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 $\Delta\left(w,w'\right)\leq d-1$ אזי $w'\notin\mathcal{C}$.

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

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

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

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

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

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

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

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

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

טענה: יהיו $m,r,d,q\in\mathbb{N}_+$ עבורם קיים קוד $[m,r,d,q]$ 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 $\left|\mathcal{C}\right|\leq q^m\cdot\left(\sum_{i=0}^{\left\lfloor\frac{d-1}{2}\right\rfloor}\left(\binom{m}{i}\cdot\left(q-1\right)^i\right)\right)^{-1}$.

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

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

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

טענה: יהי $\mathcal{C}$ קוד לינארי $[m,r,d,q]$ 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 $M_{\mathcal{D}}=\begin{pmatrix}I_r\\ A\end{pmatrix}$.

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

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 $\left|R\left(M_{\mathcal{C}}\right)\cap V\right|\leq m-d$.

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

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

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

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

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 $k = \ell$ 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': יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ יהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ 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 $\alpha_1\ldots\alpha_m\in\mathbb{F}_q$ 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 $\alpha_1\ldots\alpha_m\in\mathbb{F}_q$ 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 $\alpha_1\ldots\alpha_m\in\mathbb{F}_q$ 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 $\{(h(\alpha_i))_{i=1}^m\mid h\in L\}=\left\{w'\in\mathrm{RS}_q[m,r]\mid\exists\varepsilon\in\mathbb{F}_q^m:(y=w'+\varepsilon)\wedge(\Delta(\varepsilon,0)\le m-2\sqrt{mr})\right\}$.

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

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

טענה: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r\in\mathbb{N}_+$ אזי קיימים $k,d\in\mathbb{N}_+$ 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 $m,r\in\mathbb{N}_{\ge2}$ אזי $\mathrm{RM}_2[m,r]=\{(u,u+v)\mid(u\in\mathrm{RM}_2[m-1,r])\wedge(v\in\mathrm{RM}_2[m-1,r-1])\}$.

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`$(\varepsilon,q,m,\alpha,z,w;R)$**:**

$t\leftarrow\lceil-18\cdot\log(\varepsilon)\rceil$

$a_1\ldots a_t\in\mathbb{F}_q$

for $i\in[1,\ldots,t]$ **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 $\mathrm{Majority}(a_1,\ldots,a_t)$

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 $f\in(\mathbb{F}_q)_{\le\alpha q}[x_1,\ldots,x_m]$ באשר $(f(\alpha))_{\alpha\in\mathbb{F}_q^m}=\arg(d(\mathrm{RM}_q[m,\alpha q],w))$ אזי $\mathbb{P}_{R\leftarrow\left(\mathbb{N}\to\mathbb{F}_q^m\backslash\{0\}\right)}(\mathrm{LocalRM}(\varepsilon,q,m,\alpha,z,w;R)=f(z))\ge1-\varepsilon$.

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

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

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

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

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

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

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

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

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

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\text{Dic}}$ הינו קוד $\left[2^n,\log_2(n),2^{n-1},2\right]$ 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 $\text{Val}((M,t,\mathbb{F}))=\min_{x\in\mathbb{F}^n}(\Delta_r(Mx,t))$.

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

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

טענה: יהי $\mathbb{F}$ שדה סופי באשר $|\mathbb{F}|\geq3$ אזי $\text{NoSatEq}_{\mathbb{F}}$ הינה $\mathcal{NP}$־קשה.

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

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

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

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

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

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

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

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

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

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

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

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

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

מטריצת משחק: יהי $\mathbb{F}$ שדה אזי $M\in\mathbb{F}^{n\times m}$ עבורה לכל $i\in[n]$ מתקיים $w(R_i(M))=2$ וכן קיים $j\in[m]$ עבורו $(M)_{i,j}=1$ וכן $R_i(M)\cdot\mathbb{1}_m=0$.

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

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

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

השערת המשחקים היחודיים [חות' 2002]: יהי $\varepsilon>0$ אזי $\text{UG}(\varepsilon)$ הינה Promise-$\mathcal{NP}$־קשה. השערה פתוחה

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

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

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

משפט [חות'־מינזר־ספרא 2018]: יהי $\varepsilon>0$ אזי $\text{PCP}_{2\to1}[\varepsilon,1-\varepsilon]$ 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 $\text{Promise-}\mathcal{NP}$־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)
```

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

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

הגדרה: יהי $n\in\mathbb{N}_{+}$ אזי נגדיר $\nu:\mathbb{R}^{n}\times\mathbb{R}^{n}\to\left\{ \pm1\right\}$ כך $\nu_{p}\left(\xi\right)=\begin{cases} 1 & \left\langle \xi,p\right\rangle \ge0\\ -1 & \text{else} \end{cases}$.

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

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

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

מסקנה: יהי $n\in\mathbb{N}_{+}$ יהי G גרף באשר $\left|V\left(G\right)\right|=n$ ותהא $X\in\mathbb{R}^{n\times n}$ באשר $X=\arg\text{MaxCut-VP}\left(G\right)$ אזי $\mathbb{E}_{p\in\mathbb{S}^{n-1}}\left[\left|E\left(S_{p}\left(X\right),\overline{S_{p}\left(X\right)}\right)\right|\right]\ge0.878567\cdot\text{MaxCut}\left(G\right)$.

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

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

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

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

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

$$\begin{aligned} \max\quad & 1\\ \text{s.t.}\quad & A\ge0\\ & A_{v,v}=1 & ,\forall v\in V\left(G\right)\\ & A_{v,u}=-\frac{1}{2} & ,\forall\left\{ v,u\right\} \in E\left(G\right) \end{aligned}$$

טענה: יהי $n\in\mathbb{N}_{+}$ יהי G גרף באשר $\left|V\left(G\right)\right|=n$ 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 פיזיבילי של $\text{3Colorable-SDP}(G)$ אז $\text{Chol}(X)^T$ פתרון פיזיבילי של $\text{3Colorable-VP}(G)$.

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 $\text{3Colorable-VecCol}(G, \varepsilon; R)$ צביעה חוקית של G.

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

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

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

אלגוריתם ויגרדזון 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 $|\text{Im}(\text{Wigderson}(G))| = \mathcal{O}\left(\sqrt{|V(G)|}\right)$.

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

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

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

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

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

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 $n \in \mathbb{N}_{\geq 2}$.

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 $\Theta(G) \geq \alpha(G)$.

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

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 $\vartheta(G) = \min\left\{\min\left\{\max\left\{\frac{1}{\langle R_u, c\rangle^2} \,\middle|\, u \in V(G)\right\} \,\middle|\, \begin{smallmatrix} c \in \mathbb{R}^d \\ \|c\|=1 \end{smallmatrix}\right\} \,\middle|\, \begin{smallmatrix} d \in \mathbb{N}_+ \\ \text{ייצוג אורתונורמלי } d \text{ מימדי של } G \ R \end{smallmatrix}\right\}$.

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 $\vartheta(G) = \mathrm{MinMaxEigenvalue}\left(B_\varnothing, (B_e)_{e \in E(G_{\mathrm{dc}})}\right)$.

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

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 $\mathrm{MatMul}(\mathbb{F}, A, B) = AB$.

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`$(\mathbb{F}, A, B)$:
- $C \in \mathbb{F}^{n \times m}$; $\quad C \leftarrow 0$
- **for** $i \in [1, \ldots, n]$ **do**
  - **for** $j \in [1, \ldots, m]$ **do**
    - **for** $\ell \in [1, \ldots, k]$ **do**
      - $(C)_{i,j} \leftarrow (C)_{i,j} + (A)_{i,\ell} \cdot (B)_{\ell,j}$
    - **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 $\Theta(kmn)$.

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

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

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 $\mathcal{B}_{n_0}(A)\in\left(\mathbb{F}^{n_0\times n_0}\right)^{\frac{n}{n_0}\times\frac{n}{n_0}}$ כך $\left(\mathcal{B}_{n_0}(A)\right)_{i,j}=(A)_{((i-1)\cdot n_0,(j-1)\cdot n_0)+[n_0]^2}$.

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)
    M1 ∈ 𝔽^{2^{n-1}};    M1 ← Strassen(𝔽, a + d, α + δ)
    M2 ∈ 𝔽^{2^{n-1}};    M2 ← Strassen(𝔽, c + d, α)
    M3 ∈ 𝔽^{2^{n-1}};    M3 ← Strassen(𝔽, a, β − δ)
    M4 ∈ 𝔽^{2^{n-1}};    M4 ← Strassen(𝔽, d, γ − α)
    M5 ∈ 𝔽^{2^{n-1}};    M5 ← Strassen(𝔽, a + b, δ)
    M6 ∈ 𝔽^{2^{n-1}};    M6 ← Strassen(𝔽, c − a, α + β)
    M7 ∈ 𝔽^{2^{n-1}};    M7 ← Strassen(𝔽, b − d, γ + δ)
    return (M1+M4−M5+M7   M2+M4; M3+M5   M1−M2+M3+M6)
```

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 $\mathcal{O}\left(m^{\log_2(7)}\right)$.

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 $\text{BiLinMatMul}_{U,V,W}(A,B)=W^T\left(\left(U\overrightarrow{\mathcal{B}_{n_0}(A)}\right)\circ\left(V\overrightarrow{\mathcal{B}_{n_0}(B)}\right)\right)$.

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 $\mathcal{O}(n^\omega)$.

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 $A\in\mathbb{F}^{n\times n}$ אזי $\text{MatDet}(\mathbb{F},A)=\det(A)$.

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

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

משפט: תהא $T:\mathbb{N}\to\mathbb{N}$ אזי (בעיית MatMul חשיבה בזמן T)$\Longleftrightarrow$(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 $\text{LinEqSol}(A,b)=v$ באשר $Av=b$.

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

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

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

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

חוג דיסקרטי: חוג $(R,+,*)$ באשר $(R,+)$ 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 דיסקטי 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 $(\mathcal{L},k)$ באשר

- לכל $x,y\in\mathcal{L}$ מתקיים $x-y\in\mathcal{L}$.
- $\max\left\{|V|\mid(V\subseteq\mathcal{L})\wedge(\text{קבוצה בת"ל } V)\right\}=k$.
- קיים $r>0$ המקיים $B_r\left(0\right)\cap\mathcal{L}=\{0\}$.

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

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

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

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

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 $\left(\mathcal{L}\left[A\right]=\mathcal{L}\left[B\right]\right)\iff\left(\exists U\in\text{GL}_n\left(\mathbb{Z}\right):A=BU\right)$.

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 $\left\{\Phi^+_{i,j,a}\;\middle|\;\left(\begin{smallmatrix}i,j\in[n]\\ i\neq j\end{smallmatrix}\right)\wedge(a\in\mathbb{Z})\right\}\cup\left\{\Phi^{\leftrightarrow}_{i,j}\;\middle|\;\begin{smallmatrix}i,j\in[n]\\ i\neq j\end{smallmatrix}\right\}\cup\left\{\Phi^-_i\mid i\in[n]\right\}$.

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

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

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

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

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

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 $\left(\mathcal{P}\left[B\right]\cap\mathcal{L}\left[A\right]=\{0\}\right)\iff\left(\mathcal{L}\left[A\right]=\mathcal{L}\left[B\right]\right)$.

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

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 $\det\left(\mathcal{L}\left[M\right]\right)=\mathrm{Vol}\left(\mathcal{P}\left[M\right]\right)$.

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

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

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

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 $i\in\left[k\right]$ אזי $\lambda_i\left[\mathcal{L}\right]=\inf\left\{r\geq0\mid\dim\mathrm{span}\left(B_r\left(0\right)\cap\mathcal{L}\right)\geq i\right\}$.

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 $i\in\left[n\right]$ מתקיים $u_i^{\perp}\in\mathrm{span}\left(u_1\ldots u_i\right)\backslash\mathrm{span}\left(u_1\ldots u_{i-1}\right)$.

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 $i\in\left[n\right]$.

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 $i\in\left[n\right]$.

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

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 $i\in\left[n\right]$.

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 $n\in\left[4\right]$ 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)$\Longleftrightarrow$(B בסיס עוקבים מינימליים).

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

```
Algorithm Lagrange(B):
    do
        (C_1(B), C_2(B)) ← (C_2(B), C_1(B))
        C_2(B) ← C_2(B) − ⌈⟨C_1(B), C_2(B)⟩ / ‖C_1(B)‖²⌋ · C_1(B)
    while ‖C_2(B)‖ < ‖C_1(B)‖
    return B
```

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

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

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

משפט בליכפלדט: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n ותהא $S\subseteq\mathbb{R}^n$ מדידה באשר $\mathrm{Vol}\left(S\right)>\det\left(\mathcal{L}\right)$ 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 $\mathrm{Vol}\left(S\right)>2^n\cdot\det\left(\mathcal{L}\right)$ אזי $\mathcal{L}\cap S\neq\left\{0\right\}$.

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 $\left\|u_i\right\|=\lambda_i\left[\mathcal{L}\right]$ לכל $i\in\left[n\right]$ 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 $\left\|u_i\right\|=\lambda_i\left[\mathcal{L}\right]$ לכל $i\in\left[n\right]$ אזי $\mathcal{E}_{\mathcal{L}}\cap\mathcal{L}=\left\{0\right\}$.

משפט מינקובסקי השני: יהי $n\in\mathbb{N}_+$ יהי $\mathcal{L}$ סריג מדרגה מלאה n אזי $\prod_{i=1}^{n}\lambda_i\left[\mathcal{L}\right]\le 2^n\cdot\frac{\det(\mathcal{L})}{\mathrm{Vol}(B_1(0))}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\pi_{\perp u}\left(v\right)=v-\frac{\langle u,v\rangle}{\|u\|^2}\cdot u$.

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

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 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

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

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 $\mathcal{L}\left[M\right]=\mathcal{L}$ אזי M בסיס KZ של $\mathcal{L}$ אם הבאים מתקיימים

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

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

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

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**
  - $M^{\perp} \leftarrow \text{Orthonormalization}(M)$
  - **for** $i \leftarrow [2, \ldots, n]$ **do**
    - **for** $j \leftarrow [i-1, \ldots, 1]$ **do**
      - $C_i(M) \leftarrow C_i(M) - \left\lfloor \frac{\langle C_i(M), C_j(M^{\perp}) \rangle}{\langle C_j(M), C_j(M^{\perp}) \rangle} \right\rceil \cdot C_j(M)$
    - **end**
  - **end**
  - $f \leftarrow \text{True}; \qquad i \leftarrow 1$
  - **while** $(i \leq n) \wedge (f = \text{True})$ **do**
    - **if** $\delta \left\langle C_i(M), C_i(M^{\perp}) \right\rangle^2 > \left\langle C_{i+1}(M), C_i(M^{\perp}) \right\rangle^2 + \left\langle C_{i+1}(M), C_{i+1}(M^{\perp}) \right\rangle^2$ **then**
      - $(C_i(M), C_{i+1}(M)) \leftarrow (C_{i+1}(M), C_i(M))$
      - $f \leftarrow \text{False}$
    - **end**
    - $i \leftarrow i + 1$
  - **end**
  - **if** $f = \text{True}$ **then return** M
- **end**

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

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

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 $S'(M) \leq \sqrt{\delta} \cdot S(M)$.

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

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 $\frac{1}{2}\lambda_n[\mathcal{L}] \leq \mu(\mathcal{L})$.

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`$_\delta(M, t)$:

- $v \in \mathbb{R}^n; \qquad v \leftarrow 0$
- $M^{\perp} \leftarrow \text{Orthonormalization}(M)$
- **for** $i \in [n, \ldots, 1]$ **do**
  - $k \leftarrow \left\lfloor \langle t, C_i(M^{\perp}) \rangle \right\rceil$
  - $v \leftarrow v + k \cdot C_i(M)$
  - $t \leftarrow t - k \cdot C_i(M)$
- **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 $\mu(\mathcal{L}[M]) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{n} \langle C_i(M), C_i(M^{\perp}) \rangle^2}$.

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

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 $\left\| t - \text{Babai}_{\frac{3}{4}}(M, t) \right\| \leq 2^{\frac{n}{2}-1} \left| \left\langle C_n(M), C_n(M^{\perp}) \right\rangle \right|$.

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 $\|Mv - t\| \leq \varepsilon$ 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.

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 $v \in \mathcal{F}^n \setminus \{0\}$.

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

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: $\text{SVP-lattice-search-exact}^{\text{CVP-lattice-search-exact}} \in \mathcal{P}$.

סימון: תהא $C \subseteq \mathcal{P}(\{0,1\}^*)$ 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 $\gamma \in \mathbb{R}_{\ge 1}$ 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: $\text{GAP-CVP}_{\sqrt{n}}, \text{GAP-SVP}_{\sqrt{n}} \in \mathcal{NP} \cap \text{co}\mathcal{NP}$.

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

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

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 $\|v_i\| \le T(n)\cdot\lambda_n[\mathcal{L}[M]]$ 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 $\gamma, c \in \mathbb{R}_{\geq 1}$ 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** $|b-a| < \varepsilon$ **then** **return** $\frac{a+b}{2}$
- **if** $f\left(\frac{a+b}{2}\right) = 1$ **then**
  - **return** `BinarySearch`$(f, a, \frac{a+b}{2}, \varepsilon)$
- **else**
  - **return** `BinarySearch`$(f, \frac{a+b}{2}, b, \varepsilon)$

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 $\mathrm{BinarySearch}(f, a, b, \varepsilon) = d$ 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 $\mathrm{Time}(\mathrm{BinarySearch}) = \mathcal{O}\left(\mathrm{Time}(f) \cdot \log\left(\frac{b-a}{\varepsilon}\right)\right)$.

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

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`$[\mathcal{A}](M, t)$**:**
- $d \leftarrow \mathrm{BinarySearch}\left(\mathcal{A}(M,t), \mathrm{RootList}\left(\sum_{i=1}^n \|C_i(M)\|\right)\right)$ `// Search for` $\mathcal{A}(M,t)(?)$ `on the list given by` $\mathrm{RootList}$
- **for** $i \in [1, \ldots, n]$ **do**
  - **for** $? \in [1, \ldots, n + \log(d)]$ **do**
    - $M' \leftarrow M + C_i(M) \cdot e_i^T$
    - **if** $\mathcal{A}(M', t, d) = \mathrm{No}$ **then** $t \leftarrow t - C_i(M)$
    - $M \leftarrow M'$
  - **end**
- **end**
- **return** $\mathrm{Babai}_{\frac{3}{4}}\left(\mathrm{LLL\text{-}Algo}\left(\frac{3}{4}, M\right), t\right)$

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: $\text{CVP-lattice-search-exact}^{\text{GAP-CVP}_1} \in \mathcal{P}$.

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