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 $\Delta\left(x,y\right)=\left|\left\{i\in[m]\mid x_i\neq y_i\right\}\right|$.

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 $\mathcal{C}\subseteq[q]^m$.

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 $d\left[\mathcal{C}\right]=\min_{x\neq y}\Delta\left(x,y\right)$.

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

סימון: יהיו $q,m\in\mathbb{N}_+$ ויהי $\mathcal{C}\subseteq[q]^m$ 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 $[m,r,d,q]$ לתיקון שגיאות יהי $w\in\mathcal{C}$ ויהי $w'\in[q]^m$ באשר $\Delta\left(w,w'\right)\le d-1$ 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 $\Delta\left(w,w'\right)\le\left\lfloor\frac{d-1}{2}\right\rfloor$ אזי $\arg\min_{v\in\mathcal{C}}\Delta\left(v,w'\right)=w$.

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

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

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

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

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

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

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 $d'\ge d$ 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 $[m,r,d,q]$ 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 $\left|\mathcal{C}\right|\le q^m\cdot\left(\sum_{i=0}^{\left\lfloor\frac{d-1}{2}\right\rfloor}\left(\binom{m}{i}\cdot\left(q-1\right)^i\right)\right)^{-1}$.

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

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

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

מטריצה יוצרת: יהי $\mathcal{C}$ קוד לינארי $[m,r,d,q]$ 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 $i\in[r]$.

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

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

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 $R\left(M\right)=\left\{R_i\left(M\right)\mid i\in[m]\right\}$.

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

- לכל $V\subseteq\mathcal{C}$ באשר $\dim\left(V\right)=r-1$ מתקיים $\left|R\left(M_{\mathcal{C}}\right)\cap V\right|\le m-d$.
- קיים $V\subseteq\mathcal{C}$ המקיים $\dim\left(V\right)=r-1$ וכן $\left|R\left(M_{\mathcal{C}}\right)\cap V\right|=m-d$.

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

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

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: ...

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 $(M,t,\mathbb{F})$.

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

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 $\|Mv-t\|_0\le\varepsilon$.

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

בעיית הוקטור הקצר ביותר: $\text{SVP-code}=\{\langle(M,0,\mathbb{F}),\varepsilon\rangle\mid\exists v\ne0.\|Mv\|_0\le\varepsilon\}$.

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

טענה: קיים $\varepsilon\in(0,1)$ עבורו $\text{GAP}_{[\varepsilon,1-\varepsilon]}\text{MaxCut}$ 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 $w\left(R_i\left(M\right)\right) = 2$ וכן קיים $j \in [m]$ עבורו $\left(M\right)_{i,j} = 1$ וכן $R_i\left(M\right) \cdot \vec{1} = 0$.

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

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

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

השערת המשחקים היחודיים: יהי $\varepsilon > 0$ אזי $\mathrm{UG}\left(\varepsilon\right)$ 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 $\mathrm{Interpol}\left(u,v\right) = \left\{t \in \mathbb{F}^m \mid \forall i \in [m].t_i \in \left\{u_i, v_i\right\}\right\}$.

הגדרה: יהי $\mathbb{F}$ שדה תהא $M \in \mathbb{F}^{n\times m}$ מטריצת משחק ויהיו $u,v \in \mathbb{F}^m$ אזי $\mathrm{Val}_{2\to 1}\left(\left(M,\left\{u,v\right\},\mathbb{F}\right)\right) = \min_{t\in\mathrm{Interpol}(u,v)} \mathrm{Val}\left(\left(M,t,\mathbb{F}\right)\right)$.

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

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

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

מסקנה: יהי $\varepsilon > 0$ אזי $\frac{1}{2}\mathrm{UG}\left(\varepsilon\right)$ 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 $\mathrm{MatMul}\left(\mathbb{F},A,B\right) = AB$.

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 $\Theta\left(kmn\right)$.

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

Function KaratsubaMult(a,b):
- **if** $n = 1$ **then return** $a_1 \cdot b_1$
- $\alpha \leftarrow (a_1 \ldots a_{\frac{n}{2}})$; $\quad \beta \leftarrow (a_{\frac{n}{2}+1} \ldots a_n)$
- $\gamma \leftarrow (b_1 \ldots b_{\frac{n}{2}})$; $\quad \delta \leftarrow (b_{\frac{n}{2}+1} \ldots b_n)$
- $A \leftarrow$ KaratsubaMult(α,γ)
- $B \leftarrow$ KaratsubaMult(β,δ)
- $C \leftarrow$ 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 $\left(\mathrm{KaratsubaMult}\left(\left(a\right)_2, \left(b\right)_2\right)\right)_{10} = ab$.

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 $A,B \in \mathbb{F}^{2^n\times 2^n}$ אזי ...

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

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 $\mathrm{MatInv}\left(\mathbb{F},A\right) = A^{-1}$.

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 $\mathrm{MatDet}\left(\mathbb{F},A\right) = \det\left(A\right)$.

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 $\mathcal{L}_{\mathbb{F}|\mathcal{F}}\left[M\right] = \left\{M \cdot x \mid x \in \mathcal{F}^k\right\}$.

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

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

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

סריג אבסטרקטי: יהיו $k,n \in \mathbb{N}_+$ ותהא $\mathcal{L} \subseteq \mathbb{R}^n$ אזי $\left(\mathcal{L},k\right)$ באשר
- לכל $x,y \in \mathcal{L}$ מתקיים $x - y \in \mathcal{L}$.
- $\max\left\{\left|V\right| \mid \left(V \subseteq \mathcal{L}\right) \wedge \left(\text{קבוצה בת"ל מעל } \mathbb{Z} \; V\right)\right\} = k$.

- 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)$\iff$(קיימת $M\in\mathbb{R}^{n\times k}$ מדרגה k עבורה $\mathcal{L}=\mathcal{L}[M]$).

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

חיבור עמודות: יהי $n\in\mathbb{N}_+$ יהיו $i,j\in[n]$ שונים ויהי $a\in\mathbb{Z}$ אזי נגדיר $\Phi^+_{i,j,a}:\mathbb{R}^{n\times n}\to\mathbb{R}^{n\times n}$ כך $\Phi^+_{i,j,a}(M)=M+a\cdot\left(C_j(M)\cdot e_i^T\right)$.

החלפת עמודות: יהי $n\in\mathbb{N}_+$ ויהיו $i,j\in[n]$ שונים אזי נגדיר $\Phi^{\leftrightarrow}_{i,j}:\mathbb{R}^{n\times n}\to\mathbb{R}^{n\times n}$ כך $\Phi^{\leftrightarrow}_{i,j}(M)=M+C_j(M)\cdot(e_i-e_j)^T+C_i(M)\cdot(e_j-e_i)^T$.

שלילת עמודה: יהי $n\in\mathbb{N}_+$ ויהי $i\in[n]$ אזי נגדיר $\Phi^-_i:\mathbb{R}^{n\times n}\to\mathbb{R}^{n\times n}$ כך $\Phi^-_i(M)=M-2\cdot\left(C_i(M)\cdot e_i^T\right)$.

טרנספורמציות אלמנטריות: יהי $n\in\mathbb{N}_+$ אזי $\left\{\Phi^+_{i,j,a}\;\middle|\;\left(\substack{i,j\in[n]\\ i\neq j}\right)\wedge(a\in\mathbb{Z})\right\}\cup\left\{\Phi^{\leftrightarrow}_{i,j}\;\middle|\;\substack{i,j\in[n]\\ i\neq j}\right\}\cup\left\{\Phi^-_i\mid i\in[n]\right\}$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times n}$ הפיכה ותהא φ טרנספורמציה אלמנטרית אזי $\mathcal{L}[\varphi(M)]=\mathcal{L}[M]$.

משפט: יהי $n\in\mathbb{N}_+$ ותהיינה $A,B\in\mathbb{R}^{n\times n}$ הפיכות אזי ($\mathcal{L}[A]=\mathcal{L}[B]$)$\iff$(קיים $m\in\mathbb{N}_+$ וקיימות טרנספורמציות אלמנטריות $\varphi_1\ldots\varphi_m$ עבורן $A=(\varphi\circ\ldots\circ\varphi_m)(B)$).

סריג דואלי: יהי $\mathcal{L}$ סריג ממשי אזי $\mathcal{L}^\vee=\{v\in\mathrm{span}(\mathcal{L})\mid\forall v\in\mathcal{L}:\langle u,v\rangle\in\mathbb{Z}\}$.

טענה: יהי $\mathcal{L}$ סריג ממשי אזי $\mathcal{L}^\vee$ סריג ממשי.

טענה: יהי $\mathcal{L}$ סריג ממשי אזי $(\mathcal{L}^\vee)^\vee=\mathcal{L}$.

מטריצה דואלית: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $M^\vee=M^{-T}$.

טענה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $(M^\vee)^\vee=M$.

טענה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\mathcal{L}[M]^\vee=\mathcal{L}[M^\vee]$.

מתיחת סריג: יהי $\mathcal{L}$ סריג ממשי ויהי $q\in\mathbb{R}_{>0}$ אזי $q\cdot\mathcal{L}=\{q\cdot v\mid v\in\mathcal{L}\}$.

טענה: יהיו $k,n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times k}$ מדרגה k אזי $q\cdot\mathcal{L}[M]=\mathcal{L}[q\cdot M]$.

טענה: יהי $\mathcal{L}$ סריג ממשי ויהי $q\in\mathbb{R}_{>0}$ אזי $(q\cdot\mathcal{L})^\vee=q^{-1}\cdot\mathcal{L}^\vee$.

בעיית מלאות דרגת מטריצה: $\mathrm{MatInd}=\left\{\langle\mathbb{F},M\rangle\;\middle|\;(\mathbb{F}\text{ שדה})\wedge(n,k\in\mathbb{N}_+)\wedge\left(M\in\mathbb{F}^{n\times k}\right)\wedge(M\text{ מדרגה }k)\right\}$.

בעיית שייכות לסריג בהינתן בסיס: $\mathrm{LatIn}=\left\{\langle M,v\rangle\;\middle|\;(n,k\in\mathbb{N}_+)\wedge\left(M\in\mathbb{R}^{n\times k}\right)\wedge(M\text{ מדרגה }k)\wedge(v\in\mathcal{L}[M])\right\}$.

בעיית ההכלה של סריג: $\mathrm{LatInc}=\left\{\langle A,B\rangle\;\middle|\;(n,k,m\in\mathbb{N}_+)\wedge\left(\substack{A\in\mathbb{R}^{n\times k}\\ B\in\mathbb{R}^{n\times m}}\right)\wedge\left(\substack{A\text{ מדרגה }k\\ B\text{ מדרגה }m}\right)\wedge(\mathcal{L}[A]\subseteq\mathcal{L}[B])\right\}$.

בעיית בסיס לחיתוך סריגים: יהיו $n,k,m\in\mathbb{N}_+$ תהא $A\in\mathbb{R}^{n\times k}$ מדרגה k ותהא $B\in\mathbb{R}^{n\times m}$ מדרגה m אזי $\mathrm{LatInterBasis}(A,B)=\mathrm{basis}(\mathcal{L}[A]\cap\mathcal{L}[B])$.

משפט: $\mathrm{MatInd},\mathrm{LatIn},\mathrm{LatInc},\mathrm{LatInterBasis}\in\mathcal{P}$.

המקבילון היסודי: יהיו $n,k\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times k}$ אזי $\mathcal{P}[M]=\mathcal{L}_{\mathbb{R}|[0,1)}[M]$.

עיגול לפי המקבילון היסודי: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k ויהי $a\in\mathbb{R}^k$ אזי $\lfloor M\cdot a\rfloor_{\mathcal{P}[M]}=M\cdot\lfloor a\rfloor$.

טענה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k ויהי $v\in\mathbb{R}^k$ אזי $\lfloor v\rfloor_{\mathcal{P}[M]}=\arg\min_{u\in\mathcal{L}[M]}(\|v-u\|)$.

מודולו המקבילון היסודי: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k ויהי $v\in\mathbb{R}^k$ אזי $(v\mod\mathcal{P}[M])=v-\lfloor v\rfloor_{\mathcal{P}[M]}$.

טענה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k ויהי $v\in\mathbb{R}^k$ אזי $(v\mod\mathcal{P}[M])\in\mathcal{P}[M]$.

למה: יהי $n\in\mathbb{N}_+$ ותהיינה $A,B\in\mathbb{R}^{n\times n}$ הפיכות באשר $\mathcal{L}[B]\subseteq\mathcal{L}[A]$ אזי $(\mathcal{P}[B]\cap\mathcal{L}[A]=\{0\})\iff(\mathcal{L}[A]=\mathcal{L}[B])$.

טענה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\mathrm{Vol}(\mathcal{P}[M])=|\det(M)|$.

מסקנה: יהי $n\in\mathbb{N}_+$ ותהיינה $A,B\in\mathbb{R}^{n\times n}$ הפיכות באשר $\mathcal{L}[B]=\mathcal{L}[A]$ אזי $|\det(A)|=|\det(B)|$.

דטרמיננטה של סריג: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\det(\mathcal{L}[M])=\mathrm{Vol}(\mathcal{P}[M])$.

בעיית הדטרמיננטה של סריג: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\mathrm{LatDet}(M)=\det(\mathcal{L}[M])$.

מסקנה: $\mathrm{LatDet}\in\mathcal{P}$.

טענה: יהי $\mathcal{L}$ סריג ממשי אזי $\lim_{r\to\infty}\frac{|\mathcal{L}\cap B_r(0)|}{\mathrm{Vol}(B_r(0))}=\frac{1}{\det(\mathcal{L})}$.

טענה: יהי $\mathcal{L}$ סריג ממשי אזי $\det(\mathcal{L})\cdot\det(\mathcal{L}^\vee)=1$.

העוקבים המינימליים: יהי $k\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג ממשי מדרגה k ויהי $i\in[k]$ אזי $\lambda_i[\mathcal{L}]=\inf\{r\ge0\mid\dim\mathrm{span}(B_r(0)\cap\mathcal{L})\ge i\}$.

אורתונורמליזציה: יהי $n\in\mathbb{N}_+$ ויהיו $u_1\ldots u_n\in\mathbb{R}^n$ באשר $\{u_1\ldots u_n\}$ בסיס אזי $u_1^\perp,\ldots,u_n^\perp\in\mathbb{R}^n$ המקיימים

- $\left\{u_1^{\perp},\ldots,u_n^{\perp}\right\}$ בסיס אורתונורמלי.
- לכל $i\in[n]$ מתקיים $u_i^{\perp}\in\operatorname{span}(u_1\ldots u_i)\setminus\operatorname{span}(u_1\ldots u_{i-1})$.

טענה: יהי $n\in\mathbb{N}_+$ ויהיו $u_1\ldots u_n\in\mathbb{R}^n$ באשר $u_1\ldots u_n$ בסיס אזי קיימת ויחידה אורתונורמליזציה של $u_1\ldots u_n$.

מטריצת האורתונורמליזציה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $M^{\perp}\in\mathbb{R}^{n\times n}$ המקיימת $C_i\left(M^{\perp}\right)=C_i(M)^{\perp}$ לכל $i\in[n]$.

משפט: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\lambda_1[\mathcal{L}[M]]\geq\min_{i\in[n]}\left|\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle\right|$.

סריג מדרגה מלאה: יהי $n\in\mathbb{N}_+$ אזי סריג ממשי $\mathcal{L}\subseteq\mathbb{R}^n$ מדרגה n.

טענה: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי קיימים $u_1\ldots u_n\in\mathcal{L}$ בת"ל המקיימים $\|u_i\|=\lambda_i[\mathcal{L}]$ לכל $i\in[n]$.

מסקנה: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהיו $u_1\ldots u_n\in\mathcal{L}$ בת"ל המקיימים $\|u_i\|=\lambda_i[\mathcal{L}]$ לכל $i\in[n]$ אזי לכל $i\in[n]$ מתקיים $B_{\lambda_{i+1}[\mathcal{L}]}(0)\cap\mathcal{L}\subseteq\operatorname{span}(u_1\ldots u_i)$.

סריג סטנדרטי: יהי $n\in\mathbb{N}_+$ אזי סריג $\mathcal{L}$ מדרגה מלאה n עבורו קיימת $M\in\mathbb{R}^{n\times n}$ המקיימת $\mathcal{L}=\mathcal{L}[M]$ וכן $\|C_i(M)\|=\lambda_i[\mathcal{L}]$ לכל $i\in[n]$.

טענה: יהי $n\in\mathbb{N}_{\geq5}$ אזי קיים סריג $\mathcal{L}$ מדרגה מלאה n באשר $\mathcal{L}$ אינו סריג סטנדרטי.

טענה: יהי $n\in[4]$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\mathcal{L}$ סריג סטנדרטי.

משפט ההעברה של בנשצ'יק: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $1\leq\lambda_1[\mathcal{L}]\cdot\lambda_n[\mathcal{L}^{\vee}]\leq n$.

משפט בליכפלדט: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ותהא $S\subseteq\mathbb{R}^n$ מדידה באשר $\operatorname{Vol}(S)>\det(\mathcal{L})$ אזי קיימים $u,v\in S$ שונים עבורם $u-v\in\mathcal{L}$.

גוף קמור סימטרי ביחס לראשית: יהי $n\in\mathbb{N}_+$ אזי קבוצה קמורה $S\subseteq\mathbb{R}^n$ המקיימת $S=-S$.

משפט הגוף הקמור של מינקובסקי: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ותהא $S\subseteq\mathbb{R}^n$ קבוצה קמורה סימטרית ביחס לראשית באשר $\operatorname{Vol}(S)>2^n\cdot\det(\mathcal{L})$ אזי $\mathcal{L}\cap S\neq\{0\}$.

אליפסואיד של סריג: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהיו $u_1\ldots u_n\in\mathcal{L}$ באשר $\|u_i\|=\lambda_i[\mathcal{L}]$ לכל $i\in[n]$ אזי $\mathcal{E}_{\mathcal{L}}=\left\{v\in\mathbb{R}^n\;\middle|\;\sum_{i=1}^n\frac{\left\langle v,u_k^{\perp}\right\rangle^2}{\lambda_k[\mathcal{L}]^2}<1\right\}$.

למה: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהיו $u_1\ldots u_n\in\mathcal{L}$ באשר $\|u_i\|=\lambda_i[\mathcal{L}]$ לכל $i\in[n]$ אזי $\mathcal{E}_{\mathcal{L}}\cap\mathcal{L}=\{0\}$.

משפט מינקובסקי השני: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\prod_{i=1}^n\lambda_i[\mathcal{L}]\leq2^n\cdot\frac{\det(\mathcal{L})}{\operatorname{Vol}(B_1(0))}$.

מסקנה משפט מינקובסקי הראשון: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\lambda_1[\mathcal{L}]\leq(\det(\mathcal{L}))^{\frac{1}{n}}\cdot\sqrt{n}$.

טרנספורמציית פוריה: יהי $n\in\mathbb{N}_+$ ותהא $f\in L^1(\mathbb{R}^n)$ אזי נגדיר $\hat{f}:\mathbb{R}\to\mathbb{R}$ כך $\hat{f}(\omega)=\int_{\mathbb{R}^n}f(x)\,e^{-2\pi i\cdot\langle x,\omega\rangle}\mathrm{d}x$.

טענה: יהי $n\in\mathbb{N}_+$ ותהיינה $f,g\in L^1(\mathbb{R}^n)$ אזי $\widehat{f+g}=\hat{f}+\hat{g}$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $f\in L^1(\mathbb{R}^n)$ ויהי $\lambda\in\mathbb{R}$ אזי $\widehat{\lambda\cdot f}=\lambda\cdot\hat{f}$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $f\in L^1(\mathbb{R}^n)$ יהי $z\in\mathbb{R}^n$ ונגדיר $h:\mathbb{R}^n\to\mathbb{R}$ כך $h(x)=f(x+z)$ אזי לכל $\omega\in\mathbb{R}^n$ מתקיים $\hat{h}(\omega)=e^{2\pi i\cdot\langle w,z\rangle}\cdot\hat{f}(\omega)$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $f\in L^1(\mathbb{R}^n)$ יהי $\lambda\in\mathbb{R}$ ונגדיר $h:\mathbb{R}^n\to\mathbb{R}$ כך $h(x)=f(\lambda x)$ אזי לכל $\omega\in\mathbb{R}^n$ מתקיים $\hat{h}(\omega)=\frac{1}{\lambda^n}\cdot\hat{f}\left(\frac{\omega}{\lambda}\right)$.

טענה: יהי $n\in\mathbb{N}_+$ תהיינה $f_1\ldots f_n\in L^1(\mathbb{R})$ ונגדיר $h:\mathbb{R}^n\to\mathbb{R}$ כך $h(x)=\prod_{i=1}^nf_i(x_i)$ אזי לכל $\omega\in\mathbb{R}^n$ מתקיים $\hat{h}(\omega)=\prod_{i=1}^n\hat{f}_i(\omega_i)$.

גאוסיאן: יהי $n\in\mathbb{N}_+$ ויהי $\sigma\in\mathbb{R}$ אזי נגדיר $\mathcal{N}_n[\sigma]:\mathbb{R}^n\to\mathbb{R}$ כך $\mathcal{N}_n[\sigma](x)=\frac{1}{(2\pi)^{\frac{n}{2}}\cdot\sigma^n}\cdot e^{-\frac{1}{2\sigma^2}\cdot\|x\|^2}$.

טענה: יהי $n\in\mathbb{N}_+$ ויהי $\sigma\in\mathbb{R}$ אזי $\widehat{\mathcal{N}_n[\sigma]}=\left(\frac{\sqrt{2\pi}}{\sigma}\right)^n\cdot\mathcal{N}_n\left[\frac{1}{\sigma}\right]$.

הגדרה: יהי $n\in\mathbb{N}_+$ יהיו $\alpha,\beta\in\mathbb{N}^n$ ותהא $f\in C^{\infty}(\mathbb{R}^n,\mathbb{C})$ אזי $\|f\|_{\alpha,\beta}=\sup_{x\in\mathbb{R}^n}\left|x^{\alpha}\cdot\mathcal{D}^{\beta}(f)(x)\right|$.

מרחב שוורץ: יהי $n\in\mathbb{N}_+$ ותהא $A\subseteq\mathbb{C}$ אזי $\mathcal{S}(\mathbb{R}^n,A)=\left\{f\in C^{\infty}(\mathbb{R}^n,A)\;\middle|\;\forall\alpha,\beta\in\mathbb{N}^n:\|f\|_{\alpha,\beta}<\infty\right\}$.

טענה נוסחאת הסכימה של פואסון: יהי $n\in\mathbb{N}_+$ תהא $f\in\mathcal{S}(\mathbb{R}^n,\mathbb{R})$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\sum_{v\in\mathcal{L}}f(v)=\frac{1}{\det(\mathcal{L})}\cdot\sum_{v\in\mathcal{L}^{\vee}}\hat{f}(v)$.

משפט: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהי $\varepsilon>0$ אזי קיים $r\in\mathbb{R}$ המקיים $\mathbb{P}_{v\sim\mathcal{N}_n[\lambda_n[\mathcal{L}]\cdot r]}\left(v\notin B_{\lambda_n[\mathcal{L}]}(0)\;\middle|\;v\in\mathcal{L}^{\vee}\right)\leq\varepsilon$.

הטלה של וקטור על וקטור: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהי $u\in\mathcal{L}$ אזי נגדיר $\pi_{\perp u}:\mathbb{R}^n\to\mathbb{R}^n$ כך $\pi_{\perp u}(v)=v-\frac{\langle u,v\rangle}{\|u\|^2}\cdot u$.

הטלה של סריג על וקטור: יהי $\mathcal{L}$ סריג ממשי מדרגה מלאה ויהי $u\in\mathcal{L}$ אזי $\mathcal{L}_{\perp u}=\{\pi_{\perp u}(v)\mid v\in\mathcal{L}\}$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהי $u\in\mathcal{L}$ אזי $\mathcal{L}_{\perp u}$ סריג ממשי מדרגה $n-1$.

בסיס קורקין־זולוטרב (KZ): יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $M\in\mathbb{R}^{n\times n}$ המקיימת

- $\mathcal{L}=\mathcal{L}[M]$.
- $\|C_1(M)\|=\lambda_1[\mathcal{L}]$.
- $\pi_{\perp C_1(M)}(C_2(M)),\ldots,\pi_{\perp C_1(M)}(C_n(M))$ הינו בסיס קורקין־זולוטרב עבור $\mathcal{L}_{\perp C_1(M)}$.
- לכל $i\in[n]$ מתקיים $\left|\left\langle C_i(M),C_1\left(M^{\perp}\right)\right\rangle\right|\le\frac{1}{2}\left|\left\langle C_1(M),C_1\left(M^{\perp}\right)\right\rangle\right|$.

משפט: יהי $\mathcal{L}$ סריג מדרגה מלאה אזי קיים בסיס KZ ל־$\mathcal{L}$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ותהא $M\in\mathbb{R}^{n\times n}$ באשר $\mathcal{L}[M]=\mathcal{L}$ אזי M בסיס KZ של $\mathcal{L}$ אם הבאים מתקיימים

- לכל $i\in[n]$ מתקיים $\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle\cdot C_i\left(M^{\perp}\right)=\arg\min\left\{\|v\|\mid v\in\pi_{\mathrm{span}^{\perp}(C_1(M),\ldots,C_{i-1}(M))}(\mathcal{L})\right\}$.
- לכל $i,j\in[n]$ באשר $j<i$ מתקיים $\left|\left\langle C_i(M),C_j\left(M^{\perp}\right)\right\rangle\right|\le\frac{1}{2}\left|\left\langle C_j(M),C_j\left(M^{\perp}\right)\right\rangle\right|$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ויהי $M\in\mathbb{R}^{n\times n}$ בסיס KZ של $\mathcal{L}$ אזי

- לכל $i\in[n]$ מתקיים $\left|\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle\right|\le\lambda_i[\mathcal{L}]$.
- לכל $i,j\in[n]$ באשר $j\ge i$ מתקיים $\left|\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle\right|\le\|C_l(M)\|$.
- לכל $i\in[n]$ מתקיים $\frac{1}{\sqrt{\frac{i-1}{4}+1}}\cdot\|C_i(M)\|\le\lambda_i[\mathcal{L}]\le\sqrt{\frac{i-1}{4}+1}\cdot\|C_i(M)\|$.

ערך של סריג: יהי $\mathbb{F}$ שדה יהי $\mathcal{F}\subseteq\mathbb{F}$ יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{F}^{n\times n}$ הפיכה ויהי $t\in\mathbb{F}^n$ אזי $\mathrm{Val\text{-}lattice}(M,t,\mathbb{F},\mathcal{F})=\min_{x\in\mathcal{F}^n}\|Mx-t\|$.

בעיית חיפוש הוקטור הקרוב ביותר בסריג: יהי $\mathbb{F}$ שדה יהי $\mathcal{F}\subseteq\mathbb{F}$ יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{F}^{n\times n}$ הפיכה יהי $t\in\mathbb{F}^n$ ויהי $\varepsilon>0$ אזי $\mathrm{CVP\text{-}lattice\text{-}search}((M,t,\mathbb{F},\mathcal{F}),\varepsilon)=v$ באשר $\|Mv-t\|\le\varepsilon$.

בעיית הוקטור הקרוב ביותר בסריג: $\mathrm{CVP\text{-}lattice}=\{\langle M,t,\mathbb{F},\mathcal{F},\varepsilon\rangle\mid\mathrm{Val\text{-}lattice}(M,t,\mathbb{F},\mathcal{F})\le\varepsilon\}$.

מטריצה מצומצמת לנסטרה־לנסטרה־לובאס (LLL): יהי $n\in\mathbb{N}_+$ ויהי $\delta>0$ אזי $M\in\mathbb{R}^{n\times n}$ המקיימת

- כמעט אורתוגונלית: לכל $i,j\in[n]$ באשר $j<i$ מתקיים $\left|\left\langle C_j(M),C_j\left(M^{\perp}\right)\right\rangle\right|\ge2\left|\left\langle C_i(M),C_j\left(M^{\perp}\right)\right\rangle\right|$.
- תנאי לובאס: לכל $i\in[n-1]$ מתקיים $\delta\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle^2\le\left\langle C_{i+1}(M),C_i\left(M^{\perp}\right)\right\rangle^2+\left\langle C_{i+1}(M),C_{i+1}\left(M^{\perp}\right)\right\rangle^2$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $\delta>0$ ותהא $M\in\mathbb{R}^{n\times n}$ מצומצמת δ-LLL אזי לכל $i\in[n-1]$ מתקיים $\left\langle C_{i+1}(M),C_{i+1}\left(M^{\perp}\right)\right\rangle\ge\sqrt{\delta-\frac{1}{4}}\cdot\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $\delta>0$ ותהא $M\in\mathbb{R}^{n\times n}$ מצומצמת δ-LLL אזי $\lambda_1[\mathcal{L}[M]]\ge\|C_1(M)\|\cdot\left(\frac{\sqrt{4\delta-1}}{2}\right)^{n-1}$.

אלגוריתם LLL: יהי $n\in\mathbb{N}_+$ יהי $\delta>0$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי ...

הגדרה: יהי $n\in\mathbb{N}_+$ אזי נגדיר $\mathcal{DD}:\mathbb{Z}^{n\times n}\to\mathbb{N}$ כך $\mathcal{DD}[M]=\prod_{i=1}^{n}\left|\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle\right|^{n-i+1}$.

טענה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{Z}^{n\times n}$ אזי $1\le\mathcal{DD}[M]\le\left(\max_{i\in[n]}\|C_i(M)\|\right)^{\frac{n(n+1)}{2}}$.

טענה: ...

רדיוס כיסוי: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\mu(\mathcal{L})=\max_{t\in\mathbb{R}^n}\mathrm{dist}(t,\mathcal{L})$.

טענה: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\frac{1}{2}\lambda_n[\mathcal{L}]\le\mu(\mathcal{L})$.

אלגוריתם באבאי: יהי $n\in\mathbb{N}_+$ יהי $\delta>0$ תהא $M\in\mathbb{R}^{n\times n}$ מצומצמת δ-LLL ויהי $t\in\mathbb{R}^n$ אזי ...

טענה: יהי $n\in\mathbb{N}_+$ אזי סיבוכיות הריצה של NaiveMatMul הינה $O\left(n^2\right)$.

מסקנה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי $\mu(\mathcal{L}[M])\le\frac{1}{2}\sqrt{\sum_{i=1}^{n}\left\langle C_i(M),C_i\left(M^{\perp}\right)\right\rangle^2}$.

מסקנה: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\mu(\mathcal{L})\le\frac{\sqrt{n}}{2}\lambda_n[\mathcal{L}]$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times n}$ מצומצמת $\frac{3}{4}$-LLL ויהי $t\in\mathbb{R}^n$ אזי $\|t-\mathrm{Babai}(M,t)\|\le2^{\frac{n}{2}-1}\left|\left\langle C_n(M),C_n\left(M^{\perp}\right)\right\rangle\right|$.

מסקנה: $\mathrm{Babai}\circ\frac{3}{4}\text{-LLL}$ הינו אלגוריתם $2^{\frac{n}{2}}$־קירוב של $\mathrm{CVP\text{-}lattice\text{-}search}$.

בעיית המרווח לוקטור הקרוב ביותר בסריג: תהיינה $T,S:\mathbb{N}\to\mathbb{N}$ אזי $\mathrm{GAP}_{[T,S]}\mathrm{CVP}=\mathrm{GAP}_{[T,S]}\mathrm{Val\text{-}lattice}$.

הגדרה: תהא $T:\mathbb{N}\to\mathbb{N}$ ויהי $r\in\mathbb{R}_{>0}$ אזי $\mathrm{GAP\text{-}CVP}_T=\mathrm{GAP}_{[r,r\cdot T]}\mathrm{CVP}$.

הגדרה: יהי $\mathbb{F}$ שדה יהי $\mathcal{F}\subseteq\mathbb{F}$ יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{F}^{n\times n}$ הפיכה אזי $\mathrm{Val\text{-}lattice}_0(M,\mathbb{F},\mathcal{F})=\min_{x\in\mathcal{F}^n\setminus\{0\}}\|Mx\|$.