

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

**מרחק האמינג:** תהא  $X$  קבוצה אזי נגדיר  $\Delta : X^n \times X^n \rightarrow \mathbb{N}$  כך  $\Delta(x, y) = |\{i \in [n] \mid x_i \neq y_i\}|$

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

**טענה:** תהא  $X$  קבוצה אזי  $\Delta$  משרה את נורמת  $\ell_0$ .

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

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

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

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

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

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

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

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

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

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

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

**קוד שאריות:** יהיו  $q, m \in \mathbb{N}_+$  אזי  $\mathcal{C}_{\text{parity}} = \left\{ w \in [q]^{m+1} \mid w_{m+1} = (\sum_{i=1}^m w_i \bmod q) \right\}$

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

**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  $d' \geq d$  עבורו קיים קוד

$[m \lceil \log(q) \rceil, r \log(q), d', 2]$  לתיקון שגיאות.

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

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

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

**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  $|\mathcal{C}| \leq \frac{d}{d + \frac{m}{q} - m}$

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

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

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

**מטריצה יוצרת:** יהי  $\mathcal{C}$  קוד לינארי  $[m, r, d, q]$  לתיקון שגיאות ויהי  $b_1 \dots b_r \in \mathcal{C}$  בסיס אזי נגדיר  $M_{\mathcal{C}} \in \mathbb{F}_q^{m \times r}$  כך  $C_i(M_{\mathcal{C}}) = b_i$

לכל  $i \in [r]$

**טענה:** יהי  $\mathcal{C}$  קוד לינארי  $[m, r, d, q]$  לתיקון שגיאות אזי  $\mathcal{C} = \{M_{\mathcal{C}} \cdot v \mid v \in \mathbb{F}_q^r\}$

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

**מסקנה:** יהיו  $q, m, k \in \mathbb{N}_+$  אזי  $M_{\mathcal{C}_{k\text{-rep}}} = \begin{pmatrix} I_m \\ \vdots \\ I_m \end{pmatrix}$

**טענה:** יהיו  $q, m \in \mathbb{N}_+$  אזי  $\mathcal{C}_{\text{parity}}$  קוד לינארי לתיקון שגיאות.

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

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

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

**טענה:** יהי  $\mathcal{C}$  קוד לינארי  $[m, r, d, q]$  לתיקון שגיאות אזי קיים קוד לינארי  $[m, r, d, q]$  לתיקון שגיאות  $\mathcal{D}$  עבורו קיימת  $A \in \mathbb{F}_q^{(m-r) \times r}$

המקיימת  $M_{\mathcal{D}} = \begin{pmatrix} I_r \\ A \end{pmatrix}$

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

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

• לכל  $V \subseteq \mathcal{C}$  באשר  $\dim(V) = r-1$  מתקיים  $|R(M_{\mathcal{C}}) \cap V| \leq m-d$

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

**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  $m > r$  והי  $x \in \mathbb{F}_q^r \setminus \{0\}$  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  $m > r$  והי  $M \in \mathbb{F}_q^{m \times r}$  אזי  $\mathcal{C}_M = \{M \cdot v \mid v \in \mathbb{F}_q^r\}$ .

**משפט:** יהי  $q \in \mathbb{N}_+$  באשר  $\mathbb{F}_q$  שדה יהיו  $m, r \in \mathbb{N}_+$  באשר  $m > r$  והי  $\delta \in (0, 1)$  אזי  $\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}} \left( d[\mathcal{C}_M] \leq (1 - \delta) \left( m - \frac{m}{q} \right) \right) \leq |\mathcal{C}_M| \cdot \exp \left( -\frac{\delta^2}{2} \left( m - \frac{m}{q} \right) \right)$ .

**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  $H_C = M_{\mathcal{C}^\vee}$ .

**טענה:** יהי  $\mathcal{C}$  קוד לינארי לתיקון שגיאות אזי  $\mathcal{C} = \ker(H_C^T)$ .

**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  $m > r$  והי  $M \in \mathbb{F}_q^{m \times r}$  אזי  $\mathcal{C}_M$  קוד לינארי מקסימלי לתיקון שגיאות  $\iff A \in \mathcal{P}_r(R(M))$  מתקיים כי  $A$  "ב"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  $d \leq m$  והי  $q \in \mathbb{P}$  אזי קיים קוד לינארי  $[m, k, d, q]$  לתיקון שגיאות  $\mathcal{C}$  המקיים  $|\mathcal{C}| \geq q^m \cdot \left( \sum_{i=0}^{d-1} \binom{m-1}{i} \cdot (q-1)^i \right)^{-1}$ .

**למה:** יהי  $d \in \mathbb{N}_{\geq 2}$  יהיו  $k, m \in \mathbb{N}_+$  באשר  $k \leq m$  והי  $q \in \mathbb{P}$  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  $A$  "ב"ל.

**משפט גילברט-וורשאמוב:** יהי  $d \in \mathbb{N}_{\geq 2}$  יהיו  $k, m \in \mathbb{N}_+$  באשר  $k \leq m$  והי  $q \in \mathbb{P}$  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  $|\mathcal{C}| \geq q^m \cdot \left( 1 + \sum_{i=0}^{d-2} \binom{m-1}{i} \cdot (q-1)^i \right)^{-1}$ .

**סכימת חלוקת סוד מושלמת:** תהיינה  $X, Y$  קבוצות יהי  $n \in \mathbb{N}_+$  והי  $k \in [n]$  אזי  $f : X \rightarrow Y^n$  עבודה

• קיימת  $g : Y^k \rightarrow X$  עבורה לכל  $s \in X$  ולכל  $p_1, \dots, p_k \in [n]$  מתקיים  $g(f(s)_{p_1}, \dots, f(s)_{p_k}) = s$ .

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

**טענה:** יהיו  $\ell, k \in \mathbb{N}_+$  באשר  $\ell \leq k$  יהי  $\mathbb{F}$  שדה סופי באשר  $|\mathbb{F}| \geq k$  יהיו  $x_1 \dots x_\ell \in \mathbb{F}$  שונים ונגדיר  $\varphi : \mathbb{F}_{\leq k-1}[x] \rightarrow \mathbb{F}^\ell$  כך  $\varphi(p) = (p(x_i))_{i=1}^\ell$ .

• אם  $\ell = k$  אז  $\varphi$  איזומורפיזם וכן  $\varphi, \varphi^{-1}$  חשיבות בזמן פולינומי.

• אם  $\ell < k$  אז לכל  $y \in \mathbb{F}^\ell$  מתקיים כי  $\varphi^{-1}(y)$  מרחב אפני ממימד  $k - \ell$ .

**סכימת שמיר:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $n \in \mathbb{N}_+$  באשר  $n < q$  והי  $k \in [n]$  אזי נגדיר  $f : \mathbb{F}_q \times (\mathbb{F}_q \setminus \{0\})^{k-1} \rightarrow (\mathbb{F}_q^2)^n$  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  $s_1 \dots s_n \in \mathbb{F}_q \setminus \{0\}$  שונים.

**מסקנה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $n \in \mathbb{N}_+$  באשר  $n < q$  והי  $k \in [n]$  אזי סכימת שמיר הינה סכימת חלוקת סוד מושלמת.

**קוד ריד-סולומון:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in [q]$  והי  $r \in [m]$  והי  $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$  שונים אזי

$$RS_q[m, r] = \left\{ (f(\alpha_i))_{i=1}^m \mid f \in (\mathbb{F}_q)_{\leq r-1}[x] \right\}.$$

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

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

**מטריצת ונדרמונד:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in [q]$  והי  $r \in [m]$  והי  $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$  שונים אזי נגדיר

$$(H_q(r, \{\alpha_1 \dots \alpha_m\}))_{i,j} = \alpha_i^{j-1} \text{ כך } H_q(r, \{\alpha_1 \dots \alpha_m\}) \in \mathbb{F}_q^{m \times r}.$$

**טענה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in [q]$  והי  $r \in [m]$  והי  $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$  אזי  $M_{RS_q[m, r]} = H_q(r, \{\alpha_1 \dots \alpha_m\})$ .

**טענה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה והי  $i \in \{0, \dots, q-2\}$  אזי  $\sum_{x \in \mathbb{F}_q} x^i = 0$ .

**טענה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה והי  $r \in [q]$  אזי  $RS_q[q, r]^\vee = RS_q[q, q - r]$ .

**אלגוריתם ברלקמפ-וולץ:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in [q]$  יהי  $r \in [m]$  יהיו  $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$  שונים תהא  $w \in \text{RS}_q[m, r]$  יהי  $e \in \mathbb{F}_q^m$  באשר  $\Delta(e, 0) \leq \frac{m-r}{2}$  ונגדיר  $y = w + e$  אזי

**Algorithm BerlekampWelch( $q, m, r, \alpha, y$ ):**

```

 $g \in (\mathbb{F}_q)[x]; \quad \deg(g) = r + \lceil \frac{m-r}{2} \rceil - 1$ 
 $h \in (\mathbb{F}_q)[x]; \quad \deg(h) = \lfloor \frac{m-r}{2} \rfloor$ 
 $(g, h) \leftarrow \text{LinearEqSolver}((g(\alpha_i) = h(\alpha_i) \cdot y_i)_{i=1}^m) \quad // \text{ We do not accept } g = h = 0$ 
return PolynomialDivision( $g, h$ )
```

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

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

**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  $|B_r(w) \cap \mathcal{C}| \leq \ell$

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

**טענה:** יהי  $\mathcal{C}$  קוד  $[m, k, d, q]$  לתיקון שגיאות אזי  $\mathcal{C}$  הינו קוד  $(m, k, \frac{d}{2}, 1, q)$  לתיקון שגיאות רשימתי.

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

**Algorithm Sudan( $q, m, r, \alpha, y$ ):**

```

 $Q \in (\mathbb{F}_q)[x, y]; \quad \deg_x(Q) = \sqrt{mr}; \quad \deg_y(Q) = \sqrt{\frac{m}{r}}$ 
 $Q \leftarrow \text{LinearEqSolver}((Q(y_i, \alpha_i) = 0)_{i=1}^m) \quad // \text{ We do not accept } Q = 0$ 
 $S \in \text{List}((\mathbb{F}_q)[x]); \quad S \leftarrow \text{PolynomialSolutions}(Q) \quad // \text{ We view } Q \text{ as a polynomial in } (\mathbb{F}_q[x])[y]$ 
return  $[h \text{ for } h \in S \text{ if } \Delta((h(\alpha_i))_{i=1}^m, y) < m - 2\sqrt{mr}]$ 
```

**טענה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in [q]$  יהי  $r \in [m]$  יהיו  $\alpha_1 \dots \alpha_m \in \mathbb{F}_q$  שונים תהא  $w \in \text{RS}_q[m, r]$  יהי  $e \in \mathbb{F}_q^m$  באשר  $\Delta(e, 0) \leq m - 2\sqrt{mr}$  ונגדיר  $y = w + e$  אזי  $\text{Sudan}(q, m, r, \alpha, y) = L$  באשר

$\{(h(\alpha_i))_{i=1}^m \mid h \in L\} = \{w' \in \text{RS}_q[m, r] \mid \exists \varepsilon \in \mathbb{F}_q^m : (y = w' + \varepsilon) \wedge (\Delta(\varepsilon, 0) \leq m - 2\sqrt{mr})\}$

**קוד ריד-מיולר:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה ויהיו  $m, r \in \mathbb{N}_+$  אזי  $\text{RM}_q[m, r] = \left\{ (f(\alpha))_{\alpha \in \mathbb{F}_q^m} \mid f \in (\mathbb{F}_q)_{\leq r}[x_1, \dots, x_m] \right\}$

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

**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  $\text{RM}_q[m, r]$  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  $r[\text{RM}_q[m, r]] = \binom{m+r}{r}$

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

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

**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

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

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

**טענה:** יהיו  $m, r \in \mathbb{N}_{\geq 2}$  אזי  $\text{RM}_2[m, r] = \{(u, u+v) \mid (u \in \text{RM}_2[m-1, r]) \wedge (v \in \text{RM}_2[m-1, r-1])\}$

**אלגוריתם תיקון שגיאות מקומי בקוד ריד-מיולר:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in \mathbb{N}_+$  ויהי  $\alpha, \varepsilon \in (0, 1)$  יהי  $z \in \mathbb{F}_q^m$  ותהא  $w \in \mathbb{F}_q^m$  באשר  $d(\text{RM}_q[m, \alpha q], w) \leq q^m \cdot \frac{1-\alpha}{6}$  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
     $a_i \leftarrow (\text{BerlekampWelch}(q, q, \alpha q + 1, x, w_{z+\mathbb{F}_q \cdot R(v)})) (0)$ 
end
return Majority( $a_1, \dots, a_t$ )
```

**טענה:** יהי  $q \in \mathbb{N}$  באשר  $\mathbb{F}_q$  שדה יהי  $m \in \mathbb{N}_+$  ויהי  $\alpha, \varepsilon \in (0, 1)$  יהי  $z \in \mathbb{F}_q^m$  ותהא  $w \in \mathbb{F}_q^m$  באשר

$(f(\alpha))_{\alpha \in \mathbb{F}_q^m} = \arg(d(\text{RM}_q[m, \alpha q], w))$  באשר  $f \in (\mathbb{F}_q)_{\leq \alpha q}[x_1, \dots, x_m]$  ותהא  $d(\text{RM}_q[m, \alpha q], w) \leq q^m \cdot \frac{1-\alpha}{6}$  אזי

$$\mathbb{P}_{R \leftarrow (\mathbb{N} \rightarrow \mathbb{F}_2^m \setminus \{0\})} (\text{LocalRM}(\varepsilon, q, m, \alpha, z, w; R) = f(z)) \geq 1 - \varepsilon$$

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

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

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

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

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

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

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

**קוד דיקטטורות:** יהי  $n \in \mathbb{N}_+$  אזי  $\mathcal{C}_{\text{Dic}} = \left\{ (\chi_{\{i\}}(x))_{x \in \mathbb{F}_2^n} \mid i \in [n] \right\}$   $\mathcal{C}_{\text{Dic}}$  הינו קוד  $[2^n, \log_2(n), 2^{n-1}, 2]$  לתיקון שגיאות.

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

**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  $\text{NoSatEq}_{\mathbb{F}} = \{(M, t) \mid (M \in \mathbb{R}^{n \times n}) \wedge (t \in \mathbb{R}^n) \wedge (\exists x \in \mathbb{R}^n : \forall i \in [n] : (Mx)_i \neq t_i)\}$  **טענה:**  $\text{NoSatEq}_{\mathbb{F}_2} \in \mathcal{P}$ .

**טענה:** יהי  $\mathbb{F}$  שדה סופי באשר  $|\mathbb{F}| \geq 3$  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:**  $\text{CVP-code} = \{((M, t, \mathbb{F}), \varepsilon) \mid \text{Val}((M, t, \mathbb{F})) \leq \varepsilon\}$ .

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

**בעיית החתך המקסימלי:** יהי  $G$  גרף סופי אזי  $\text{MaxCut}(G) = \max \{|E(S, \bar{S})| \mid S \subseteq V(G)\}$ .

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

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

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

**מסקנה:** אם קיים אלגוריתם פולינומי  $A$  אשר מהווה  $\frac{1-\varepsilon}{\varepsilon}$ -קירוב לבעיית  $\text{CVP-code-search}$  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  $\text{Val}_{1 \leftrightarrow 1}((M, t, \mathbb{F})) = \text{Val}((M, t, \mathbb{F}))$ .

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

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

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

$$\text{Val}_{2 \rightarrow 1}((M, \{u, v\}, \mathbb{F})) = \min_{t \in \text{Interpol}(u, v)} \text{Val}((M, t, \mathbb{F}))$$

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

**משפט [חות' מינור-ספרא 2018]:** יהי  $\varepsilon > 0$  אזי  $\text{PCP}_{2 \rightarrow 1}[\varepsilon, 1 - \varepsilon]$  הינה Promise- $\mathcal{NP}$ -קשה. לא הוכח בקורס

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

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

**רדוקציית טיורינג:** תהיינה  $A, B$  שפות אזי מ"ט דטרמיניסטית  $A^B$  המכריע את  $A$ .

**סימון:** תהיינה  $A, B$  שפות באשר קיימת רדוקציית טיורינג מ- $A$  ל- $B$  אזי  $A \leq_T B$

**רדוקציית קוק:** תהיינה  $A, B$  שפות אזי מ"ט פולינומית דטרמיניסטית  $A^B$  המכריע את  $A$ .

**סימון:** תהיינה  $A, B$  שפות באשר קיימת רדוקציית קוק מ- $A$  ל- $B$  אזי  $A \leq_T^p B$

**סימון:** תהיינה  $A, B$  שפות באשר  $A \leq_T^p B$  וכן  $B \leq_T^p A$  אזי  $A =_T^p B$

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

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

**טענה:** יהי  $G$  גרף סופי ויהי  $\text{MaxCut-IP}(G) = x$  כאשר  $x \in \mathbb{F}_2^{|V(G)|}$

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

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

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

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

**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  $\langle A, B \rangle = \text{trace}(A^T B)$

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

$R \in (\mathbb{R}^{n \times n})^\ell$  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  $\{\langle P_i, X \rangle \leq p_i \mid i \in [\text{len}(p)]\} \cup \{\langle Q_i, X \rangle \geq q_i \mid i \in [\text{len}(q)]\} \cup \{\langle R_i, X \rangle = r_i \mid i \in [\text{len}(r)]\}$

**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  $\varepsilon$ -קירוב של SDP.

**בעיית חיפוש פתרון פיזיבילי 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  $i \in [\text{len}(p)]$  וכן  $\langle Q_i, X \rangle \geq q_i$  לכל  $i \in [\text{len}(q)]$  וכן

$\langle R_i, X \rangle = r_i$  לכל  $i \in [\text{len}(r)]$

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

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

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

**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  $\text{Chol}(A) = L \cdot L^T$  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):**

```

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

```

**טענה:** יהי  $n \in \mathbb{N}_+$  ותהא  $A \in \mathbb{R}^{n \times n}$  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  $\nu: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \{\pm 1\}$  כך  $\nu_p(\xi) = \begin{cases} 1 & \langle \xi, p \rangle \geq 0 \\ -1 & \text{else} \end{cases}$ .

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

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

**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  $\mathbb{E}_{p \in \mathbb{S}^{n-1}} \left[ \left| E(S_p(X), \overline{S_p(X)}) \right| \right] \geq 0.878567 \cdot \text{MaxCut}(G)$ .

**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  $\mathbb{E}_{p \in \mathbb{S}^{n-1}} \left[ \left| E(S_p(X), \overline{S_p(X)}) \right| \right] \geq (1 - \frac{2}{\pi} \sqrt{\varepsilon} - \mathcal{O}(\varepsilon^{1.5})) |E(G)|$ .

**משפט חות'ק-קנדלר-אדל-דונל-מוסל:** יהי  $\varepsilon > 0$  ויהי  $\rho \in (0, 1)$  אזי  $\text{UG}(\varepsilon) = \frac{p}{T} \text{GAP}_{[\rho, 1 - \arccos(\rho) + \varepsilon]} \text{MaxCut}$ .

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

**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 פיזיבילי  $\iff (p = \sum_{i=1}^m q_i^2 \text{ עבור } q_1 \dots q_m \in \mathbb{R}[x])$ .

**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  $p = \sum_{i=1}^m q_i^2$   $\iff (p \geq 0)$ .

**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  $n, k \in \mathbb{N}_+$  ותהינה  $A_0 \dots A_k \in \mathbb{R}^{n \times n}$  אזי  $\text{MinMaxEigenvalue}(A_0 \dots A_k) = \min \left\{ \max \left( \text{spec} \left( A_0 + \sum_{i=1}^k A_i x_i \right) \right) \mid x \in \mathbb{R}^k \right\}$ .

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

**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  $E(G \boxtimes H) = \left\{ ((u, u'), (v, v')) \in V(G \boxtimes H)^2 \mid (u \in N^-(v) \cup \{v\}) \wedge (u' \in N^-(v') \cup \{v'\}) \right\}$ .

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

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

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

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



**הגדרה:** יהי  $G$  מכוון אזי נגדיר גרף לא מכוון  $G_{dc}$  כך  $V(G_{dc}) = V(G)$  וכן

$$E(G_{dc}) = \{e \in P_2(V(G)) \mid ((e_1, e_2) \in E(G)) \vee ((e_2, e_1) \in E(G))\}$$

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

**מספר לובאס של גרף:** יהי  $G$  גרף אזי  $R$  ייצוג אורתונורמלי  $d$  מימדי של  $G$   $\left\{ \min_{\|c\|=1} \max_{u \in V(G)} \left\{ \frac{1}{\langle R_u, c \rangle^2} \mid u \in V(G) \right\} \mid c \in \mathbb{R}^d \right\}$   $d \in \mathbb{N}_+$

**משפט:** יהי  $G$  גרף נגדיר  $B_\emptyset \in \mathbb{R}^{V(G) \times V(G)}$  כך  $B_\emptyset = \begin{cases} \frac{1}{0} & \{u, v\} \notin E(G_{dc}) \\ \frac{1}{1} & \{u, v\} \in E(G_{dc}) \end{cases}$  ונגדיר  $B: E(G_{dc}) \rightarrow \mathbb{R}^{V(G) \times V(G)}$   $(B_\emptyset)_{u,v} = \begin{cases} \frac{1}{0} & \{u, v\} \notin E(G_{dc}) \\ \frac{1}{1} & \{u, v\} \in E(G_{dc}) \end{cases}$   $\text{MinMaxEigenvalue}(B_\emptyset, (B_e)_{e \in E(G_{dc})}) = \vartheta(G)$  אזי  $(B_{\{u,v\}})_{t,s} = \begin{cases} \frac{1}{0} & \{t,s\} = \{u,v\} \\ \frac{1}{1} & \text{else} \end{cases}$   $\vartheta(G) \geq \Theta(G)$  **משפט:** יהי  $G$  גרף מכוון אזי

**הגדרה משוואה לינארית בעלת שני משתנים:**  $A \{ (A, v) \in \mathbb{F}_2^{m \times n} \times \mathbb{F}_2^m \mid \mathbb{F}_2 \}$  מטריצת משחק מעל  $\mathbb{F}_2$

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

**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  $2\text{Lin}_{\mathbb{F}_2}\text{-IP}(A, v)$  כך

$$\max \sum_{\substack{\ell \in [m] \\ i, j \in [n]}} \mathbb{1} \left[ \begin{matrix} i < j \\ (A)_{\ell, i} = 1 \\ (A)_{\ell, j} = 1 \end{matrix} \right] \cdot (1 - x_i + x_j + v_\ell)$$

$$\text{s.t. } x_i \in \{-1, 1\}, \forall i \in [n]$$

**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  $2\text{Lin}_{\mathbb{F}_2}\text{-SDP}(A, v)$  כך

$$\max \sum_{\substack{\ell \in [m] \\ i, j \in [n]}} \mathbb{1} \left[ \begin{matrix} i < j \\ (A)_{\ell, i} = 1 \\ (A)_{\ell, j} = 1 \end{matrix} \right] \cdot \left( \mathbb{1}[v_\ell = 0] \cdot \left( \frac{1 + \langle V_i, V_j \rangle}{2} \right) + \mathbb{1}[v_\ell = 1] \cdot \left( \frac{1 - \langle V_i, V_j \rangle}{2} \right) \right)$$

$$\text{s.t. } V_i \in \mathbb{S}^{n-1}, \forall i \in [n]$$

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

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

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

**טענה:** יהי  $\varepsilon \in [0, 1]$  יהיו  $m, n \in \mathbb{N}$  תהא  $A \in \mathbb{F}_2^{m \times n}$  ותהא  $v \in \mathbb{F}_2^m$  באשר  $\text{Val}((A, v, \mathbb{F}_2)) \leq \varepsilon$  ונגדיר  $V = 2\text{Lin}_{\mathbb{F}_2}\text{-SDP}(A, v)$

$$\text{אזי } \sum_{\substack{\ell \in [m] \\ i, j \in [n]}} \mathbb{1} \left[ \begin{matrix} i < j \\ (A)_{\ell, i} = 1 \\ (A)_{\ell, j} = 1 \end{matrix} \right] \cdot \mathbb{P}_{p \in \mathbb{S}^{n-1}} \left( \frac{\nu_p(V_i) - \nu_p(V_j)}{2} = v_\ell \right) \geq m(1 - \mathcal{O}(\sqrt{\varepsilon}))$$

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

$$\max A + B + C + D$$

$$\text{s.t. } A = \sum_{x_i \wedge x_j \in \mathcal{C}} 1 - \left( \frac{1 - y_0 y_i}{2} \right) \left( \frac{1 - y_0 y_j}{2} \right); \quad B = \sum_{x_i \wedge \neg x_j \in \mathcal{C}} 1 - \left( \frac{1 - y_0 y_i}{2} \right) \left( \frac{1 + y_0 y_j}{2} \right)$$

$$C = \sum_{\neg x_i \wedge x_j \in \mathcal{C}} 1 - \left( \frac{1 + y_0 y_i}{2} \right) \left( \frac{1 - y_0 y_j}{2} \right); \quad D = \sum_{\neg x_i \wedge \neg x_j \in \mathcal{C}} 1 - \left( \frac{1 + y_0 y_i}{2} \right) \left( \frac{1 + y_0 y_j}{2} \right)$$

$$y_i \in \{-1, 1\}, \forall i \in \{0, \dots, n\}$$

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

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

**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  $\beta$ -קירוב של  $\text{MAXE2SAT}$ .

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

**מסקנה:**  $2SAT \in \mathcal{P}$ .

**בעיית 3-צביעה כתכנות וקטורי:** יהי  $G$  גרף אזי נגדיר 3Colorable-VP ( $G$ ) כך

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

**טענה:** יהי  $G$  גרף 3-צביע אזי 3Colorable-VP ( $G$ ) פיזבילית.

**בעיית 3-צביעה כתכנות חצי מוגדר:** יהי  $G$  גרף אזי נגדיר 3Colorable-SDP ( $G$ ) כך

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

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

• אם  $X$  פתרון פיזבילי של 3Colorable-VP ( $G$ ) אז  $X^T X$  פתרון פיזבילי של 3Colorable-SDP ( $G$ ).

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

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

**Algorithm 3Colorable-VecCol( $G, \varepsilon; R$ ):**

```

 $t \leftarrow 1 + \lceil \log_3(\Delta(G)) \rceil$  //  $\Delta(G)$  is the max degree of  $G$ 
 $X \in \text{Approx-Feasibility-Search}(\varepsilon, 3\text{Colorable-VP}(G))$  // poly time  $\varepsilon$ -approx for the feasibility problem
 $c \in V(G) \rightarrow \{\pm 1\}^*$ 
for  $v \in V(G)$  do
     $c(v) \leftarrow (\nu_{R(i)}(X_v))_{i=1}^t$ 
end
 $S \in \mathcal{P}(V(G)); \quad S \leftarrow \emptyset$ 
for  $v \in V(G)$  do
    for  $u \in N(v) \setminus S$  do
        if  $c(v) = c(u)$  then
             $S \leftarrow S \cup \{v\}$ 
        end
    end
end
 $c_{|V(G[S])} \leftarrow 3\text{Colorable-VecCol}(G[S], \varepsilon; R_{|_{\mathbb{N}_{>t}}})$ 
return  $c$ 

```

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

**טענה:** יהי  $G$  גרף 3-צביע יהי  $X$  פתרון פיזבילי של 3Colorable-VP ( $G$ ) ויהי  $\{u, v\} \in E(G)$  אזי

$$\mathbb{P}_{p \leftarrow \mathbb{S}^{|V(G)|-1}}(\nu_p(X_u) = \nu_p(X_v)) = \frac{1}{3}$$

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

**מסקנה:** יהי  $G$  גרף 3-צביע אזי קיים  $\varepsilon \in \mathbb{R}_{\geq 1}$  המקיים



$$\mathbb{E}_{R \leftarrow (\mathbb{N}_+ \rightarrow \mathbb{S}^{|V(G)|-1})} [|\text{Im}(\text{3Colorable-VecCol}(G, \varepsilon; R))|] = \mathcal{O}(|V(G)|^{\log_3(2)} \cdot \log(|V(G)|))$$

אלגוריתם ויגדרזון לצביעת גרף 3-צבעי: יהי  $G$  גרף 3-צבעי אזי

**Algorithm Wigderson( $G$ ):**

```

 $n \leftarrow |V(G)|$ 
if  $\Delta(G) \leq \sqrt{n}$  then
    | return GreedyColoring( $G, \{0, \dots, \sqrt{n}\}$ ) // Coloring with  $\sqrt{n} + 1$  colors
 $v \leftarrow \{t \in V(G) \mid \deg(t) \geq \sqrt{n} + 1\}$ 
 $c \in (N(v) \cup \{v\}) \rightarrow \{\text{Black}_v, \text{Red}_v, \text{Blue}_v\}; \quad c(v) \leftarrow \text{Black}_v$ 
 $c|_{N(v)} \leftarrow \text{GreedyColoring}(G[N(v)], \{\text{Red}_v, \text{Blue}_v\})$ 
 $c' \leftarrow \text{Wigderson}(G[V(G) \setminus (N(v) \cup \{v\})])$ 
return  $c \cup c'$ 

```

**טענה:** יהי  $G$  גרף 3-צבעי אזי  $|\text{Im}(\text{Wigderson}(G))| = \mathcal{O}(\sqrt{|V(G)|})$

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

**Algorithm WigdersonVectorHybrid( $G, \tau, \varepsilon; R$ ):**

```

if  $\Delta(G) < \tau$  then return 3Colorable-VecCol( $G, \varepsilon; R$ )
 $v \leftarrow \{t \in V(G) \mid \deg(t) \geq \tau\}$ 
 $c \in (N(v) \cup \{v\}) \rightarrow \{\text{Black}_v, \text{Red}_v, \text{Blue}_v\}; \quad c(v) \leftarrow \text{Black}_v$ 
 $c|_{N(v)} \leftarrow \text{GreedyColoring}(G[N(v)], \{\text{Red}_v, \text{Blue}_v\})$ 
 $c' \leftarrow \text{WigdersonVectorHybrid}(G[V(G) \setminus (N(v) \cup \{v\})], \tau, \varepsilon; R)$ 
return  $c \cup c'$ 

```

**טענה:** יהי  $G$  גרף 3-צבעי ויהי  $\tau \in \mathbb{R}_{\geq 1}$  אזי קיים  $\varepsilon \in \mathbb{R}_{\geq 1}$  המקיים

$$\mathbb{E}_{R \leftarrow (\mathbb{N}_+ \rightarrow \mathbb{S}^{|V(G)|-1})} [|\text{Im}(\text{WigdersonVectorHybrid}(G, \tau, \varepsilon; R))|] = \mathcal{O}\left(\frac{|V(G)|}{\tau} + \tau^{\log_3(2)} \cdot \log(|V(G)|)\right)$$

**מסקנה:** יהי  $n \in \mathbb{N}$  יהי  $G$  גרף 3-צבעי באשר  $|V(G)| = n$  ונגדיר  $\alpha = \log_3(2)$  כך  $\alpha \in \mathbb{R}$  אזי קיים  $\varepsilon \in \mathbb{R}_{\geq 1}$  המקיים

$$\mathbb{E}_{R \leftarrow (\mathbb{N}_+ \rightarrow \mathbb{S}^{|V(G)|-1})} \left[ \left| \text{Im} \left( \text{WigdersonVectorHybrid} \left( G, \left( \frac{3n}{\alpha \log(n)} \right)^{\frac{1}{\alpha+1}}, \varepsilon; R \right) \right) \right| \right] = \mathcal{O} \left( n^{\frac{\alpha}{\alpha+1}} + \log(n)^{\frac{1}{\alpha+1}} \right)$$

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

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

**אלגוריתם כפל מטריצות נאיבי:** יהי  $\mathbb{F}$  שדה יהיו  $n, k, m \in \mathbb{N}_+$  ותהא  $A \in \mathbb{F}^{n \times k}$  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  $i \in [1, \dots, n]$  do
    | for  $j \in [1, \dots, m]$  do
        | | for  $\ell \in [1, \dots, k]$  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  $k, m, n \in \mathbb{N}_+$  ותהא  $A \in \mathbb{F}^{k \times m}$  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 בינארי.

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

**Algorithm KaratsubaMult( $a, b$ ):**

```

if  $n = 1$  then return  $a_1 \cdot b_1$ 
 $\alpha \leftarrow (a_1 \dots a_{\frac{n}{2}}); \quad \beta \leftarrow (a_{\frac{n}{2}+1} \dots a_n)$ 
 $\gamma \leftarrow (b_1 \dots b_{\frac{n}{2}}); \quad \delta \leftarrow (b_{\frac{n}{2}+1} \dots b_n)$ 
 $A \leftarrow \text{KaratsubaMult}(\alpha, \gamma)$ 
 $B \leftarrow \text{KaratsubaMult}(\beta, \delta)$ 
 $C \leftarrow \text{KaratsubaMult}(\alpha + \beta, \gamma + \delta)$ 
return  $B \cdot 2^n + (C - B - A) \cdot 2^{\frac{n}{2}} + A$ 

```

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

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

**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  $\mathcal{B}_{n_0}(A) \in (\mathbb{F}^{n_0 \times n_0})^{\frac{n}{n_0} \times \frac{n}{n_0}}$  כך

$$(\mathcal{B}_{n_0}(A))_{i,j} = (A)_{((i-1) \cdot n_0, (j-1) \cdot n_0) + [n_0]^2}$$

**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( $\mathbb{F}, A, B$ ):**

```

if  $n = 0$  then return  $A \cdot B$  //  $A, B$  are scalars
 $a, b, c, d \in \mathbb{F}^{2^{n-1}}; \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftarrow \mathcal{B}_{2^{n-1}}(A)$ 
 $\alpha, \beta, \gamma, \delta \in \mathbb{F}^{2^{n-1}}; \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \leftarrow \mathcal{B}_{2^{n-1}}(B)$ 
 $M_1 \in \mathbb{F}^{2^{n-1}}; \quad M_1 \leftarrow \text{Strassen}(\mathbb{F}, a + d, \alpha + \delta)$ 
 $M_2 \in \mathbb{F}^{2^{n-1}}; \quad M_2 \leftarrow \text{Strassen}(\mathbb{F}, c + d, \alpha)$ 
 $M_3 \in \mathbb{F}^{2^{n-1}}; \quad M_3 \leftarrow \text{Strassen}(\mathbb{F}, a, \beta - \delta)$ 
 $M_4 \in \mathbb{F}^{2^{n-1}}; \quad M_4 \leftarrow \text{Strassen}(\mathbb{F}, d, \gamma - \alpha)$ 
 $M_5 \in \mathbb{F}^{2^{n-1}}; \quad M_5 \leftarrow \text{Strassen}(\mathbb{F}, a + b, \delta)$ 
 $M_6 \in \mathbb{F}^{2^{n-1}}; \quad M_6 \leftarrow \text{Strassen}(\mathbb{F}, c - a, \alpha + \beta)$ 
 $M_7 \in \mathbb{F}^{2^{n-1}}; \quad M_7 \leftarrow \text{Strassen}(\mathbb{F}, b - d, \gamma + \delta)$ 
return  $\begin{pmatrix} M_1 + M_4 - M_5 + M_7 & M_2 + M_4 \\ M_3 + M_5 & M_1 - M_2 + M_3 + M_6 \end{pmatrix}$ 

```

**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  $\mathcal{O}(m^{\log_2(7)})$

**וקטוריציה 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  $\vec{A}_i = (A)_{(i-1)\%n+1, \lfloor \frac{i-1}{n} \rfloor + 1}$

**כפל אדמר:** יהי  $\mathbb{F}$  שדה ויהיו  $n, m \in \mathbb{N}_+$  אזי נגדיר  $\circ : (\mathbb{F}^{n \times m})^2 \rightarrow \mathbb{F}^{n \times m}$  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  $\omega \in \mathbb{N}$  ותהיינה  $U, V, W \in \mathbb{F}^{n_0^\omega \times n_0^2}$

אזי נגדיר  $\text{BiLinMatMul}_{U,V,W} : (\mathbb{F}^{n \times n})^2 \rightarrow \mathbb{F}^{n \times n}$  כך  $\text{BiLinMatMul}_{U,V,W}(A, B) = W^T \left( \left( U \overline{\mathcal{B}_{n_0}(A)} \right) \circ \left( V \overline{\mathcal{B}_{n_0}(B)} \right) \right)$

**מכפלה פנימית משולשת:** יהי  $\mathbb{F}$  שדה ויהי  $n \in \mathbb{N}_+$  אזי נגדיר  $\langle \cdot, \cdot, \cdot \rangle : (\mathbb{F}^n)^3 \rightarrow \mathbb{F}$  כך  $\langle u, v, w \rangle = \sum_{i=1}^n u_i v_i w_i$

**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  $\omega \in \mathbb{N}$  ותהיינה  $U, V, W \in \mathbb{F}^{n_0^\omega \times n_0^2}$  אזי  $\text{BiLinMatMul}_{U,V,W}$

הינו אלגוריתם כפל מטריצות  $\iff$  (לכל  $i, i', j, j', k, k' \in [n_0]$  מתקיים  $\delta_{i,i'} \cdot \delta_{j,j'} \cdot \delta_{k,k'} = \langle U_{i,j'}, V_{j,k'}, W_{k,i'} \rangle$ )

**טענה:** יהי  $\mathbb{F}$  שדה יהיו  $n, n_0 \in \mathbb{N}_+$  באשר  $n_0 | n$  יהי  $\omega \in \mathbb{R}$  באשר  $\omega \in \mathbb{N}$  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  $T : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{MatMul} = \overset{p}{T} \text{MatInv}$

**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  $T : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{MatMul} = \overset{p}{T} \text{MatDet}$

**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  $T : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{MatMul} =_T^p \text{Mat-LU}$

**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  $\text{LinEqSol}(A, b) = v$  כאשר  $Av = b$

**משפט:** תהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  אזי  $\text{MatMul} =_T^p \text{LinEqSol}$

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

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

• רציפות כפל:  $(a, b) \mapsto ab$  הינה רציפה מעל  $(G^2, \mathcal{T}_{\text{prod}})$

• רציפות הופכי:  $a \mapsto a^{-1}$  הינה רציפה מעל  $(G, \mathcal{T})$

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

**חוג דיסקרטי:** חוג  $(R, +, *)$  כאשר  $(R, +)$  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  $\dim(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]) = k$

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

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

**סריג אבסטרקטי:** יהיו  $k, n \in \mathbb{N}_+$  ותהא  $\mathcal{L} \subseteq \mathbb{R}^n$  אזי  $(\mathcal{L}, k)$  כאשר

• לכל  $x, y \in \mathcal{L}$  מתקיים  $x - y \in \mathcal{L}$

•  $\max\{|V| \mid (V \subseteq \mathcal{L}) \wedge (V \text{ קבוצה בת"ל})\} = k$

• קיים  $r > 0$  המקיים  $B_r(0) \cap \mathcal{L} = \{0\}$

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

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

**למה:** יהי  $\mathcal{L}$  סריג אבסטרקטי אזי קיים  $v \in \mathcal{L} \setminus \{0\}$  עבורו לכל  $u \in \mathcal{L} \setminus \{0\}$  מתקיים  $\|v\| \leq \|u\|$

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

**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

$\mathcal{L} = \mathcal{L}[M]$

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

**חיבור עמודות:** יהי  $n \in \mathbb{N}_+$  יהיו  $i, j \in [n]$  שונים ויהי  $a \in \mathbb{Z}$  אזי נגדיר  $\Phi_{i,j,a}^+ : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}^{n \times n}$  כך

$$\Phi_{i,j,a}^+(M) = M + a \cdot (C_j(M) \cdot e_i^T)$$

**החלפת עמודות:** יהי  $n \in \mathbb{N}_+$  ויהיו  $i, j \in [n]$  שונים אזי נגדיר  $\Phi_{i,j}^{\leftrightarrow} : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}^{n \times n}$  כך

$$\Phi_{i,j}^{\leftrightarrow}(M) = M + C_j(M) \cdot (e_i - e_j)^T + C_i(M) \cdot (e_j - e_i)^T$$

**שליטת עמודה:** יהי  $n \in \mathbb{N}_+$  ויהי  $i \in [n]$  אזי נגדיר  $\Phi_i^- : \mathbb{R}^{n \times n} \rightarrow \mathbb{R}^{n \times n}$  כך  $\Phi_i^-(M) = M - 2 \cdot (C_i(M) \cdot e_i^T)$

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

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

**משפט:** יהי  $n \in \mathbb{N}_+$  ותהיינה  $A, B \in \mathbb{R}^{n \times n}$  הפיכות אזי  $(\mathcal{L}[A] = \mathcal{L}[B]) \iff$  קיימים  $m \in \mathbb{N}_+$  וקיימות טרנספורמציות אלמנטריות

$$(A = (\varphi \circ \dots \circ \varphi_m)(B))$$

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

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

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

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

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

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

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

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

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

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

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

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

**בעיית בסיס לחיתוך סריגים:** יהיו  $n, k, m \in \mathbb{N}_+$  תהא  $A \in \mathbb{R}^{n \times k}$  מדרגה  $k$  ותהא  $B \in \mathbb{R}^{n \times m}$  מדרגה  $m$  אזי

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

**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  $\mathcal{P}[M] = \mathcal{L}_{\mathbb{R}[0,1]}[M]$

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

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

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

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

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

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

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

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

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

**מסקנה:**  $\text{LatDet} \in \mathcal{P}$

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

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

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

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

•  $\{u_1^\perp, \dots, u_n^\perp\}$  בסיס אורתונורמלי.

• לכל  $i \in [n]$  מתקיים  $u_i^\perp \in \text{span}(u_1 \dots u_i) \setminus \text{span}(u_1 \dots u_{i-1})$

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

**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  $C_i(M^\perp) = C_i(M)^\perp$  לכל

$i \in [n]$

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

**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  $u_1 \dots u_n \in \mathcal{L}$  בת"ל המקיימים  $\|u_i\| = \lambda_i[\mathcal{L}]$  לכל  $i \in [n]$

**מסקנה:** יהי  $n \in \mathbb{N}_+$  יהי  $\mathcal{L}$  סריג מדרגה מלאה  $n$  ויהיו  $u_1 \dots u_n \in \mathcal{L}$  בת"ל המקיימים  $\|u_i\| = \lambda_i[\mathcal{L}]$  לכל  $i \in [n]$  אזי לכל  $i \in [n]$

מתקיים  $B_{\lambda_{i+1}[\mathcal{L}]}(0) \cap \mathcal{L} \subseteq \text{span}(u_1 \dots u_i)$

**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  $\mathcal{L} = \mathcal{L}[M]$  וכן

$\|C_i(M)\| = \lambda_i[\mathcal{L}]$  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  $n \in \mathbb{N}_{\geq 5}$  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  $\|C_1(B)\| \leq \|C_2(B)\|$  וכן  $\|C_1(B) + C_2(B)\| \leq \|C_2(B)\|$  וכן

$\|C_2(B)\| \leq \|C_1(B) - C_2(B)\|$

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

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

**Algorithm Lagrange(B):**

```

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

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

**טענה:** סיבוכיות הריצה של  $\text{Lagrange}$  הינה  $\mathcal{O}(\log(n))$

**הקבוע ההרמטי:** נגדיר  $\gamma : \mathbb{N} \rightarrow \mathbb{N}$  כך  $\gamma_n = \sup \left\{ \frac{\lambda_1^2[\mathcal{L}]}{\det \frac{n}{2}(\mathcal{L})} \mid \mathcal{L} \subseteq \mathbb{R}^n \text{ סריג מדרגה מלאה} \right\}$

**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  $1 \leq \lambda_1[\mathcal{L}] \cdot \lambda_n[\mathcal{L}^\vee] \leq n$

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

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

**למה:** יהי  $n \in \mathbb{N}_+$  יהי  $\mathcal{L}$  סריג מדרגה מלאה  $n$  ויהיו  $u_1 \dots u_n \in \mathcal{L}$  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  $\prod_{i=1}^n \lambda_i[\mathcal{L}] \leq 2^n \cdot \frac{\det(\mathcal{L})}{\text{Vol}(B_1(0))}$

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

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

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

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

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

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

**טענה:** יהי  $n \in \mathbb{N}_+$  ותהינה  $f_1 \dots f_n \in L^1(\mathbb{R})$  ונגדיר  $h : \mathbb{R}^n \rightarrow \mathbb{R}$  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  $\mathcal{N}_n : \mathbb{R}^n \rightarrow \mathbb{R}$  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  $\|f\|_{\alpha, \beta} = \sup_{x \in \mathbb{R}^n} |x^\alpha \cdot \mathcal{D}^\beta(f)(x)|$

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

**טענה נוסחאת הסכימה של פואסון:** יהי  $n \in \mathbb{N}_+$  ותהא  $f \in \mathcal{S}(\mathbb{R}^n, \mathbb{R})$  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

$$\mathbb{P}_{v \sim \mathcal{N}_n[\lambda_n[\mathcal{L}], r]}(v \notin B_{\lambda_n[\mathcal{L}]}(0) \mid v \in \mathcal{L}^\vee) \leq \varepsilon$$

**הטלה של וקטור על וקטור:** יהי  $n \in \mathbb{N}_+$  יהי  $\mathcal{L}$  סריג מדרגה מלאה  $n$  ויהי  $u \in \mathcal{L}$  אזי נגדיר  $\pi_{\perp u} : \mathbb{R}^n \rightarrow \mathbb{R}^n$  כך

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

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

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

**בסיס KZ [קורקיין-זולוטוב 1877]:** יהי  $n \in \mathbb{N}_+$  ויהי  $\mathcal{L}$  סריג מדרגה מלאה  $n$  אזי  $M \in \mathbb{R}^{n \times n}$  המקיימת

$$\mathcal{L} = \mathcal{L}[M] \bullet$$

$$\|\mathcal{C}_1(M)\| = \lambda_1[\mathcal{L}] \bullet$$

$$\mathcal{L}_{\perp \mathcal{C}_1(M)} \text{ הינו בסיס קורקיין-זולוטוב עבור } (\mathcal{C}_2(M)), \dots, \pi_{\perp \mathcal{C}_1(M)}(\mathcal{C}_n(M)) \bullet$$

$$\text{לכל } i \in [n] \text{ מתקיים } |\langle \mathcal{C}_i(M), \mathcal{C}_1(M^\perp) \rangle| \leq \frac{1}{2} |\langle \mathcal{C}_1(M), \mathcal{C}_1(M^\perp) \rangle| \bullet$$

**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

$$\bullet \text{ לכל } i \in [n] \text{ מתקיים } \langle \mathcal{C}_i(M), \mathcal{C}_i(M^\perp) \rangle \cdot \mathcal{C}_i(M^\perp) = \arg \min \{ \|v\| \mid v \in \pi_{\text{span}^+(\mathcal{C}_1(M), \dots, \mathcal{C}_{i-1}(M))}(\mathcal{L}) \}$$

$$\bullet \text{ לכל } i, j \in [n] \text{ באשר } j < i \text{ מתקיים } |\langle \mathcal{C}_i(M), \mathcal{C}_j(M^\perp) \rangle| \leq \frac{1}{2} |\langle \mathcal{C}_j(M), \mathcal{C}_j(M^\perp) \rangle|$$

**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  $|\langle C_i(M), C_i(M^\perp) \rangle| \leq \lambda_i[\mathcal{L}]$ .
- לכל  $i, j \in [n]$  באשר  $j \geq i$  מתקיים  $|\langle C_i(M), C_j(M^\perp) \rangle| \leq \|C_i(M)\| \cdot \sqrt{\frac{i-1}{4} + 1} \cdot \|C_j(M)\|$ .
- לכל  $i \in [n]$  מתקיים  $\frac{1}{\sqrt{\frac{i-1}{4} + 1}} \cdot \|C_i(M)\| \leq \lambda_i[\mathcal{L}] \leq \sqrt{\frac{i-1}{4} + 1} \cdot \|C_i(M)\|$ .

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

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

**טענה:** יהי  $n \in \mathbb{N}_+$  ויהי  $\delta \in (\frac{1}{4}, 1)$  ותהא  $M \in \mathbb{R}^{n \times n}$  מצומצמת  $\delta$ -LLL אזי לכל  $i \in [n-1]$  מתקיים

$$\langle C_{i+1}(M), C_{i+1}(M^\perp) \rangle \geq \sqrt{\delta - \frac{1}{4}} \cdot \langle C_i(M), C_i(M^\perp) \rangle$$

**טענה:** יהי  $n \in \mathbb{N}_+$  ותהא  $M \in \mathbb{R}^{n \times n}$  מצומצמת  $\frac{3}{4}$ -LLL אזי  $i \in [n]$  ויהי  $\frac{3}{4}$ -LLL אזי

**טענה:** יהי  $n \in \mathbb{N}_+$  ותהא  $M \in \mathbb{R}^{n \times n}$  מצומצמת  $\frac{3}{4}$ -LLL ויהי  $i, j \in [n]$  באשר  $j \leq i$  אזי

$$\|C_j(M)\| \leq 2^{\frac{i-1}{2}} |\langle C_i(M), C_i(M^\perp) \rangle|$$

**טענה:** יהי  $n \in \mathbb{N}_+$  ותהא  $M \in \mathbb{R}^{n \times n}$  מצומצמת  $\frac{3}{4}$ -LLL אזי  $\det(\mathcal{L}[M]) \leq \prod_{i=1}^n \|C_i(M)\| \leq 2^{\frac{n(n-1)}{4}} \cdot \det(\mathcal{L}[M])$

**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  $\mathcal{A}(M) \in \mathcal{L}[M]$  וכן

$$\|\mathcal{A}(M)\| \leq 2^{\frac{n-1}{4}} \cdot \det(\mathcal{L}[M])^{\frac{1}{n}}$$

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

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

**Algorithm LLL-Algo( $\delta, M$ ):**

```

while True do
     $M^\perp \leftarrow \text{Orthonormalization}(M)$ 
    for  $i \leftarrow [2, \dots, n]$  do
        for  $j \leftarrow [i-1, \dots, 1]$  do
             $C_i(M) \leftarrow C_i(M) - \left\lfloor \frac{\langle C_i(M), C_j(M^\perp) \rangle}{\langle C_j(M), C_j(M^\perp) \rangle} \right\rfloor \cdot C_j(M)$ 
        end
    end
    end
     $f \leftarrow \text{True}; \quad i \leftarrow 1$ 
    while  $(i \leq n) \wedge (f = \text{True})$  do
        if  $\delta \langle C_i(M), C_i(M^\perp) \rangle^2 > \langle C_{i+1}(M), C_i(M^\perp) \rangle^2 + \langle C_{i+1}(M), C_{i+1}(M^\perp) \rangle^2$  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  $\mathcal{DD} : \mathbb{Z}^{n \times n} \rightarrow \mathbb{N}$  כך  $\mathcal{DD}[M] = \prod_{i=1}^n |\langle C_i(M), C_i(M^\perp) \rangle|^{n-i+1}$

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

**טענה:** יהי  $n \in \mathbb{N}_+$  ויהי  $\delta \in (\frac{1}{4}, 1)$  ותהא  $M \in \mathbb{R}^{n \times n}$  הפיכה ויהיו  $S, S'$  מצבים בריצת LLL-Algo באשר  $S'$  תוצאת לולאת ה-while

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

**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  $\delta \in (\frac{1}{4}, 1)$  יהי  $n \in \mathbb{N}_+$  תהא  $M \in \mathbb{R}^{n \times n}$  הפיכה מצומצמת  $\delta$ -LLL ויהי  $t \in \mathbb{R}^n$  אזי

**Algorithm Babai $_\delta$ (M, t):**

```

 $v \in \mathbb{R}^n; \quad v \leftarrow 0$ 
 $M^\perp \leftarrow \text{Orthonormalization}(M)$ 
for  $i \in [n, \dots, 1]$  do
     $k \leftarrow \lfloor \langle t, C_i(M^\perp) \rangle \rfloor$ 
     $v \leftarrow v + k \cdot C_i(M)$ 
     $t \leftarrow t - k \cdot C_i(M)$ 
end
return  $v$ 

```

**טענה:** יהי  $\delta \in (\frac{1}{4}, 1)$  אזי סיבוכיות הריצה של Babai $_\delta$  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

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

**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  $v \in \mathcal{F}^n$  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 המדויק 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  $v \in \mathcal{F}^n$  CVP-lattice-search-exact  $((M, t, \mathbb{F}, \mathcal{F}), \varepsilon) = v$  באשר  $\|Mv - t\| = \text{Val-lattice}(M, t, \mathbb{F}, \mathcal{F})$  וכן  $v \in \mathcal{F}^n$ .

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

**מסקנה:** 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  $v \in \mathcal{F}^n \setminus \{0\}$  וכן  $\|Mv\| \leq \varepsilon$  באשר SVP-lattice-search  $((M, \mathbb{F}, \mathcal{F}), \varepsilon) = v$ .

**בעיית חיפוש הוקטור המדויק 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

$v \in \mathcal{F}^n$  וכן  $\|Mv\| = \lambda_i[\mathcal{L}[M]]$  באשר SVP-lattice-search-exact  $(M, \mathbb{F}, \mathcal{F}) = v$ .

**בעיית הוקטור הקצר ביותר בסריג:**  $\text{SVP-lattice} = \{(M, \mathbb{F}, \mathcal{F}, \varepsilon) \mid \exists v \in \mathcal{F}^n \setminus \{0\} . \|Mv\| \leq \varepsilon\}$ .

**אלגוריתם חיפוש הקצר ביותר בהינתן הקרוב ביותר** [גולדרייך-מיצ'אנצ'ר-ספרא-זייפט 1999]: יהי  $n \in \mathbb{N}_+$  תהא  $M \in \mathbb{R}^{n \times n}$  הפיכה

ויהי  $\mathcal{A}$  אלגוריתם CVP-lattice-search-exact $_{\mathbb{R}|\mathbb{Z}}$  אזי

**Algorithm SVP-via-CVP[ $\mathcal{A}$ ](M):**

```

 $v \leftarrow C_1(M)$ 
for  $i \in [1, \dots, n]$  do
     $u \leftarrow \mathcal{A}(M + C_i(M) \cdot e_i^T, C_i(M)) - C_i(M)$ 
    if  $\|u\| < \|v\|$  then  $v \leftarrow u$ 
end
return  $v$ 

```

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

**מסקנה:**  $\text{SVP-lattice-search-exact} \leq_T^P \text{CVP-lattice-search-exact}$ .

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

**בעיית המרווח לוקטור הקרוב ביותר בסריג:** תהיינה  $T, S : \mathbb{N} \rightarrow \mathbb{N}$  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  $t \in \mathbb{F}^n$  ותהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  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  $T, S : \mathbb{N} \rightarrow \mathbb{N}$  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  $n \in \mathbb{N}_+$  ותהא  $M \in \mathbb{F}^{n \times n}$  הפיכה ותהא  $T : \mathbb{N} \rightarrow \mathbb{N}$  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  $\text{GAP-CVP}_\gamma$  הינה  $\mathcal{NP}$ -קשה.

**מסקנה:** יהי  $\gamma \in \mathbb{R}_{\geq 1}$  אזי  $\text{GAP-SVP}_\gamma$  הינה  $\mathcal{NP}$ -קשה.

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

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

**משפט:** תהא  $\gamma : \mathbb{N} \rightarrow \mathbb{N}$  באשר  $\gamma = 2^{\mathcal{O}(n \cdot \frac{\log \log(n)}{\log(n)})}$  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  $T : \mathbb{N} \rightarrow \mathbb{N}$  ותהא  $M \in \mathbb{R}^{n \times n}$  הפיכה אזי

$$\text{SIVP}_T(M) = (v_1 \dots v_n) \text{ באשר } v_1 \dots v_n \in \mathbb{R}^n \text{ וכן } \|v_i\| \leq T(n) \cdot \lambda_n[\mathcal{L}[M]] \text{ לכל } i \in [n]$$

**טענה:** יהי  $\gamma \in \mathbb{R}_{\geq 1}$  אזי  $\text{SIVP}_{\gamma \cdot \sqrt{n}} \leq_T^p \text{GAP-SVP}_\gamma$

**טענה:** יהי  $\gamma \in \mathbb{R}_{\geq 1}$  אזי  $\text{SIVP}_\gamma \leq_T^p \text{GAP-CVP}_\gamma$

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

**אלגוריתם חיפוש בינארי כללי:** יהי  $\varepsilon > 0$  ותהא  $f : \mathbb{R} \rightarrow \{0, 1\}$  על ועולה ויהיו  $a, b \in \mathbb{R}$  באשר  $\inf(f^{-1}[\{1\}]) \in [a, b]$  אזי

**Algorithm BinarySearch( $f, a, b, \varepsilon$ ):**

```

    if  $|b - a| < \varepsilon$  then return  $\frac{a+b}{2}$ 
    if  $f(\frac{a+b}{2}) = 1$  then
        return BinarySearch( $f, a, \frac{a+b}{2}, \varepsilon$ )
    else
        return BinarySearch( $f, \frac{a+b}{2}, b, \varepsilon$ )

```

**טענה:** יהי  $\varepsilon > 0$  ותהא  $f : \mathbb{R} \rightarrow \{0, 1\}$  על עולה ויהיו  $a, b \in \mathbb{R}$  באשר  $\inf(f^{-1}[\{1\}]) \in [a, b]$  אזי  $\text{BinarySearch}(f, a, b, \varepsilon) = d$

באשר  $|d - \inf(f^{-1}[\{1\}])| < \frac{\varepsilon}{2}$ .

**טענה:** יהי  $\varepsilon > 0$  ותהא  $f : \mathbb{R} \rightarrow \{0, 1\}$  על עולה חשיבה ויהיו  $a, b \in \mathbb{R}$  באשר  $\inf(f^{-1}[\{1\}]) \in [a, b]$

$\text{Time}(\text{BinarySearch}) = \mathcal{O}(\text{Time}(f) \cdot \log(\frac{b-a}{\varepsilon}))$

**הגדרה:** יהי  $R \in \mathbb{N}_+$  אזי  $\text{RootList}(R) = \text{Sort}([0, \dots, R] \parallel [\sqrt{n} \text{ for } n \in [0, \dots, R]])$

**אלגוריתם הכרעה לחיפוש לבעיית הוקטור הקרוב ביותר:** יהי  $n \in \mathbb{N}_+$  ותהא  $M \in \mathbb{Z}^{n \times n}$  הפיכה יהי  $t \in \mathbb{Z}^n$  ויהי  $\mathcal{A}$  אלגוריתם

$(\text{GAP-CVP}_1)_{\mathbb{R}|\mathbb{Z}}$  אזי

**Algorithm CVP-Decidability-Search[ $\mathcal{A}$ ]( $M, t$ ):**

```

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

```

**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:**  $\text{CVP-lattice-search-exact} \leq_T^p \text{GAP-CVP}_1$

**משפט:** יהי  $\gamma \leq 1 + \mathcal{O}(\frac{\log(n)}{n})$  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( $M, t, R$ ):**

```

 $M^\perp \leftarrow \text{Orthonormalization}(M)$ 
 $c \leftarrow \langle t, C_k(M^\perp) \rangle$ 
 $Z \in \mathcal{P}(\mathbb{Z}); \quad Z \leftarrow \{z \in \mathbb{Z} \mid |c - z \cdot \langle C_k(M), C_k(M^\perp) \rangle| \leq R\}$ 
 $M' \in \mathbb{R}^{n \times (k-1)}; \quad (M')_{i,j} \leftarrow (M)_{i,j}$ 
 $\mathcal{E} \leftarrow \mathcal{P}(\mathbb{R}^n); \quad \mathcal{E} \leftarrow \emptyset$ 
for  $z \in Z$  do
     $A \leftarrow \text{Enum}(M', \pi_{\text{span}(C_1(M), \dots, C_{k-1}(M))} (t - z \cdot C_k(M)), R)$ 
    for  $v \in A$  do  $\mathcal{E} \leftarrow \mathcal{E} \cup \{z \cdot C_k(M) + v\}$ 
end
return  $\mathcal{E}$ 

```

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

•  $\text{Yes} = \{\langle M, t, d \rangle \mid \exists z \in \{0, 1\}^n. \|Mz - t\| \leq d\}$

•  $\text{No} = \{\langle M, t, d \rangle \mid \forall z \in \mathbb{Z}^n. \forall k \in \mathbb{N}. \|Mz - kt\| \geq d \cdot T(n)\}$

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

**סריג צפוף מקומי:** 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 באשר  $(A, r, x, T)$

•  $\lambda_1[\mathcal{L}[A]] \geq r$

•  $\{0, 1\}^\ell \subseteq T((x + \mathcal{L}[A]) \cap B_{\alpha r}(0))$

**משפט:** יהיו  $n \in \mathbb{N}_+$  ויהיו  $\alpha, \gamma, \gamma' \in \mathbb{R}_{>0}$  באשר  $\frac{1}{\alpha} > \gamma' \geq 1$  וכן  $\gamma \geq \gamma' \cdot \frac{1}{\sqrt{1 - (\alpha\gamma')^2}}$  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  $(\alpha, \ell, k)$ -צפוף מקומי מתקיים

•  $(M, t, d), (A, r, x, T) = (M', d')$  באשר  $M' \in \mathbb{R}^{n \times n}$  מדרגה  $k$  וכן  $d' \in \mathbb{R}_{>0}$

•  $(\text{GAP-SVP}_{\gamma'}(\mathcal{A}((M, t, d), (A, r, x, T))) \in \text{Yes}) \iff (\text{gapBinCVP}_\gamma((M, t, d)) \in \text{Yes})$

**סריג שור-אדמלן למספרים ראשוניים:** יהי  $m \in \mathbb{N}_+$  יהיו  $a_1 \dots a_m \in \mathbb{N}_{\text{odd}}$  זרים ויהי  $\alpha \in \mathbb{R}_{>0}$  אזי נגדיר  $M_{\{a_1 \dots a_m\}} \in \mathbb{R}^{(m+1) \times m}$

$$(M_{\{a_1 \dots a_m\}})_{i,j} = \begin{cases} \sqrt{\ln(a_i)} & i=j \\ \alpha \ln(a_j) & i=m+1 \\ 0 & \text{else} \end{cases} \quad \text{כד}$$

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

**למה:** יהי  $m \in \mathbb{N}_+$  יהיו  $a_1 \dots a_m \in \mathbb{N}_{\text{odd}}$  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

$$\|M_{\{a_1 \dots a_m\}} \cdot z - e_{m+1} \cdot \alpha \ln(\beta)\| \leq \sqrt{\ln(\beta) + 2}$$

**מרחב המטריצות האקראית:** יהיו  $n, m \in \mathbb{N}_+$  ויהי  $p \in [0, 1]$  אזי  $\mathcal{M}(n, m, p) = (\mathbb{F}_2^{n \times m}, \mathbb{P})$  באשר

$$\mathbb{P}(A) = \prod_{i=1}^n \prod_{j=1}^m \left( \mathbb{1}[(A)_{i,j} = 1] \cdot p + \mathbb{1}[(A)_{i,j} = 0] \cdot (1 - p) \right)$$

**למה:** יהיו  $n, m, m' \in \mathbb{N}_+$  יהי  $\varepsilon \in (0, \frac{1}{7})$  תהא  $Z \subseteq \mathbb{F}_2^n$  באשר לכל  $z \in Z$  מתקיים  $\Delta(z, 0) = m'$  וכן  $|Z| \geq m'! \cdot m^{\frac{4\sqrt{m'} \cdot n}{\varepsilon}}$  אזי

$$\mathbb{P}_{C \leftarrow \mathcal{M}(n, m, \frac{1}{4nm'})} (\forall x \in \mathbb{F}_2^n. \exists z \in Z^m. Cz = x) > 1 - 7\varepsilon$$

**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

$$C \in \{0, 1\}^{(m+1) \times (m+1)} \text{ עבורם } (M_{\mathcal{S}}, \sqrt{2 \ln(\alpha)}, e_{m+1} \cdot \alpha \ln(\beta), C)$$

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

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

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

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

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

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

**משפט:** יהי  $q \in \mathbb{P}$  תהא  $S \subseteq \mathbb{F}_q$  ויהי  $k \in \mathbb{N}_{\leq \lfloor \frac{1}{2}|S| \rfloor}$  ונגדיר  $T \in \mathbb{Z}^{k \times |S|}$  כך  $T = (I_k \ 0_{k \times (|S|-k)})$  אזי קיים  $\alpha \in \mathbb{R}_{>0}$  עבורו

$(\text{basis}(L_q^\perp(H_q(k, S)^T)), \sqrt{2k}, 0, T)$  הינו סריג  $(\alpha, k, k)$ -צפוף מקומית.

**רדוקציית קארפ אקראית:** יהי  $\Sigma$  אלפבית ותהייה  $A, B \subseteq \Sigma^*$  אזי מ"ט פולינומית אקראית  $M$  עברה לכל  $x \in \Sigma^*$  מתקיים

$$\mathbb{P}_r(A(x) = B(M(x; r))) \geq \frac{2}{3}.$$

**סימון:** יהי  $\Sigma$  אלפבית ותהייה  $A, B \subseteq \Sigma^*$  באשר קיימת רדוקציית קארפ אקראית מ- $A$  ל- $B$  אזי  $A \leq_m^{\mathcal{BPP}} B$ .

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

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

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

**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  $q \in [N^d]$  וקיים  $u \in \mathbb{Z}^d$  עבורם לכל  $i \in [d]$

$$\left| v_i - \frac{1}{q} u_i \right| < \frac{1}{qN}.$$

**בעיית פתרון השלם הקטן ביותר:** יהי  $\mathbb{F}$  שדה סופי יהיו  $n, m \in \mathbb{N}_+$  יהי  $\kappa \in \mathbb{R}_{>0}$  ותהא  $M \in \mathbb{F}^{m \times n}$  אזי  $\text{SIS}[n, m, \mathbb{F}, \kappa](M) = x$

באשר  $x \in \ker(M) \setminus \{0\}$  וכן  $\|x\| \leq \kappa$ .

**סימון:** יהי  $q \in \mathbb{N}_+$  באשר  $\mathbb{F}_q$  שדה יהיו  $n, m \in \mathbb{N}_+$  ויהי  $\kappa \in \mathbb{R}_{>0}$  אזי  $\text{SIS}[n, m, q, \kappa] = \text{SIS}[n, m, \mathbb{F}_q, \kappa]$ .

**טענה:** יהי  $q \in \mathbb{N}_+$  באשר  $\mathbb{F}_q$  שדה יהיו  $n, m \in \mathbb{N}_+$  באשר  $m < \frac{n}{\log(q)}$  ויהי  $\kappa \in \mathbb{R}_{>0}$  באשר  $\kappa > \sqrt{n}$  אזי

$$\mathbb{P}_{M \leftarrow \text{Uni}(\mathbb{Z}_q^{m \times n})}(\exists x \in \ker(M) \setminus \{0\} : \|x\| \leq \kappa) \geq 1 - \frac{2}{q^{n-m}}.$$

**פונקציה זניחה:** פונקציה  $\mathbb{R} \rightarrow \mathbb{R}$   $\varepsilon$  עברה לכל  $k \in \mathbb{N}$  קיים  $N \in \mathbb{N}$  עבורו לכל  $n \in \mathbb{N}_{\geq N}$  מתקיים  $|\varepsilon(n)| \leq \frac{1}{n^k}$ .

**סימון:**  $\text{negl} = \{\varepsilon : \mathbb{N} \rightarrow \mathbb{R} \mid \varepsilon \text{ פונקציה זניחה}\}$ .

**סימון:** יהי  $r \in \mathbb{N}_+$  ויהי  $i \in [r]$  אזי  $\text{negl}(x_i) = \{\varepsilon : \mathbb{N}^r \rightarrow \mathbb{R} \mid \forall y \in \mathbb{R}^r : (\lambda z \in \mathbb{R}^\varepsilon(y_{\{1, \dots, i-1\}}, z, y_{\{i+1, \dots, r\}})) \in \text{negl}\}$

**טענה:** יהי  $q \in \mathbb{N}_+$  באשר  $\mathbb{F}_q$  שדה ויהיו  $n, m \in \mathbb{N}_+$  באשר  $m > n \log(q)$  אזי

$$\mathbb{P}_{M \leftarrow \text{Uni}(\mathbb{Z}_q^{m \times n})}(\lambda_1[L_q^\perp(M)] = \Theta(\sqrt{n} \cdot q^{\frac{n}{m}})) \geq 1 - \text{negl}(n)$$

**טענה:** יהי  $q \in \mathbb{N}_+$  באשר  $\mathbb{F}_q$  שדה יהי  $n \in \mathbb{N}_+$  יהי  $\kappa \in \mathbb{R}_{>0}$  ותהא  $M \in \mathbb{R}^{n \times n}$  אזי

$$\text{SIS}[n, n, q, \kappa](M) = \text{SVP-lattice-search}((\text{basis}(L_q^\perp(M)), \mathbb{R}, \mathbb{Z}), \kappa)$$

**משפט [אייטאיי 1996, רגב-מיצ'אנצ'ו 2005]:** יהי  $n \in \mathbb{N}_+$  יהי  $m = n^{\mathcal{O}(1)}$  יהי  $\kappa \in \mathbb{R}_{>0}$  יהי  $q = n^{\mathcal{O}(1)}\kappa$  באשר  $\mathbb{F}_q$  שדה ויהי

$$\text{SIS}[n, m, q, \kappa] =_T^p \text{GAP-SVP}_\gamma \text{ אזי } \gamma = n^{\mathcal{O}(1)}\kappa.$$