```
\Delta_r\left(x,y
ight)=rac{1}{n}\left|\left\{i\in[m]\mid x_i
eq y_i
ight\}
ight| כך \Delta:X^n	imes X^n	o\mathbb{N} מרחק האמינג יחסי: תהא
                                                                                                                            \ell_0 טענה: תהא א קבוצה אזי \Delta משרה את נורמת 
                                                                                         .w\left(x
ight)=\Delta\left(x,0
ight) כך w:\mathbb{F}^{n}	o\mathbb{N} משקל האמינג: יהי\,\mathbb{F}\, שדה אזי נגדיר
                                                                                                                          \mathcal{C} \subseteq [q]^m אזי q,m \in \mathbb{N}_+ יהיו שגיאות: לתיקון שגיאות:
                                                       q,m\in\mathbb{N}_+ ויהי לתיקון שגיאות לתיקון אזי פוד לתיקון ויהי ויהי איזי אויהי לתיקון איזי גודל האלפבית בקוד לתיקון איזי איזי איזי ויהיו
                                                         m אזי אוירי לתיקון אייאות אזי לתיקון ויהי q,m\in\mathbb{N}_+ ויהי שגיאות: הבלוק בקוד לתיקון אייאות אזי
                              d\left[\mathcal{C}
ight]=\min_{x
eq y}\Delta\left(x,y
ight) אזי לתיקון שגיאות אזי לתיקון ויהי q,m\in\mathbb{N}_{+} ויהי יהיו מרחק בקוד לתיקון שגיאות:
                                      r[\mathcal{C}] = \log_a |\mathcal{C}| אזי אויקון שגיאות אזי \mathcal{C} \subseteq [q]^m ויהי q,m \in \mathbb{N}_+ יהיו איזי שגיאות אזי מימד/קצב בקוד לתיקון שגיאות: יהיו
                               . לתיקון שגיאות [m,r\,[\mathcal{C}]\,,d\,[\mathcal{C}]\,,q] הינו קוד איי \mathcal{C} הינו קוד לתיקון שגיאות איי קוד לתיקון שגיאות \mathcal{C}
                             w' 
otin \mathcal{C} אזי \Delta \left( w, w' 
ight) \leq d-1 באשר w' \in \left[ q 
ight]^m ויהי w \in \mathcal{C} אזי לתיקון שגיאות יהי w \in \mathcal{C} אזי
rg \min_{v \in \mathcal{C}} \Delta\left(v, w'
ight) = w אזי \Delta\left(w, w'
ight) \leq \left\lfloor rac{d-1}{2} \right
floor באשר w' \in [q]^m ויהי w \in \mathcal{C} ויהי w \in \mathcal{C} לתיקון שגיאות יהי
                                                        (w,w) \leq \lfloor \frac{1}{2} \rfloor און אול מול און און אול מול מול מול מאר משפט חסם הסינגלטון: יהי \mathcal{C} קוד [m,r,d,q] לתיקון שגיאות אזי m,k \in \mathbb{N} מענה: יהיו m,k \in \mathbb{N} אזי m,k \in \mathbb{N} הינו קוד m,k \in \mathbb{N} לתיקון שגיאות. m,k \in \mathbb{N} אזי m,k \in \mathbb{N} אזי m,k \in \mathbb{N} מענה: יהיו m,k \in \mathbb{N} אזי m,k \in \mathbb{N} הינו קוד m,k \in \mathbb{N} לתיקון שגיאות. m,k \in \mathbb{N} מענה: יהיו m,k \in \mathbb{N} אזי m,k \in \mathbb{N} הינו קוד m,k \in \mathbb{N} לתיקון שגיאות.
                                              \mathcal{C}_{\mathrm{Hamming}} = \left\{ x \in \mathbb{F}_2^{2^m-1} \ \middle| \ \forall i \in [m] \ . \left( igoplus_{k \in [2^m-1]} x_k = 0 
ight) 
ight\} אזי m \in \mathbb{N}_+ אזי m \in \mathbb{N}_+ אזי m \in \mathbb{N}_+ אזי מינג: יהי
                                                               . טענה: יהי [2^m-1,2^m-m-1,3,2] הינו קוד \mathcal{C}_{\mathrm{Hamming}} אזי אזי אזי הינו קוד
                                      עבורו קיים קוד d' \geq d עבורו אזי קיים [m,r,d,q] לתיקון שגיאות עבורם m,r,d,q \in \mathbb{N}_+ עבורו קיים קוד
                                                                                                                                   . לתיקון שגיאות [m \lceil \log(q) \rceil, r \log(q), d', 2]
 . טענה: יהיו \ell m, \ell r, d, q עבורם קיים קוד [m, r, d, q] לתיקון שגיאות ויהי m, r, d, q \in \mathbb{N}_+ אזי קיים קוד שגיאות.
טענה: יהי d\in\mathbb{N}_{\text{odd}} ויהיו m,r,d+1,2 עבורם קיים קוד [m,r,d,2] לתיקון שגיאות אזי קיים קוד m,r\in\mathbb{N}_+ ויהיו m,r\in\mathbb{N}_+ ויהיו m,r,d+1,2 לתיקון שגיאות m,r\in\mathbb{N}_+ ויהיו m,r,d,q לתיקון שגיאות אזי [m,r,d,q] משפט האמינג: יהי m,r,d,q קוד m,r,d,q לתיקון שגיאות אזי
                   . באשר \mathcal{C} מרחב המקיים כי \mathcal{C}\subseteq\mathbb{F}_q^m המיאות לינארי לתיקון שהיאות שבה אזי קוד באשר באשר \mathbb{F}_q באשר שבה אזי קוד לינארי לתיקון שגיאות. יהיו
                                                                                              \dim\left(\mathcal{C}\right)=r יסענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות יהי
C_i\left(M_{\mathcal{C}}
ight)=b_i כך אזי נגדיר נגדיר M_{\mathcal{C}}\in\mathbb{F}_q^{m	imes r} כך אזי נגדיר נגדיר לינארי לינארי [m,r,d,q] לתיקון שגיאות ויהי
                                                                           \mathcal{C} = \left\{ M_{\mathcal{C}} \cdot v \;\middle|\; v \in \mathbb{F}_q^r 
ight\} יסענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות יהי
                                                                                                       M_{\mathcal{C}_{k	ext{-rep}}} = \left(egin{array}{c} I_m \ dots \end{array}
ight)אזי q,m,k\in\mathbb{N}_+ מסקנה: יהיו
                                                                                                         . טענה: יהיו לתיקון אזי אזי \mathcal{C}_{\mathrm{parity}} אזי אזי אזי q,m\in\mathbb{N}_+ יהיו יהיו
                                                                            i\in[n] לכל (\mathbb{1}_n)_i=1 כך בך \mathbb{1}_n\in\mathbb{F}^n אאי נגדיר איי מידיה ויהי \mathbb{1}_n\in\mathbb{R}^n לכל
                                                                                                                               M_{\mathcal{C}_{\mathrm{parity}}} = \left(egin{array}{c} I_m \\ \mathbb{1}_n^T \end{array}
ight) אזי q,m \in \mathbb{N}_+ מסקנה: יהיו
                                                                               d = \min_{v \in \mathcal{C}} \Delta\left(v,0\right) טענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי
A \in \mathbb{F}_q^{(m-r) 	imes r} עבורו קיימת \mathcal{D} עבורו אזי קיים קוד לינארי [m,r,d,q] לתיקון שגיאות אזי קיים קוד לינארי (ווארי ביימת [m,r,d,q]
                                                                                                                                                                       M_{\mathcal{D}} = \left( \begin{smallmatrix} I_r \\ A \end{smallmatrix} \right) המקיימת
                                                            R\left(M
ight)=\left\{R_{i}\left(M
ight)\mid i\in\left[m
ight]
ight\} אזי M\in\mathbb{F}^{m	imes n} ותהא m,n\in\mathbb{N}_{+} שדה יהי \mathbb{F} שדה יהי
                                                                                                                    טענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי
                                                                                |R\left(M_{\mathcal{C}}\right)\cap V|\leq m-d מתקיים \dim\left(V
ight)=r-1 באשר V\subseteq\mathcal{C} לכל
```

 $\mathbb{F}^{m imes n} = M_{m imes n}\left(\mathbb{F}
ight)$  אזי  $m,n \in \mathbb{N}_+$  שדה ויהיו שדה  $\mathbb{F}$  יהי

 $\Delta\left(x,y
ight)=\left|\left\{i\in\left[m
ight]\mid x_{i}
eq y_{i}
ight\}
ight|$  כך ל $\Delta:X^{n} imes X^{n}
ightarrow\mathbb{N}$  מרחק האמינג: תהא

```
|R\left(M_{\mathcal{C}}\right)\cap V|=m-d וכן \dim\left(V
ight)=r-1 המקיים V\subseteq\mathcal{C} המקיים •
טענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי קיים d'\geq \left[rac{d}{q}
ight] עבורו שיים קוד לינארי [m,r,d,q] לתיקון שגיאות.
                                                                                                   .m \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil אזי שגיאות לתיקון לתיקון לינארי קוד לינארי קוד לינארי יהי משפט הייסמר: יהי
                                             למה: יהי x\in\mathbb{F}_q^m אזי לכל m>r באשר m,r\in\mathbb{N}_+ שדה יהיו שדה לכל m>r באשר m,r\in\mathbb{N}_+ מתקיים
                                                                                                                                                                                                                          \mathbb{P}_{M \in \mathbb{F}_{a}^{m} \times r} (Mx = b) = \frac{1}{a^{m}}
                                \mathcal{C}_M=\left\{M\cdot v\mid v\in\mathbb{F}_q^r
ight\} אזי M\in\mathbb{F}_q^{m	imes r} ויהי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו m>r באשר m,r\in\mathbb{N}_+
                                                     משפט: יהי \delta\in(0,1) באשר m>r באשר m,r\in\mathbb{N}_+ שדה יהיו m>r באשר m>r 
. לתיקון שגיאות [m, m-r, d', q] לינארי קוד לינארי [m, r, d, q] לתיקון שגיאות אזי קיים d' \in \mathbb{N}_+ עבורו לינארי לינארי
                                                                                                                      H_{\mathcal{C}}=M_{\mathcal{C}^{\vee}} אזי שאריות: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי מטריצת בדיקת שאריות:
                                                                                                                                                       \mathcal{C} = \ker \left( H_{\mathcal{C}}^T \right) יטענה: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי
                                                                                             d=m-r+1 לתיקון שגיאות לתיקון שגיאות: קוד [m,r,d,q] לתיקון שגיאות מקסימלי לתיקון לתיקון שגיאות:
טענה: יהי \mathcal{C}_M אזי (\mathcal{C}_M) אזי M\in\mathbb{F}_q^{m	imes r} ויהי האטר m>r באשר m,r\in\mathbb{N}_+ שדה יהיו קוד לינארי מקסימלי לתיקון
                                                                                                                                                             שגיאות)\Longleftrightarrow(לכל A \in \mathcal{P}_r(R(M)) מתקיים כי A \in \mathcal{P}_r(R(M))
                                                                  . טענה: יהי \mathcal{C}^{\vee} קוד לינארי מקסימלי לתיקון שגיאות אזי לענה: יהי לינארי מקסימלי לתיקון שגיאות טענה: יהי \mathcal{C}^{\vee}
משפט גילברט־וורשאמוב: יהיו m,k,d,q באשר שנים d\leq m ויהי וויהי באשר לינארי לתיקון שגיאות לאזי המקיים משפט d,m\in\mathbb{N}_+ לתיקון שגיאות
                                                                                                                                                                                            |\mathcal{C}| \ge q^m \cdot \left(\sum_{i=0}^{d-1} \left(\binom{m}{i} \cdot (q-1)^i\right)\right)^{-1}
H\in \mathbb{F}_q^{m	imes(m-k)} אזי קיים \sum_{i=0}^{d-2} {m-1\choose i} \left(q-1
ight)^i < q^{m-k} עבורו עבורן k\leq m באשר באשר אזי קיים k\leq m באשר למה: יהי k\leq m באשר
                                                                                                                                                                        עבורו לכל A\in\mathcal{P}_{d-1}\left(R\left(M
ight)
ight) מתקיים כי A\in\mathcal{P}_{d-1}\left(R\left(M
ight)
ight)
אזי \sum_{i=0}^{d-2} \binom{m-1}{i} \left(q-1
ight)^i < q^{m-k} אזי עבורו q \in \mathbb{P} איי איי k \leq m באשר באשר k, m \in \mathbb{N}_+ יהיו d \in \mathbb{N}_{\geq 2} אזי יהי
                                                    |\mathcal{C}| \geq q^m \cdot \left(1 + \sum_{i=0}^{d-2} \left({m-1 \choose i} \cdot (q-1)^i\right)\right)^{-1} קיים קוד לינארי [m,k,d,q] לתיקון שגיאות \mathcal{C} המקיים f:X \to Y^n אזי f:X \to Y^n אזי f:X \to Y^n אויהי f:X \to Y^n עבורה
                                           .g\left(f\left(s
ight)_{p_{1}},\ldots,f\left(s
ight)_{p_{k}}
ight)=s מתקיים p_{1},\ldots,p_{k}\in\left[n
ight] ולכל ולכל s\in X עבורה לכל g:Y^{k}	o X
g\left(f\left(s\right)_{p_1},\ldots,f\left(s\right)_{p_{k-1}}
ight)=s מתקיים p_1,\ldots,p_{k-1}\in[n] ולכל s\in X ולכל g:Y^{k-1}\to X מתקיים g:Y^{k-1}\to X שונים ונגדיר \varphi:\mathbb{F}_{\leq k-1}\left[x
ight]\to \mathbb{F}^\ell יהי שונים ונגדיר x_1\ldots x_\ell\in\mathbb{F} יהי שדה סופי באשר g:Y^{k-1}\to X שונים ונגדיר \ell\in X יהי \ell\in X יהי שדה סופי באשר שדה סופי באשר אונים ונגדיר \ell\in X
                                                                                                                                                                                                                                    אזי \varphi(p) = (p(x_i))_{i=1}^{\ell}
                                                                                                                                 . אם אז \varphi איזומורפיזם וכן \varphi, \varphi^{-1} חשיבות איזומורפיזם פולינומי.
                                                                                                           k-\ell ממימד אפיני מרחב \varphi^{-1}\left(y\right)כי מתקיים y\in\mathbb{F}^{\ell} אז לכל \ell< k שם •
כך f: \mathbb{F}_q 	imes (\mathbb{F}_q ackslash \{0\})^{k-1} 	o \left(\mathbb{F}_q^2\right)^n אזי נגדיר k \in [n] אזי נאדיר n < q באשר שמיר: יהי q \in \mathbb{N} שדה יהי n \in \mathbb{N}_+ שדה יהי
```

שונים.  $s_1\dots s_n\in \mathbb{F}_qackslash\{0\}$  באשר  $f\left(s,a
ight)=\left(\left(s_i,s+\sum_{j=1}^{k-1}a_js_i^j
ight)
ight)_{i=1}^n$ 

 $k \in [n]$  ויהי וויהי  $k \in [n]$  אזי סכימת שמיר הינה סכימת חלוקת סוד מושלמת. באשר  $n \in \mathbb{N}_+$  שדה יהי  $\mathbb{F}_q$  שדה יהי  $n \in \mathbb{N}_+$  באשר

שונים אזי  $lpha_1 \ldots lpha_m \in \mathbb{F}_q$  ויהיו  $r \in [m]$  יהי יהי שדה יהי  $\mathbb{F}_q$  שדה יהי באשר קב

 $.\mathrm{RS}_{q}\left[m,r\right] = \left\{ \left(f\left(\alpha_{i}\right)\right)_{i=1}^{m} \mid f \in \left(\mathbb{F}_{q}\right)_{\leq r-1}\left[x\right] \right\}$ 

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

לתיקון שגיאות. [m, r, m - r + 1, q]

 $(i,j)\in[m] imes[r]$  לכל  $\left(M_{\mathrm{RS}_q[m,r]}
ight)_{i,j}=lpha_i^{j-1}$  אזי  $lpha_1\ldotslpha_m\in\mathbb{F}_q$  יהי  $m\in[q]$  לכל לכל ענה: יהי  $m\in[q]$  איהי שדה יהי יהי שדה יהי  $\sum_{x\in\mathbb{F}_q}x^i=0$  אזי  $i\in\{0,\ldots,q-2\}$  שדה ויהי  $\mathbb{F}_q$  באשר באשר  $q\in\mathbb{N}$ 

 $ext{RS}_q\left[q,r
ight]^ee = ext{RS}_q\left[q,q-r
ight]$  אזי  $r \in [q]$  שדה ויהי  $q \in \mathbb{N}$  יהי  $q \in \mathbb{N}$ 

 $w\in\mathrm{RS}_q\left[m,r
ight]$  אלגוריתם ברלקמפ־וולץ': יהי  $lpha\in\mathbb{R}_q$  שדה יהי ווא יהי  $m\in[q]$  שדה יהי שנים עהא עלגוריתם ברלקמפ־וולץ: יהי

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

```
Algorithm BerlekampWelch(q, m, r, \alpha, y):
                                 \deg(g) = r + \left\lceil \frac{m-r}{2} \right\rceil - 1
      g \in (\mathbb{F}_q)[x];
                                \deg(h) = \left| \frac{m-r}{2} \right|
      h \in (\mathbb{F}_q)[x];
     (g,h) \leftarrow \operatorname{LinearEqSolver}\left(\left(g\left(\alpha_{i}\right)=h\left(\alpha_{i}\right)\cdot y_{i}\right)_{i=1}^{m}\right) // We do not accept g=h=0
      return PolynomialDivision (g, h)
טענה: יהי w\in\mathrm{RS}_q[m,r] שונים תהא שונים lpha_1\ldotslpha_m\in\mathbb{F}_q יהי יהי m\in[q] יהי יהי m\in[q] יהי יהי m\in[q]
 \Delta\left(P,y
ight) \leq rac{m-r}{2} וכן P \in (\mathbb{F}_q)_{\leq r-1}[x] באשר BerlekampWelch (q,m,r,lpha,y)=P אזי y=w+e ונגדיר \Delta\left(e,0
ight) \leq rac{m-r}{2}
                                                              .B_{r}\left(x
ight)=\left\{ y\in X\mid\Delta\left(x,y
ight)\leq r
ight\} אזי איז x\in X וויהי ויהי קבוצה יהי קבוצה יהי הא
|B_r(w)\cap\mathcal{C}|\leq \ell מתקיים w\in[q]^m מתקיים לתיקון שגיאות \mathcal{C} אזי קוד לתיקון אזי קוד r,\ell\in\mathbb{N}_+ אזי קוד לתיקון שגיאות רשימתי: יהיו
סימון: יהיו r,\ell\in\mathbb{N}_+ ויהי \mathcal{C} קוד [m,k,d,q] לתיקון שגיאות רשימתי [m,k,d,q] אזי [m,k,d,q] לתיקון שגיאות רשימתי.
                                           . טענה: יהי \mathcal C קוד [m,k,d,q] לתיקון שגיאות אזי \mathcal C הינו קוד [m,k,d,q] לתיקון שגיאות רשימתי
e\in\mathbb{F}_q^m יהי w\in\mathrm{RS}_q\left[m,r
ight] שונים תהא שונים lpha_1\ldotslpha_m\in\mathbb{F}_q יהי יהי m\in[q] שדה יהי שדה יהי יהי אלגוריתם סודן: יהי
                                                                                                               אזי y=w+e ונגדיר \Delta\left(e,0
ight)\leq m-2\sqrt{mr} באשר
Algorithm Sudan(q, m, r, \alpha, y):
                                                                      \deg_u(Q) = \sqrt{\frac{m}{r}}
                                   \deg_x(Q) = \sqrt{mr};
      Q \in (\mathbb{F}_q)[x,y];
      Q \leftarrow \operatorname{LinearEqSolver}\left(\left(Q\left(y_{i}, \alpha_{i}\right) = 0\right)_{i=1}^{m}\right) \ / / \ \text{We do not accept } Q = 0
                                    S \leftarrow \operatorname{PolymonialSolutions}\left(Q\right) // We view Q as a polynomial in \left(\mathbb{F}_q[x]\right)[y]
     \text{return } [h \quad \text{for} \quad h \in S \quad \text{if} \quad \Delta \left( \left( h \left( \alpha_i \right) \right)_{i=1}^m, y \right) < m - 2 \sqrt{mr}]
טענה: יהי w\in\mathrm{RS}_q\left[m,r
ight] שונים תהא שונים lpha_1\ldotslpha_m\in\mathbb{F}_q יהי יהי m\in[q] יהי יהי שדה יהי יהי m\in[q]
                                                                      באשר Sudan (q,m,r,lpha,y)=L אזי y=w+e ונגדיר \Delta\left(e,0
ight)\leq m-2\sqrt{mr}
                                      .\{\left(h\left(\alpha_{i}\right)\right)_{i=1}^{m}\mid h\in L\}=\left\{w'\in\mathrm{RS}_{q}\left[m,r\right]\mid \exists\varepsilon\in\mathbb{F}_{q}^{m}:\left(y=w'+\varepsilon\right)\wedge\left(\Delta\left(\varepsilon,0\right)\leq m-2\sqrt{mr}\right)\right\}
      	ext{RM}_q\left[m,r
ight] = \left\{ (f\left(lpha
ight))_{lpha \in \mathbb{F}_q^m} \;\middle|\; f \in (\mathbb{F}_q)_{\leq r}\left[x_1,\ldots,x_m
ight] 
ight\} אזי m,r \in \mathbb{N}_+ שדה ויהיו שדה ויהיו q \in \mathbb{N} אזי q \in \mathbb{N}
                                                      \mathrm{RM}_q\left[m,r
ight]\simeq (\mathbb{F}_q)_{\leq r}\left[x_1,\ldots,x_m
ight] אזי m,r\in\mathbb{N}_+ שדה ויהיו שדה באשר q\in\mathbb{N} הערה: יהי
טענה: יהי \mathrm{RM}_q\left[m,r
ight] הינו קוד לינארי m,r\in\mathbb{N}_+ אזי קיימים שדה ויהיו m,r\in\mathbb{N}_+ שבה ויהיו לינארי m,r\in\mathbb{N}_+
                                                   r\left[\mathrm{RM}_q\left[m,r
ight]
ight] = inom{m+r}{r} אזי r < q אזי איזי m,r \in \mathbb{N}_+ שדה ויהיו \mathbb{F}_q שדה יהי יהי
                                        d\left[\mathrm{RM}_q\left[m,r
ight]
ight] \geq (q-r)\,q^{m-1} אזי r < q באשר m,r \in \mathbb{N}_+ שדה ויהיו \mathbb{F}_q שדה יהי q \in \mathbb{N} אזי יהי
                                                                                                         r\left[\mathrm{RM}_2\left[m,r
ight]
ight] = \sum_{i=0}^r inom{m}{i} אזי m,r \in \mathbb{N}_+ טענה: יהיו
                                    משפט: יהי r=a\left(q-1
ight)+b באשר m,r,a,b\in\mathbb{N}_{+} שדה ויהיו \mathbb{F}_{q} באשר באשר q\in\mathbb{N} יהי
                                                                                                                                         d[RM_{q}[m,r]] \ge (q-b)q^{m-a-1}
                                                                                           	ext{RM}_2\left[m,r
ight]^ee = 	ext{RM}_2\left[m,m-r-1
ight] אזי m,r \in \mathbb{N}_+ טענה: יהיי
                       \mathrm{RM}_2\left[m,r
ight] = \left\{(u,u+v) \mid (u \in \mathrm{RM}_2\left[m-1,r
ight]) \wedge (v \in \mathrm{RM}_2\left[m-1,r-1
ight])
ight\} אזי m,r \in \mathbb{N}_{\geq 2} טענה: יהיו
אלגוריתם תיקון שגיאות מקומי בקוד ריד־מיולר: יהי q\in\mathbb{N} באשר q\in\mathbb{N} יהי הי \alpha,arepsilon\in(0,1) יהי ויהי m\in\mathbb{N}_+ שדה יהי m\in\mathbb{N}_+ שדה יהי מקומי בקוד ריד־מיולר:
                                                                                                            אזי d\left(\mathrm{RM}_q\left[m,lpha q
ight],w
ight)\leq q^m\cdot rac{1-lpha}{6} באשר w\in\mathbb{F}_q^{m}
Algorithm LocalRM(\varepsilon, q, m, \alpha, z, w; R):
     t \leftarrow [-18 \cdot \log{(\varepsilon)}]
     a_1 \dots a_t \in \mathbb{F}_q
     for i \in [1, \ldots, t] do
      a_i \leftarrow \left( \text{BerlekampWelch} \left( q, q, \alpha q + 1, x, w_{z + \mathbb{F}_q \cdot R(v)} \right) \right) (0)
     return Majority (a_1, \ldots, a_t)
                                           טענה: יהי x\in\mathbb{F}_q^m שדה יהי a,arepsilon\in(0,1) יהי יהי m\in\mathbb{N}_+ שדה יהי שדה q\in\mathbb{N} באשר טענה: יהי יהי מ
       אזי (f\left(lpha
ight))_{lpha\in\mathbb{F}_{n}^{m}}=rg\left(d\left(\mathrm{RM}_{q}\left[m,lpha q\right],w
ight) באשר f\in\left(\mathbb{F}_{q}
ight)_{<lpha q}\left[x_{1},\ldots,x_{m}
ight] ותהא d\left(\mathrm{RM}_{q}\left[m,lpha q\right],w
ight)\leq q^{m}\cdot\frac{1-lpha}{6}
```

```
שרשור קודים לתיקון שגיאות: יהי \mathcal{C} קוד [m,r,d,q] לתיקון שגיאות יהי \mathcal{C}' קוד [m,r,d,q] לתיקון שגיאות ותהא
                                                                                                                \mathcal{C}\circ\mathcal{C}'=\left\{\left(
ho\left(w_{i}
ight)
ight)_{i=1}^{m}\mid w\in\mathcal{C}
ight\} הפיכה אזי 
ho:\left[q
ight]
ightarrow\mathcal{C}'
                       טענה: יהי \mathcal{C}\circ\mathcal{C}' אזי אזי לתיקון שגיאות אזי [m',\log_{q'}(q)\,,d',q'] קוד קוד לתיקון שגיאות אזי לתיקון שגיאות ויהי
                                                                                                                               לתיקון שגיאות. \left[m \cdot m', r \cdot \log_{q'}(q), d \cdot d', q'\right]
הפיכה אזי 
ho:[q]	o \mathcal{C}' הותהא ותהא לתיקון שגיאות יהי [m',\log_{a'}(q)\,,d',q'] הוד קוד לתיקון שגיאות היהי לתיקון שגיאות יהי לתיקון שגיאות היהי
                                                                      \mathcal{C}\circ\mathcal{C}'\simeq\left\{h:[m]	imes[m']	o[q]\ \Big|\ \exists w\in\mathcal{C}.h\left(i,j
ight)=\left(
ho\left(w_{i}
ight)
ight)_{j}
ight\} . \chi_{S}\left(x
ight)=\sum_{i\in S}x_{i} כך \chi_{S}:\mathbb{F}_{2}^{n}	o\mathbb{F}_{2} אזי נגדיר S\subseteq\left[n
ight] אזי נגדיר n\in\mathbb{N} הגדרה: יהי
                                                                                          \mathcal{C}_{\mathrm{Hadamard}} = \left\{ \left(\chi_{S}\left(x
ight)
ight)_{x \in \mathbb{F}_{2}^{n}} \;\middle|\; S \subseteq [n] 
ight\} אזי n \in \mathbb{N}_{+} יהי יהי
                                                                      . טענה: יהי [2^n,n,2^{n-1},2] הינו קוד לינארי \mathcal{C}_{\mathrm{Hadamard}} אזי אות איאות יהי יהי יהי
                                                                                                                    \mathcal{C}_{	ext{Hadamard}} \simeq \{\chi_S \mid S \subseteq [n]\} אזי n \in \mathbb{N}_+ הערה: יהי היי
                                                                                          .\Big\{(\chi_{S}\left(x
ight))_{x\in\mathbb{F}_{2}^{n}\setminus\{0\}}\ \Big|\ S\subseteq[n]\Big\}^{ee}=\mathcal{C}_{\mathrm{Hamming}} אזי n\in\mathbb{N}_{+} יהי היי היי n\in\mathbb{N}_{+}
                                                                                           \mathcal{C}_{\mathrm{Dic}}=\left\{ \left(\chi_{\{i\}}\left(x
ight)
ight)_{x\in\mathbb{F}_{2}^{n}}\,\middle|\,i\in[n]
ight\} אזי n\in\mathbb{N}_{+} איזי יהי
                                                                                . טענה: יהי [2^n,\log_2{(n)},2^{2^{n-1}},2] הינו קוד \mathcal{C}_{	ext{Dic}} לתיקון שגיאות. n\in\mathbb{N}_+ יהי
                                                                                                                             \mathcal{C}_{	ext{Dic}}\simeq ig\{\chi_{\{i\}} \mid i\in[n]ig\} אזי n\in\mathbb{N}_+ יהי הערה: יהי
                                            M,t,\mathbb{F} אזי t\in\mathbb{F}^m ויהי M\in\mathbb{F}^{m	imes n} תהא תהא m,n\in\mathbb{N}_+ אזי שדה יהי \mathbb{F} אזי M\in\mathbb{F}^m
       \mathrm{Val}\left((M,t,\mathbb{F})
ight)=\min_{x\in\mathbb{F}^n}\left(\Delta_r\left(Mx,t
ight)
ight) אינאריות אזי לינארית: תהא (M,t,\mathbb{F}) מערכת משוואות לינארית
       \mathrm{NoSatEq}_{\mathbb{F}} = \{ \langle M, t \rangle \mid (M \in \mathbb{R}^{n 	imes n}) \land (t \in \mathbb{R}^n) \land (\exists x \in \mathbb{R}^n : \forall i \in [n] : (Mx)_i \neq t_i) \} בעיית אי־סיפוק: יהי
                                                                                                                                                                    \mathrm{NoSatEq}_{\mathbb{F}_2} \in \mathcal{P} :טענה
                                                                                           \mathrm{NoSatEq}_{\mathbb{F}} אזי \mathrm{NoSatEq}_{\mathbb{F}} הינה שדה סופי באשר אוי שדה סופי באשר
	ext{CVP-code-search}\left((M,t,\mathbb{F}),arepsilon
ight)=v איז arepsilon>0 איז מערכת משוואות אינאריות ויהי מערכת (M,t,\mathbb{F}) מערכת משוואות לינאריות ויהי
                                                                                                                                                                      \Delta_r(Mv,t) \leq \varepsilon באשר
                                                                        \mathrm{CVP\text{-}code} = \{ \langle (M, t, \mathbb{F}), \varepsilon \rangle \mid \mathrm{Val}((M, t, \mathbb{F})) \leq \varepsilon \} בעיית הוקטור הקרוב ביותר:
                                                                         .SVP-code = \{\langle M, \mathbb{F}, \varepsilon \rangle \mid \exists v \neq 0. \Delta_r (Mv, 0) \leq \varepsilon \} בעיית הוקטור הקצר ביותר:
                                                    \operatorname{MaxCut}(G) = \max\left\{\left|E\left(S,\overline{S}
ight)\right| \mid S \subseteq V\left(G
ight)
ight\} בעיית החתך המקסימלי: יהי
ולכל e\in E\left(G
ight) לכל \left(M\left(G
ight)
ight)_{e,v}=\mathbb{1}\left[v\in e
ight] כך מטריצת החתכים: יהי G גרף סופי אזי נגדיר M\left(G
ight)\in\mathbb{F}_{2}^{|E\left(G
ight)|	imes|V\left(G
ight)|} לכל ולכל
                                                                                                                                                                                         v \in V(G)
                                                                                      \operatorname{Val}\left(\left(M\left(G\right),\mathbb{1}_{|V\left(G\right)|},\mathbb{F}_{2}\right)\right)=\operatorname{MaxCut}\left(G\right) טענה: יהי G גרף סופי אזי
                                                                            . קשה. Promise-\mathcal{NP} הינה \mathrm{GAP}_{[1-\varepsilon,1-\varepsilon]}\mathrm{MaxCut} סענה: קיים \varepsilon\in(0,1)
                                                                                                            . מסקנה: קיים \mathcal{NP} הינה \mathcal{C}\mathrm{VP\text{-}code}_{arepsilon} עבורו arepsilon \in (0,1)
                                                                                               . הינה \mathcal{NP} הינה CVP-code-search עבורו \varepsilon \in (0,1) הינה מסקנה:
                                                           . הינה Promise-\mathcal{NP} הינה \mathrm{GAP}_{[1-\varepsilon,1-(1+\delta)\varepsilon]}\mathrm{MaxCut} קשה. עבורם \varepsilon,\delta\in(0,1)
                                                   \mathrm{GAP}_{[a,b]}\mathrm{CVP\text{-}code} = \mathrm{GAP}_{[a,b]}\mathrm{Val} איי a,b \in [0,1] יהיו ביותר: יהיו
                                              . הינה \mathcal{NP} הינה \mathrm{GAP}_{[arepsilon,1-arepsilon]}\mathrm{CVP\text{-}code}_{\mathbb{F}} עבורו עבורו \varepsilon>0 הינה \varepsilon>0
                                     \mathcal{P}=\mathcal{NP} אז CVP-code-search מסקנה: אם קיים אלגוריתם פולינומי A אשר מהווה אשר פולינומי
(M)_{i,j}=1 עבורו איז j\in[m] וכן קיים w\left(R_i\left(M
ight)
ight)=2 מתקיים i\in[n] עבורה לכל עבורה אזי M\in\mathbb{F}^{n	imes m} עבורו אזי M\in\mathbb{F}^{n	imes m}
                                                                                                                                                                        R_i(M) \cdot \mathbb{1}_m = 0 וכן
                             \mathrm{Val}_{1\leftrightarrow 1}\left((M,t,\mathbb{F})
ight)=\mathrm{Val}\left((M,t,\mathbb{F})
ight) אזי t\in\mathbb{F}^m מטריצת משחק ויהי M\in\mathbb{F}^{n	imes m} שדה תהא
                                                              \mathrm{.PCP}_{1\leftrightarrow 1}\left[a,b
ight] = \mathrm{GAP}_{[a,b]}\mathrm{Val}_{1\leftrightarrow 1} אזי a,b\in[0,1] יהיו על אחד: יהיו
                                                                                        \mathrm{UG}\left(arepsilon
ight)=\mathrm{PCP}_{1\leftrightarrow1}\left[arepsilon,1-arepsilon
ight] אזי arepsilon>0 אזי היחודיים: יהי
                                   השערת המשחקים היחודיים [חות' 2002]: יהי arepsilon > 0 אזי והינה \mathcal{P}ריקשה. השערה פתוחה
                               .Interpol (u,v)=\{t\in\mathbb{F}^m\mid \forall i\in[m]\,.t_i\in\{u_i,v_i\}\} אזי v,u\in\mathbb{F}^m ויהיו m\in\mathbb{N}_+ יהי שדה יהי m\in\mathbb{N}_+ איזי שדה יהי m\in\mathbb{N}_+
                                                                                       אזי u,v\in\mathbb{F}^m אזי מטריצת משחק ויהיו M\in\mathbb{F}^{n	imes m} אזי הגדרה: יהי
                                                                                                      .\mathrm{Val}_{2\rightarrow1}\left(\left(M,\left\{u,v\right\},\mathbb{F}\right)\right)=\mathrm{min}_{t\in\mathrm{Interpol}(u,v)}\,\mathrm{Val}\left(\left(M,t,\mathbb{F}\right)\right)
                                                            \mathrm{.PCP}_{2	o 1}\left[a,b
ight] = \mathrm{GAP}_{[a,b]}\mathrm{Val}_{2	o 1} אזי a,b\in[0,1] יהיו על אחד: יהיו
                            משפט [חות'־מינזר־ספרא 2018]: יהי arepsilon>0 אזי אזי איזי אזי איזי ריהי פררס אזי איזי איזי איזי ריהי פררס אזי arepsilon>0 הינה משפט [חות'־מינזר־ספרא 2018]: יהי
```

 $ext{adjent}$  - Promise- $\mathcal{NP}$  הינה  $\frac{1}{2}\mathrm{UG}\left(arepsilon
ight)$  אזי arepsilon>0 אזי הינה  $\frac{1}{2}\mathrm{UG}\left(arepsilon
ight)$  הינה  $\mathrm{MaxCut}$ -IP (G) בעיית החתך המקטימלי כתכנות שלם: יהי  $\mathcal{D}$  גרף אזי נגדיר

$$\max \sum_{(u,v)\in E} \frac{1 - x_u x_v}{2}$$

s.t. 
$$x_v \in \{-1, 1\}$$
 ,  $\forall v \in V(G)$ 

G אוי אוי  $\{v\in V(G)\mid x_v=1\}$  אוי  $\mathbb{F}_2^{|V(G)|}$  חתך מקסימלי של  $x\in \mathbb{F}_2^{|V(G)|}$  חתך מקסימלי של אוי איי היי G גרף אוי נגדיר המקסימלי כתכנות לינארי: יהי G גרף אוי נגדיר G אוי גדיר יהי החתך המקסימלי בתכנות לינארי: יהי

$$\max \sum_{(u,v)\in E} \frac{1 - x_u x_v}{2}$$

s.t. 
$$x_v \in [-1, 1]$$
 ,  $\forall v \in V(G)$ 

כך  $\operatorname{MaxCut-VP}(G)$  כגדיר גריף אזי גריי. יהי G יהי כתכנות וקטורי: יהי

$$\max \sum_{(u,v)\in E} \frac{1 - \langle X_u, X_v \rangle}{2}$$

s.t. 
$$X_v \in \mathbb{S}^{|V(G)|-1}$$
 ,  $\forall v \in V(G)$ 

 $x\in\mathbb{R}^n$  לכל  $x^TAx\geq 0$  סימטרית המקיימת  $A\in\mathbb{R}^{n imes n}$  אזי אזי  $n\in\mathbb{N}_+$  לכל לכל

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

 $\langle A,B
angle=\mathrm{trace}\left(A^TB
ight)$  אזי  $A,B\in\mathbb{R}^{n imes n}$  ותהיינה  $n\in\mathbb{N}_+$  יהי מכפלה פנימית של מטריצות: יהי

תהא  $q\in\mathbb{R}^k$  יהי  $Q\in(\mathbb{R}^{n imes n})^k$  תהא יהי  $P\in(\mathbb{R}^{m imes n})^m$  תהא תהא  $R,k,\ell\in\mathbb{N}$  יהי יהיו  $R\in(\mathbb{R}^{n imes n})^m$  יהי  $R\in(\mathbb{R}^{n imes n})^\ell$ 

בעיית תכנות חצי מוגדרת אזי מציאת נקודת קיצון מסוג  $m \in \{\max, \min\}$ : יהי  $(\mathrm{SDP})$ : יהי  $m \in \{\max, \min\}$ : יהי  $m \in \{\max, \min\}$ : יהי  $m \in \{\min, i \in [\ln(p)]\}$ :  $m \in \{(P_i, X) \leq p_i \mid i \in [\ln(p)]\} \cup \{(Q_i, X) \geq q_i \mid i \in [\ln(q)]\} \cup \{(Q_i, X) \leq p_i \mid i \in [\ln(p)]\}$  תחת ההנחות  $m \in \{\min, i \in [n]\}$ : הערה: כל ההגדרות של תכנות לינארי מורחבות בצורה טבעית לתכנות חצי מוגדר.

 ${
m SDP}$  משפט: תהא  ${
m SDP}$  בעיית תכנות חצי מוגדר ויהי  ${
m c}>0$  אזי קיים אלגוריתם פולינומי

בעיית חיפוש פתרון פיזבילי של תוכנה חצי מוגדרת: תהא (C,P,p,Q,q,R,r) תוכנה חצי מוגדרת אזי

וכן  $i \in [\mathrm{len}\,(q)]$  לכל  $\langle Q_i, X \rangle \geq q_i$  וכן  $i \in [\mathrm{len}\,(p)]$  לכל השר Feasibility-Search (C, P, p, Q, q, R, r) = X וכן  $i \in [\mathrm{len}\,(q)]$  לכל  $\langle R_i, X \rangle = r_i$ 

. Feasibility-Search (P) של הינו  $\varepsilon$  באשר A הינו  $\varepsilon$  באשר אויריתם פולינומי  $\varepsilon$  אזי קיים אלגוריתם פולינומי  $\varepsilon$  באשר אוי מוגדר. על האר האר מוגדר: יהי  $\varepsilon$  גרף אזי נגדיר אוי נגדיר בעיית החתך המקטימלי כתכנות חצי מוגדר: יהי  $\varepsilon$  גרף אזי נגדיר בעיית החתך המקטימלי בתכנות חצי מוגדר:

$$\max \sum_{\{u,v\}\in E(G)} \frac{1 - A_{u,v}}{2}$$

s.t. 
$$A \ge 0$$

$$A_{t,t} = 1$$
 ,  $\forall t \in V(G)$ 

 $X=rg\operatorname{MaxCut-VP}\left(G
ight)$  באשר באשר אזי  $X\in\mathbb{R}^{n imes n}$  ותהא ותהא אוי אוי באשר  $X\in\mathbb{R}^{n imes n}$  באשר  $X=\operatorname{Arg}\operatorname{MaxCut-VP}\left(G
ight)$  באשר אזי  $X=\operatorname{Arg}\operatorname{MaxCut-SDP}\left(G
ight)$ 

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

```
Algorithm Cholesky (A):
```

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

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

אזי  $A=rg\operatorname{MaxCut-SDP}\left(G
ight)$  באשר באשר  $A\in\mathbb{R}^{n imes n}$  ותהא ותהא  $V\left(G
ight)=n$  אזי  $n\in\mathbb{N}_{+}$  יהי  $n\in\mathbb{N}_{+}$ 

 $.\mathrm{Chol}\left(A\right)^{T}=\mathrm{arg\,MaxCut\text{-}VP}\left(G\right)$  .  $.\nu_{p}\left(\xi\right)=\left\{ \begin{smallmatrix} 1 & \langle \xi,p\rangle\geq 0 \\ -1 & \mathrm{else} \end{smallmatrix} \right. \nu:\mathbb{R}^{n}\times\mathbb{R}^{n}\to\left\{\pm1\right\} \text{ אז: (גדיר }\left\{\pm1\right\}+1 \right\}$  אזי נגדיר  $n\in\mathbb{N}_{+}$  אזי נגדיר  $n\in\mathbb{N}_{+}$  איזי יהי  $n\in\mathbb{N}_{+}$  יהי  $n\in\mathbb{N}_{+}$  יהי  $n\in\mathbb{N}_{+}$  ויהיו  $n\in\mathbb{N}_{+}$  שונים  $n\in\mathbb{N}_{+}$  $\mathbb{P}_{p\in\mathbb{S}^{n-1}}\left(
u_p\left(C_u\left(X
ight)
ight)
eq
u_p\left(C_v\left(X
ight)
ight)=rac{\arccos\left(\left\langle C_u\left(X
ight),C_v\left(X
ight)
ight)
ight)}{\pi}$  אזי  $p\in\mathbb{R}^n$  יהי  $X=rg\operatorname{MaxCut-VP}\left(G
ight)$  באשר  $X\in\mathbb{R}^{n imes n}$  תהא  $X\in\mathbb{R}^{n imes n}$  באשר  $X\in\mathbb{R}^n$  אזי

 $S_{p}(X) = \{v \in V(G) \mid \nu_{p}(C_{u}(X)) = 1\}$ 

אזי  $X=rg\operatorname{MaxCut-VP}\left(G
ight)$  באשר באשר אזי ותהא  $X\in\mathbb{R}^{n imes n}$  ותהא ותהא גרף באשר היי  $n\in\mathbb{N}_{+}$  אזי  $n\in\mathbb{N}_{+}$ 

 $\operatorname{GAP}_{[\rho,1-\arccos(\rho)+\varepsilon]}\operatorname{MaxCut}$ )

כך 3Colorable-VP (G) בעיית G גרף אזי נגדיר יהי G גרף יהי בעיית G

max 1

s.t. 
$$X_{v} \in \mathbb{S}^{|V(G)|-1}$$
 ,  $\forall v \in V(G)$   
 $\langle X_{v}, X_{v} \rangle = 1$  ,  $\forall v \in V(G)$   
 $\langle X_{v}, X_{u} \rangle = -\frac{1}{2}$  ,  $\forall \{u, v\} \in E(G)$ 

3Colorable-VP (G) פיזבילית. גרף 3 גר

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

max 1

s.t. 
$$A \ge 0$$
 
$$A_{v,v} = 1 \qquad , \forall v \in V\left(G\right)$$
 
$$A_{v,u} = -\frac{1}{2} \qquad , \forall \{v,u\} \in E\left(G\right)$$

טענה: יהי  $X \in \mathbb{R}^{n imes n}$  ותהא וער $|V\left(G
ight)| = n$  אזי ארף יהי  $n \in \mathbb{N}_+$  יהי יהי

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

```
.3Colorable-VP (G) אז \operatorname{Chol}(X)^T אז \operatorname{3Colorable-SDP}(G) אם X פתרון פיזבילי של X
                                   אזי R:\mathbb{N}_+	o\mathbb{S}^{|V(G)|-1} אותהא arepsilon\in\mathbb{R}_{\geq 1} יהי גרף S-צביע: יהי אלגוריתם צביעה וקטורית של גרף S-צביע: יהי
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) \to \{\pm 1\}^*
      for v \in V(G) do
            c(v) \leftarrow \left(\nu_{R(i)}(X_v)\right)_{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) \backslash S do
                   if c(v) = c(u) then
                    S \leftarrow S \cup \{v\}
                   end
             end
      end
      c_{\upharpoonright_{V(G[S])}} \leftarrow \texttt{3Colorable-VecCol}(G[S], \varepsilon; R_{\upharpoonright_{\mathbb{N}_{>t}}})
       G צביעה חוקית של 3Colorable-VecCol (G,arepsilon;R) אזי אזי R:\mathbb{N}_+	o\mathbb{S}^{|V(G)|-1} ותהא arepsilon\in\mathbb{R}_{>1} ותהא
                                                    אזי \{u,v\}\in E\left(G
ight) ויהי 3Colorable-VP (G) אזי פענה: יהי G גרף 3־צביע יהי X פתרון פיזבילי של
                                                                                                                                                \mathbb{P}_{p \leftarrow \mathbb{S}^{|V(G)|-1}} \left( \nu_p \left( X_u \right) = \nu_p \left( X_v \right) \right) = \frac{1}{2}
   \mathbb{E}_{R \leftarrow \left(\mathbb{N}_{+} 
ightarrow \mathbb{S}^{|V(G)|-1}
ight)} \left[\mathrm{Time}\left(3\mathrm{Colorable-VecCol}\left(G, arepsilon; R
ight)
ight)
ight] \in \mathrm{poly}\left(|V\left(G
ight)|
ight) איז arepsilon \in \mathbb{R}_{\geq 1} איז arepsilon \in \mathbb{R}_{\geq 1} איז מסקנה: יהי
                                                                                                                            מסקנה: יהי arepsilon גרף \varepsilon \in \mathbb{R}_{>1} קיים אזי קיים גרף 3 גרף מסקנה: יהי
                                              \mathbb{E}_{R \leftarrow \left(\mathbb{N}_{+} \to \mathbb{S}^{|V(G)|-1}\right)}\left[\left|\operatorname{Im}\left(\operatorname{3Colorable-VecCol}\left(G, \varepsilon; R\right)\right)\right|\right] = \mathcal{O}\left(\left|V\left(G\right)\right|^{\log_{3}(2)} \cdot \log\left(\left|V\left(G\right)\right|\right)\right)
                                                                                                               אלגוריתם ויגרדזון לצביעת גרף 3־צביע: יהי אוי ביע אזי אלגוריתם ויגרדזון אדי ארי
Algorithm Wigderson(G):
      n \leftarrow |V(G)|
      if \Delta(G) \leq \sqrt{n} then
       return GreedyColoring (G,\{0,\ldots,\sqrt{n}\}) // Coloring with \sqrt{n}+1 colors
      v \leftarrow \{t \in V(G) \mid \deg(t) \ge \sqrt{n} + 1\}
      c \in (N(v) \cup \{v\}) \to \{\operatorname{Black}_v, \operatorname{Red}_v, \operatorname{Blue}_v\};
      c_{\upharpoonright_{N(v)}} \leftarrow \text{GreedyColoring}\left(G\left[N\left(v\right)\right], \left\{\text{Red}_{v}, \text{Blue}_{v}\right\}\right)
      c' \leftarrow \mathtt{Wigderson}(G[V(G) \setminus (N(v) \cup \{v\})])
      return c \cup c'
                                                                                           .|{
m Im}\left({
m Wigderson}\left(G
ight)|
ight.|=\mathcal{O}\left(\sqrt{|V\left(G
ight)|}
ight) איזי G גרף G־צביע איזי מענה: יהי
         אזי R:\mathbb{N}_+	o\mathbb{S}^{|V(G)|-1} אחזי 	au,arepsilon\in\mathbb{R}_{\geq 1} ותהא זרף T,arepsilon\in\mathbb{R}_{\geq 1} אזי יהי T,arepsilon\in\mathbb{R}_{\geq 1} ותהא אלגוריתם ויגרדזון וקטורי היברידי לצביעת גרף צביע: יהי
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) \ge \tau\}
      c \in (N(v) \cup \{v\}) \to \{\text{Black}_v, \text{Red}_v, \text{Blue}_v\};
                                                                                         c(v) \leftarrow \text{Black}_v
      c_{\upharpoonright_{N(v)}} \leftarrow \text{GreedyColoring}\left(G\left[N\left(v\right)\right], \left\{\text{Red}_{v}, \text{Blue}_{v}\right\}\right)
      c' \leftarrow \mathtt{WigdersonVectorHybrid}(G[V(G) \setminus (N(v) \cup \{v\})], \tau, \varepsilon; R)
      return c \cup c'
                                                                                                      טענה: יהי \varepsilon \in \mathbb{R}_{\geq 1} אזי קיים \tau \in \mathbb{R}_{\geq 1}ויהי ויהי גרף 3־צביע אזי יהי 
                           \mathbb{E}_{R \leftarrow \left(\mathbb{N}_{+} \rightarrow \mathbb{S}^{|V(G)|-1}\right)}\left[|\operatorname{Im}\left(\operatorname{WigdersonVectorHybrid}\left(G, \tau, \varepsilon; R\right)\right)|\right] = \mathcal{O}\left(\frac{|V(G)|}{\tau} + \tau^{\log_{3}(2)} \cdot \log\left(|V(G)|\right)\right)
```

```
מסקנה: יהי lpha=\log_3\left(2
ight) יהי lpha\in\mathbb{R} אי קיים lpha\in\mathbb{R} המקיים באשר lpha=\log_3\left(2
ight) ונגדיר lpha\in\mathbb{R} כך lpha\in\mathbb{R} אי קיים lpha המקיים
                        \mathbb{E}_{R \leftarrow \left(\mathbb{N}_{+} \to \mathbb{S}^{|V(G)|-1}\right)} \left[ \left| \operatorname{Im} \left( \operatorname{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) \right]
                                                   בעיית מינימליות הערך העצמי המקסימלי לפונקציה אפינית: יהיו n,k\in\mathbb{N}_+ ותהיינה A_0\ldots A_k\in\mathbb{R}^{n	imes n} אזי
                                                                                        .MinMaxEigenvalue (A_0 ... A_k) = \min \left\{ \max \left( \operatorname{spec} \left( A_0 + \sum_{i=1}^k A_i x_i \right) \right) \mid x \in \mathbb{R}^k \right\}
                                                                         \dot{\mathcal{A}} באשר \dot{\mathcal{A}} הינו \dot{\mathcal{E}}>0 אזי קיים אלגוריתם פולינומי \dot{\mathcal{A}} באשר \dot{\mathcal{A}} הינו \dot{\mathcal{E}}>0 אזי קיים אלגוריתם פולינומי
                                                                                    lpha\left(G
ight)=\max\left\{\left|I\right|\mid\left(I\subset V\left(G
ight)
ight)\wedge\left(יציבות פנימית של גרף: יהי G גרף אזי Iו בלתי תלויה
                         וכן V\left(G\boxtimes H\right)=V\left(G\right)	imes V\left(H\right) כך אזי באיר אוין אזי נגדיר אוינ מכוונים אזי נגדיר גרף מכוון G\boxtimes H כך
                                                             .E\left(G\boxtimes H\right) = \left\{ \left( \left( u, u' \right), \left( v, v' \right) \right) \in V\left( G\boxtimes H \right)^{2} \; \middle| \; \left( u \in N^{-}\left( v \right) \cup \left\{ v \right\} \right) \wedge \left( u' \in N^{-}\left( v' \right) \cup \left\{ v' \right\} \right) \right\}
                                                                                                              a_n\in\mathbb{N}_{\geq 2} לכל G^{oxtimes n}=G^{oxtimes (n-1)}oxtimes G וכן G וכן G^{oxtimes 1}=G לכל G^{oxtimes 1}
                                                                                                                          \Theta\left(G
ight)=\lim_{k	o\infty}\sqrt[k]{lpha\left(G^{oxtimes k}
ight)} אזי \sqrt[k]{lpha\left(G^{oxtimes k}
ight)} ארף מכוון אזי יהי
                                                                                                                                                             \Theta\left(G
ight)=\sup_{k\in\mathbb{N}_{+}}\sqrt[k]{lpha\left(G^{\boxtimes k}
ight)} אזי מכוון אזי מכוון אזי מכוון אזי
                                                                                                                                                                                                  \Theta\left(G
ight) \geq lpha\left(G
ight) אזי מכוון אזי G יהי יהי
                                                                                                                          וכן V\left(G_{\mathrm{dc}}
ight)=V\left(G
ight) כך כך לא מכוון אזי נגדיר גרף אזי נגדיר מכוון אזי נגדיר גרף אזי מכוון אזי נגדיר גרף אזי מכוון אזי נגדיר גרף איי נגדיר גרף איי נגדיר גרף אזי נגדיר גרף איי נגדיר ג
                                                                                                                           E(G_{dc}) = \{e \in \mathcal{P}_2(V(G)) \mid ((e_1, e_2) \in E(G)) \lor ((e_2, e_1) \in E(G))\}
 \{u,v\}
otin E\left(G_{
m dc}
ight) המקיימים u,v\in V\left(G
ight) באשר לכל R:V\left(G
ight)
ightarrow\mathbb{R}^{d} אזי d\in\mathbb{N}_{+} אזי d\in\mathbb{N}_{+} המקיימים
R_u \perp R_v מתקיים
                       \mathrm{MatMul}\left(\mathbb{F},A,B
ight)=AB אזי B\in\mathbb{F}^{k	imes m} ותהא A\in\mathbb{F}^{n	imes k} ותהא n,k,m\in\mathbb{N}_{+} אזי שדה יהיו
                                                          הערה: בסיבוכיות של אלגוריתמים על מטריצות נתייחס לסיבוכיות כפונקציה של מספר עמודות המטריצה.
                                                                  אזי B\in\mathbb{F}^{k	imes m} ותהא A\in\mathbb{F}^{n	imes k} אזי n,k,m\in\mathbb{N}_+ אדה יהיו שדה יהי\mathbb{F} שדה מטריצות נאיבי: יהי
 Algorithm NaiveMatMul(\mathbb{F}, A, B):
          C \in \mathbb{F}^{n \times m}:
                                                   C \leftarrow 0
          for i \in [1, \ldots, n] do
                   for j \in [1, \ldots, m] do
                           \begin{array}{l} \text{for } \ell \in [1,\ldots,k] \text{ do} \\ \mid \ (C)_{i,j} \leftarrow (C)_{i,j} + (A)_{i,\ell} \cdot (B)_{\ell,j} \end{array}
                   end
           end
          \mathbf{return}\ C
  A\in\mathbb{F}^{k	imes n} ותהא A\in\mathbb{F}^{k	imes n} ותהא A\in\mathbb{F}^{k	imes n} אזי סיבוכיות הריצה של NaiveMatMul טענה: יהי
                                                                 הערה: בסיבוכיות של אלגוריתמים על מספרים נתייחס לסיבוכיות כפונקציה של אורך המספר בבינארי.
                                                                                                                                                                        אזי a,b\in \left\{0,1
ight\}^n ויהיו n\in \mathbb{N} אזי אלגוריתם קרטסובה: יהי
 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 \mathtt{KaratsubaMult}(\alpha, \gamma)
```

 $B \leftarrow \texttt{KaratsubaMult}(\beta, \delta)$ 

 $C \leftarrow \texttt{KaratsubaMult}(\alpha + \beta, \gamma + \delta)$ return  $B \cdot 2^n + (C - B - A) \cdot 2^{\frac{n}{2}} + A$ 

```
כך \mathcal{B}_{n_0}\left(A
ight)\in (\mathbb{F}^{n_0	imes n_0})^{rac{n}{n_0}	imes rac{n}{n_0}} אזי נגדיר A\in \mathbb{F}^{n	imes n} ותהא n_0|n ותהא n_0|n באשר n,n_0\in \mathbb{N}_+ אזי יהי
                                                                                                            .(\mathcal{B}_{n_0}\left(A
ight))_{i,j}=(A)_{((i-1)\cdot n_0,(j-1)\cdot n_0)+[n_0]^2}אלגוריתם סטרסן: יהי A,B\in\mathbb{F}^{2^n	imes 2^n} ותהיינה n\in\mathbb{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}}; \qquad {a \choose c \choose d} \leftarrow \mathcal{B}_{2^{n-1}}(A)
\alpha, \beta, \gamma, \delta \in \mathbb{F}^{2^{n-1}}; \qquad {\alpha \choose \gamma} \xrightarrow{\beta} \leftarrow \mathcal{B}_{2^{n-1}}(B)
M_1 \in \mathbb{F}^{2^{n-1}}; \qquad M_1 \leftarrow \text{Strassen}(\mathbb{F}, a+d, \alpha+\delta)
M_2 \in \mathbb{F}^{2^{n-1}}; \qquad M_2 \leftarrow \text{Strassen}(\mathbb{F}, c+d, \alpha)
       M_3 \in \mathbb{F}^{2^{n-1}}; \qquad M_3 \leftarrow \operatorname{Strassen}(\mathbb{F}, a, \beta - \delta) \ M_4 \in \mathbb{F}^{2^{n-1}}; \qquad M_4 \leftarrow \operatorname{Strassen}(\mathbb{F}, d, \gamma - \alpha) \ M_5 \in \mathbb{F}^{2^{n-1}}; \qquad M_5 \leftarrow \operatorname{Strassen}(\mathbb{F}, a + b, \delta)
                                         M_6 \leftarrow \mathtt{Strassen}(\mathbb{F}, c-a, \alpha+\beta)
       \begin{split} M_7 \in \mathbb{F}^{2^{n-1}}; & M_7 \leftarrow \texttt{Strassen}(\mathbb{F}, b-d, \gamma+\delta) \\ \texttt{return} & \left( \begin{smallmatrix} 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{smallmatrix} \right) \end{split}
                                                             \operatorname{StrassenMatMul}(\mathbb{F},A,B)=AB אזי A,B\in\mathbb{F}^{2^n}	imes 2^n ותהיינה n\in\mathbb{N} שדה יהי \mathbb{F} שדה יהי
                                                                                                                   \mathcal{O}\left(m^{\log_2(7)}\right) הינה StrassenMatMul טענה: סיבוכיות הריצה של
   ec{A_i}=(A)_{(i-1)\%n+1,\lfloorrac{i-1}{2}
floor+1} כך ec{A}\in\mathbb{F}^{nm} כך ec{A}\in\mathbb{F}^{nm} ותהא ec{A}\in\mathbb{F}^{n	imes m} אאי נגדיר ec{A}\in\mathbb{F}^{nm} כך שדה יהיו
                                     (A \circ B)_{i,j} = (A)_{i,j} \cdot (B)_{i,j} \cdot (B)_{i,j} \circ (\mathbb{F}^{n 	imes m})^2 	o \mathbb{F}^{n 	imes m} אזי נגדיר n,m \in \mathbb{N}_+ שדה ויהיו n,m \in \mathbb{N}_+ אזי נגדיר
U,V,W\in\mathbb{F}^{n_0^\omega	imes n_0^2} אלגוריתם בי־לינארי לכפל מטריצות: יהי \mathbb{F} שדה יהיו n_0|n באשר שn,n_0\in\mathbb{N}_+ יהי שדה יהיו יהי שלגוריתם בי־לינארי לכפל מטריצות: יהי
 .BiLinMatMul_{U,V,W}\left(A,B\right)=W^{T}\left(\left(U\overrightarrow{\mathcal{B}_{n_{0}}\left(A\right)}\right)\circ\left(V\overrightarrow{\mathcal{B}_{n_{0}}\left(B\right)}\right)\right) בך BiLinMatMul_{U,V,W}:\left(\mathbb{F}^{n\times n}\right)^{2}\to\mathbb{F}^{n\times n} איי נגדיר
                                \langle u,v,w
angle =\sum_{i=1}^n u_iv_iw_i כך כך כך אזי נגדיר \mathbb{F}^n אזי נגדיר n\in\mathbb{N}_+ אזי נגדיר יהי \mathbb{F} שדה ויהי n\in\mathbb{N}_+
A\in\mathbb{F}^{n	imes m^2} ויהיי A\in\mathbb{F}^{n	imes m^2} אזי A\in\mathbb{F}^{n	imes m^2} תהא n,m\in\mathbb{N}_+ ויהיי n,m\in\mathbb{N}_+ אזי n,m\in\mathbb{N}_+ וותהיינה n,m\in\mathbb{N}_+ שזי n,n_0\in\mathbb{N}_+ באשר n,n_0\in\mathbb{N}_+ ותהיינה n,n_0\in\mathbb{N}_+ אזי n,n_0\in\mathbb{N}_+ משפט: יהי n,n_0\in\mathbb{N}_+ שזי n,n_0\in\mathbb{N}_+ אזי n,n_0\in\mathbb{N}_+
                               \langle U_{i:j'}, V_{j:k'}, W_{k:i'} \rangle = \delta_{i,i'} \cdot \delta_{j,j'} \cdot \delta_{k,k'} מתקיים i,i',j,j',k,k' \in [n_0] הינו אלגוריתם כפל מטריצות)
	ext{BiLinMatMul}_{U,V,W} באשר U,V,W\in\mathbb{F}^{n_0^\omega	imes n_0^2} ותהיינה n_0^\omega\in\mathbb{N} ותהיינה יהיn_0^\omega\in\mathbb{N} באשר n_0^\omega\in\mathbb{N} באשר n_0^\omega\in\mathbb{N}
                                                                                 \mathcal{O}\left(n^{\omega}
ight) הינה Bi\mathrm{LinMatMul}_{U,V,W} של הריצה איז סיבוכיות איז סיבוכיות מטריצות איז הינה
                                                      \mathrm{MatInv}\left(\mathbb{F},A
ight)=A^{-1} הפיכה אזי A\in\mathbb{F}^{n	imes n} ותהא n\in\mathbb{N}_+ יהי שדה יהי \mathbb{F} שדה יהי n\in\mathbb{N}_+
                                                      (T אזי (בעיית \mathrm{MatInv} חשיבה בזמן \mathrm{MatMul} חשיבה בזמן T:\mathbb{N}\to\mathbb{N} משפט: תהא א
                                                               \mathrm{MatDet}\left(\mathbb{F},A
ight)=\det\left(A
ight) אזי A\in\mathbb{F}^{n	imes n} ותהא n\in\mathbb{N}_{+} ותהא שדה יהי\mathbb{F} שדה יהי
                                                     \mathrm{MatDet} חשיבה בזמן \mathrm{MatDet} חשיבה בזמן \mathrm{MatMul} חשיבה בזמן \mathrm{T}:\mathbb{N} \to \mathbb{N}
באשר L,U באשר \mathrm{MatDet}\,(\mathbb{F},A)=L\cdot U אזי אזי בעלת פירוק ותהא A\in\mathbb{F}^{n	imes n} ותהא ותהא n\in\mathbb{N}_+ יהי שדה יהי \mathbb{E} יהי שדה יהי בעיית פירוק
                                                    משפט: תהא \mathbb{N} \to \mathbb{N} אזי (בעיית \mathrm{Mat}\mathrm{-LU} חשיבה בזמן \mathrm{Mat}\mathrm{-LU} חשיבה בזמן \mathrm{Mat}\mathrm{-LU} חשיבה בזמן \mathrm{Mat}\mathrm{-LU}
באשר {
m LinEqSol}\,(A,b)=v אזי איי איי איי בערכת משוואות לינארית: יהי \mathbb{F} שדה יהי n\in\mathbb{N}_+ תהא היהי A\in\mathbb{F}^{n	imes n} באשר
                                                  \mathrm{LinEqSol} חשיבה בזמן \mathrm{MatMul} חשיבה בזמן T:\mathbb{N} \to \mathbb{N} משפט: תהא T:\mathbb{N} \to \mathbb{N} אזי (בעיית
                                                  \mathcal{L}_{\mathbb{F}|\mathcal{F}}[M] = \{M \cdot x \mid x \in \mathcal{F}^k\} אזי M \in \mathbb{F}^{n 	imes k} ותהא n, k \in \mathbb{N}_+ יהיו \mathcal{F} \subseteq \mathbb{F} יהיו שדה יהי
                                                                                                חבורה (G,\mathcal{T}) אזי אזי טופולוגיה על G טופולוגיה חבורה חבורה G אזי חבורה חבורה
```

.(KaratsubaMult  $((a)_2\,,(b)_2))_{10}=ab$  אזי  $a,b\in\mathbb{N}$  טענה: יהיו  $\mathcal{O}\left(n^{\log_2(3)}\right)$  הינה KaratsubaMult טענה: סיבוכיות הריצה של

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

חבורה חבורה נקודות הצטברות. באשר G חסרת נקודות הצטברות. חבורה חבורה

```
חוג דיסקרטי: חוג (R,+,*) באשר (R,+,*) הינה חבורה דיסקרטית.
        \mathrm{dim}\left(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]
ight)=k אאי M\in\mathbb{F}^{n	imes k} מדרגה M\in\mathbb{F}^{n	imes k} מדרגה M\in\mathbb{F}^{n	imes k} מדרגה M\in\mathbb{F}^{n	imes k}
      \mathrm{basis}\left(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]
ight)=M מדרגה k מדרגה M\in\mathbb{F}^{n	imes k} ותהא n,k\in\mathbb{N}_+ ותהא חוג דיסקטי היי \mathcal{F}\subseteq\mathbb{F} חוג דיסקטי היי חוג דיסקטי חוג אזי
                                                                                 \mathcal{L}\left[M
ight]=\mathcal{L}_{\mathbb{R}|\mathbb{Z}}\left[M
ight] אזי M\in\mathbb{R}^{n	imes k} ותהא n,k\in\mathbb{N}_{+} אזי יהיו
                                                                                                           סריג אבסטרקטי: יהיו k,n\in\mathbb{N}_+ ותהא אזי \mathcal{L}\subseteq\mathbb{R}^n אזי איזי באשר
                                                                                                                                                      x-y\in\mathcal{L} מתקיים x,y\in\mathcal{L} •
                                                                                                                             \max\{|V| \mid (V \subseteq \mathcal{L}) \land (V) \cap V\} = k \bullet
                                                                                                                                             B_r(0) \cap \mathcal{L} = \{0\} המקיים r > 0 היים •
                               \dim(\mathcal{L},k)=k מימד של סריג אבסטרקטי: יהיו k,n\in\mathbb{N}_+ ותהא ותהא של סריג אבטרקטי: יהיו אריג k,n\in\mathbb{N}_+ ותהא
                                                                                                                          \mathcal{L} = (\mathcal{L}, k) סריג אבסטרקטי אזי נסמן (\mathcal{L}, k) הערה: יהי
                                                        \|v\| \leq \|u\| מתקיים u \in \mathcal{L} \setminus \{0\} עבורו לכל v \in \mathcal{L} \setminus \{0\} מתקיים אזי קיים למה: יהי
M\in\mathbb{R}^{n	imes k} מדרגה M\in\mathbb{R}^n מדרגה M\in\mathbb{R}^n משפט: יהיו איזי (\mathcal{L},k) אזי (\mathcal{L},k) אזי (\mathcal{L},k) אזי איזי (\mathcal{L},k) אזי איזי (\mathcal{L},k) אזי משפט: יהיו
מסקנה: יהי M\in\mathbb{R}^{n	imes n} ותהא איי (L\subseteq\mathbb{R}^n אזי בעלת וקטורים בעלת n הפיכה עבורה איי חבורה L אזי וותהא איי וותהא הפיכה עבורה איי
                                                                                                                                                                                                      \mathcal{L} = \mathcal{L}[M]
                                   A,B\in\mathbb{R}^{n	imes n} ותהיינה A,B\in\mathbb{R}^{n	imes n} ותהיינה A,B\in\mathbb{R}^{n	imes n} ותהיינה n\in\mathbb{N}_+ יהי
                                                  כך \Phi^+_{i,j,a}:\mathbb{R}^{n	imes n}	o\mathbb{R}^{n	imes n} אזי נגדיר עמודות: יהי n\in\mathbb{N}_+ יהיו i,j\in[n] שונים ויהי n\in\mathbb{N}_+ אזי נגדיר
                                                                                                                                                        \Phi_{i,j,a}^+(M) = M + a \cdot \left(C_i(M) \cdot e_i^T\right)
                                                                     כך \Phi_{i,j}^{\leftrightarrow}:\mathbb{R}^{n	imes n}	o\mathbb{R}^{n	imes n} כך שונים אזי נגדיר n\in\mathbb{N}_+ יהי כך החלפת עמודות: יהי
                                                                                                             \Phi_{i,j}^{\leftrightarrow}\left(M\right) = M + C_{j}\left(M\right) \cdot \left(e_{i} - e_{j}\right)^{T} + C_{i}\left(M\right) \cdot \left(e_{j} - e_{i}\right)^{T}
                         \Phi_i^-(M)=M-2\cdot \left(C_i\left(M
ight)\cdot e_i^T
ight) כך \Phi_i^-:\mathbb{R}^{n	imes n}	o\mathbb{R}^{n	imes n} אזי נגדיר i\in[n] אזי נגדיר ויהי n\in\mathbb{N}_+ יהי יהי n\in\mathbb{N}_+ יהי
                    טרנספורמציות אלמנטריות: יהי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ טרנספורמציות אלמנטריות: יהי n\in\mathbb{N}_+ הפיכה ותהא n\in\mathbb{N}_+ טרנספורמציה אלמנטרית אזי n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ הפיכה ותהא n\in\mathbb{N}_+ טרנספורמציה אלמנטרית אזי n\in\mathbb{N}_+
משפט: יהי \mathbb{N}_+ ותהיינה A,B\in\mathbb{R}^{n	imes n} הפיכות אזי (\mathcal{L}[A]=\mathcal{L}[B]) משפט: יהי A,B\in\mathbb{R}^{n	imes n} ותהיינה
                                                                                                                                                (A = (\varphi \circ \ldots \circ \varphi_m)(B) עבורן \varphi_1 \ldots \varphi_m
                                                                            \mathcal{L}^ee = \{v \in \mathrm{span}\,(\mathcal{L}) \mid \forall v \in \mathcal{L} : \langle u,v 
angle \in \mathbb{Z} \} הסריג הדואלי: יהי \mathcal{L} סריג ממשי אזי
                                                                                                                                               .טענה: יהי \mathcal{L} סריג ממשי אזי \mathcal{L}^{\vee} סריג ממשי
                                                                                                                                                    (\mathcal{L}^{ee})^{ee}=\mathcal{L} טענה: יהי \mathcal{L} סריג ממשי אזי
                                                                                            M^ee = M^{-T} מטריצה דואלית: יהי n \in \mathbb{N}_+ ותהא ותהא תואלית: יהי
                                                                                                             M \in \mathbb{R}^{n 	imes n} ותהא M \in \mathbb{R}^{n 	imes n} ותהא ותהא n \in \mathbb{N}_+ יהי
                                                                                                    \mathcal{L}\left[M
ight]^ee=\mathcal{L}\left[M^ee
ight] הפיכה אזי M\in\mathbb{R}^{n	imes n} ותהא ותהא n\in\mathbb{N}_+ יהי
                                                                                            q\cdot\mathcal{L}=\{q\cdot v\mid v\in\mathcal{L}\} אזי q\in\mathbb{R}_{>0} סריג ממשי ויהי סריג: יהי
                                                                                     q\cdot\mathcal{L}\left[M
ight]=\mathcal{L}\left[q\cdot M
ight] אזי k מדרגה k מדרגה אות אk,n\in\mathbb{N}_{+} יהיו טענה: יהיו
                                                                                                             (q\cdot\mathcal{L})^ee = q^{-1}\cdot\mathcal{L}^ee אזי q\in\mathbb{R}_{>0} טענה: יהי \mathcal{L} סריג ממשי ויהי
                           \mathrm{MatInd} = \{\langle \mathbb{F}, M \rangle \mid (\mathsf{n} + \mathbb{F}) \land (n, k \in \mathbb{N}_+) \land (M \in \mathbb{F}^{n 	imes k}) \land (k \; \mathsf{atrice} \; M) \} בעיית מלאות דרגת מטריצה: \{(\mathbb{F}, M) \mid (n, k \in \mathbb{N}_+) \land (M \in \mathbb{F}^{n 	imes k}) \land (k \; \mathsf{atrice} \; M) \}
              \operatorname{LatIn} = \left\{ \langle M, v 
angle \mid (n, k \in \mathbb{N}_+) \land \left(M \in \mathbb{R}^{n 	imes k} 
ight) \land (k \; 	ext{atra} \; M) \land (v \in \mathcal{L}\left[M
ight]) 
ight\} בעיית שייכות לסריג בהינתן בסיס:
                       \operatorname{LatInc} = \left\{ \langle A, B \rangle \; \middle| \; (n, k, m \in \mathbb{N}_+) \land \left( egin{array}{c} A \in \mathbb{R}^{n \times k} \\ B \in \mathbb{R}^{n \times m} \end{array} \right) \land \left( egin{array}{c} k \text{ atran } A \\ m \text{ atran } B \end{array} \right) \land \left( \mathcal{L}\left[A\right] \subseteq \mathcal{L}\left[B\right] \right) \right\} בעיית ההכלה של סריג: B \in \mathbb{R}^{n \times m} מדרגה A \in \mathbb{R}^{n \times k} תהא A \in \mathbb{R}^{n \times k} מדרגה אזי A \in \mathbb{R}^{n \times k} מדרגה אזי
                                                                                                                                        .LatInterBasis (A, B) = basis (\mathcal{L}[A] \cap \mathcal{L}[B])
                                                                                                                               .MatInd, LatIn, LatInc, LatInterBasis \in \mathcal{P} משפט:
                                                                                  \mathcal{P}\left[M
ight]=\mathcal{L}_{\mathbb{R}|[0,1)}\left[M
ight] אזי M\in\mathbb{R}^{n	imes k} ותהא n,k\in\mathbb{N}_{+} יהיו יהיו
                       \|A\cdot a\|_{\mathcal{P}[M]}=M\cdot \|a\| אזי אזי a\in \mathbb{R}^k מדרגה k ויהי מקבילון היסודי: יהיו n,k\in \mathbb{N}_+ תהא n,k\in \mathbb{N}_+
                                    \|v\|_{\mathcal{P}[M]}=rg\min_{u\in\mathcal{L}[M]}\left(\|v-u\|
ight) אזי v\in\mathbb{R}^k מדרגה M\in\mathbb{R}^{n	imes k} תהא n,k\in\mathbb{N}_+ יהיו יהיו
            (v \mod \mathcal{P}[M]) = v - \lfloor v 
floor_{\mathcal{P}[M]} אזי v \in \mathbb{R}^k מדרגה k ויהי ויהי m \in \mathbb{R}^{n 	imes k} תהא n, k \in \mathbb{N}_+ יהיו
                                                        M\in\mathbb{R}^{n	imes k} מדרגה v\in\mathbb{R}^k אזי M\in\mathbb{R}^{n	imes k} תהא n,k\in\mathbb{N}_+ יהיי יהיו n,k\in\mathbb{N}_+ מדרגה אויהי
        \mathcal{L}[A]=\mathcal{L}[B]) \Longleftrightarrow (\mathcal{P}[B]\cap \mathcal{L}[A]=\{0\}) איי \mathcal{L}[B]\subseteq \mathcal{L}[A] הפיכות באשר A,B\in \mathbb{R}^{n	imes n} ותהיינה n\in \mathbb{N}_+ ותהיינה n\in \mathbb{N}_+
```

```
.\mathrm{Vol}\left(\mathcal{P}\left[M
ight]
ight)=\left|\det\left(M
ight)
ight| אזי הפיכה M\in\mathbb{R}^{n	imes n} ותהא ותהא n\in\mathbb{N}_{+} יהי
```

 $|\det{(A)}| = |\det{(B)}|$  אזי  $\mathcal{L}[B] = \mathcal{L}[A]$  מסקנה: יהי  $n \in \mathbb{N}_+$  אזי ותהיינה  $n \in \mathbb{N}_+$  ותהיינה

 $\det\left(\mathcal{L}\left[M
ight]
ight)=\mathrm{Vol}\left(\mathcal{P}\left[M
ight]
ight)$  הפיכה אזי  $M\in\mathbb{R}^{n imes n}$  ותהא ותהא  $n\in\mathbb{N}_{+}$  יהי

 $\mathrm{LatDet}\left(M
ight)=\det\left(\mathcal{L}\left[M
ight]
ight)$  הפיכה אזי  $M\in\mathbb{R}^{n imes n}$  ותהא ותהא חדטרמיננטה של סריג: יהי  $n\in\mathbb{N}_{+}$  יהי

 $. Lat Det \in \mathcal{P}$  :מסקנה

 $\lim_{r o\infty}rac{|\mathcal{L}\cap B_r(0)|}{ ext{Vol}(B_r(0))}=rac{1}{\det(\mathcal{L})}$  אזי אחי סענה: יהי  $\mathcal{L}$  סענה: יהי

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

 $.\lambda_i\left[\mathcal{L}
ight]=\inf\left\{r\geq 0\mid \dim \mathrm{span}\left(B_r\left(0
ight)\cap\mathcal{L}
ight)\geq i
ight\}$  אזי  $i\in[k]$  אזי ממשי מדרגה k סריג ממשי מדרגה  $k\in\mathbb{N}_+$  יהי אוי המקיימים  $u_1^\perp,\ldots,u_n^\perp\in\mathbb{R}^n$  בסיס אזי  $u_1^\perp,\ldots,u_n^\perp\in\mathbb{N}_+$  המקיימים אורתונורמליזציה: יהי  $n\in\mathbb{N}_+$  וויהיו  $n\in\mathbb{N}_+$  וויהיו

- בסיס אורתונורמלי.  $\{u_1^\perp,\ldots,u_n^\perp\}$  •
- $.u_i^\perp\in \mathrm{span}\,(u_1\ldots u_i)\, ackslash \mathrm{span}\,(u_1\ldots u_{i-1})$  מתקיים  $i\in [n]$  לכל

 $u_1\dots u_n$  טענה: יהי  $\mathbb{N}_+$  ויהיו  $n\in\mathbb{N}_+$  ויהיו  $u_1\dots u_n$  באשר  $u_1\dots u_n$  באשר בסיס אזי קיימת ויחידה אורתונורמליזציה  $u_1\dots u_n\in\mathbb{R}^n$  ותהא  $u_1\dots u_n\in\mathbb{N}_+$  הפיכה אזי  $u_1\dots u_n\in\mathbb{N}_+$  המקיימת  $u_1\dots u_n\in\mathbb{N}_+$  לכל  $u_1\dots u_n\in\mathbb{N}_+$  הוא האורתונורמליזציה: יהי  $u_1\dots u_n\in\mathbb{N}_+$  ותהא  $u_1\dots u_n\in\mathbb{N}_+$  הפיכה אזי  $u_1\dots u_n\in\mathbb{N}_+$  המקיימת  $u_1\dots u_n\in\mathbb{N}_+$  לכל  $u_1\dots u_n\in\mathbb{N}_+$  הוא האורתונורמליזציה: יהי  $u_1\dots u_n\in\mathbb{N}_+$  ותהא  $u_1\dots u_n\in\mathbb{N}_+$  הפיכה אזי  $u_1\dots u_n\in\mathbb{N}_+$  המקיימת  $u_1\dots u_n\in\mathbb{N}_+$  לכל  $u_1\dots u_n\in\mathbb{N}_+$  המקיימת  $u_1\dots u_n\in\mathbb{N}_+$  האורתונורמליזציה: יהי  $u_1\dots u_n\in\mathbb{N}_+$  ותהא  $u_1\dots u_n\in\mathbb{N}_+$  הפיכה אזי  $u_1\dots u_n\in\mathbb{N}_+$  המקיימת  $u_1\dots u_n\in\mathbb{N}_+$ 

 $\lambda_{1}\left[\mathcal{L}\left[M
ight]
ight]\geq\min_{i\in\left[n
ight]}\left|\left\langle C_{i}\left(M
ight),C_{i}\left(M^{\perp}
ight)
ight
angle 
ight|$  הפיכה אזי  $M\in\mathbb{R}^{n imes n}$  ותהא  $n\in\mathbb{N}_{+}$  יהי הי

n מדרגה מלאה: יהי  $n\in\mathbb{N}_+$  אזי סריג ממשי סריג מדרגה מלאה: יהי

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

וכן  $\mathcal{L}=\mathcal{L}[M]$  מדרגה k מדרגה  $M\in\mathbb{R}^{n imes k}$  אזי  $M\in\mathbb{R}^{n imes k}$  ווהי  $n,k\in\mathbb{N}_+$  ויהי  $n,k\in\mathbb{N}_+$  ויהי יהיו  $n,k\in\mathbb{N}_+$  לכל  $i\in[n]$  לכל  $\|C_i(M)\|=\lambda_i[\mathcal{L}]$ 

. שריג סטנדרטי: יהי עוקבים מינימליים. מדרגה מלאה אזי סריג  $n\in\mathbb{N}_+$  יהי יהי יהי סריג מינימליים.

. טענה: יהי אינו סריג סטנדרטי באשר  $\mathcal L$  אינו סריג סריג סטנדרטי יהי יהי יהי אינו יהי יהי אזי סיים סריג מדרגה מלאה והי

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

וכן  $\|C_2\left(B\right)\| \leq \|C_1\left(B\right) + C_2\left(B\right)\|$  וכן  $\|C_1\left(B\right)\| \leq \|C_1\left(B\right)\| \leq \|C_2\left(B\right)\|$  של  $\mathcal{L}$  המקיים של  $\mathcal{L}$  המקיים  $\|C_2\left(B\right)\| \leq \|C_1\left(B\right) - C_2\left(B\right)\|$  וכן  $\|C_2\left(B\right)\| \leq \|C_1\left(B\right) - C_2\left(B\right)\|$ 

Bטענה: יהי B סינ מדרגה B ויהי ויהי B בסיס של B אזי וויהי B בסיס של ויהי B ויהי B טענה: יהי B סינ מינימליים).

אזי  $\mathcal L$  אזי בסיס של B ויהי ויהי  $\mathcal L$  יהי יהי לגראנז': יהי אלגוריתם לגראנז': יהי

Algorithm Lagrange (B):

```
\label{eq:continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous_continuous
```

 $\mathcal{L}$  בסיס מופחת של Lagrange (B) עוצר אזי בסיס של בסיס של בסיס של בסיס בסיט ענה: יהי  $\mathcal{L}$  סענה:  $\mathcal{L}$  סריג מדרגה  $\mathcal{L}$  ויהי בסיס של בסיס  $\mathcal{L}$  בחים בסיס מופחת של  $\mathcal{L}$  בסיס מופחת של בסיס מופחת ב

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

 $u,v\in S$  משפט אזי קיימים  $\mathrm{Vol}\left(S
ight)>\det\left(\mathcal{L}
ight)$  משפט בליכפלדט: יהי  $n\in\mathbb{N}_{+}$  יהי יהי  $n\in\mathbb{N}_{+}$  יהי שונים עבורם  $u,v\in S$ 

S=-S המקיימת  $S\subseteq\mathbb{R}^n$  המורה קבוצה קבוצה יהי יהי יהי יהי לראשית: יהי לראשית:

משפט הגוף הקמור של מינקובטקי: יהי  $n\in\mathbb{N}_+$  יהי יהי קבוצה קמורה חותהא אות משפט הגוף הקמור יהי יהי  $n\in\mathbb{N}_+$  יהי יהי אזי  $S\subseteq\mathbb{R}^n$  אזי  $S\subseteq\mathbb{R}^n$  אזי  $S=\mathbb{R}^n$  אזי  $S=\mathbb{R}^n$  אזי  $S=\mathbb{R}^n$  אזי  $S=\mathbb{R}^n$  אזי אזי  $S=\mathbb{R}^n$ 

אליפטואיד של סריג:  $u_i \| = \lambda_i [\mathcal{L}]$  איז של סריג: יהי  $n \in \mathbb{N}_+$  יהי  $n \in \mathbb{N}_+$  יהי איז איז  $u_i \| = \lambda_i [\mathcal{L}]$  איז איז שליפטואיד של סריג: יהי  $u_i \| = \lambda_i [\mathcal{L}]$  איז סריג מדרגה מלאה  $v_i \| = \lambda_i [\mathcal{L}]$  באשר  $v_i \| = \lambda_i [\mathcal{L}]$  לכל  $v_i \| = \lambda_i [\mathcal{L}]$ 

 $\mathcal{E}_{\mathcal{L}}\cap\mathcal{L}=\{0\}$  אזי  $i\in[n]$  לכל  $\|u_i\|=\lambda_i\left[\mathcal{L}
ight]$  באשר באשר  $u_1\ldots u_n\in\mathcal{L}$  אזי  $u_i$  אזי  $u_i\in\mathbb{N}_+$  היהי  $u_i\in\mathbb{N}_+$  יהי  $u_i\in\mathbb{N}_+$  למה:

```
\widehat{h}(\omega) = e^{2\pi i \cdot \langle w, z \rangle} \cdot \widehat{f}(\omega)
מתקיים \omega\in\mathbb{R}^n אזי לכל h\left(x
ight)=f\left(\lambda x
ight) כך h:\mathbb{R}^n	o\mathbb{R} ונגדיר \lambda\in\mathbb{R} יהי h\in L^1\left(\mathbb{R}^n
ight) אזי לכל n\in\mathbb{N}_+ מתקיים
                                                                                                                                                                                                                                                         \hat{h}(\omega) = \frac{1}{\lambda^n} \cdot \hat{f}(\frac{\omega}{\lambda})
מתקיים \omega\in\mathbb{R}^n אזי לכל h\left(x
ight)=\prod_{i=1}^nf_i\left(x_i
ight) כך h:\mathbb{R}^n	o\mathbb{R} אזי לכל f_1\dots f_n\in L^1(\mathbb{R}) אזי לכל n\in\mathbb{N}_+ מתקיים
                                                                                                                                                                                                                                                    \hat{h}(\omega) = \prod_{i=1}^{n} \hat{f}_i(\omega_i)
                                                       \mathcal{N}_{n}\left[\sigma
ight](x)=rac{1}{(2\pi)^{rac{n}{2}}\cdot\sigma^{n}}\cdot e^{-rac{1}{2\sigma^{2}}\cdot\|x\|^{2}} כך \mathcal{N}_{n}\left[\sigma
ight]:\mathbb{R}^{n}	o\mathbb{R} אזי נגדיר \sigma\in\mathbb{R} אזי נגדיר \sigma\in\mathbb{R} אזי נגדיר \sigma\in\mathbb{R}
                                                      \widehat{\mathcal{N}_n[\sigma]} = \left(rac{\sqrt{2\pi}}{\sigma}
ight)^n\cdot\mathcal{N}_n\left[rac{1}{\sigma}
ight] איזי n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+
                                         \mathcal{S}\left(\mathbb{R}^n,A\right)=\left\{f\in C^\infty\left(\mathbb{R}^n,A\right)\ \middle|\ orall lpha,eta\in\mathbb{N}^n:\|f\|_{lpha,eta}<\infty
ight\} אזי A\subseteq\mathbb{C} אורץ: יהי n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+ אזי מענה נוסחאת הסכימה של פואסון: יהי n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ ויהי n\in\mathbb{N}_+ סריג מדרגה מלאה 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{R} המקיים r\in\mathbb{R} אזי קיים arepsilon>0 המקיים משפט: יהי n\in\mathbb{N}_+ יהי
                                                                                                                                                                                         \mathbb{P}_{v \sim \mathcal{N}_n[\lambda_n[\mathcal{L}] \cdot r]} \left( v \notin B_{\lambda_n[\mathcal{L}]} \left( 0 \right) \mid v \in \mathcal{L}^{\vee} \right) \le \varepsilon
                                         כך \pi_{\pm u}:\mathbb{R}^n	o\mathbb{R}^n אזי נגדיר u\in\mathcal{L} אזי מדרגה מלאה n\in\mathbb{N}_+ יהי יהי n\in\mathbb{N}_+ יהי לוקטור על וקטור על וקטור יהי
                                                                                                                                                                                                                                               .\pi_{\perp u}\left(v\right) = v - \frac{\langle u, v \rangle}{\|u\|^2} \cdot u
                                                              \mathcal{L}_{\perp u} = \{\pi_{\perp u}\left(v
ight) \mid v \in \mathcal{L}\} אזי u \in \mathcal{L} אזי u \in \mathcal{L} הטלה של סריג על וקטור: יהי
                                                                             n-1 טענה: יהי \mathcal{L}_{\pm u} סריג מדרגה מלאה n ויהי n\in\mathbb{N}_{\pm} אזי n\in\mathbb{N}_{\pm} סריג ממשי מדרגה n
                                                             בסיס KZ בסיס M\in\mathbb{R}^{n	imes n} אזי n\in\mathbb{R}_+ המקיימת המקיימת יהי M\in\mathbb{R}^n ביסיס
                                                                                                                                                                                                                                                               \mathcal{L} = \mathcal{L}[M] \bullet
                                                                                                                                                                                                                                          ||C_1(M)|| = \lambda_1[\mathcal{L}] \bullet
                                                                          \mathcal{L}_{\perp C_{1}(M)} הינו בסיס קורקין־זולוטרב עבור \pi_{\perp C_{1}(M)}\left(C_{2}\left(M\right)\right),\ldots,\pi_{\perp C_{1}(M)}\left(C_{n}\left(M\right)\right)
                                                                                                             \left.\left|\left\langle C_{i}\left(M\right),C_{1}\left(M^{\perp}\right)\right
ight
angle
ight|\leq\frac{1}{2}\left|\left\langle C_{1}\left(M\right),C_{1}\left(M^{\perp}\right)
ight
angle מתקיים i\in\left[n\right] לכל
                                                                                                                                                                    \mathcal{L}ל־\mathrm{KZ} לים בסיס משפט: יהי \mathcal{L} סריג מדרגה מלאה אזי קיים בסיס
טענה: יהי \mathcal L סריג מדרגה מלאה M \in \mathbb R^{n 	imes n} באשר בשר אזי M \in \mathbb R^n אזי אזי M \in \mathbb R^n אם הבאים אזי n \in \mathbb R_+ יהי n \in \mathbb R_+ יהי
                                                                                                                                                                                                                                                                                   מתקיימים
                        .\left\langle C_{i}\left(M\right),C_{i}\left(M^{\perp}\right)\right\rangle \cdot C_{i}\left(M^{\perp}\right)=\arg\min\left\{\left\Vert v\right\Vert \;\middle|\; v\in\pi_{\mathrm{span}^{\perp}\left(C_{1}\left(M\right),\ldots,C_{i-1}\left(M\right)\right)}\left(\mathcal{L}\right)\right\} מתקיים i\in\left[n\right] לכל •
                                                                          |\langle C_i(M), C_j(M^\perp) \rangle| \leq \frac{1}{2} |\langle C_j(M), C_j(M^\perp) \rangle| מתקיים j < i באשר i, j \in [n] לכל •
                                                                                                    טענה: יהי M\in\mathbb{R}^{n	imes n} בסיס אזי מדרגה מלאה n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+ יהי יהי n\in\mathbb{N}_+ יהי
                                                                                                                                                             \left|\left\langle C_{i}\left(M\right),C_{i}\left(M^{\perp}\right)\right
ight
angle \right|\leq\lambda_{i}\left[\mathcal{L}\right] מתקיים i\in\left[n\right] לכל
                                                                                                              .\left|\left\langle C_{i}\left(M
ight),C_{i}\left(M^{\perp}
ight)
ight
angle 
ight|\leq\left\|C_{l}\left(M
ight)
ight\| מתקיים j\geq i באשר i,j\in\left[n\right] לכל •
                                     . \frac{1}{\sqrt{\frac{i-1}{4}+1}}\cdot\|C_i\left(M
ight)\|\leq \lambda_i\left[\mathcal{L}
ight]\leq \sqrt{\frac{i-1}{4}+1}\cdot\|C_i\left(M
ight)\| מטריצה מצומצמת בומצמת LLL לנסטרה־לנסטרה־לובאס (1982): יהי n\in\mathbb{N}_+ ויהי בומצמת M\in\mathbb{R}^{n	imes n}
                            \left.\left|\left\langle C_{j}\left(M
ight),C_{j}\left(M^{\perp}
ight)
ight
angle
ight|\geq2\left|\left\langle C_{i}\left(M
ight),C_{j}\left(M^{\perp}
ight)
ight
angle
ight| מתקיים j< i מתקיים j< i באשר באשר לכל •
```

 $\delta\left\langle C_{i}\left(M
ight),C_{i}\left(M^{\perp}
ight)
ight
angle ^{2}\leq\left\langle C_{i+1}\left(M
ight),C_{i}\left(M^{\perp}
ight)
ight
angle ^{2}+\left\langle C_{i+1}\left(M
ight),C_{i+1}\left(M^{\perp}
ight)
ight
angle ^{2}$ מתקיים  $i\in\left[n-1
ight]$  מתקיים  $i\in\left[n-1
ight]$ 

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

טענה: יהי  $\delta$ -LLL מצומצמת  $M\in\mathbb{R}^{n imes n}$  ותהא  $\delta\in(rac{1}{4},1)$  יהי  $n\in\mathbb{N}_+$  יהי יהי  $n\in\mathbb{N}_+$ 

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

 $\prod_{i=1}^n \lambda_i \left[\mathcal{L}
ight] \leq 2^n \cdot rac{\det(\mathcal{L})}{\operatorname{Vol}(B_1(0))}$  אזי משפט מינקובסקי השני: יהי  $n \in \mathbb{N}_+$  יהי יהי מדרגה מלאה מינקובסקי השני:

 $\lambda_1\left[\mathcal{L}
ight] \leq \left(\det\left(\mathcal{L}
ight)
ight)^{rac{1}{n}}\cdot\sqrt{n}$  אזי n אזי  $n\in\mathbb{N}_+$  ויהי ויהי  $n\in\mathbb{N}_+$  ויהי מסקנה משפט מינקובסקי הראשון: יהי

 $\hat{f}(\omega)=\int_{\mathbb{R}^n}f\left(x
ight)e^{-2\pi i\cdot\langle x,\omega
angle}\mathrm{d}x$  כך כך  $\hat{f}:\mathbb{R} o\mathbb{R}$  אזי נגדיר  $f\in L^1\left(\mathbb{R}^n
ight)$  ותהא  $n\in\mathbb{N}_+$  ותהא

סענה: יהי  $h\left(x
ight)=f\left(x+z
ight)$  כך  $h:\mathbb{R}^{n} o\mathbb{R}$  כן ונגדיר  $z\in\mathbb{R}^{n}$  יהי  $f\in L^{1}\left(\mathbb{R}^{n}
ight)$  אזי לכל  $n\in\mathbb{N}_{+}$  יהי הי  $n\in\mathbb{N}_{+}$  יהי

```
Algorithm LLL-Algo (\delta, M):
       while True do
              M^{\perp} \leftarrow \text{Orthonormalization}(M)
               for i \leftarrow [2, \ldots, n] do
                     end
               f \leftarrow \text{True};
                                      i \leftarrow 1
               while (i \le n) \land (f = \text{True}) do
                      \begin{array}{l} \text{if } \delta \left\langle C_{i}\left(M\right), C_{i}\left(M^{\perp}\right)\right\rangle^{2} > \left\langle C_{i+1}\left(M\right), C_{i}\left(M^{\perp}\right)\right\rangle^{2} + \left\langle C_{i+1}\left(M\right), C_{i+1}\left(M^{\perp}\right)\right\rangle^{2} \text{ then } \\ \mid \left(C_{i}\left(M\right), C_{i+1}\left(M\right)\right) \leftarrow \left(C_{i+1}\left(M\right), C_{i}\left(M\right)\right) \end{array} 
               if f = \text{True} then return M
       end
                                                1\leq\mathcal{DD}\left[M
ight]\leq\left(\max_{i\in\left[n
ight]}\left\Vert C_{i}\left(M
ight)
ight\Vert 
ight)^{rac{n(n+1)}{2}} אזי M\in\mathbb{Z}^{n	imes n} ותהא n\in\mathbb{N}_{+} יהי יהי n\in\mathbb{N}_{+}
M \in \mathbb{R}^{n 	imes n} באשר S' באשר ברוצת LLL-Algo טענה: יהי S,S' הפיכה ויהיו הפיכה M \in \mathbb{R}^{n 	imes n} תהא \delta \in \left(rac{1}{4},1\right) יהי n \in \mathbb{N}_+ יהי
                                                                                                                                                                               S'(M) < \sqrt{\delta} \cdot S(M) על S אזי
                                                                                                                                       \operatorname{poly}(n) הינה LLL-Algo מסקנה: סיבוכיות הריצה של
                                                                         \mu\left(\mathcal{L}
ight)=\max_{t\in\mathbb{R}^n}\mathrm{dist}\left(t,\mathcal{L}
ight) אזי מדרגה מלאה n ויהי n\in\mathbb{N}_+ ויהי חייהי מדרגה מלאה n\in\mathbb{N}_+
                                                                                                           1, rac{1}{2}\lambda_n\left[\mathcal{L}
ight] \leq \mu\left(\mathcal{L}
ight) אזי n \in \mathbb{N}_+ יהי חיהי n \in \mathbb{N}_+ יהי טענה: יהי
             ויהי \delta	ext{-LLL} ויהי \delta	ext{-LLL} ויהי \delta\in\mathbb{R}^n אזי הפיכה מצומצמת הפיכה M\in\mathbb{R}^{n	imes n} תהא היהי \delta\in(rac{1}{4},1) ויהי \delta\in(rac{1}{4},1)
Algorithm Babai_{\delta}(M,t):
      v \in \mathbb{R}^n;
                            v \leftarrow 0
       M^{\perp} \leftarrow \text{Orthonormalization}(M)
       for i \in [n, \ldots, 1] do
            k \leftarrow \left| \langle t, C_i \left( M^{\perp} \right) \rangle \right|
       return v
                                                      \mathrm{poly}\,(n) הינה \mathrm{Babai}_\delta אזי סיבוכיות הריצה של \delta\in\left(\frac{1}{4},1\right) אזי סיבוכיות הריצה של \delta\in\left(\frac{1}{4},1\right) הינה \mu\left(\mathcal{L}\left[M\right]\right)\leq\frac{1}{2}\sqrt{\sum_{i=1}^{n}\left\langle C_i\left(M\right),C_i\left(M^{\perp}\right)\right\rangle^2} הפיכה אזי M\in\mathbb{R}^{n\times n} ותהא n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+
                                                                                                    \mu(\mathcal{L}) \leq rac{\sqrt{n}}{2} \lambda_n \, [\mathcal{L}] אזי אזי חברגה מדרגה טריג מדרגה n \in \mathbb{N}_+ יהי יהי מסקנה:
                                                                                          טענה: יהי \frac{3}{4}\text{-LLL} הפיכה מצומצמת הפיכה תהא n\in\mathbb{R}^n ויהי יהי אזיי ויהי יהי
                                           . \left\| t - \mathrm{Babai}_{\frac{3}{4}} \left( M, t \right) \right\| \leq 2^{\frac{n}{2} - 1} \left| \left\langle C_n \left( M \right), C_n \left( M^\perp \right) \right\rangle \right| ערך של סריג: יהי M \in \mathbb{F}^n חוג דיסקרטי יהי n \in \mathbb{N}_+ תהא n \in \mathbb{F}^n הפיכה ויהי n \in \mathbb{F}^n אזי
```

 $t\in\mathbb{F}^n$  הפיכה היה  $M\in\mathbb{F}^{n imes n}$  תהא תיפוש הוקטור הקרוב ביותר בסריג: יהי  $\mathbb{F}$  שדה יהי הי $\mathcal{F}\subseteq\mathbb{F}$  חוג דיסקרטי יהי  $m\in\mathbb{F}^n$  תהא הפיכה הפיכה יהי  $m\in\mathbb{F}^n$  הפיכה יהי  $m\in\mathbb{F}^n$  וכן באור בסריג: יהי  $mv-t\|\leq \varepsilon$  באשר בסריג: יהי  $mv-t\|\leq \varepsilon$  באשר בסריג: יהי בסריג: יהי של בסריג: יהי בסריג:

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

```
הפיכה ווהי M\in\mathbb{F}^{n	imes n} תהא תיפוש הוקטור המדוייק הקרוב ביותר בסריג: יהי \mathbb{F} שדה יהי יהי \mathcal{F}\subseteq\mathbb{F} חוג דיסקרטי יהי n\in\mathbb{N}_+ תהא
                      v\in\mathcal{F}^nוכן ווא \|Mv-t\|=	ext{Val-lattice}(M,t,\mathbb{F},\mathcal{F}) באשר CVP-lattice-search-exact (M,t,\mathbb{F},\mathcal{F})=v איז t\in\mathbb{F}^n
                                                      .CVP-lattice = \{\langle M, t, \mathbb{F}, \mathcal{F}, \varepsilon \rangle \mid \text{Val-lattice}(M, t, \mathbb{F}, \mathcal{F}) \leq \varepsilon \} בעיית הוקטור הקרוב ביותר בסריג:
                                                                                                                        .
CVP-lattice-search מסקנה: 2^{\frac{n}{2}}הינו אלגוריתם Babai_{\frac{3}{4}}
                                                                                                                                                                                      . משפט: CVP-lattice משפט:
arepsilon>0 הויהי M\in\mathbb{F}^{n	imes n} תהא n\in\mathbb{N}_+ חוג דיסקרטי יהי דיסקרטי הקצר ביותר בסריג: יהי \mathbb{F} שדה יהי \mathcal{F}\subseteq\mathbb{F} חוג דיסקרטי יהי
                                                                                           v \in \mathcal{F}^n \setminus \{0\} וכן \|Mv\| \le \varepsilon באשר SVP-lattice-search ((M, \mathbb{F}, \mathcal{F}), \varepsilon) = v אזי
בעיית חיפוש הוקטור המדוייק הקרוב ביותר בסריג: יהי \mathbb F\subseteq\mathbb F שדה יהי ביהער ביותר בסריג: היו M\in\mathbb F^{n	imes n} ותהא ותהא n\in\mathbb N_+ ותהא
                                                                                       v \in \mathcal{F}^n וכן \|Mv\| = \lambda_i [\mathcal{L}[M]] באשר SVP-lattice-search-exact (M, \mathbb{F}, \mathcal{F}) = v
                                                               .SVP-lattice = \{\langle M, \mathbb{F}, \mathcal{F}, \varepsilon \rangle \mid \exists v \in \mathcal{F}^n \setminus \{0\} . \|Mv\| \leq \varepsilon \} בעיית הוקטור הקצר ביותר בסריג:
אלגוריתם חיפוש הקצר ביותר בהינתן הקרוב ביותר [גולדרייך־מיצ'אנצ'ו־ספרא־זייפט 1999]: יהי M\in\mathbb{R}^{n	imes n} תהא אלגוריתם חיפוש הקצר ביותר בהינתן הקרוב ביותר ביותר הקרוב ביות
                                                                                                                                                       אזי CVP-lattice-search-exact_{\mathbb{R}|\mathbb{Z}} אזי אלגוריתם
Algorithm SVP-via-CVP[\mathcal{A}](M):
       v \leftarrow C_1(M)
       for i \in [1, \ldots, n] do
               u \leftarrow \mathcal{A}\left(M + C_i(M) \cdot e_i^T, C_i(M)\right) - C_i(M)
               if ||u|| < ||v|| then v \leftarrow u
        end
 \mathrm{SVP}	ext{-lattice-search-exact} הינו אלגוריתם \mathrm{SVP}	ext{-via-CVP}[\mathcal{A}] אזי איני \mathrm{CVP}	ext{-lattice-search-exact} הינו אלגוריתם
                                                                                                                                .SVP-lattice-search-exact ^{	ext{CVP-lattice-search-exact}} \in \mathcal{P} מסקנה:
                                                                                                                                                        .C = 	ext{Promise-}C אזי C \subseteq \mathcal{P}\left(\{0,1\}^*
ight) איני תהא
                                 \mathrm{GAP}_{[T,S]}\mathrm{CVP}=\mathrm{GAP}_{[T,S]}\mathrm{Val\text{-lattice}} אזי אזי תהיינה תהיינה בסריג: תהיינה בסריג: תהיינה אזי
r\in\mathbb{R}_{>0} וויהי T:\mathbb{N}	o\mathbb{N} תהא תהא t\in\mathbb{F}^n הפיכה יהי היM\in\mathbb{F}^{n	imes n} תהא תהא תהא תייהי T:\mathbb{N}	o\mathbb{N} חוג דיסקרטי יהי
                                                                                                                           .GAP-CVP_T(M, t, \mathbb{F}, \mathcal{F}, r) = \text{GAP}_{[r,r\cdot T]}\text{CVP}(M, t, \mathbb{F}, \mathcal{F}) איי
                                                                                                                                                                                                        \mathrm{GAP\text{-}CVP}_{2^{rac{n}{2}}} \in \mathcal{P} :מסקנה
                                                                                   הפיכה אזי M\in\mathbb{F}^{n	imes n} ותהא ותהא n\in\mathbb{N}_+ חוג דיסקרטי הי חוג \mathcal{F}\subseteq\mathbb{F} חוג הגדרה: יהי
                                                                                                                                                                .Val-lattice<sub>0</sub> (M, \mathbb{F}, \mathcal{F}) = \min_{x \in \mathcal{F}^n \setminus \{0\}} ||Mx||
                                  \mathrm{GAP}_{[T,S]}\mathrm{SVP}=\mathrm{GAP}_{[T,S]}\mathrm{Val\text{-}lattice}_0 אזי אזי T,S:\mathbb{N}	o\mathbb{N} בעיית המרווח לוקטור הקצר ביותר בסריג: תהיינה
r\in\mathbb{R}_{>0} הגדרה: יהי \mathbb{R} שדה יהי T:\mathbb{N}	o\mathbb{N} חוג דיסקרטי יהי n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ הגדרה: יהי שדה יהי חוג דיסקרטי יהי ויהי n\in\mathbb{R}_+
                                                                                                                                             .GAP-SVP_{T}(M, \mathbb{F}, \mathcal{F}, r) = GAP_{[r,r-T]}SVP(M, \mathbb{F}, \mathcal{F})
                                                                                                                                                    . סענה: יהי \gamma \in \mathbb{R}_{\geq 1} הינה \gamma \in \mathbb{R}_{\geq 1} סענה: יהי
                                                                                                                                                 . הינה \mathcal{NP} הינה \gamma \in \mathbb{R}_{>1} הינה מסקנה: יהי \gamma \in \mathbb{R}_{>1}
                                                                                                                                                                                                     .GAP-SVP_n \in \text{co}\mathcal{NP} טענה:
                                                                                                               . הינה \mathcal{NP} הינה \mathrm{GAP\text{-}CVP}_{\exp\left(c\cdot \frac{\log(n)}{\log\log(n)}\right)} עבורו c\in\mathbb{R}_{>0} הינה משפט:
                                                                                                          \mathrm{GAP\text{-}CVP}_{\gamma} \in \mathcal{P} אזי \gamma = 2^{\mathcal{O}\left(n \cdot \frac{\log\log(n)}{\log(n)}\right)}באשר \gamma : \mathbb{N} \to \mathbb{N} אזי \gamma : \mathbb{N} \to \mathbb{N} משפט: תהא
                                                                                                                                                 .GAP-CVP_{\sqrt{n}}, GAP-SVP_{\sqrt{n}} \in \mathcal{NP} \cap \mathrm{co}\mathcal{NP} :משפט
                                                                                                                             A את איט מ"ט A^B המכריע את A את היינה A המכריע את רדוקציית טיורינג:
                                                                                                A \leq B אזי A \in B ל־ל מיר מיורינג מיר אזיית באשר היימת באשר אזיי מיורינג מ-A \in B איזי
                                                                                                               A את אוי מ"ט פולינומית \mathcal{A}^B המכריע את \mathcal{A}^B המכריע את אוי מ"ט פולינומית אוינה
                                                                                                    A \leq_n B אזי A ל־A איזי קוק מימת באשר קיימת באשר קיימת אזי A,B ל־מון: תהיינה
\mathrm{SIVP}_T(M)= בעיית הוקטורים הבלתי תלויים הקצרים ביותר: תהא T:\mathbb{N}	o\mathbb{N} יהי די הפיכה אזיM\in\mathbb{R}^{n	imes n} ותהא
                                                                                         i \in [n] לכל \|v_i\| \leq T(n) \cdot \lambda_n [\mathcal{L}[M]] באשר v_1 \dots v_n \in \mathbb{R}^n באשר (v_1 \dots v_n
                                                                                                                                                      \mathrm{SIVP}_{\gamma\cdot\sqrt{n}} \leq_p \mathrm{GAP}\text{-SVP}_{\gamma} אזי \gamma \in \mathbb{R}_{\geq 1} טענה: יהי
```

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

```
\mathcal{NP} טענה: יהיו \mathrm{SIVP}_{\gamma} אזי \gamma,c\in\mathbb{R}_{\geq 1} הינו \gamma,c\in\mathbb{R}_{\geq 1}
          אזי \inf\left(f^{-1}\left[\{1\}
ight]
ight)\in\left[a,b
ight] באשר a,b\in\mathbb{R} ועולה ויהיו f:\mathbb{R}	o\{0,1\} תהא arepsilon>0 תהא
Algorithm BinarySearch(f, a, b, \varepsilon):
      if |b-a|<\varepsilon then return \frac{a+b}{2}
      if f\left(\frac{a+b}{2}\right) = 1 then
       return BinarySearch(f, a, \frac{a+b}{2}, \varepsilon)
      else
       \mid return BinarySearch(f, rac{a+b}{2}, b, arepsilon)
	ext{BinarySearch}\left(f,a,b,arepsilon
ight)=d איי \inf\left(f^{-1}\left[\{1\}
ight]
ight)\in\left[a,b
ight] באשר באשר a,b\in\mathbb{R} על עולה ויהיו f:\mathbb{R}	o\{0,1\} איי arepsilon>0 תהא
                                                                                                                                             \left|d-\inf\left(f^{-1}\left[\left\{1\right\}
ight]
ight)
ight|<rac{arepsilon}{2} באשר
                                  טענה: \inf\left(f^{-1}\left[\{1\}
ight]
ight)\in[a,b] באשר בא ויהיו על עולה חשיבה f:\mathbb{R}	o\{0,1\} תהא arepsilon>0 אזי יהי
                                                                                                                .Time (BinarySearch) = \mathcal{O}\left(\text{Time}\left(f\right) \cdot \log\left(\frac{b-a}{\varepsilon}\right)\right)
                                                       .RootList (R)=\mathrm{Sort}\left([0,\ldots,R]\,\|\,[\sqrt{n}\quad\text{for}\quad n\in[0,\ldots,R]]\right) אזי R\in\mathbb{N}_+ הגדרה: יהי הי
אלגוריתם הכרעה לחיפוש לבעיית הוקטור הקרוב ביותר: יהי n\in\mathbb{N}_+ תהא הפיכה t\in\mathbb{Z}^n ויהי אלגוריתם אלגוריתם הכרעה לחיפוש לבעיית הוקטור הקרוב ביותר:
                                                                                                                                                                אזי (\mathrm{GAP\text{-}CVP}_1)_{\mathbb{R}|\mathbb{Z}}
Algorithm CVP-Decidability-Search[\mathcal{A}](M,t):
      d \leftarrow \operatorname{BinarySearch}\left(\mathcal{A}\left(M,t\right), \operatorname{RootList}\left(\sum_{i=1}^{n}\|C_{i}(M)\|\right)\right) / / \operatorname{Search} \text{ for } \mathcal{A}(M,t)(?) \text{ on the list given by RootList}
      for i \in [1, \ldots, 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
      return Babai\frac{3}{4} (LLL-Algo \left(\frac{3}{4}, M\right), t)
 \mathrm{CVP	ext{-}lattice	ext{-}search	ext{-}exact}_{\mathbb{R}|\mathbb{Z}} הינו אלגוריתם \mathrm{CVP	ext{-}Decidability	ext{-}Search} אזי ווריתם \mathrm{CVP	ext{-}lattice	ext{-}search	ext{-}exact}
                                                                                                                .CVP-lattice-search-exact^{\mathrm{GAP}\text{-}\mathrm{CVP}_1} \in \mathcal{P} מסקנה:
          .CVP-lattice-search-exact ^{\mathrm{GAP-CVP}_{\gamma}} השפט: יהי \gamma^{\mathcal{O}(n)} אזי קיים אלגוריתם פולינומי פולינומי \gamma^{+}
```