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 $\Delta:X^n\times X^n\to\mathbb{N}$ כך $\Delta(x,y)=|\{i\in[m]\mid x_i\neq y_i\}|$.

טענה: תהא X קבוצה אזי Δ משרה את נורמת ℓ_0.

משקל האמינג: יהי $\mathbb{F}$ שדה אזי נגדיר $w:\mathbb{F}^n\to\mathbb{N}$ 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 $\mathcal{C}$ הינו קוד $[m,r[\mathcal{C}],d[\mathcal{C}],q]$ לתיקון שגיאות.

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

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

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

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

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

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 $b_1\ldots b_r\in\mathcal{C}$ בסיס אזי נגדיר $M_{\mathcal{C}}\in\mathbb{F}_q^{m\times r}$ כך $C_i(M_{\mathcal{C}})=b_i$ 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.

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

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

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

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 $|R(M_{\mathcal{C}})\cap V|\le m-d$.
- 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 $d' \geq \left\lceil \frac{d}{q} \right\rceil$ 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 $m \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil$.

למה: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה יהיו $m,r \in \mathbb{N}_+$ באשר $m > r$ ויהי $x \in \mathbb{F}_q^r \backslash \{0\}$ 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 $\mathbb{P}_{\substack{M \in \mathbb{F}_q^{m \times r} \\ \text{קוד לינארי } \mathcal{C}_M}}\left(d[\mathcal{C}_M] \leq (1-\delta)\left(m - \frac{m}{q}\right)\right) \leq |\mathcal{C}_M| \cdot \exp\left(-\frac{\delta^2}{2}\left(m - \frac{m}{q}\right)\right)$.

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)$\iff$(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 $|\mathcal{C}| \geq q^m \cdot \left(\sum_{i=0}^{d-1}\left(\binom{m}{i} \cdot (q-1)^i\right)\right)^{-1}$.

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 $|\mathcal{C}| \geq q^m \cdot \left(1 + \sum_{i=0}^{d-2}\left(\binom{m-1}{i} \cdot (q-1)^i\right)\right)^{-1}$.

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 $\ell \leq k$ יהי $\mathbb{F}$ שדה סופי באשר $|\mathbb{F}| \geq k$ יהיו $x_1 \ldots x_\ell \in \mathbb{F}$ שונים ונגדיר $\varphi : \mathbb{F}_{\leq k-1}[x] \to \mathbb{F}^\ell$ 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 $\mathrm{RS}_q[m,r] = \left\{(f(\alpha_i))_{i=1}^m \mid f \in (\mathbb{F}_q)_{\leq r-1}[x]\right\}$.

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

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 $\mathrm{RM}_q[m,r] = \left\{(f(\alpha))_{\alpha \in \mathbb{F}_q^m} \,\middle|\, f \in (\mathbb{F}_q)_{\leq r}[x_1,\ldots,x_m]\right\}$.

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

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

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

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

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

משפט: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r,a,b\in\mathbb{N}_+$ באשר $r=a\left(q-1\right)+b$ חלוקה עם שארית אזי $d\left[\mathrm{RM}_q\left[m,r\right]\right]\geq\left(q-b\right)q^{m-a-1}$.

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

טענה: יהיו $m,r\in\mathbb{N}_{\geq2}$ אזי $\mathrm{RM}_2\left[m,r\right]=\left\{\left(u,u+v\right)\mid\left(u\in\mathrm{RM}_2\left[m-1,r\right]\right)\wedge\left(v\in\mathrm{RM}_2\left[m-1,r-1\right]\right)\right\}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: יהי $\mathcal{C}$ קוד $\left[m,k,d,q\right]$ 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 $\left(M,t,\mathbb{F}\right)$.

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

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

בעיית הוקטור הקצר ביותר: $\text{SVP-code}=\left\{\left\langle\left(M,0,\mathbb{F}\right),\varepsilon\right\rangle\mid\exists v\neq0.\left\Vert Mv\right\Vert_0\leq\varepsilon\right\}$.

בעיית החתך המקסימלי: יהי G גרף סופי אזי $\mathrm{MaxCut}\left(G\right)=\max\left\{\left|E\left(S,S^{\mathcal{C}}\right)\right|\,\middle|\,S\subseteq V\left(G\right)\right\}$.

מטריצת החתכים: יהי G גרף סופי אזי נגדיר $M\left(G\right)\in\mathbb{F}_2^{\left|E\left(G\right)\right|\times\left|V\left(G\right)\right|}$ כך $\left(M\left(G\right)\right)_{e,v}=\mathbb{1}\left[v\in e\right]$ לכל $e\in E\left(G\right)$ ולכל $v\in V\left(G\right)$.

טענה: יהי G גרף סופי אזי $\mathrm{Val}\left(\left(M\left(G\right),\mathbb{1}_{\left|V\left(G\right)\right|},\mathbb{F}_2\right)\right)=\mathrm{MaxCut}\left(G\right)$.

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

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

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

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

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

מסקנה: יהי $\varepsilon>0$ אזי קיים שדה סופי $\mathbb{F}$ עבורו $\mathrm{GAP}_{\left[\varepsilon,1-\varepsilon\right]}\text{CVP-code}_{\mathbb{F}}$ 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 $R_i\left(M\right) \cdot \mathbb{1}_m = 0$.

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 $\mathrm{Promise}\text{-}\mathcal{NP}$־קשה. השערה פתוחה

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

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 $\mathrm{Promise}\text{-}\mathcal{NP}$־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 $\mathrm{Promise}\text{-}\mathcal{NP}$־קשה.

בעיית החתך המקסימלי כתכנות שלם: יהי G גרף סופי אזי נגדיר $\mathrm{MaxCut\text{-}IP}\left(G\right)$ כך

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} \frac{1 - x_u x_v}{2} \\ \text{s.t.} \quad & x_v \in \{-1,1\} \qquad ,\forall v \in V \end{aligned}$$

טענה: יהי G גרף סופי ויהי $x \in \mathbb{F}_2^{|V(G)|}$ באשר $\mathrm{MaxCut\text{-}IP}\left(G\right) = x$ אזי $\left\{v \in V\left(G\right) \mid x_v = 1\right\}$ חתך מקסימלי של G.

בעיית החתך המקסימלי כתכנות לינארי: יהי G גרף סופי אזי נגדיר $\mathrm{MaxCut\text{-}LP}\left(G\right)$ כך

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} \frac{1 - x_u x_v}{2} \\ \text{s.t.} \quad & x_v \in [-1,1] \qquad ,\forall v \in V \end{aligned}$$

מטריצה מוגדרת חיובית: יהי $n \in \mathbb{N}_+$ אזי $A \in \mathbb{R}^{n\times n}$ המקיימת $x^T A x \geq 0$ לכל $x \in \mathbb{R}^n$.

סימון: יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{R}^{n\times n}$ מוגדרת חיובית אזי $A \geq 0$.

מכפלה פנימית של מטריצות: יהי $n \in \mathbb{N}_+$ ותהיינה $A,B \in \mathbb{R}^{n\times n}$ אזי $\langle A,B\rangle = \mathrm{trace}\left(A^T B\right)$.

תוכנה חצי מוגדרת: יהיו $n,m,k,\ell \in \mathbb{N}$ תהא $C \in \mathbb{R}^{n\times n}$ יהי $P \in \left(\mathbb{R}^{n\times n}\right)^m$ תהא $p \in \mathbb{R}^m$ יהי $Q \in \left(\mathbb{R}^{n\times n}\right)^k$ תהא $q \in \mathbb{R}^k$ יהי $R \in \left(\mathbb{R}^{n\times n}\right)^\ell$ ויהי $r \in \mathbb{R}^\ell$ אזי $\left(C,P,p,Q,q,R,r\right)$.

בעיית תכנות חצי מוגדר (SDP): יהי $m \in \{\max, \min\}$ ותהא $\left(C,P,p,Q,q,R,r\right)$ תוכנה חצי מוגדרת אזי מציאת נקודת קיצון מסוג m של $\langle C,X\rangle$ תחת ההנחות $\left\{\langle R_i,X\rangle = r_i \mid i \in [\mathrm{len}\left(r\right)]\right\} \cup \left\{\langle Q_i,X\rangle \geq q_i \mid i \in [\mathrm{len}\left(q\right)]\right\} \cup \left\{\langle P_i,X\rangle \leq p_i \mid i \in [\mathrm{len}\left(p\right)]\right\}$.

הערה: מכאן והלאה נשתמש במונח תוכנה לינארית גם עבור בעיית תכנות לינארי.

סימון: תהא $\left(c,P,p,Q,q,R,r\right)$ בעיית תכנות לינארית מקסימלית אזי נסמן את בעיית התכנות החצי מוגדר כך

$$\begin{aligned} \max \quad & \langle C,X\rangle \\ \text{s.t.} \quad & X \geq 0 \\ & \langle P_i,X\rangle \leq p_i \qquad ,\forall i \in [\mathrm{len}\left(p\right)] \\ & \langle Q_i,X\rangle \geq q_i \qquad ,\forall i \in [\mathrm{len}\left(q\right)] \\ & \langle R_i,X\rangle = r_i \qquad ,\forall i \in [\mathrm{len}\left(r\right)] \end{aligned}$$

סימון: תהא $\left(c,P,p,Q,q,R,r\right)$ בעיית תכנות לינארית מינימלית אזי נסמן את בעיית התכנות החצי מוגדר כך

$$\begin{aligned}\min \quad & \langle C, X\rangle \\ \text{s.t.} \quad & X \geq 0 \\ & \langle P_i, X\rangle \leq p_i \qquad , \forall i \in [\operatorname{len}(p)] \\ & \langle Q_i, X\rangle \geq q_i \qquad , \forall i \in [\operatorname{len}(q)] \\ & \langle R_i, X\rangle = r_i \qquad , \forall i \in [\operatorname{len}(r)]\end{aligned}$$

בעיית החתך המקסימלי כתכנות חצי מוגדר: יהי G גרף סופי אזי נגדיר $\text{MaxCut-SDP}(G)$ כך

$$\begin{aligned}\max \quad & \sum_{\{u,v\}\in E(G)} \frac{1-A_{u,v}}{2} \\ \text{s.t.} \quad & A \geq 0 \\ & A_{t,t} = 1 \qquad , \forall t \in V(G)\end{aligned}$$

פירוק צ'ולסקי: יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{R}^{n\times n}$ סימטרית מוגדרת חיובית אזי $L = \text{Chol}(A)$ באשר $A = L \cdot L^T$.

אלגוריתם צ'ולסקי: יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{R}^{n\times n}$ סימטרית מוגדרת חיובית אזי

Algorithm `CholeskyAlgorithm(`A`)`:
- $A^{(1)} \ldots A^{(n)}, L^{(1)} \ldots L^{(n)} \in \mathbb{R}^{n\times n}$; $\qquad A^{(1)} \leftarrow A$
- **for** $k \in [1 \ldots n]$ **do**
  - $a_k \leftarrow \left(A^{(k)}\right)_{k,k}$; $\qquad b_{(k)} \leftarrow \left(A^{(k)}\right)_{\{k+1,\ldots,n\}\times\{k\}}$; $\qquad B^{(k)} \leftarrow \left(A^{(k)}\right)_{\{k+1,\ldots,n\}\times\{k+1,\ldots,n\}}$
  - $L^{(k)} \leftarrow \begin{pmatrix} I_{k-1} & 0 & 0 \\ 0 & \sqrt{a_k} & 0 \\ 0 & \frac{1}{a_k}\cdot b_{(k)} & I_{n-k}\end{pmatrix}$
  - $A^{(k+1)} \leftarrow \begin{pmatrix} I_k & 0 \\ 0 & B^{(k)} - \frac{1}{a_k}\cdot b_{(k)}\cdot b_{(k)}^T\end{pmatrix}$
- **end**
- **return** $\prod_{k=1}^{n} L^{(k)}$

טענה: יהי $n \in \mathbb{N}_+$ ותהא $A \in \mathbb{R}^{n\times n}$ סימטרית מוגדרת חיובית אזי $\text{CholeskyAlgorithm}(A) = \text{Chol}(L)$.

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

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

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 $\text{StrassenMatMul}(\mathbb{F}, A, B) = AB$.

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

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

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

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 $B_{r}\left(0\right)\cap\mathcal{L}=\left\{ 0\right\}$.

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

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

למה: יהי $\mathcal{L}$ סריג אבסטרקטי אזי קיים $v\in\mathcal{L}\backslash\left\{ 0\right\}$ עבורו לכל $u\in\mathcal{L}\backslash\left\{ 0\right\}$ מתקיים $\left\Vert v\right\Vert \le\left\Vert u\right\Vert$.

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

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

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

החלפת עמודות: יהי $n\in\mathbb{N}_+$ ויהיו $i,j\in\left[n\right]$ שונים אזי נגדיר $\Phi_{i,j}^{\leftrightarrow}:\mathbb{R}^{n\times n}\to\mathbb{R}^{n\times n}$ כך $\Phi_{i,j}^{\leftrightarrow}\left(M\right)=M+C_{j}\left(M\right)\cdot\left(e_{i}-e_{j}\right)^{T}+C_{i}\left(M\right)\cdot\left(e_{j}-e_{i}\right)^{T}$.

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

טרנספורמציות אלמנטריות: יהי $n\in\mathbb{N}_+$ אזי $\left\{ \Phi_{i,j,a}^{+}\mid\left(\begin{smallmatrix}i,j\in\left[n\right]\\ i\ne j\end{smallmatrix}\right)\wedge\left(a\in\mathbb{Z}\right)\right\} \cup\left\{ \Phi_{i,j}^{\leftrightarrow}\mid\begin{smallmatrix}i,j\in\left[n\right]\\ i\ne j\end{smallmatrix}\right\} \cup\left\{ \Phi_{i}^{-}\mid i\in\left[n\right]\right\}$.

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

משפט: יהי $n\in\mathbb{N}_+$ ותהיינה $A,B\in\mathbb{R}^{n\times n}$ הפיכות אזי ($\mathcal{L}\left[A\right]=\mathcal{L}\left[B\right]$)$\Longleftrightarrow$(קיים $m\in\mathbb{N}_+$ וקיימות טרנספורמציות אלמנטריות $\varphi_{1}\ldots\varphi_{m}$ עבורן $A=\left(\varphi\circ\ldots\circ\varphi_{m}\right)\left(B\right)$).

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

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

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

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 $\left(M^{\vee}\right)^{\vee}=M$.

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

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

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

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

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

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

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

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 $\text{LatInterBasis}\left(A,B\right)=\text{basis}\left(\mathcal{L}\left[A\right]\cap\mathcal{L}\left[B\right]\right)$.

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

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

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 $\lfloor v\rfloor_{\mathcal{P}[M]}=\arg\min_{u\in\mathcal{L}[M]}\left(\|v-u\|\right)$.

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 $\lambda_{i}[\mathcal{L}]=\inf\left\{r\geq0\mid\dim\mathrm{span}\left(B_{r}(0)\cap\mathcal{L}\right)\geq i\right\}$.

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 $u_{i}^{\perp}\in\mathrm{span}(u_{1}\ldots u_{i})\backslash\mathrm{span}(u_{1}\ldots u_{i-1})$.

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 $B_{\lambda_{i+1}[\mathcal{L}]}(0)\cap\mathcal{L}\subseteq\mathrm{span}(u_{1}\ldots u_{i})$.

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 $\mathrm{Vol}(S)>\det(\mathcal{L})$ 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 $\mathrm{Vol}(S)>2^{n}\cdot\det(\mathcal{L})$ 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 $\prod_{i=1}^{n}\lambda_{i}[\mathcal{L}]\leq2^{n}\cdot\frac{\det(\mathcal{L})}{\mathrm{Vol}(B_{1}(0))}$.

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 $\widehat{h}(\omega)=e^{2\pi i\cdot\langle w,z\rangle}\cdot\hat{f}(\omega)$.

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 $\widehat{h}(\omega)=\frac{1}{\lambda^n}\cdot\hat{f}\left(\frac{\omega}{\lambda}\right)$.

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 $h(x)=\prod_{i=1}^n f_i(x_i)$ 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 $\mathbb{P}_{v\sim\mathcal{N}_n[\lambda_n[\mathcal{L}]\cdot r]}\left(v\notin B_{\lambda_n[\mathcal{L}]}(0)\;\middle|\;v\in\mathcal{L}^\vee\right)\le\varepsilon$.

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 $\left\langle C_i(M),C_i\left(M^\perp\right)\right\rangle\cdot C_i\left(M^\perp\right)=\arg\min\left\{\|v\|\;\middle|\;v\in\pi_{\mathrm{span}^\perp(C_1(M),\ldots,C_{i-1}(M))}(\mathcal{L})\right\}$.
- 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 $\left|\left\langle C_i(M),C_j\left(M^\perp\right)\right\rangle\right|\ge2\left|\left\langle C_j(M),C_j\left(M^\perp\right)\right\rangle\right|$.
- 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 $\mu(\mathcal{L}) = \max_{t \in \mathbb{R}^n} \text{dist}(t, \mathcal{L})$.

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 $O(n^2)$.

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

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 $\|t - \text{Babai}(M, t)\| \le 2^{\frac{n}{2}-1}\left|\left\langle C_n(M), C_n\left(M^{\perp}\right)\right\rangle\right|$.

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

משפט: CVP-lattice הינה $\mathcal{NP}$-קשה.

סימון: תהא $C \subseteq \mathcal{P}\left(\{0,1\}^*\right)$ אזי $C = \text{Promise-}C$.

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

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

מסקנה: $\text{GAP-CVP}_{2^{\frac{n}{2}}} \in \mathcal{P}$.

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 $\text{Val-lattice}_0(M, \mathbb{F}, \mathcal{F}) = \min_{x \in \mathcal{F}^n \setminus \{0\}} \|Mx\|$.

בעיית המרווח לוקטור הקצר ביותר בסריג: תהיינה $T, S : \mathbb{N} \to \mathbb{N}$ אזי $\text{GAP}_{[T,S]}\text{SVP} = \text{GAP}_{[T,S]}\text{Val-lattice}_0$.

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

טענה: יהי $\gamma \in \mathbb{R}_{\ge 1}$ אזי GAP-CVP_γ הינה $\mathcal{NP}$-קשה.

מסקנה: יהי $\gamma \in \mathbb{R}_{\ge 1}$ אזי GAP-SVP_γ הינה $\mathcal{NP}$-קשה.

טענה: $\text{GAP-SVP}_n \in \text{co}\mathcal{NP}$.

משפט: קיים $c \in \mathbb{R}_{>0}$ עבורו $\text{GAP-CVP}_{\exp\left(c \cdot \frac{\log(n)}{\log\log(n)}\right)}$ הינה $\mathcal{NP}$-קשה.

משפט: תהא $\gamma : \mathbb{N} \to \mathbb{N}$ באשר $\gamma = 2^{\mathcal{O}\left(n \cdot \frac{\log\log(n)}{\log(n)}\right)}$ אזי $\text{GAP-CVP}_\gamma \in \mathcal{P}$.

משפט: $\text{GAP-CVP}_{\sqrt{n}}, \text{GAP-SVP}_{\sqrt{n}} \in \mathcal{NP} \cap \text{co}\mathcal{NP}$.

בעיית הוקטורים הבלתי תלויים הקצרים ביותר: תהא $T : \mathbb{N} \to \mathbb{N}$ יהי $n \in \mathbb{N}_+$ ותהא $M \in \mathbb{R}^{n \times n}$ הפיכה אזי $\text{SIVP}_T(M) = (v_1 \ldots v_n)$ באשר $v_1 \ldots v_n$ בת"ל וכן $\|v_i\| \le T(n) \cdot \lambda_n[\mathcal{L}[M]]$ לכל $i \in [n]$.

טענה: יהי $\gamma \in \mathbb{R}_{\ge 1}$ אזי $\text{SIVP}_{\gamma \cdot \sqrt{n}} \le_p \text{GAP-SVP}_\gamma$.

טענה: יהי $\gamma \in \mathbb{R}_{\ge 1}$ אזי $\text{SIVP}_\gamma \le_p \text{GAP-CVP}_\gamma$.

טענה: יהיו $\gamma, c \in \mathbb{R}_{\ge 1}$ אזי c-קירוב של SIVP_γ הינו $\mathcal{NP}$-קשה.