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

מרחק האמינג יחסי: תהא X קבוצה אזי נגדיר $\Delta:X^n\times X^n\to\mathbb{N}$ כך $\Delta_r\left(x,y\right)=\frac{1}{n}\left|\left\{i\in[m]\mid x_i\neq y_i\right\}\right|$.

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

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 $\left[m\left\lceil\log\left(q\right)\right\rceil,r\log\left(q\right),d',2\right]$ 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 $d\ge\left(1-\frac{1}{q}\right)m$ 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.

הגדרה: יהי $\mathbb{F}$ שדה ויהי $n\in\mathbb{N}_+$ אזי נגדיר $\mathbb{1}_n\in\mathbb{F}^n$ כך $\left(\mathbb{1}_n\right)_i=1$ 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 $d=\min_{v\in\mathcal{C}}\Delta\left(v,0\right)$.

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 $\dim(V) = r-1$ 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)$\Longleftrightarrow$(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 $d \leq m$ 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 $k \leq \ell$ 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.

מטריצת ונדרמונד: ייהי $q \in \mathbb{N}$ 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 נגדיר $H_q(r, \{\alpha_1 \ldots \alpha_m\}) \in \mathbb{F}_q^{m \times r}$ כך $(H_q(r, \{\alpha_1 \ldots \alpha_m\}))_{i,j} = \alpha_i^{j-1}$.

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 $M_{\mathrm{RS}_q[m,r]} = H_q(r, \{\alpha_1 \ldots \alpha_m\})$.

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': יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ שונים תהא $w \in \mathrm{RS}_q[m,r]$ יהי $e \in \mathbb{F}_q^m$ באשר $\Delta(e,0) \le \frac{m-r}{2}$ ונגדיר $y = w + e$ אזי

Algorithm `BerlekampWelch`(q,m,r,α,y):
- $g \in (\mathbb{F}_q)[x]; \qquad \deg(g) = r + \left\lceil \frac{m-r}{2} \right\rceil - 1$
- $h \in (\mathbb{F}_q)[x]; \qquad \deg(h) = \left\lfloor \frac{m-r}{2} \right\rfloor$
- $(g,h) \leftarrow \mathrm{LinearEqSolver}\left((g(\alpha_i) = h(\alpha_i) \cdot y_i)_{i=1}^m\right)$ `// We do not accept` $g = h = 0$
- **return** $\mathrm{PolynomialDivision}(g,h)$

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ שונים תהא $w \in \mathrm{RS}_q[m,r]$ יהי $e \in \mathbb{F}_q^m$ באשר $\Delta(e,0) \le \frac{m-r}{2}$ ונגדיר $y = w + e$ אזי $\mathrm{BerlekampWelch}(q,m,r,\alpha,y) = P$ באשר $P \in (\mathbb{F}_q)_{\le r-1}[x]$ וכן $\Delta(P,y) \le \frac{m-r}{2}$.

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: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ שונים תהא $w \in \mathrm{RS}_q[m,r]$ יהי $e \in \mathbb{F}_q^m$ באשר $\Delta(e,0) \le m - 2\sqrt{mr}$ ונגדיר $y = w + e$ אזי

Algorithm `Sudan`(q,m,r,α,y):
- $Q \in (\mathbb{F}_q)[x,y]; \qquad \deg_x(Q) = \sqrt{mr}; \qquad \deg_y(Q) = \sqrt{\frac{m}{r}}$
- $Q \leftarrow \mathrm{LinearEqSolver}\left((Q(y_i,\alpha_i) = 0)_{i=1}^m\right)$ `// We do not accept` $Q = 0$
- $S \in \mathrm{List}(\mathbb{F}_q[x]); \qquad S \leftarrow \mathrm{PolymonialSolutions}(Q)$ `// We view` Q `as a polynomial in` $(\mathbb{F}_q[x])[y]$
- **return** $[h \quad \textbf{for} \quad h \in S \quad \textbf{if} \quad \Delta\left((h(\alpha_i))_{i=1}^m, y\right) < m - 2\sqrt{mr}]$

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$ שונים תהא $w \in \mathrm{RS}_q[m,r]$ יהי $e \in \mathbb{F}_q^m$ באשר $\Delta(e,0) \le m - 2\sqrt{mr}$ ונגדיר $y = w + e$ אזי $\mathrm{Sudan}(q,m,r,\alpha,y) = L$ באשר $\{(h(\alpha_i))_{i=1}^m \mid h \in L\} = \left\{w' \in \mathrm{RS}_q[m,r] \mid \exists \varepsilon \in \mathbb{F}_q^m : (y = w' + \varepsilon) \wedge \left(\Delta(\varepsilon,0) \le m - 2\sqrt{mr}\right)\right\}$.

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

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

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m, r \in \mathbb{N}_+$ אזי קיימים $k, d \in \mathbb{N}_+$ עבורם $\mathrm{RM}_q[m,r]$ הינו קוד לינארי $[q^m,k,d,q]$ 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 $m, r \in \mathbb{N}_{\ge 2}$ אזי $\mathrm{RM}_2[m,r] = \{(u,u+v) \mid (u \in \mathrm{RM}_2[m-1,r]) \wedge (v \in \mathrm{RM}_2[m-1,r-1])\}$.

אלגוריתם תיקון שגיאות מקומי בקוד ריד־מיולר: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in \mathbb{N}_+$ ויהיו $\alpha, \varepsilon \in (0,1)$ יהי $z \in \mathbb{F}_q^m$ ותהא $w \in \mathbb{F}_q^{q^m}$ באשר $d(\mathrm{RM}_q[m,\alpha q], w) \le q^m \cdot \frac{1-\alpha}{6}$ אזי

Algorithm `LocalRM`$(\varepsilon,q,m,\alpha,z,w;R)$:
- $t \leftarrow \lceil -18 \cdot \log(\varepsilon) \rceil$
- $a_1 \dots a_t \in \mathbb{F}_q$
- **for** $i \in [1,\dots,t]$ **do**
  - $a_i \leftarrow \left(\mathrm{BerlekampWelch}\left(q,q,\alpha q + 1, x, w_{z + \mathbb{F}_q \cdot R(v)}\right)\right)(0)$
- **end**
- **return** $\mathrm{Majority}(a_1,\dots,a_t)$

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in \mathbb{N}_+$ ויהיו $\alpha, \varepsilon \in (0,1)$ יהי $z \in \mathbb{F}_q^m$ תהא $w \in \mathbb{F}_q^{q^m}$ באשר $d(\mathrm{RM}_q[m,\alpha q], w) \le q^m \cdot \frac{1-\alpha}{6}$ ותהא $f \in (\mathbb{F}_q)_{\le \alpha q}[x_1,\dots,x_m]$ באשר $(f(\alpha))_{\alpha \in \mathbb{F}_q^m} = \arg(d(\mathrm{RM}_q[m,\alpha q], w))$ אזי

$\mathbb{P}_{R\leftarrow\left(\mathbb{N}\to\mathbb{F}_q^m\setminus\{0\}\right)}\left(\mathrm{LocalRM}\left(\varepsilon,q,m,\alpha,z,w;R\right)=f\left(z\right)\right)\geq 1-\varepsilon$.

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

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

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

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

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

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

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

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

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

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

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

בעיית אי־סיפוק: יהי $\mathbb{F}$ שדה אזי $\mathrm{NoSatEq}_{\mathbb{F}}=\left\{\langle M,t\rangle \mid \left(M\in\mathbb{R}^{n\times n}\right)\wedge\left(t\in\mathbb{R}^n\right)\wedge\left(\exists x\in\mathbb{R}^n:\forall i\in[n]:\left(Mx\right)_i\neq t_i\right)\right\}$.

טענה: $\mathrm{NoSatEq}_{\mathbb{F}_2}\in\mathcal{P}$.

טענה: יהי $\mathbb{F}$ שדה סופי באשר $|\mathbb{F}|\geq 3$ אזי $\mathrm{NoSatEq}_{\mathbb{F}}$ הינה $\mathcal{NP}$־קשה.

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

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: $\text{SVP-code}=\left\{\langle M,\mathbb{F},\varepsilon\rangle \mid \exists v\neq 0.\Delta_r\left(Mv,0\right)\leq\varepsilon\right\}$.

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

מטריצת החתכים: יהי G גרף סופי אזי נגדיר $M\left(G\right)\in\mathbb{F}_2^{|E(G)|\times|V(G)|}$ 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 $\mathrm{Val}\left(\left(M\left(G\right),\mathbb{1}_{|V(G)|},\mathbb{F}_2\right)\right)=\mathrm{MaxCut}\left(G\right)$.

טענה: קיים $\varepsilon\in(0,1)$ עבורו $\mathrm{GAP}_{[1-\varepsilon,1-\varepsilon]}\mathrm{MaxCut}$ 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 $w\left(R_i\left(M\right)\right)=2$ 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 [חות' 2002]: יהי $\varepsilon>0$ אזי $\mathrm{UG}\left(\varepsilon\right)$ הינה $\text{Promise-}\mathcal{NP}$־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 $\mathrm{Val}_{2\to 1}\left(\left(M,\{u,v\},\mathbb{F}\right)\right)=\min_{t\in\mathrm{Interpol}(u,v)}\mathrm{Val}\left(\left(M,t,\mathbb{F}\right)\right)$.

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 2018]: יהי $\varepsilon > 0$ אזי $\mathrm{PCP}_{2\to 1}[\varepsilon, 1-\varepsilon]$ הינה Promise-$\mathcal{NP}$־קשה. לא הוכח בקורס

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

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

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

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

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

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

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

בעיית החתך המקסימלי כתכנות וקטורי: יהי G גרף אזי נגדיר $\text{MaxCut-VP}(G)$ כך

$$\begin{aligned} \max \quad & \sum_{(u,v)\in E} \frac{1 - \langle X_u, X_v \rangle}{2} \\ \text{s.t.} \quad & X_v \in \mathbb{S}^{|V(G)|-1} \qquad , \forall v \in V(G) \end{aligned}$$

מטריצה מוגדרת חיובית: יהי $n \in \mathbb{N}_+$ אזי $A \in \mathbb{R}^{n\times n}$ סימטרית 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 $C \in \mathbb{R}^{n\times n}$ תהא $P \in \left(\mathbb{R}^{n\times n}\right)^m$ יהי $p \in \mathbb{R}^m$ תהא $Q \in \left(\mathbb{R}^{n\times n}\right)^k$ יהי $q \in \mathbb{R}^k$ תהא $R \in \left(\mathbb{R}^{n\times n}\right)^\ell$ ויהי $r \in \mathbb{R}^\ell$ אזי (C, P, p, Q, q, R, r).

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

הערה: כל ההגדרות של תכנות לינארי מורחבות בצורה טבעית לתכנות חצי מוגדר.

משפט: תהא SDP בעיית תכנות חצי מוגדר ויהי $\varepsilon > 0$ אזי קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו ε־קירוב של SDP.

בעיית חיפוש פתרון פיזבילי של תוכנה חצי מוגדרת: תהא (C, P, p, Q, q, R, r) תוכנה חצי מוגדרת אזי $\text{Feasibility-Search}(C, P, p, Q, q, R, r) = X$ באשר $\langle P_i, X \rangle \leq p_i$ לכל $i \in [\mathrm{len}(p)]$ וכן $\langle Q_i, X \rangle \geq q_i$ לכל $i \in [\mathrm{len}(q)]$ וכן $\langle R_i, X \rangle = r_i$ לכל $i \in [\mathrm{len}(r)]$.

משפט: תהא P תוכנה חצי מוגדרת ויהי $\varepsilon > 0$ אזי קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו ε־קירוב של $\text{Feasibility-Search}(P)$.

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

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

טענה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ ותהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg \text{MaxCut-VP}(G)$ אזי $X^T X = \arg \text{MaxCut-SDP}(G)$.

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

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

```
Algorithm Cholesky(A):
    A^(1) ... A^(n), L^(1) ... L^(n) ∈ R^{n×n};    A^(1) ← A
    for k ∈ [1 ... n] do
        a_k ← (A^(k))_{k,k};    b_(k) ← (A^(k))_{{k+1,...,n}×{k}};    B^(k) ← (A^(k))_{{k+1,...,n}×{k+1,...,n}}
        L^(k) ← ( I_{k-1}  0  0 ; 0  √a_k  0 ; 0  (1/a_k)·b_(k)  I_{n-k} )
        A^(k+1) ← ( I_k  0 ; 0  B^(k) − (1/a_k)·b_(k)·b_(k)^T )
    end
    return ∏_{k=1}^n L^(k)
```

$$A^{(1)}\dots A^{(n)},L^{(1)}\dots L^{(n)}\in\mathbb{R}^{n\times n};\qquad A^{(1)}\leftarrow A$$
$$a_k\leftarrow\left(A^{(k)}\right)_{k,k};\quad b_{(k)}\leftarrow\left(A^{(k)}\right)_{\{k+1,\dots,n\}\times\{k\}};\quad B^{(k)}\leftarrow\left(A^{(k)}\right)_{\{k+1,\dots,n\}\times\{k+1,\dots,n\}}$$
$$L^{(k)}\leftarrow\begin{pmatrix}I_{k-1}&0&0\\0&\sqrt{a_k}&0\\0&\frac{1}{a_k}\cdot b_{(k)}&I_{n-k}\end{pmatrix}\qquad A^{(k+1)}\leftarrow\begin{pmatrix}I_k&0\\0&B^{(k)}-\frac{1}{a_k}\cdot b_{(k)}\cdot b_{(k)}^T\end{pmatrix}$$
$$\textbf{return}\ \prod_{k=1}^n L^{(k)}$$

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

מסקנה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ ותהא $A \in \mathbb{R}^{n\times n}$ באשר $A = \arg\text{MaxCut-SDP}(G)$ אזי $\text{Chol}(A)^T = \arg\text{MaxCut-VP}(G)$.

הגדרה: יהי $n \in \mathbb{N}_+$ אזי נגדיר $\nu : \mathbb{R}^n \times \mathbb{R}^n \to \{\pm 1\}$ כך $\nu_p(\xi) = \begin{cases}1 & \langle\xi,p\rangle\ge 0\\ -1 & \text{else}\end{cases}$.

טענה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ תהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg\text{MaxCut-VP}(G)$ ויהיו $u, v \in V(G)$ שונים אזי $\mathbb{P}_{p\in\mathbb{S}^{n-1}}\left(\nu_p(C_u(X)) \ne \nu_p(C_v(X))\right) = \frac{\arccos(\langle C_u(X), C_v(X)\rangle)}{\pi}$.

הגדרה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ תהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg\text{MaxCut-VP}(G)$ ויהי $p \in \mathbb{R}^n$ אזי $S_p(X) = \{v \in V(G) \mid \nu_p(C_u(X)) = 1\}$.

מסקנה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ ותהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg\text{MaxCut-VP}(G)$ אזי $\mathbb{E}_{p\in\mathbb{S}^{n-1}}\left[\left|E\left(S_p(X), \overline{S_p(X)}\right)\right|\right] = \frac{1}{\pi}\sum_{\{u,v\}\in E(G)}\arccos(\langle C_u(X), C_v(X)\rangle)$.

מסקנה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ ותהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg\text{MaxCut-VP}(G)$ אזי $\mathbb{E}_{p\in\mathbb{S}^{n-1}}\left[\left|E\left(S_p(X), \overline{S_p(X)}\right)\right|\right] \ge 0.878567 \cdot \text{MaxCut}(G)$.

טענה: יהי $\varepsilon > 0$ יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V(G)| = n$ וכן $\text{MaxCut}(G) = (1-\varepsilon)|E(G)|$ ותהא $X \in \mathbb{R}^{n\times n}$ באשר $X = \arg\text{MaxCut-VP}(G)$ אזי $\mathbb{E}_{p\in\mathbb{S}^{n-1}}\left[\left|E\left(S_p(X), \overline{S_p(X)}\right)\right|\right] \ge \left(1 - \frac{2}{\pi}\sqrt{\varepsilon} - \mathcal{O}\left(\varepsilon^{1.5}\right)\right)|E(G)|$.

משפט חות'־קינדלר־או'דונל־מוסל: יהי $\varepsilon > 0$ יהי $\rho \in (0,1)$ ותהא $T : \mathbb{N} \to \mathbb{N}$ אזי ($\text{UG}(\varepsilon)$ חשיבה בזמן T)$\Longleftrightarrow$($\text{GAP}_{[\rho, 1-\arccos(\rho)+\varepsilon]}\text{MaxCut}$ חשיבה בזמן T).

טענה: יהי $\mathbb{F}$ שדה יהי $n \in \mathbb{N}_+$ ותהיינה $A, B \in \mathbb{F}^{n\times n}$ אזי קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו 0.878־קירוב של $\max_{x\in\{\pm1\}^n}\left(\sum_{\substack{i,j\in[n]\\ i<j}}\left((A)_{i,j}(1 - x_ix_j) + (B)_{i,j}(1 + x_ix_j)\right)\right)$.

טענה: יהי $d \in \mathbb{N}$ ויהי $p \in \mathbb{R}[x]$ באשר $\deg(p) = d$ אזי קיימת בעיית תכנות חצי מוגדר $\mathcal{A}$ המקיימת ($\mathcal{A}$ בעלת פתרון פיזבילי)$\Longleftrightarrow$(קיימים $q_1 \dots q_m \in \mathbb{R}[x]$ עבורם $p = \sum_{i=1}^m q_i^2$).

טענה: יהי $d \in \mathbb{N}$ ויהי $p \in \mathbb{R}[x]$ באשר $\deg(p) = d$ אזי (קיימים $q_1 \dots q_m \in \mathbb{R}[x]$ עבורם $p = \sum_{i=1}^m q_i^2$)$\Longleftrightarrow$($p \ge 0$).

טענה: קיימת בעיית תכנות חצי מוגדר $\mathcal{A}$ עבורה לכל $p \in \mathbb{R}[x]$ מתקיים $\mathcal{A}(p) = \min(\text{Im}(p))$.

בעיית מינימליות הערך העצמי המקסימלי לפונקציה אפינית: יהיו $n, k \in \mathbb{N}_+$ ותהיינה $A_0 \dots A_k \in \mathbb{R}^{n\times n}$ אזי $\text{MinMaxEigenvalue}(A_0 \dots A_k) = \min\left\{\max\left(\text{spec}\left(A_0 + \sum_{i=1}^k A_ix_i\right)\right) \,\middle|\, x \in \mathbb{R}^k\right\}$.

טענה: יהי $\varepsilon > 0$ אזי קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו ε־קירוב של MinMaxEigenvalue.

יציבות פנימית של גרף: יהי G גרף אזי $\alpha(G) = \max\{|I| \mid (I \subseteq V(G)) \wedge (I \text{ בלתי תלויה})\}$.

מכפלה חזקה של גרפים: יהיו G, H גרפים מכוונים אזי נגדיר גרף מכוון $G \boxtimes H$ כך $V(G \boxtimes H) = V(G) \times V(H)$ וכן $E(G \boxtimes H) = \left\{((u,u'),(v,v')) \in V(G \boxtimes H)^2 \,\middle|\, (u \in N^-(v) \cup \{v\}) \wedge (u' \in N^-(v') \cup \{v'\})\right\}$.

סימון: יהי G גרף מכוון אזי $G^{\boxtimes 1} = G$ וכן $G^{\boxtimes n} = G^{\boxtimes(n-1)} \boxtimes G$ לכל $n \in \mathbb{N}_{\ge 2}$.

קיבולת שאנון של גרף: יהי G גרף מכוון אזי $\Theta(G) = \lim_{k\to\infty}\sqrt[k]{\alpha\left(G^{\boxtimes k}\right)}$.

טענה: יהי G גרף מכוון אזי $\Theta(G) = \sup_{k\in\mathbb{N}_+}\sqrt[k]{\alpha\left(G^{\boxtimes k}\right)}$.

טענה: יהי G גרף מכוון אזי $\Theta(G) \ge \alpha(G)$.

הגדרה: יהי G מכוון אזי נגדיר גרף לא מכוון G_{dc} כך $V(G_{\text{dc}}) = V(G)$ וכן $E(G_{\text{dc}}) = \{e \in \mathcal{P}_2(V(G)) \mid ((e_1, e_2) \in E(G)) \vee ((e_2, e_1) \in E(G))\}$.

ייצוג אורתונורמלי של גרף: יהי G גרף ויהי $d\in\mathbb{N}_+$ אזי $R:V(G)\to\mathbb{R}^d$ באשר לכל $u,v\in V(G)$ המקיימים $\{u,v\}\notin E(G_{\mathrm{dc}})$ מתקיים $R_u\perp R_v$.

מספר לובאס של גרף: יהי G גרף אזי $\vartheta(G)=\min\left\{\min\left\{\max\left\{\frac{1}{\langle R_u,c\rangle^2}\;\middle|\;u\in V(G)\right\}\;\middle|\;\substack{c\in\mathbb{R}^d\\ \|c\|=1}\right\}\;\middle|\;\substack{d\in\mathbb{N}_+\\ R\text{ ייצוג אורתונורמלי } d \text{ מימדי של } G}\right\}$.

משפט: יהי G גרף נגדיר $B_\varnothing\in\mathbb{R}^{V(G)\times V(G)}$ כך $(B_\varnothing)_{u,v}=\begin{cases}1 & u=v\\ 1 & \{u,v\}\notin E(G_{\mathrm{dc}})\\ 0 & \text{else}\end{cases}$ ונגדיר $B:E(G_{\mathrm{dc}})\to\mathbb{R}^{V(G)\times V(G)}$ כך $\left(B_{\{u,v\}}\right)_{t,s}=\begin{cases}1 & \{t,s\}=\{u,v\}\\ 0 & \text{else}\end{cases}$ אזי $\mathrm{MinMaxEigenvalue}\left(B_\varnothing,(B_e)_{e\in E(G_{\mathrm{dc}})}\right)=\vartheta(G)$.

משפט: יהי G גרף מכוון אזי $\vartheta(G)\geq\Theta(G)$.

הגדרה משוואה לינארית בעלת שני משתנים: $\mathrm{2Lin}_{\mathbb{F}_2}=\left\{(A,v)\in\mathbb{F}_2^{m\times n}\times\mathbb{F}_2^m\;\middle|\;\mathbb{F}_2 \text{ מטריצת משחק מעל } A\right\}$.

טענה: יהיו $m,n\in\mathbb{N}$ תהא $A\in\mathbb{F}_2^{m\times n}$ ותהא $v\in\mathbb{F}_2^m$ אזי $\mathbb{E}_{x\leftarrow\mathbb{F}_2^n}\left[1-\Delta_r(Ax,v)\right]=\frac{1}{2}$.

בעיית המשוואות הלינאריות בעלות שני משתנים כתכנות שלם: יהיו $m,n\in\mathbb{N}$ תהא $A\in\mathbb{F}_2^{m\times n}$ ותהא $v\in\mathbb{F}_2^m$ אזי נגדיר $\mathrm{2Lin}_{\mathbb{F}_2}\text{-IP}(A,v)$ כך

$$\begin{aligned}\max\quad & \sum_{\substack{\ell\in[m]\\ i,j\in[n]}}\mathbb{1}\left[\substack{i<j\\ (A)_{\ell,i}=1\\ (A)_{\ell,j}=1}\right]\cdot(1-x_i+x_j+v_\ell)\\ \text{s.t.}\quad & x_i\in\{-1,1\}\qquad,\forall i\in[n]\end{aligned}$$

בעיית המשוואות הלינאריות בעלות שני משתנים כתכנות חצי מוגדר: יהיו $m,n\in\mathbb{N}$ תהא $A\in\mathbb{F}_2^{m\times n}$ ותהא $v\in\mathbb{F}_2^m$ אזי נגדיר $\mathrm{2Lin}_{\mathbb{F}_2}\text{-SDP}(A,v)$ כך

$$\begin{aligned}\max\quad & \sum_{\substack{\ell\in[m]\\ i,j\in[n]}}\mathbb{1}\left[\substack{i<j\\ (A)_{\ell,i}=1\\ (A)_{\ell,j}=1}\right]\cdot\left(\mathbb{1}[v_\ell=0]\cdot\left(\frac{1+\langle V_i,V_j\rangle}{2}\right)+\mathbb{1}[v_\ell=1]\cdot\left(\frac{1-\langle V_i,V_j\rangle}{2}\right)\right)\\ \text{s.t.}\quad & V_i\in\mathbb{S}^{n-1}\qquad,\forall i\in[n]\end{aligned}$$

טענה: יהי $\varepsilon\in[0,1]$ תהא $A\in\mathbb{F}_2^{m\times n}$ ותהא $v\in\mathbb{F}_2^m$ באשר $\mathrm{Val}((A,v,\mathbb{F}_2))\leq\varepsilon$ אזי קיימת $V:[n]\to\mathbb{S}^{n-1}$ המקיימת

- $\sum_{\substack{\ell\in[m]\\ i,j\in[n]}}\mathbb{1}\left[\substack{i<j\\ (A)_{\ell,i}=1\\ (A)_{\ell,j}=1}\right]\cdot\mathbb{1}[v_\ell=0]\cdot\langle V_i,V_j\rangle\geq\frac{m}{2}(1-2\varepsilon)$.
- $\sum_{\substack{\ell\in[m]\\ i,j\in[n]}}\mathbb{1}\left[\substack{i<j\\ (A)_{\ell,i}=1\\ (A)_{\ell,j}=1}\right]\cdot\mathbb{1}[v_\ell=1]\cdot\langle V_i,V_j\rangle\leq-\frac{m}{2}(1-2\varepsilon)$.

טענה: יהי $\varepsilon\in[0,1]$ יהיו $m,n\in\mathbb{N}$ תהא $A\in\mathbb{F}_2^{m\times n}$ תהא $v\in\mathbb{F}_2^m$ באשר $\mathrm{Val}((A,v,\mathbb{F}_2))\leq\varepsilon$ ונגדיר $V=\mathrm{2Lin}_{\mathbb{F}_2}\text{-SDP}(A,v)$ אזי $\sum_{\substack{\ell\in[m]\\ i,j\in[n]}}\mathbb{1}\left[\substack{i<j\\ (A)_{\ell,i}=1\\ (A)_{\ell,j}=1}\right]\cdot\mathbb{P}_{p\in\mathbb{S}^{n-1}}\left(\frac{\nu_p(V_i)-\nu_p(V_j)}{2}=v_\ell\right)\geq m\left(1-\mathcal{O}(\sqrt{\varepsilon})\right)$.

בעיית הספיקות בשני משתנים כתכנות שלם: תהא $\varphi\in\mathrm{2CNF}$ באשר $\mathrm{FV}(\varphi)=\{x_1\ldots x_n\}$ ותהא $\mathcal{C}$ קבוצת נוסחאות באשר $\varphi=\bigwedge_{i=1}^m\mathcal{C}_i$ אזי נגדיר $\mathrm{2SAT\text{-}IP}(\varphi)$ כך

$$\begin{aligned}\max\quad & A+B+C+D\\ \text{s.t.}\quad & A=\sum_{x_i\wedge x_j\in\mathcal{C}}1-\left(\frac{1-y_0y_i}{2}\right)\left(\frac{1-y_0y_j}{2}\right);\qquad B=\sum_{x_i\wedge\neg x_j\in\mathcal{C}}1-\left(\frac{1-y_0y_i}{2}\right)\left(\frac{1+y_0y_j}{2}\right)\\ & C=\sum_{\neg x_i\wedge x_j\in\mathcal{C}}1-\left(\frac{1+y_0y_i}{2}\right)\left(\frac{1-y_0y_j}{2}\right);\qquad D=\sum_{\neg x_i\wedge\neg x_j\in\mathcal{C}}1-\left(\frac{1+y_0y_i}{2}\right)\left(\frac{1+y_0y_j}{2}\right)\\ & y_i\in\{-1,1\}\qquad,\forall i\in\{0,\ldots,n\}\end{aligned}$$

טענה: תהא $\varphi\in\mathrm{2CNF}$ נגדיר $y=\mathrm{2SAT\text{-}IP}(\varphi)$ ונגדיר השמה x כך $x_i=\mathbb{1}[y_0=y_i]$ אזי (φ ספיקה)$\Longleftrightarrow$(x מספק את φ).

טענה: קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו 0.878־קירוב של MAX2SAT.

מסקנה: נגדיר $\beta\in\mathbb{R}$ כך $\beta=\min_{x\in[-1,1]}\left(\frac{\frac{1}{2}+\frac{\arccos(x)}{2\pi}}{\frac{3}{4}-\frac{1}{4}x}\right)$ אזי קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו β־קירוב של MAXE2SAT.

מסקנה: קיים אלגוריתם פולינומי $\mathcal{A}$ באשר $\mathcal{A}$ הינו 0.943־קירוב של MAXE2SAT.

מסקנה: $\mathrm{2SAT}\in\mathcal{P}$.

בעיית 3-צביעה כתכנות וקטורי: יהי G גרף אזי נגדיר $\text{3Colorable-VP}\left(G\right)$ כך

$$\begin{aligned} \max \quad & 1 \\ \text{s.t.} \quad & X_v \in \mathbb{S}^{|V(G)|-1} \qquad ,\forall v \in V\left(G\right) \\ & \langle X_v, X_v \rangle = 1 \qquad ,\forall v \in V\left(G\right) \\ & \langle X_v, X_u \rangle = -\frac{1}{2} \qquad ,\forall \{u,v\} \in E\left(G\right) \end{aligned}$$

טענה: יהי G גרף 3-צביע אזי $\text{3Colorable-VP}\left(G\right)$ פיזבילית.

בעיית 3-צביעה כתכנות חצי מוגדר: יהי G גרף אזי נגדיר $\text{3Colorable-SDP}\left(G\right)$ כך

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

טענה: יהי $n \in \mathbb{N}_+$ יהי G גרף באשר $|V\left(G\right)| = n$ ותהא $X \in \mathbb{R}^{n \times n}$ אזי

- אם X פתרון פיזבילי של $\text{3Colorable-VP}\left(G\right)$ אז $X^T X$ פתרון פיזבילי של $\text{3Colorable-SDP}\left(G\right)$.
- אם X פתרון פיזבילי של $\text{3Colorable-SDP}\left(G\right)$ אז $\text{Chol}\left(X\right)^T$ פתרון פיזבילי של $\text{3Colorable-VP}\left(G\right)$.

אלגוריתם צביעה וקטורית של גרף 3-צביע: יהי G גרף 3-צביע יהי $\varepsilon \in \mathbb{R}_{\geq 1}$ ותהא $R : \mathbb{N}_+ \to \mathbb{S}^{|V(G)|-1}$ אזי

```
Algorithm 3Colorable-VecCol(G, ε; R):
    t ← 1 + ⌈log_3(Δ(G))⌉  // Δ(G) is the max degree of G
    X ∈ Approx-Feasibility-Search(ε, 3Colorable-VP(G))  // poly time ε-approx for the feasibility problem
    c ∈ V(G) → {±1}*
    for v ∈ V(G) do
        c(v) ← (ν_{R(i)}(X_v))_{i=1}^{t}
    end
    S ∈ P(V(G));    S ← ∅
    for v ∈ V(G) do
        for u ∈ N(v)\S do
            if c(v) = c(u) then
                S ← S ∪ {v}
            end
        end
    end
    c↾_{V(G[S])} ← 3Colorable-VecCol(G[S], ε; R↾_{N>t})
    return c
```

טענה: יהי G גרף 3-צביע יהי $\varepsilon \in \mathbb{R}_{\geq 1}$ ותהא $R : \mathbb{N}_+ \to \mathbb{S}^{|V(G)|-1}$ אזי $\text{3Colorable-VecCol}\left(G, \varepsilon; R\right)$ צביעה חוקית של G.

טענה: יהי G גרף 3-צביע יהי X פתרון פיזבילי של $\text{3Colorable-VP}\left(G\right)$ ויהי $\{u,v\} \in E\left(G\right)$ אזי $\mathbb{P}_{p \leftarrow \mathbb{S}^{|V(G)|-1}}\left(\nu_p\left(X_u\right) = \nu_p\left(X_v\right)\right) = \frac{1}{3}$.

מסקנה: יהי G גרף 3-צביע ויהי $\varepsilon \in \mathbb{R}_{\geq 1}$ אזי $\mathbb{E}_{R \leftarrow \left(\mathbb{N}_+ \to \mathbb{S}^{|V(G)|-1}\right)}\left[\text{Time}\left(\text{3Colorable-VecCol}\left(G, \varepsilon; R\right)\right)\right] \in \text{poly}\left(|V\left(G\right)|\right)$.

מסקנה: יהי G גרף 3-צביע אזי קיים $\varepsilon \in \mathbb{R}_{\geq 1}$ המקיים $\mathbb{E}_{R \leftarrow \left(\mathbb{N}_+ \to \mathbb{S}^{|V(G)|-1}\right)}\left[\left|\text{Im}\left(\text{3Colorable-VecCol}\left(G, \varepsilon; R\right)\right)\right|\right] = \mathcal{O}\left(|V\left(G\right)|^{\log_3(2)} \cdot \log\left(|V\left(G\right)|\right)\right)$.

אלגוריתם ויגדרזון לצביעת גרף 3-צביע: יהי G גרף 3-צביע אזי

```
Algorithm Wigderson(G):
    n ← |V(G)|
    if Δ(G) ≤ √n then
        return GreedyColoring(G, {0, ..., √n})  // Coloring with √n + 1 colors
    v ← {t ∈ V(G) | deg(t) ≥ √n + 1}
    c ∈ (N(v) ∪ {v}) → {Black_v, Red_v, Blue_v};    c(v) ← Black_v
    c|_{N(v)} ← GreedyColoring(G[N(v)], {Red_v, Blue_v})
    c' ← Wigderson(G[V(G) \ (N(v) ∪ {v})])
    return c ∪ c'
```

טענה: יהי G גרף 3-צביע אזי $|\mathrm{Im}\left(\mathrm{Wigderson}\left(G\right)\right)|=\mathcal{O}\left(\sqrt{|V\left(G\right)|}\right)$.

אלגוריתם ויגדרזון וקטורי היברידי לצביעת גרף 3-צביע: יהי G גרף 3-צביע יהיו $\tau,\varepsilon\in\mathbb{R}_{\ge1}$ ותהא $R:\mathbb{N}_+\to\mathbb{S}^{|V(G)|-1}$ אזי

```
Algorithm WigdersonVectorHybrid(G, τ, ε; R):
    if Δ(G) < τ then  return 3Colorable-VecCol(G, ε; R)
    v ← {t ∈ V(G) | deg(t) ≥ τ}
    c ∈ (N(v) ∪ {v}) → {Black_v, Red_v, Blue_v};    c(v) ← Black_v
    c|_{N(v)} ← GreedyColoring(G[N(v)], {Red_v, Blue_v})
    c' ← WigdersonVectorHybrid(G[V(G) \ (N(v) ∪ {v})], τ, ε; R)
    return c ∪ c'
```

טענה: יהי G גרף 3-צביע ויהי $\tau\in\mathbb{R}_{\ge1}$ אזי קיים $\varepsilon\in\mathbb{R}_{\ge1}$ המקיים $\mathbb{E}_{R\leftarrow\left(\mathbb{N}_+\to\mathbb{S}^{|V(G)|-1}\right)}\left[|\mathrm{Im}\left(\mathrm{WigdersonVectorHybrid}\left(G,\tau,\varepsilon;R\right)\right)|\right]=\mathcal{O}\left(\frac{|V(G)|}{\tau}+\tau^{\log_3(2)}\cdot\log\left(|V\left(G\right)|\right)\right)$.

מסקנה: יהי $n\in\mathbb{N}$ יהי G גרף 3-צביע באשר $|V\left(G\right)|=n$ ונגדיר $\alpha\in\mathbb{R}$ כך $\alpha=\log_3\left(2\right)$ אזי קיים $\varepsilon\in\mathbb{R}_{\ge1}$ המקיים $\mathbb{E}_{R\leftarrow\left(\mathbb{N}_+\to\mathbb{S}^{|V(G)|-1}\right)}\left[\left|\mathrm{Im}\left(\mathrm{WigdersonVectorHybrid}\left(G,\left(\frac{3n}{\alpha\log(n)}\right)^{\frac{1}{\alpha+1}},\varepsilon;R\right)\right)\right|\right]=\mathcal{O}\left(n^{\frac{\alpha}{\alpha+1}}+\log\left(n\right)^{\frac{1}{\alpha+1}}\right)$.

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

הערה: בסיבוכיות של אלגוריתמים על מטריצות נתייחס לסיבוכיות כפונקציה של מספר עמודות המטריצה.

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

```
Algorithm NaiveMatMul(F, A, B):
    C ∈ F^{n×m};    C ← 0
    for i ∈ [1, ..., n] do
        for j ∈ [1, ..., m] do
            for ℓ ∈ [1, ..., k] do
                (C)_{i,j} ← (C)_{i,j} + (A)_{i,ℓ} · (B)_{ℓ,j}
            end
        end
    end
    return C
```

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

הערה: בסיבוכיות של אלגוריתמים על מספרים נתייחס לסיבוכיות כפונקציה של אורך המספר בבינארי.

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

```
Algorithm 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 $(\text{KaratsubaMult}\left((a)_2,(b)_2\right))_{10}=ab$.

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

חלוקה לבלוקים: יהי $\mathbb{F}$ שדה יהיו $n,n_0\in\mathbb{N}_+$ באשר $n_0|n$ ותהא $A\in\mathbb{F}^{n\times n}$ אזי נגדיר $\mathcal{B}_{n_0}\left(A\right)\in\left(\mathbb{F}^{n_0\times n_0}\right)^{\frac{n}{n_0}\times\frac{n}{n_0}}$ כך $(\mathcal{B}_{n_0}\left(A\right))_{i,j}=(A)_{((i-1)\cdot n_0,(j-1)\cdot n_0)+[n_0]^2}$.

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

```
Algorithm Strassen(F, A, B):
    if n = 0 then return A · B // A, B are scalars
    a, b, c, d ∈ F^{2^{n-1}};        (a b; c d) ← B_{2^{n-1}}(A)
    α, β, γ, δ ∈ F^{2^{n-1}};        (α β; γ δ) ← B_{2^{n-1}}(B)
    M_1 ∈ F^{2^{n-1}};    M_1 ← Strassen(F, a + d, α + δ)
    M_2 ∈ F^{2^{n-1}};    M_2 ← Strassen(F, c + d, α)
    M_3 ∈ F^{2^{n-1}};    M_3 ← Strassen(F, a, β − δ)
    M_4 ∈ F^{2^{n-1}};    M_4 ← Strassen(F, d, γ − α)
    M_5 ∈ F^{2^{n-1}};    M_5 ← Strassen(F, a + b, δ)
    M_6 ∈ F^{2^{n-1}};    M_6 ← Strassen(F, c − a, α + β)
    M_7 ∈ F^{2^{n-1}};    M_7 ← Strassen(F, b − d, γ + δ)
    return (M_1+M_4−M_5+M_7   M_2+M_4; M_3+M_5   M_1−M_2+M_3+M_6)
```

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

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

וקטוריזציה של מטריצה: יהי $\mathbb{F}$ שדה יהיו $n,m\in\mathbb{N}_+$ ותהא $A\in\mathbb{F}^{n\times m}$ אזי נגדיר $\vec{A}\in\mathbb{F}^{nm}$ כך $\vec{A}_i=(A)_{(i-1)\%n+1,\left\lfloor\frac{i-1}{n}\right\rfloor+1}$.

כפל אדמר: יהי $\mathbb{F}$ שדה ויהיו $n,m\in\mathbb{N}_+$ אזי נגדיר $\circ:\left(\mathbb{F}^{n\times m}\right)^2\to\mathbb{F}^{n\times m}$ כך $(A\circ B)_{i,j}=(A)_{i,j}\cdot(B)_{i,j}$.

אלגוריתם בי־לינארי לכפל מטריצות: יהי $\mathbb{F}$ שדה יהיו $n,n_0\in\mathbb{N}_+$ באשר $n_0|n$ יהי $\omega\in\mathbb{R}$ באשר $n_0^\omega\in\mathbb{N}$ ותהיינה $U,V,W\in\mathbb{F}^{n_0^\omega\times n_0^2}$ אזי נגדיר $\text{BiLinMatMul}_{U,V,W}:\left(\mathbb{F}^{n\times n}\right)^2\to\mathbb{F}^{n\times n}$ כך $\text{BiLinMatMul}_{U,V,W}\left(A,B\right)=W^T\left(\left(U\overrightarrow{\mathcal{B}_{n_0}\left(A\right)}\right)\circ\left(V\overrightarrow{\mathcal{B}_{n_0}\left(B\right)}\right)\right)$.

מכפלה פנימית משולשת: יהי $\mathbb{F}$ שדה ויהי $n\in\mathbb{N}_+$ אזי נגדיר $\langle\cdot,\cdot,\cdot\rangle:\left(\mathbb{F}^n\right)^3\to\mathbb{F}$ כך $\langle u,v,w\rangle=\sum_{i=1}^n u_iv_iw_i$.

סימון: יהי $\mathbb{F}$ שדה יהיו $n,m\in\mathbb{N}_+$ תהא $A\in\mathbb{F}^{n\times m^2}$ ויהיו $i,j\in[m]$ אזי $(A)_{i:j}=(A)_{(i-1)\cdot m+j}$.

משפט: יהי $\mathbb{F}$ שדה יהיו $n,n_0\in\mathbb{N}_+$ באשר $n_0|n$ יהי $\omega\in\mathbb{R}$ באשר $n_0^\omega\in\mathbb{N}$ ותהיינה $U,V,W\in\mathbb{F}^{n_0^\omega\times n_0^2}$ אזי ($\text{BiLinMatMul}_{U,V,W}$ הינו אלגוריתם כפל מטריצות)$\Longleftrightarrow$(לכל $i,i',j,j',k,k'\in[n_0]$ מתקיים $\langle U_{i:j'},V_{j:k'},W_{k:i'}\rangle=\delta_{i,i'}\cdot\delta_{j,j'}\cdot\delta_{k,k'}$).

טענה: יהי $\mathbb{F}$ שדה יהיו $n,n_0\in\mathbb{N}_+$ באשר $n_0|n$ יהי $\omega\in\mathbb{R}$ באשר $n_0^\omega\in\mathbb{N}$ ותהיינה $U,V,W\in\mathbb{F}^{n_0^\omega\times n_0^2}$ באשר $\text{BiLinMatMul}_{U,V,W}$ אלגוריתם כפל מטריצות אזי סיבוכיות הריצה של $\text{BiLinMatMul}_{U,V,W}$ הינה $\mathcal{O}\left(n^\omega\right)$.

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

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 $A\in\mathbb{F}^{n\times n}$ 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: יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}_+$ ותהא $A\in\mathbb{F}^{n\times n}$ בעלת פירוק LU אזי $\text{MatDet}\left(\mathbb{F},A\right)=L\cdot U$ באשר L,U הינו פירוק LU של A.

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

בעיית פתרון מערכת משוואות לינארית: יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}_+$ תהא $A\in\mathbb{F}^{n\times n}$ ויהי $b\in\mathbb{F}^n$ אזי $\text{LinEqSol}\left(A,b\right)=v$ באשר $Av=b$.

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

חבורה טופולוגית: תהא G חבורה ותהא $\mathcal{T}$ טופולוגיה על G אזי $\left(G,\mathcal{T}\right)$ באשר

- רציפות כפל: $\left(a,b\right)\mapsto ab$ הינה רציפה מעל $\left(G^2,\mathcal{T}_{\text{prod}}\right)$.
- רציפות הופכי: $a\mapsto a^{-1}$ הינה רציפה מעל $\left(G,\mathcal{T}\right)$.

חבורה דיסקרטית: חבורה טופולוגית $\left(G,\mathcal{T}\right)$ באשר G חסרת נקודות הצטברות.

חוג דיסקרטי: חוג $\left(R,+,*\right)$ באשר $\left(R,+\right)$ הינה חבורה דיסקרטית.

מימד של סריג: יהי $\mathbb{F}$ שדה יהי $\mathcal{F}\subseteq\mathbb{F}$ חוג דיסקרטי 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 דיסקרטי 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 $x-y\in\mathcal{L}$.
- $\max\left\{|V|\mid\left(V\subseteq\mathcal{L}\right)\wedge\left(\text{קבוצה בת״ל } V\right)\right\}=k$.
- 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 $\|v\|\le\|u\|$.

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

מסקנה: יהי $n\in\mathbb{N}_+$ ותהא $L\subseteq\mathbb{R}^n$ אזי (L חבורה דיסקרטית בעלת n וקטורים בת״ל)$\iff$(קיימת $M\in\mathbb{R}^{n\times n}$ הפיכה 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 $\left(\exists U\in\text{GL}_n\left(\mathbb{Z}\right):A=BU\right)\iff\left(\mathcal{L}\left[A\right]=\mathcal{L}\left[B\right]\right)$.

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 $\Phi^+_{i,j,a}\left(M\right)=M+a\cdot\left(C_j\left(M\right)\cdot e_i^T\right)$.

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

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

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

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

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

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

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

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

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 $\mathcal{P}\left[M\right]=\mathcal{L}_{\mathbb{R}\mid[0,1)}\left[M\right]$.

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 $\left\lfloor M\cdot a\right\rfloor_{\mathcal{P}[M]}=M\cdot\left\lfloor a\right\rfloor$.

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

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 $\left(v\mod\mathcal{P}\left[M\right]\right)=v-\left\lfloor v\right\rfloor_{\mathcal{P}[M]}$.

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

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

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

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

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

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

מסקנה: $\text{LatDet}\in\mathcal{P}$.

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

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

העוקבים המינימליים: יהי $k\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג ממשי מדרגה k ויהי $i\in[k]$ אזי $\lambda_i\left[\mathcal{L}\right]=\inf\left\{r\geq0\mid\dim\text{span}\left(B_r\left(0\right)\cap\mathcal{L}\right)\geq i\right\}$.

אורתונורמליזציה: יהי $n\in\mathbb{N}_+$ ויהיו $u_1\ldots u_n\in\mathbb{R}^n$ באשר $\left\{u_1\ldots u_n\right\}$ 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 $u_i^\perp\in\text{span}\left(u_1\ldots u_i\right)\backslash\text{span}\left(u_1\ldots u_{i-1}\right)$.

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 $C_i\left(M^\perp\right)=C_i\left(M\right)^\perp$ לכל $i\in[n]$.

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

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 $\left\|u_i\right\|=\lambda_i\left[\mathcal{L}\right]$ 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 $\left\|u_i\right\|=\lambda_i\left[\mathcal{L}\right]$ לכל $i\in[n]$ אזי לכל $i\in[n]$ מתקיים $B_{\lambda_{i+1}[\mathcal{L}]}\left(0\right)\cap\mathcal{L}\subseteq\text{span}\left(u_1\ldots u_i\right)$.

בסיס עוקבים מינימליים: יהיו $n,k\in\mathbb{N}_+$ ויהי $\mathcal{L}\subseteq\mathbb{R}^n$ סריג מדרגה k אזי $M\in\mathbb{R}^{n\times k}$ מדרגה k המקיימת $\mathcal{L}=\mathcal{L}\left[M\right]$ וכן $\left\|C_i\left(M\right)\right\|=\lambda_i\left[\mathcal{L}\right]$ לכל $i\in[n]$.

סריג סטנדרטי: יהי $n\in\mathbb{N}_+$ אזי סריג $\mathcal{L}$ מדרגה מלאה n עבורו קיים בסיס עוקבים מינימליים.

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.

בסיס מופחת: יהי $\mathcal{L}$ סריג מדרגה 2 אזי בסיס B של $\mathcal{L}$ המקיים $\left\|C_1\left(B\right)\right\|\leq\left\|C_2\left(B\right)\right\|$ וכן $\left\|C_2\left(B\right)\right\|\leq\left\|C_1\left(B\right)+C_2\left(B\right)\right\|$ וכן $\left\|C_2\left(B\right)\right\|\leq\left\|C_1\left(B\right)-C_2\left(B\right)\right\|$.

טענה: יהי $\mathcal{L}$ סריג מדרגה 2 ויהי B בסיס של $\mathcal{L}$ אזי (B בסיס מופחת)$\iff$(B בסיס עוקבים מינימליים).

אלגוריתם לגראנז': יהי $\mathcal{L}$ סריג מדרגה 2 ויהי B בסיס של $\mathcal{L}$ אזי

Algorithm Lagrange(B):

- **do**
  - $\left(C_1\left(B\right),C_2\left(B\right)\right)\leftarrow\left(C_2\left(B\right),C_1\left(B\right)\right)$
  - $C_2\left(B\right)\leftarrow C_2\left(B\right)-\left\lfloor\frac{\left\langle C_1(B),C_2(B)\right\rangle}{\left\|C_1(B)\right\|^2}\right\rceil\cdot C_1\left(B\right)$
- **while** $\left\|C_2\left(B\right)\right\|<\left\|C_1\left(B\right)\right\|$
- **return** B

טענה: יהי $\mathcal{L}$ סריג מדרגה 2 ויהי B בסיס של $\mathcal{L}$ באשר $\text{Lagrange}\left(B\right)$ עוצר אזי $\text{Lagrange}\left(B\right)$ בסיס מופחת של $\mathcal{L}$.

טענה: סיבוכיות הריצה של Lagrange הינה $\mathcal{O}\left(\log\left(n\right)\right)$.

הקבוע ההרמיטי: נגדיר $\gamma:\mathbb{N}\to\mathbb{N}$ כך $\gamma_n=\sup\left\{\frac{\lambda_1^2[\mathcal{L}]}{\det^{\frac{2}{n}}(\mathcal{L})}\;\middle|\;\mathcal{L}\subseteq\mathbb{R}^n \text{ סריג מדרגה מלאה}\right\}$.

טענה: $\gamma_2=\frac{2}{\sqrt{3}}$.

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

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 $\mathcal{E}_{\mathcal{L}}=\left\{v\in\mathbb{R}^n\;\middle|\;\sum_{i=1}^n\frac{\langle v,u_k^\perp\rangle^2}{\lambda_k[\mathcal{L}]^2}<1\right\}$.

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 $\prod_{i=1}^n\lambda_i[\mathcal{L}]\le 2^n\cdot\frac{\det(\mathcal{L})}{\mathrm{Vol}(B_1(0))}$.

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

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 $h(x)=\prod_{i=1}^n f_i(x_i)$ 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 n ויהי $u\in\mathcal{L}$ אזי $\mathcal{L}_{\perp u}$ סריג ממשי מדרגה $n-1$.

בסיס KZ [קורקין־זולוטרב 1877]: 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 $\left|\left\langle C_i\left(M\right),C_i\left(M^{\perp}\right)\right\rangle\right|\le\lambda_i\left[\mathcal{L}\right]$.
- לכל $i,j\in[n]$ באשר $j\ge i$ מתקיים $\left|\left\langle C_i\left(M\right),C_i\left(M^{\perp}\right)\right\rangle\right|\le\left\|C_l\left(M\right)\right\|$.
- לכל $i\in[n]$ מתקיים $\frac{1}{\sqrt{\frac{i-1}{4}+1}}\cdot\left\|C_i\left(M\right)\right\|\le\lambda_i\left[\mathcal{L}\right]\le\sqrt{\frac{i-1}{4}+1}\cdot\left\|C_i\left(M\right)\right\|$.

מטריצה מצומצמת LLL [לנסטרה־לנסטרה־לובאס 1982]: יהי $n\in\mathbb{N}_+$ ויהי $\delta\in\left(\frac{1}{4},1\right)$ אזי $M\in\mathbb{R}^{n\times n}$ המקיימת

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

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

טענה: יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times n}$ מצומצמת $\frac{3}{4}$-LLL ויהי $i\in[n]$ אזי $\left\|C_i\left(M\right)\right\|\le\sqrt{\frac{1+2^{i-1}}{2}}\cdot\left|\left\langle C_i\left(M\right),C_i\left(M^{\perp}\right)\right\rangle\right|$.

טענה: יהי $n\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times n}$ מצומצמת $\frac{3}{4}$-LLL ויהיו $i,j\in[n]$ באשר $j\le i$ אזי $\left\|C_j\left(M\right)\right\|\le2^{\frac{i-1}{2}}\left|\left\langle C_i\left(M\right),C_i\left(M^{\perp}\right)\right\rangle\right|$.

טענה: יהי $n\in\mathbb{N}_+$ ותהא $M\in\mathbb{R}^{n\times n}$ מצומצמת $\frac{3}{4}$-LLL אזי $\det\left(\mathcal{L}\left[M\right]\right)\le\prod_{i=1}^{n}\left\|C_i\left(M\right)\right\|\le2^{\frac{n(n-1)}{4}}\cdot\det\left(\mathcal{L}\left[M\right]\right)$.

טענה: קיים אלגוריתם פולינומי $\mathcal{A}$ עבורו לכל $n\in\mathbb{N}_+$ ולכל $M\in\mathbb{R}^{n\times n}$ מצומצמת $\frac{3}{4}$-LLL מתקיים $\mathcal{A}\left(M\right)\in\mathcal{L}\left[M\right]$ וכן $\left\|\mathcal{A}\left(M\right)\right\|\le2^{\frac{n-1}{4}}\cdot\det\left(\mathcal{L}\left[M\right]\right)^{\frac{1}{n}}$.

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

אלגוריתם LLL: יהי $n\in\mathbb{N}_+$ יהי $\delta\in\left(\frac{1}{4},1\right)$ ותהא $M\in\mathbb{R}^{n\times n}$ הפיכה אזי

```
Algorithm LLL-Algo(δ, M):
    while True do
        M^⊥ ← Orthonormalization(M)
        for i ← [2, ..., n] do
            for j ← [i − 1, ..., 1] do
                C_i(M) ← C_i(M) − ⌈ ⟨C_i(M), C_j(M^⊥)⟩ / ⟨C_j(M), C_j(M^⊥)⟩ ⌋ · C_j(M)
            end
        end
        f ← True;    i ← 1
        while (i ≤ n) ∧ (f = True) do
            if δ⟨C_i(M), C_i(M^⊥)⟩² > ⟨C_{i+1}(M), C_i(M^⊥)⟩² + ⟨C_{i+1}(M), C_{i+1}(M^⊥)⟩² then
                (C_i(M), C_{i+1}(M)) ← (C_{i+1}(M), C_i(M))
                f ← False
            end
            i ← i + 1
        end
        if f = True then return M
    end
```

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

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

טענה: יהי $n\in\mathbb{N}_+$ יהי $\delta\in\left(\frac{1}{4},1\right)$ תהא $M\in\mathbb{R}^{n\times n}$ הפיכה ויהיו S,S' מצבים בריצת LLL-Algo באשר S' תוצאת לולאת ה־while על S אזי $S'\left(M\right)\le\sqrt{\delta}\cdot S\left(M\right)$.

מסקנה: סיבוכיות הריצה של LLL-Algo הינה $\text{poly}\left(n\right)$.

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

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

אלגוריתם Babai **[באבאי 1986]**: יהי $\delta \in \left(\frac{1}{4}, 1\right)$ יהי $n \in \mathbb{N}_+$ תהא $M \in \mathbb{R}^{n\times n}$ הפיכה מצומצמת δ-LLL ויהי $t \in \mathbb{R}^n$ אזי

```
Algorithm Babai_δ(M, t):
    v ∈ ℝ^n;        v ← 0
    M^⊥ ← Orthonormalization(M)
    for i ∈ [n, ..., 1] do
        k ← ⌊⟨t, C_i(M^⊥)⟩⌉
        v ← v + k · C_i(M)
        t ← t − k · C_i(M)
    end
    return v
```

טענה: יהי $\delta \in \left(\frac{1}{4}, 1\right)$ אזי סיבוכיות הריצה של Babai_δ הינה $\text{poly}(n)$.

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 $M \in \mathbb{R}^{n\times n}$ הפיכה מצומצמת $\frac{3}{4}$-LLL ויהי $t \in \mathbb{R}^n$ אזי $\left\|t - \text{Babai}_{\frac{3}{4}}(M, t)\right\| \le 2^{\frac{n}{2}-1}\left|\left\langle C_n(M), C_n(M^\perp)\right\rangle\right|$.

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

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

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

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

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

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

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

בעיית חיפוש הוקטור המדוייק הקרוב ביותר בסריג: יהי $\mathbb{F}$ שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג דיסקרטי יהי $n \in \mathbb{N}_+$ ותהא $M \in \mathbb{F}^{n\times n}$ הפיכה אזי $\text{SVP-lattice-search-exact}(M, \mathbb{F}, \mathcal{F}) = v$ באשר $\|Mv\| = \lambda_i[\mathcal{L}[M]]$ וכן $v \in \mathcal{F}^n$.

בעיית הוקטור הקצר ביותר בסריג: $\text{SVP-lattice} = \{\langle M, \mathbb{F}, \mathcal{F}, \varepsilon\rangle \mid \exists v \in \mathcal{F}^n \backslash \{0\}. \|Mv\| \le \varepsilon\}$.

רדוקציית טיורינג: תהיינה A, B שפות אזי מ״ט דטרמיניסטית $\mathcal{A}^B$ המכריע את A.

סימון: תהיינה A, B שפות באשר קיימת רדוקציית טיורינג מ־A ל־B אזי $A \le B$.

רדוקציית קוק: תהיינה A, B שפות אזי מ״ט פולינומית דטרמיניסטית $\mathcal{A}^B$ המכריע את A.

סימון: תהיינה A, B שפות באשר קיימת רדוקציית קוק מ־A ל־B אזי $A \le_p B$.

אלגוריתם חיפוש הקצר ביותר בהינתן הקרוב ביותר [גולדרייך־מיצ'אנצ'ו־ספרא־זייפט 1999]: יהי $n \in \mathbb{N}_+$ תהא $M \in \mathbb{R}^{n\times n}$ הפיכה ויהי $\mathcal{A}$ אלגוריתם $\text{CVP-lattice-search-exact}_{\mathbb{R}|\mathbb{Z}}$ אזי

```
Algorithm SVP-via-CVP[A](M):
    v ← C_1(M)
    for i ∈ [1, ..., n] do
        u ← A(M + C_i(M) · e_i^T, C_i(M)) − C_i(M)
        if ‖u‖ < ‖v‖ then  v ← u
    end
    return v
```

טענה: יהי $\mathcal{A}$ אלגוריתם $\text{CVP-lattice-search-exact}_{\mathbb{R}|\mathbb{Z}}$ אזי $\text{SVP-via-CVP}[\mathcal{A}]$ הינו אלגוריתם $\text{SVP-lattice-search-exact}_{\mathbb{R}|\mathbb{Z}}$.

מסקנה: $\text{SVP-lattice-search-exact} \le_p \text{CVP-lattice-search-exact}$.

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: יהי $\mathbb{F}$ שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג דיסקרטי יהי $n \in \mathbb{N}_+$ תהא $M \in \mathbb{F}^{n \times n}$ הפיכה יהי $t \in \mathbb{F}^n$ תהא $T : \mathbb{N} \to \mathbb{N}$ ויהי $r \in \mathbb{R}_{>0}$ אזי $\text{GAP-CVP}_T(M, t, \mathbb{F}, \mathcal{F}, r) = \text{GAP}_{[r, r \cdot T]}\text{CVP}(M, t, \mathbb{F}, \mathcal{F})$.

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

הגדרה: יהי $\mathbb{F}$ שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג דיסקרטי 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: יהי $\mathbb{F}$ שדה יהי $\mathcal{F} \subseteq \mathbb{F}$ חוג דיסקרטי יהי $n \in \mathbb{N}_+$ תהא $M \in \mathbb{F}^{n \times n}$ הפיכה תהא $T : \mathbb{N} \to \mathbb{N}$ ויהי $r \in \mathbb{R}_{>0}$ אזי $\text{GAP-SVP}_T(M, \mathbb{F}, \mathcal{F}, r) = \text{GAP}_{[r, r \cdot T]}\text{SVP}(M, \mathbb{F}, \mathcal{F})$.

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

מסקנה: יהי $\gamma \in \mathbb{R}_{\geq 1}$ 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 $v_1 \ldots v_n \in \mathbb{R}^n$ בת"ל וכן $\|v_i\| \leq T(n) \cdot \lambda_n[\mathcal{L}[M]]$ לכל $i \in [n]$.

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

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

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

אלגוריתם חיפוש בינארי כללי: יהי $\varepsilon > 0$ תהא $f : \mathbb{R} \to \{0,1\}$ עולה ויהיו $a, b \in \mathbb{R}$ באשר $\inf\left(f^{-1}[\{1\}]\right) \in [a,b]$ אזי

```
Algorithm BinarySearch(f, a, b, ε):
    if |b − a| < ε then return (a+b)/2
    if f((a+b)/2) = 1 then
        return BinarySearch(f, a, (a+b)/2, ε)
    else
        return BinarySearch(f, (a+b)/2, b, ε)
```

טענה: יהי $\varepsilon > 0$ תהא $f : \mathbb{R} \to \{0,1\}$ עולה ויהיו $a, b \in \mathbb{R}$ באשר $\inf\left(f^{-1}[\{1\}]\right) \in [a,b]$ אזי $\text{BinarySearch}(f, a, b, \varepsilon) = d$ באשר $\left|d - \inf\left(f^{-1}[\{1\}]\right)\right| < \frac{\varepsilon}{2}$.

טענה: יהי $\varepsilon > 0$ תהא $f : \mathbb{R} \to \{0,1\}$ עולה חשיבה ויהיו $a, b \in \mathbb{R}$ באשר $\inf\left(f^{-1}[\{1\}]\right) \in [a,b]$ אזי $\text{Time}(\text{BinarySearch}) = \mathcal{O}\left(\text{Time}(f) \cdot \log\left(\frac{b-a}{\varepsilon}\right)\right)$.

הגדרה: יהי $R \in \mathbb{N}_+$ אזי $\text{RootList}(R) = \text{Sort}\left([0, \ldots, R] \,\|\, [\sqrt{n} \quad \textbf{for} \quad n \in [0, \ldots, R]]\right)$.

אלגוריתם הכרעה לחיפוש לבעיית הוקטור הקרוב ביותר: יהי $n \in \mathbb{N}_+$ תהא $M \in \mathbb{Z}^{n \times n}$ הפיכה יהי $t \in \mathbb{Z}^n$ ויהי $\mathcal{A}$ אלגוריתם $(\text{GAP-CVP}_1)_{\mathbb{R}|\mathbb{Z}}$ אזי

```
Algorithm CVP-Decidability-Search[A](M, t):
    d ← BinarySearch(A(M,t), RootList(Σ_{i=1}^n ‖C_i(M)‖))  // Search for A(M,t)(?) on the list given by RootList
    for i ∈ [1, ..., n] do
        for ? ∈ [1, ..., n + log(d)] do
            M' ← M + C_i(M) · e_i^T
            if A(M', t, d) = No then t ← t − C_i(M)
            M ← M'
        end
    end
    return Babai_{3/4}(LLL-Algo(3/4, M), t)
```

טענה: יהי $\mathcal{A}$ אלגוריתם $(\text{GAP-CVP}_1)_{\mathbb{R}|\mathbb{Z}}$ אזי $\text{CVP-Decidability-Search}[\mathcal{A}]$ הינו אלגוריתם $\text{CVP-lattice-search-exact}_{\mathbb{R}|\mathbb{Z}}$.

מסקנה: $\text{CVP-lattice-search-exact} \leq_p \text{GAP-CVP}_1$.

משפט: יהי $\gamma \le 1+\mathcal{O}\left(\frac{\log(n)}{n}\right)$ אזי קיים אלגוריתם פולינומי $\gamma^{\mathcal{O}(n)}$-קירוב לבעיה $\text{CVP-lattice-search-exact}^{\text{GAP-CVP}_\gamma}$.

אלגוריתם אנומרציה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k יהי $t\in M\mathbb{R}^k$ ויהי $R\in\mathbb{R}_{>0}$ אזי

```
Algorithm Enum(M, t, R):
    M^⊥ ← Orthonormalization(M)
    c ← ⟨t, C_k(M^⊥)⟩
    Z ∈ P(ℤ);      Z ← {z ∈ ℤ | |c − z·⟨C_k(M), C_k(M^⊥)⟩| ≤ R}
    M' ∈ ℝ^{n×(k−1)};      (M')_{i,j} ← (M)_{i,j}
    E ← P(ℝ^n);      E ← ∅
    for z ∈ Z do
        A ← Enum(M', π_{span(C_1(M),...C_{k−1}(M))}(t − z·C_k(M)), R)
        for v ∈ A do  E ← E ∪ {z·C_k(M) + v}
    end
    return E
```

טענה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k יהי $t\in M\mathbb{R}^k$ ויהי $R\in\mathbb{R}_{>0}$ אזי $B_R(t)\cap\mathcal{L}[M]\subseteq\text{Enum}(M,t,R)$.

טענה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k יהי $t\in M\mathbb{R}^k$ ויהי $R\in\mathbb{R}_{>0}$ אזי זמן הריצה של $\text{Enum}(M,t,R)$ הינו $\mathcal{O}\left(\frac{2^n\cdot R^n}{\det(\mathcal{L}[M])}\right)$.

טענה: יהיו $n,k\in\mathbb{N}_+$ תהא $M\in\mathbb{R}^{n\times k}$ מדרגה k יהי $t\in M\mathbb{R}^k$ ויהי $R\in\mathbb{R}_{>0}$ אזי $|\text{Enum}(M,t,R)|=\mathcal{O}\left(\frac{2^n\cdot R^n}{\det(\mathcal{L}[M])}\right)$.

מסקנה: $\text{CVP-lattice-search-exact}_{\mathbb{R}|\mathbb{Z}}\in\text{DTime}\left(2^{\mathcal{O}(n^2)}\right)$.

הגדרה: תהא $T:\mathbb{N}\to\mathbb{N}$ אזי נגדיר בעיית הבטחה $\text{gapBinCVP}_T=(\text{Yes},\text{No})$ באשר

- $\text{Yes}=\left\{\langle M,t,d\rangle \mid \exists z\in\{0,1\}^n.\ \|Mz-t\|\le d\right\}$.
- $\text{No}=\left\{\langle M,t,d\rangle \mid \forall z\in\mathbb{Z}^n.\forall k\in\mathbb{N}.\ \|Mz-kt\|\ge d\cdot T(n)\right\}$.

טענה: יהי $c\in\mathbb{N}_+$ אזי gapBinCVP_c הינה $\mathcal{NP}$-קשה.

סריג צפוף מקומית: יהי $\alpha\in\mathbb{R}_{>0}$ יהיו $\ell,k\in\mathbb{N}_+$ תהא $A\in\mathbb{Z}^{n\times k}$ מדרגה k יהי $r\in\sqrt{\mathbb{N}_+}$ יהי $x\in\mathbb{Z}^n$ ותהא $T\in\mathbb{Z}^{\ell\times n}$ אזי (A,r,x,T) באשר

- $\lambda_1\left[\mathcal{L}[A]\right]\ge r$.
- $\{0,1\}^\ell\subseteq T\left((x+\mathcal{L}[A])\cap B_{\alpha r}(0)\right)$.

משפט: יהיו $k,n\in\mathbb{N}_+$ ויהיו $\alpha,\gamma,\gamma'\in\mathbb{R}_{>0}$ באשר $\frac{1}{\alpha}>\gamma'\ge1$ וכן $\gamma\ge\gamma'\cdot\frac{1}{\sqrt{1-(\alpha\gamma')^2}}$ אזי קיים אלגוריתם פולינומי דטרמיניסטי $\mathcal{A}$ עבורו לכל $M\in\mathbb{R}^{n\times n}$ מדרגה k לכל $t\in\mathbb{R}^n$ לכל $d\in\mathbb{R}_{>0}$ ולכל (A,r,x,T) סריג (α,ℓ,k)-צפוף מקומית מתקיים

- $\mathcal{A}\left((M,t,d),(A,r,x,T)\right)=(M',d')$ באשר $M'\in\mathbb{R}^{n\times n}$ מדרגה k וכן $d'\in\mathbb{R}_{>0}$.
- $\left(\text{GAP-SVP}_{\gamma'}\left(\mathcal{A}\left((M,t,d),(A,r,x,T)\right)\right)\in\text{Yes}\right)\iff\left(\text{gapBinCVP}_\gamma\left((M,t,d)\right)\in\text{Yes}\right)$.

סריג שור־אדמלן למספרים ראשוניים: יהי $m\in\mathbb{N}_+$ יהיו $a_1\ldots a_m\in\mathbb{N}_{\text{odd}}$ זרים ויהי $\alpha\in\mathbb{R}_{>0}$ אזי נגדיר $M_{\{a_1\ldots a_m\}}\in\mathbb{R}^{(m+1)\times m}$ כך $\left(M_{\{a_1\ldots a_m\}}\right)_{i,j}=\begin{cases}\sqrt{\ln(a_i)} & i=j\\ \alpha\ln(a_j) & i=m+1\\ 0 & \text{else}\end{cases}$.

למה: תהא $\mathcal{S}\subseteq\mathbb{N}_{\text{odd}}$ קבוצה סופית של מספרים זרים ויהי $\alpha\in\mathbb{R}_{>0}$ אזי $\lambda_1\left[\mathcal{L}[M_\mathcal{S}]\right]>\sqrt{2\ln(\alpha)}$.

למה: יהי $m\in\mathbb{N}_+$ יהיו $a_1\ldots a_m\in\mathbb{N}_{\text{odd}}$ זרים יהיו $\alpha,\beta\in\mathbb{R}_{>0}$ ויהי $z\in\{0,1\}^m$ באשר $\prod_{i=1}^m a_i^{z_i}\in\left[\beta,\beta+\frac{\beta}{\alpha}\right]$ אזי $\left\|M_{\{a_1\ldots a_m\}}\cdot z-e_{m+1}\cdot\alpha\ln(\beta)\right\|\le\sqrt{\ln(\beta)+2}$.

מרחב המטריצות האקראית: יהיו $n,m\in\mathbb{N}_+$ ויהי $p\in[0,1]$ אזי $M(n,m,p)=\left(\mathbb{F}_2^{n\times m},\mathbb{P}\right)$ באשר $\mathbb{P}(A)=\prod_{i=1}^n\prod_{j=1}^m\left(\mathbb{1}\left[(A)_{i,j}=1\right]\cdot p+\mathbb{1}\left[(A)_{i,j}=0\right]\cdot(1-p)\right)$.

למה: יהיו $n,m,m'\in\mathbb{N}_+$ יהי $\varepsilon\in\left(0,\frac{1}{7}\right)$ תהא $Z\subseteq\mathbb{F}_2^m$ באשר לכל $z\in Z$ מתקיים $\Delta(z,0)=m'$ וכן $|Z|\ge m'!\cdot m^{\frac{4\sqrt{m'}\cdot n}{\varepsilon}}$ אזי $\mathbb{P}_{C\leftarrow M\left(n,m,\frac{1}{4nm'}\right)}\left(\forall x\in\mathbb{F}_2^n.\exists z\in Z^m.Cz=x\right)>1-7\varepsilon$.

משפט: יהי $m\in\mathbb{N}_+$ תהא $\mathcal{S}\subseteq\mathbb{N}_{\text{odd}}$ קבוצה של מספרים זרים באשר $|\mathcal{S}|=m$ ויהי $\alpha\in\mathbb{R}_{>0}$ אזי קיים $\beta\in\mathbb{R}_{>0}$ וקיים $C\in\{0,1\}^{(m+1)\times(m+1)}$ עבורם $\left(M_\mathcal{S},\sqrt{2\ln(\alpha)},e_{m+1}\cdot\alpha\ln(\beta),C\right)$ הינו סריג $(\alpha,m+1,m)$-צפוף מקומית.

הגדרה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{n\times m}$ אזי $L_q(A)=\{x\in\mathbb{Z}^n\mid\exists z\in\mathbb{Z}^m:(x\equiv Bz\mod q)\}$.

טענה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{n\times m}$ אזי $L_q(A)$ סריג מדרגה מלאה.

הגדרה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{m\times n}$ אזי $L_q^{\perp}(A)=\{z\in\mathbb{Z}^n\mid Az\equiv 0 \mod q\}$.

טענה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{m\times n}$ אזי $L_q^{\perp}(A)$ סריג מדרגה מלאה.

טענה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{m\times n}$ אזי $L_q\left(A^T\right)=q\cdot\left(L_q^{\perp}(A)\right)^{\vee}$.

טענה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{m\times n}$ אזי $\det\left(L_q^{\perp}(A)\right)\le q^n$.

מסקנה: יהי $q\in\mathbb{P}$ יהיו $n,m\in\mathbb{N}_+$ באשר $m\le n$ ותהא $A\in\mathbb{Z}_q^{m\times n}$ אזי $\left(\det\left(L_q^{\perp}(A)\right)=q^n\right)\Longleftrightarrow\left(A\right.$ מדרגה $\left.n\right)$.

משפט: יהי $q\in\mathbb{P}$ תהא $S\subseteq\mathbb{F}_q$ ויהי $k\in\mathbb{N}_{\le\left\lfloor\frac{1}{2}|S|\right\rfloor}$ אזי $\lambda_1\left[L_q^{\perp}\left(H_q(k,S)^T\right)\right]\ge\sqrt{2k}$.

רדוקציית קארפ אקראית: יהי Σ אלפבית ותהיינה $A,B\subseteq\Sigma^*$ אזי מ"ט פולינומית אקראית M עבורה לכל $x\in\Sigma^*$ מתקיים $\mathbb{P}_r\left(A(x)=B(M(x;r))\right)\ge\frac{2}{3}$.

סימון: יהי Σ אלפבית ותהיינה $A,B\subseteq\Sigma^*$ באשר קיימת רדוקציית קארפ אקראית מ־A ל־B אזי $A\le_m^{\mathcal{BPP}}B$.

משפט [מיצ'אנצ'ו 2001, מיצ'אנצ'ו־גולדווסר 2002]: יהי $\varepsilon\in\mathbb{R}_{>0}$ אזי $\text{GAP-SVP}_{\frac{\sqrt{2}}{1+2\varepsilon}}\le_m^{\mathcal{BPP}}\text{gapBinCVP}_{\frac{\sqrt{2}}{\varepsilon}}$.

טענה: יהי $n\in\mathbb{N}_+$ ויהי $\mathcal{L}\subseteq\mathbb{R}^n$ סריג מדרגה מלאה אזי קיים $v\in\mathcal{L}\backslash\{0\}$ המקיים $\|v\|_{\infty}\le\det(\mathcal{L})^{\frac{1}{n}}$.

למה: יהי $p\in\mathbb{P}$ אזי קיימים $r,s\in\mathbb{N}$ עבורם $r^2+s^2\equiv -1 \mod p$.

משפט הריבועים של לגראנז': יהי $n\in\mathbb{N}$ אזי קיימים $r,s,t,u\in\mathbb{N}$ עבורם $n=r^2+s^2+t^2+u^2$.

משפט דיריכלה המוכלל לקירוב דיופנטי: יהיו $d,N\in\mathbb{N}_+$ ויהי $v\in\mathbb{R}^d$ אזי קיים $q\in\left[N^d\right]$ וקיים $u\in\mathbb{Z}^d$ עבורם לכל $i\in[d]$ מתקיים $\left|v_i-\frac{1}{q}u_i\right|<\frac{1}{qN}$.