\mathbb{N}_{+}$ באשר $d\leq\frac{m}{2}$ ויהי $\mathcal{C}$ קוד $\left[m,r,d,2\right]$ לתיקון שגיאות אזי $\left|\mathcal{C}\right|\leq d\cdot2^{m-2d+2}$.

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 $\left[m,r,d,q\right]$ לתיקון שגיאות אזי $\dim\left(\mathcal{C}\right)=r$.

מטריצה יוצרת: יהי $\mathcal{C}$ קוד לינארי $\left[m,r,d,q\right]$ לתיקון שגיאות ויהי $b_{1}\ldots b_{r}\in\mathcal{C}$ בסיס אזי נגדיר $M_{\mathcal{C}}\in\mathbb{F}_{q}^{m\times r}$ כך $C_{i}\left(M_{\mathcal{C}}\right)=b_{i}$ לכל $i\in\left[r\right]$.

טענה: יהי $\mathcal{C}$ קוד לינארי $\left[m,r,d,q\right]$ לתיקון שגיאות אזי $\mathcal{C}=\left\{ M_{\mathcal{C}}\cdot v\,\middle|\,v\in\mathbb{F}_{q}^{r}\right\}$.

מערכת משוואות לינארית: 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 $\left(M,t,\mathbb{F}\right)$.

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

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

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

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 $M_{\mathcal{C}_{\text{parity}}}=\begin{pmatrix}I_{m}\\ 1^{T}\end{pmatrix}=\begin{pmatrix}I_{m}\\ \left(\vec{1}\right)^{T}\end{pmatrix}$.

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

בעיית הוקטור הקצר ביותר: $\text{SVP-code}=\left\{ \left\langle \left(M,0,\mathbb{F}\right),\varepsilon\right\rangle \mid\exists v\neq0.\left\Vert Mv\right\Vert _{0}\leq\varepsilon\right\}$.

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 $M_{\mathcal{D}} = \binom{I_r}{A}$.

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 $|R(M_{\mathcal{C}}) \cap V| \le m-d$.
- 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 $d' \ge \left\lceil \frac{d}{q} \right\rceil$ עבורו קיים קוד לינארי $[m-d,r-1,d',q]$ לתיקון שגיאות.

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

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

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 $\mathcal{C}_M = \left\{M \cdot v \mid v \in \mathbb{F}_q^r\right\}$.

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

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 $\mathcal{C} = \ker\left(H_{\mathcal{C}}^T\right)$.

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)$\Longleftrightarrow$(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 $d \le m$ ויהי $q \in \mathbb{P}$ אזי קיים קוד לינארי $[m,k,d,q]$ לתיקון שגיאות $\mathcal{C}$ המקיים $|\mathcal{C}| \ge q^m \cdot \left(\sum_{i=0}^{d-1}\left(\binom{m}{i} \cdot (q-1)^i\right)\right)^{-1}$.

למה: יהי $d \in \mathbb{N}_{\ge 2}$ יהיו $k,m \in \mathbb{N}_+$ באשר $k \le m$ 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 $d \in \mathbb{N}_{\ge 2}$ יהיו $k,m \in \mathbb{N}_+$ באשר $k \le m$ 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 $|\mathcal{C}| \ge q^m \cdot \left(1 + \sum_{i=0}^{d-2}\left(\binom{m-1}{i} \cdot (q-1)^i\right)\right)^{-1}$.

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

- קיימת $g : Y^k \to X$ עבורה לכל $s \in X$ ולכל $p_1,\ldots,p_k \in [n]$ מתקיים $g\left(f(s)_{p_1},\ldots,f(s)_{p_k}\right) = s$.
- לא קיימת $g : Y^{k-1} \to X$ עבורה לכל $s \in X$ ולכל $p_1,\ldots,p_{k-1} \in [n]$ מתקיים $g\left(f(s)_{p_1},\ldots,f(s)_{p_{k-1}}\right) = s$.

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

- 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 אפיני 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 $f : \mathbb{F}_q \times (\mathbb{F}_q \backslash \{0\})^{k-1} \to \left(\mathbb{F}_q^2\right)^n$ כך $f(s,a) = \left(\left(s_i, s + \sum_{j=1}^{k-1} a_j s_i^j\right)\right)_{i=1}^n$ באשר $s_1 \ldots s_n \in \mathbb{F}_q \backslash \{0\}$ 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 $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ שונים אזי $\mathrm{RS}_q[m,r] = \left\{(f(\alpha_i))_{i=1}^m \mid f \in (\mathbb{F}_q)_{\le r-1}[x]\right\}$.

הערה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $r \in [q]$ אזי $\mathrm{RS}_q[q,r] \simeq (\mathbb{F}_q)_{\le r-1}[x]$.

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

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ אזי $\left(M_{\mathrm{RS}_q[m,r]}\right)_{i,j} = \alpha_i^{j-1}$ לכל $(i,j) \in [m]\times[r]$.

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $i \in \{0,\ldots,q-2\}$ 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 $\mathrm{RS}_q[q,r]^{\vee}=\mathrm{RS}_q[q,q-r]$.

אלגוריתם ברלקמפ־וולץ': ...

קוד ריד־מיולר: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r\in\mathbb{N}_+$ אזי $\mathrm{RM}_q[m,r]=\left\{(f(\alpha))_{\alpha\in\mathbb{F}_q^m}\mid f\in(\mathbb{F}_q)_{\le r}[x_1,\ldots,x_m]\right\}$.

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

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 $\mathrm{RM}_q[m,r]$ 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 $r[\mathrm{RM}_q[m,r]]=\binom{m+r}{r}$.

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

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

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

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

טענה: יהיו $m,r\in\mathbb{N}_{\ge2}$ אזי $\mathrm{RM}_2[m,r]=\{(u,u+v)\mid(u\in\mathrm{RM}_2[m-1,r])\wedge(v\in\mathrm{RM}_2[m-1,r-1])\}$.

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 $\rho:[q]\to\mathcal{C}'$ 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 $\rho:[q]\to\mathcal{C}'$ הפיכה אזי $\mathcal{C}\circ\mathcal{C}'\simeq\left\{h:[m]\times[m']\to[q]\;\middle|\;\exists w\in\mathcal{C}.h(i,j)=(\rho(w_i))_j\right\}$.

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

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

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 $\mathcal{C}_{\text{Hadamard}}\simeq\{\chi_S\mid S\subseteq[n]\}$.

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

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

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

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

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

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 $|B_r(w)\cap\mathcal{C}|\le\ell$.

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 $\left(m,k,\frac{d}{2},1,q\right)$ לתיקון שגיאות רשימתי.

אלגוריתם סודן: ...

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

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

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

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

מסקנה: יהי $\varepsilon>0$ אזי קיים שדה סופי $\mathbb{F}$ עבורו $\mathrm{GAP}_{[\varepsilon,1-\varepsilon]}\text{CVP-code}_{\mathbb{F}}$ הינה $\text{Promise-}\mathcal{NP}$־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 $(M)_{i,j}=1$ וכן $R_i(M)\cdot\vec{1}=0$.

הגדרה: יהי $\mathbb{F}$ שדה תהא $M\in\mathbb{F}^{n\times m}$ מטריצת משחק ויהי $t\in\mathbb{F}^m$ אזי $\mathrm{Val}_{1\leftrightarrow1}((M,t,\mathbb{F}))=\mathrm{Val}((M,t,\mathbb{F}))$.

בעיית המשחקים אחד על אחד: יהיו $a,b\in[0,1]$ אזי $\mathrm{PCP}_{1\leftrightarrow1}[a,b]=\mathrm{GAP}_{[a,b]}\mathrm{Val}_{1\leftrightarrow1}$.

בעיית המשחקים היחודיים: יהי $\varepsilon>0$ אזי $\mathrm{UG}(\varepsilon)=\mathrm{PCP}_{1\leftrightarrow1}[\varepsilon,1-\varepsilon]$.

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

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

הגדרה: יהי $\mathbb{F}$ שדה תהא $M\in\mathbb{F}^{n\times m}$ מטריצת משחק ויהיו $u,v\in\mathbb{F}^m$ אזי $\mathrm{Val}_{2\to1}((M,\{u,v\},\mathbb{F}))=\min_{t\in\mathrm{Interpol}(u,v)}\mathrm{Val}((M,t,\mathbb{F}))$.

בעיית המשחקים שניים על אחד: יהיו $a,b\in[0,1]$ אזי $\mathrm{PCP}_{2\to1}[a,b]=\mathrm{GAP}_{[a,b]}\mathrm{Val}_{2\to1}$.

משפט חות־מינזר־ספרא: יהי $\varepsilon>0$ אזי $\mathrm{PCP}_{2\to1}[\varepsilon,1-\varepsilon]$ הינה $\mathrm{Promise}\text{-}\mathcal{NP}$־קשה. לא הוכח בקורס

הגדרה: יהי $\varepsilon>0$ אזי $\frac{1}{2}\mathrm{UG}(\varepsilon)=\mathrm{PCP}_{1\leftrightarrow1}\left[\frac{1}{2},1-\varepsilon\right]$.

מסקנה: יהי $\varepsilon>0$ אזי $\frac{1}{2}\mathrm{UG}(\varepsilon)$ הינה $\mathrm{Promise}\text{-}\mathcal{NP}$־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 $\mathrm{MatMul}(\mathbb{F},A,B)=AB$.

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

```
Function KaratsubaMult(a, b):
    if n = 1 then return a_1 · b_1
    α ← (a_1 ... a_{n/2});    β ← (a_{n/2+1} ... a_n)
    γ ← (b_1 ... b_{n/2});    δ ← (b_{n/2+1} ... b_n)
    A ← KaratsubaMult(α, γ)
    B ← KaratsubaMult(β, δ)
    C ← KaratsubaMult(α + β, γ + δ)
    return B · 2^n + (C − B − A) · 2^{n/2} + A
```

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

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

אלגוריתם סטרסן: יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}$ ותהיינה $A,B\in\mathbb{F}^{2^n\times2^n}$ אזי ...

טענה: יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}$ ותהיינה $A,B\in\mathbb{F}^{2^n\times2^n}$ אזי $\mathrm{StrassenMatMul}(\mathbb{F},A,B)=AB$.

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

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

משפט: תהא $T:\mathbb{N}\to\mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T)$\Longleftrightarrow$(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 $\mathrm{MatDet}(\mathbb{F},A)=\det(A)$.

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

בעיית פירוק LU: ...

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

בעיית פתרון מערכת משוואות לינארית: ...

משפט: תהא $T:\mathbb{N}\to\mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T)$\Longleftrightarrow$(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 $\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]=\left\{M\cdot x\mid x\in\mathcal{F}^k\right\}$.

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 $\dim\left(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]\right)=k$.

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 $\mathrm{basis}\left(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]\right)=M$.

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 $x-y\in\mathcal{L}$.
- $\max\{|V|\mid(V\subseteq\mathcal{L})\wedge(\text{קבוצה בת"ל מעל }\mathbb{Z}\ V)\}=k$.
- 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 $v \in \mathcal{L} \backslash \{0\}$ עבורו לכל $u \in \mathcal{L} \backslash \{0\}$ מתקיים $\|v\| \le \|u\|$.

משפט: יהיו $k, n \in \mathbb{N}_+$ ותהא $\mathcal{L} \subseteq \mathbb{R}^n$ אזי ($(\mathcal{L}, k)$ הינו סריג אבסטרקטי)$\Longleftrightarrow$(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 $(\exists U \in \mathrm{GL}_n(\mathbb{Z}) : A = BU) \Longleftrightarrow (\mathcal{L}[A] = \mathcal{L}[B])$.

טרנספורמציות אלמנטריות: