```
\mathbb{F}^{m	imes n}=M_{m	imes n}\left(\mathbb{F}
ight) אזי m,n\in\mathbb{N}_{+} שדה ויהיו \mathbb{F} יהי
                                   \Delta\left(x,y
ight)=|\{i\in[m]\mid x_i
eq y_i\}| ברחק האמינג: תהא X קבוצה אזי נגדיר X
                                                                                                   \ell_0 טענה: תהא את משרה אזי \Delta קבוצה אזי ענה: תהא
                                                                       .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:
                                            g אזי אוי לתיקון איאות לתיקון איזי g,m\in\mathbb{N}_+ ויהי לתיקון איאות לתיקון אויאות גודל האלפבית בקוד לתיקון איאות:
                                              m אזי אויהי לתיקון לתיקון איאות: יהיו q,m\in\mathbb{N}_+ ויהי אויהי לתיקון איאות אזי גודל הבלוק בקוד לתיקון איאות:
                        d\left[\mathcal{C}
ight]=\min_{x
eq y}\Delta\left(x,y
ight) אזי לתיקון שגיאות אזי q,m\in\mathbb{N}_{+} ויהי יהיו מרחק בקוד לתיקון שגיאות אזי
                              r[\mathcal{C}] = \log_a |\mathcal{C}| אזי אויאות אוי לתיקון איזי \mathcal{C} \subseteq [q]^m ויהי q,m \in \mathbb{N}_+ יהיי הייו אגיאות: יהיו
                         . לתיקון שגיאות [m,r\left[\mathcal{C}\right],d\left[\mathcal{C}\right],q] הינו אזי הינו אוי לתיקון שגיאות לתיקון שגיאות פוד יהיו q,m\in\mathbb{N}_{+} ויהי
                       w' 
otin \mathcal{C} אזי \Delta \left(w,w'
ight) \leq d-1 באשר w' \in [q]^m ויהי w \in \mathcal{C} אזי לתיקון שגיאות יהי
rg \min_{v \in \mathcal{C}} \Delta\left(v, w'
ight) = w אזי \Delta\left(w, w'
ight) \leq \left|rac{d-1}{2}
ight| באשר w' \in [q]^m ניהי w \in \mathcal{C} אזי שנה: יהי w \in \mathcal{C} לתיקון שגיאות יהי
                                                           r \leq m-d+1 משפט חסם הסינגלטון: יהי \mathcal{C} קוד [m,r,d,q] לתיקון שגיאות משפט חסם הסינגלטון
                                             \mathcal{C}_{\mathrm{Hamming}} = \left\{ x \in \mathbb{F}_2^{2^m-1} \ \middle| \ orall i \in [m] \, . \left( igoplus_{k \in [2^m-1]} x_k = 0 
ight) 
ight\} איי m \in \mathbb{N}_+ איי m \in \mathbb{N}_+ האמינג: יהי m \in \mathbb{N}_+ איי
                              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.
. אניאות [m+1,r,d+1,2] איים קוד [m,r,d,2] לתיקון שגיאות אזי קיים קוד שגיאות עבורם m,r\in\mathbb{N}_+ ויהיו ויהיו ל
                                |\mathcal{C}| \leq q^m \cdot \left(\sum_{i=0}^{\left\lfloor \frac{d-1}{2} 
ight
floor} \left(inom{m}{i} \cdot (q-1)^i
ight)
ight)^{-1} משפט האמינג: יהי \mathcal{C} קוד קוד [m,r,d,q] לתיקון שגיאות אזי
               |\mathcal{C}| \leq rac{d}{d+rac{m}{q}-m} לתיקון שגיאות אזי [m,r,d,q] קוד למה פלוטקין: יהיו למה באשר שר באשר למה לוסקין: יהיו למה בלוטקין: יהיו
                                   d \leq d \cdot 2^{m-2d+2} טענה: יהיו m,r,d, באשר שויהי d \leq rac{m}{2} ויהיd \leq m ויהי לקוד וויהי d \leq m באשר באשר
          . פורי. מרחב \mathcal{C} באשר \mathfrak{C}_q שדה אזי קוד לתיקון שגיאות אזי קוד פאשר \mathfrak{T}_q באשר \mathfrak{T}_q באשר פאר באשר פארים כי מרחב וקטורי.
                                                                           \dim(\mathcal{C})=r טענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי
C_i\left(M_{\mathcal{C}}
ight)=b_i כך M_{\mathcal{C}}\in\mathbb{F}_q^{m	imes r} בסיס אזי נגדיר b_1\dots b_r\in\mathcal{C} לתיקון שגיאות ויהי לתיקון שגיאות ויהי
                                                                                                                                                   i \in [r] לכל
```

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

טענה: יהיו R_+ אזי קוד לינארי לתיקון שגיאות. $q,m,k\in\mathbb{N}_+$ יהיו יהיו $M_{\mathcal{C}_{k\text{-rep}}}=inom{I_m}{\vdots}$ אזי $q,m,k\in\mathbb{N}_+$ יהיו יהיו יהיו יהיו $q,m,k\in\mathbb{N}_+$

. טענה: יהיו $q,m\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{parity}}$ קוד לינארי לתיקון שגיאות. $M_{\mathcal{C}_{\mathrm{parity}}}=\left(egin{array}{c}I_m\\ \hline i^T\end{array}
ight)=\left(egin{array}{c}I_m\\ \hline i^T\end{array}
ight)$ אזי $q,m\in\mathbb{N}_+$ אזי $q,m\in\mathbb{N}_+$ מסקנה: יהיו $q,m\in\mathbb{N}_+$ אזי $q,m\in\mathbb{N}_+$ לתיקון שגיאות אזי $q,m\in\mathbb{N}_+$ טענה: יהי $q,m\in\mathbb{N}_+$ לינארי $q,m\in\mathbb{N}_+$ לתיקון שגיאות אזי $q,m\in\mathbb{N}_+$ טענה: יהי $q,m\in\mathbb{N}_+$ לינארי $q,m\in\mathbb{N}_+$

 $A \in \mathbb{F}_a^{(m-r) imes r}$ טענה: יהי \mathcal{D} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי קיים קוד לינארי לינארי [m,r,d,q] לתיקון שגיאות לינארי $M_{\mathcal{D}} = \left(\begin{smallmatrix} I_r \\ A \end{smallmatrix} \right)$ 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 יהיי \mathbb{F} שדה יהיי

[m,r,d,q] טענה: יהי $\mathcal C$ קוד לינארי

- $|R\left(M_{\mathcal{C}}\right)\cap V| < m-d$ מתקיים $\dim\left(V\right) = r-1$ באשר $V\subseteq\mathcal{C}$ לכל
 - $|R\left(M_{\mathcal{C}}\right)\cap V|=m-d$ וכן $\dim\left(V
 ight)=r-1$ המקיים $V\subseteq\mathcal{C}$ המקיים

```
. לתיקון שגיאות [m-d,r-1,d',q] לעבורו קיים קוד לינארי (m,r,d,q] לתיקון שגיאות אזי קיים לונארי (m,r,d,q) לתיקון שגיאות אזי קיים לונארי
                                                  m\geq\sum_{i=0}^{r-1}\left\lceil rac{d}{q^i}
ight
ceil לתיקון שגיאות אזי שנט גרייסמר: יהי \mathcal C קוד לינארי [m,r,d,q] לתיקון שגיאות אזי לכל x\in\mathbb F_q^r\setminus\{0\} אזי לכל m>r באשר m,r\in\mathbb N_+ שדה יהיו m>r באשר m,r\in\mathbb N_+ באשר באשר אזי לכל למה: יהי
                                                                                                                                                                                                                                                       \mathbb{P}_{M \in \mathbb{F}_q^{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 q\in\mathbb{N}_+ אזי q\in\mathbb{N}_+ יהי
                                                                                                           משפט: יהי m>r ויהי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו m>r באשר m,r\in\mathbb{N}_+ באשר m,r\in\mathbb{N}_+
                                                             \mathcal{C}^ee = \{w \in [q]^m \mid orall c \in \mathcal{C}. \ \langle w,c 
angle = 0\} לתיקון שגיאות אזי [m,r,d,q] לתיקון לינארי יהי \mathcal{C} קוד לינארי
טענה: יהי \mathcal{C}^\vee קוד לינארי [m, r, d, q] לתיקון שגיאות אזי קיים d' \in \mathbb{N}_+ עבורו אי קיים m, r, d, q לתיקון שגיאות.
                                                                                                                                      H_{\mathcal{C}}=M_{\mathcal{C}^{\vee}} אזי אות שגיאות לינארי לינארי קוד לינארי יהי יהי שאריות: יהי
                                                                                                                                                                           \mathcal{C} = \ker\left(H_{\mathcal{C}}^{T}
ight) יענה: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי
                                                                                                          d=m-r+1 לתיקון שגיאות המקיים [m,r,d,q] קוד קוד [m,r,d,q]
טענה: יהי \mathcal{C}_M אזי (\mathcal{C}_M) אזי M\in\mathbb{F}_q^{m	imes r} ויהי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו קוד לינארי מקסימלי לתיקון
                                                                                                                                                                                  . בת"ל). A \in \mathcal{P}_r(R(M)) מתקיים כי A \in \mathcal{P}_r(R(M))
                                                                           . מענה: עינארי מקסימלי לתיקון אזי \mathcal{C}^{\vee} הינו אזי לתיקון שגיאות מקסימלי לתיקון לינארי קוד לינארי סענה: יהי
משפט גילברט־וורשאמוב: יהיו m,k,d,q באשר שניים d\leq m ויהי וויהי לברט־וורשאמוב: יהיו לתיקון שגיאות לברט־וורשאמוב: יהיו לברט־וורשאמוב: יהיו לברט־וורשאמוב: יהיו
                                                                                                                                                                                                                     |\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)} איי קיים \sum_{i=0}^{d-2} {m-1 \choose i} \left(q-1
ight)^i < q^{m-k} עבורו q\in \mathbb{P} אויהי k\leq m באשר באשר k,m\in \mathbb{N}_+ איי קיים למה: יהי k\leq m
                                                                                                                                                                                               עבורו לכל A \in \mathcal{P}_{d-1}\left(R\left(M\right)\right) מתקיים כי A \in \mathcal{P}_{d-1}\left(R\left(M\right)\right)
משפט גילברט־וורשאמוב: יהי d\in\mathbb{N}_+ יהיו d\in\mathbb{N}_+ אזי איי d\in\mathbb{N}_{\geq 2} אזי איי איי איי יהיו איי איי איי יהיו איי איי איי איי יהיו אויהי משפט אילברט־וורשאמוב: 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 f: X 	o Y^n וויהי f: X 	o Y^n אזי f: X 	o Y^n אזי f: X 	o 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[n] ולכל s\in X עבורה לכל g:Y^k	o X
                     .g\left(f\left(s
ight)_{p_{1}},\ldots,f\left(s
ight)_{p_{k-1}}
ight)=s מתקיים p_{1},\ldots,p_{k-1}\in\left[n
ight] ולכל ולכל s\in X עבורה לכל g:Y^{k-1}	o X
arphi כך arphi כך arphi באשר arphi יהי arphi שדה סופי באשר arphi יהיו arphi שדה סופי באשר arphi יהיו arphi שדה סופי באשר arphi יהיו arphi שדה סופי באשר אונים ונגדיר arphi באשר arepsilon באשר arphi יהיו arphi שדה סופי באשר אונים ונגדיר arphi באשר arphi יהיו arphi יהיו arphi שדה סופי באשר אונים ונגדיר arphi יהיו arph
                                                                                                                                                                                                                                                                  אזי \varphi\left(p\right)=\left(p\left(x_{i}\right)\right)_{i=1}^{\ell}
                                                                                                                                                  . אם אז \varphi איזומורפיזם וכן \varphi, \varphi^{-1} חשיבות איזומורפיזם פולינומי.
                                                                                                                          k-\ell ממימד אפיני ממימד ער מתקיים כי y \in \mathbb{F}^\ell אז לכל \ell < k אם \ell < k
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} באשר q \in \mathbb{N} באשר יהי
        s_1 \dots s_n \in \mathbb{F}_q \setminus \{0\} באשר f(s,a) = \left(\left(s_i, s + \sum_{j=1}^{k-1} a_j s_i^j\right)\right)_{i=1}^n באשר g(s,a) = \left(\left(s_i, s + \sum_{j=1}^{k-1} a_j s_i^j\right)\right)_{i=1}^n באשר g(s,a) = n באשר g(s,a) = n
                                                                    שונים אזי lpha_1 \ldots lpha_m \in \mathbb{F}_q ויהיו r \in [m] יהי יהי m \in [q] שדה יהי שדה באשר ק באשר קוד ריד־סולומון: יהי
                                                                                                                              \mathrm{RS}_q\left[m,r
ight] = \left\{ \left(f\left(lpha_i
ight)
ight)_{i=1}^m \mid f \in \left(\mathbb{F}_q
ight)_{\leq r-1}\left[x
ight] 
ight\} . \mathrm{RS}_q\left[q,r
ight] \simeq \left(\mathbb{F}_q
ight)_{\leq r-1}\left[x
ight] אזי r \in [q] שדה ויהי q \in \mathbb{N} הערה: יהי q \in \mathbb{N} באשר q \in \mathbb{N}
טענה: יהי \mathrm{RS}_q\left[m,r
ight] אזי lpha_1\ldotslpha_m\in\mathbb{F}_q ויהיו והי יהי m\in[q] שדה יהי שדה הינו קוד לינארי מקסימלי יהי יהי
                                                                                                                                                                                                                                    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 איהי m\in[q] לכל לכל ענה: יהי m\in[q] איזי יהי m\in[q]
                                                                                                                              \sum_{x\in\mathbb{F}_q} x^i = 0 אזי i\in\{0,\dots,q-2\} שדה ויהי \mathbb{F}_q שדה מענה: יהי יהי 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 \mathbb{F}_q באשר שדה q \in \mathbb{N} טענה: יהי
           \mathrm{RM}_q\left[m,r
ight] = \left\{ (f\left(lpha
ight))_{lpha \in \mathbb{F}_q^m} \mid 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}
```

 $\operatorname{RM}_q[m,r]\simeq (\mathbb{F}_q)_{< r}[x_1,\ldots,x_m]$ אזי $m,r\in\mathbb{N}_+$ שדה ויהיו \mathbb{F}_q שדה באשר $q\in\mathbb{N}$ יהי היי

```
[q^m,r,d,q] אי קיימים אין אווי הינו \mathrm{RM}_q[m,r] אי קיימים אי קיימים אי אי הינו קוד לינארי שדה ויהיו m,r\in\mathbb{N}_+ אי קיימים אי בורם באשר m,r\in\mathbb{N}_+ שבה ויהיו שדה ויהיו
                                                     r\left[\mathrm{RM}_q\left[m,r
ight]
ight] = inom{m+r}{r} אזי r < q איזי m,r \in \mathbb{N}_+ שדה ויהיו \mathbb{F}_q שדה באשר q \in \mathbb{N} 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 באשר q \in \mathbb{N} יסענה: יהי
                                                                                                              r\left[\mathrm{RM}_{2}\left[m,r
ight]
ight]=\sum_{i=0}^{r}inom{m}{i} אזי m,r\in\mathbb{N}_{+} יהיי יהיי
                                      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}_+ איי
                        \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: יהיי m,r \in \mathbb{N}_{\geq 2}
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}' = \{(\rho(w_i))_{i=1}^m \mid w \in \mathcal{C}\} הפיכה אזי \rho: [q] \to \mathcal{C}'
                      טענה: יהי \mathcal{C}\circ\mathcal{C}' לתיקון שגיאות אזי [m',\log_{q'}(q)\,,d',q'] קוד \mathcal{C}' הינו שגיאות אזי לתיקון שגיאות יהי
                                                                                                                            לתיקון שגיאות. \left[m \cdot m', r \cdot \log_{a'}(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 היהי לתיקון שגיאות היהי
                                                                    \mathcal{C}\circ\mathcal{C}'\simeq\left\{h:[m]	imes[m']	o[q]\ \Big|\ \exists w\in\mathcal{C}.h\,(i,j)=\left(
ho\,(w_i)
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[n] ותהא n\in\mathbb{N} יהי הגדרה: יהי
                                                                                        \mathcal{C}_{\mathrm{Hadamard}}=\left\{ \left(\chi_{S}\left(x
ight)
ight)_{x\in\mathbb{F}_{2}^{n}}\ \middle|\ S\subseteq\left[n
ight]
ight\} אזי n\in\mathbb{N}_{+} יהי אדמר: יהי n\in\mathbb{N}_{+}
                                                                    . טענה: יהי [2^n,n,2^{n-1},2] הינו קוד לינארי \mathcal{C}_{\mathrm{Hadamard}} לתיקון שגיאות יהי יהי
                                                                                        \mathcal{C}_{\mathrm{Hadamard}}\simeq\{\chi_S\mid S\subseteq[n]\} אזי n\in\mathbb{N}_+ הערה: יהי הי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ טענה: יהי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ יהי יהי 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}_{+} יהי יהי יהי יהי n\in\mathbb{N}_{+} אזי הינו קוד \left[2^{n},\log_{2}\left(n
ight),2^{n-1},2
ight] לתיקון שגיאות. \mathcal{C}_{\mathrm{Dic}}
                                                                                                                          \mathcal{C}_{	ext{Dic}}\simeqig\{\chi_{\{i\}}\mid i\in[n]ig\} אזי n\in\mathbb{N}_+ יהי יהי n\in\mathbb{N}_+
                                                                B_r\left(x
ight)=\{y\in X\mid \Delta\left(x,y
ight)\leq r\} אזי x\in X ויהי ויהי r\in\mathbb{R}_+ היהי קבוצה הא X
\|B_r(w)\cap\mathcal{C}\| \leq \ell מתקיים w\in[q]^m מתקיים לתיקון שגיאות [m,k,d,q] אזי קוד r,\ell\in\mathbb{N}_+ אזי היו
יסימון. אוי (m,k,r,\ell,q) ויהי (m,k,d,q) לתיקון שגיאות רשימתי (r,\ell) אוי (r,\ell) איז (r,\ell) לתיקון שגיאות רשימתי.
                                             . טענה: יהי (m,k,\frac{d}{2},1,q) לתיקון שגיאות אזי לתיקון שגיאות אזי לתיקון שגיאות רשימתי ((m,k,d,q)
                                           M\in\mathbb{F}^m אזי M\in\mathbb{F}^{m	imes n} תהא m,n\in\mathbb{N}_+ אזי שדה יהיו היי M\in\mathbb{F}^m ויהי אזי שדה לינארית: יהי
 \operatorname{Val}\left((M,t,\mathbb{F})
ight)=\min_{x\in\mathbb{F}^n}\left(rac{1}{m}\cdot\Delta\left(Mx,t
ight)
ight) איז מערכת משוואות לינארית: תהא (M,t,\mathbb{F}) מערכת משוואות לינארית
\mathrm{CVP\text{-}code\text{-}search}\left((M,t,\mathbb{F})\,,arepsilon)=v אזי arepsilon>0 אזי מערכת משוואות לינאריות מערכת משוואות לינאריות ויהי
                                                                                                                                                                  \|Mv-t\|_0 \le \varepsilon באשר
                                                                      .CVP-code = \{\langle (M, t, \mathbb{F}), \varepsilon \rangle \mid \operatorname{Val}((M, t, \mathbb{F})) \leq \varepsilon \} בעיית הוקטור הקרוב ביותר:
                                                                      .SVP-code = \{\langle (M,0,\mathbb{F}), \varepsilon \rangle \mid \exists v \neq 0. \|Mv\|_0 \leq \varepsilon \} בעיית הוקטור הקצר ביותר:
                                                                              i\in[n] לכל \left(ec{1}
ight)_{+}=1 כך ec{1}\in\mathbb{F}^{n} אאי נגדיר n\in\mathbb{N}_{+} לכל לכל
                      \operatorname{MaxCut} = \left\{ \left\langle \left(M, \vec{1}, \mathbb{F}_2\right), \varepsilon \right\rangle \mid \left( \forall i \left(w \left(R_i \left(M\right)\right) = 2 \right) \right) \wedge \left( \operatorname{Val} \left(\left(M, \vec{1}, \mathbb{F}\right)\right) \leq \varepsilon \right) \right\} בעיית החתך המקסימלי:
                                                                              . קשה. Promise-\mathcal{NP} הינה \mathrm{GAP}_{[arepsilon,1-arepsilon]}\mathrm{MaxCut} קשה. arepsilon\in(0,1)
                                                                                                         \mathcal{NP}-הינה \mathcal{NP}-קשה. \mathcal{E} \in (0,1) הינה \mathcal{E} \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-arepsilon,1-(1+\delta)arepsilon]}\mathrm{MaxCut} קשה. עבורם arepsilon,\delta\in(0,1)
                                                  \mathrm{GAP}_{[a,b]}\mathrm{CVP\text{-}code} = \mathrm{GAP}_{[a,b]}\mathrm{Val} איי אי a,b \in [0,1] יהיו ביותר: יהיו לוקטור הקרוב ביותר:
                                             \operatorname{CVP-code}_{\mathbb{F}} קשה. פופי \mathcal{P} עבורו \operatorname{GAP}_{[arepsilon,1-arepsilon]} הינה \mathcal{S}>0 הינה arepsilon
                                    \mathcal{P}=\mathcal{NP} אז CVP-code-search מסקנה: אם קיים אלגוריתם פולינומי A אשר מהווה אשר פולינומי
```

```
(M)_{i,j}=1 עבורו אזי 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} אזי אזי M\in\mathbb{F}^{n	imes m}
                                                                                                                                                                      R_i(M) \cdot \vec{1} = 0 וכן
                            \mathrm{Val}_{1\leftrightarrow 1}\left((M,t,\mathbb{F})
ight)=\mathrm{Val}\left((M,t,\mathbb{F})
ight) איז t\in\mathbb{F}^m מטריצת משחק ויהי M\in\mathbb{F}^{n	imes m} מטריצת משחק ויהי M\in\mathbb{F}^{n	imes m}
                                                            \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 אינית המשחקים היחודיים: יהי
                                                     השערה המשחקים היחודיים: יהי arepsilon>0 אזי \mathrm{UG}\left(arepsilon
ight) אזי יהי יהי 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 איזי שדה יהי
                                                                                    אזי u,v\in\mathbb{F}^m אזי מטריצת משחק ויהיו M\in\mathbb{F}^{n	imes m} אזי הגדרה: יהי
                                                                                                   .\mathrm{Val}_{2 \to 1}\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 שניים על אחד:
                                       משפט חות־מינזר־ספרא: יהי arepsilon>0 אזי אזי \mathrm{PCP}_{2	o 1}\left[arepsilon,1-arepsilon
ight] אזי אזי יהי arepsilon>0 אזי אזי אזי פורס
                                                                                                              \frac{1}{2}\mathrm{UG}\left(arepsilon
ight)=\mathrm{PCP}_{1\leftrightarrow1}\left[\frac{1}{2},1-arepsilon
ight] אזי arepsilon>0 אזי arepsilon>0
                                                                                                          יקשה. Promise-\mathcal{NP} הינה \frac{1}{2}\mathrm{UG}\left( arepsilon 
ight) אזי arepsilon > 0 אזי
             A \in \mathbb{F}^{m 	imes n} ותהא A \in \mathbb{F}^{m 	imes n} אזי A \in \mathbb{F}^{k 	imes m} תהא תהא A \in \mathbb{F}^{k 	imes m} תהא הייו A \in \mathbb{F}^{k 	imes m} תהא
                                     ... אזי B\in\mathbb{F}^{m	imes n} ותהא A\in\mathbb{F}^{k	imes m} תהא k,m,n\in\mathbb{N}_+ שדה יהיי \mathbb{F} שדה שלגוריתם כפל מטריצות נאיבי: יהי
A \in \mathbb{F}^{k 	imes n} הינה NaiveMatMul אזי סיבוכיות הריצה של A \in \mathbb{F}^{k 	imes m} ותהא אA \in \mathbb{F}^{k 	imes m} הינה A \in \mathbb{F}^{k 	imes m}
                                                                                                               אזי a,b\in \left\{0,1
ight\}^n ויהיו n\in \mathbb{N} אזי אלגוריתם קרטסובה: יהי
Function 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 \texttt{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
                                                                                                 .(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
                                                                                      A,B\in\mathbb{F}^{2^n	imes 2^n} ותהיינה n\in\mathbb{N} אזי שדה יהי \mathbb{F} אזי אלגוריתם סטרסן: יהי
                                                  .\operatorname{StrassenMatMul}\left(\mathbb{F},A,B\right)=AB אזי A,B\in\mathbb{F}^{2^{n}\times2^{n}} ותהיינה n\in\mathbb{N} ותהיינה יהי n\in\mathbb{N}
                                                                                                \mathcal{O}\left(m^{\log_2(7)}\right) הינה StrassenMatMul טענה: סיבוכיות הריצה של
                                            A \in \mathbb{F}^{n \times n} ותהא n \in \mathbb{N}_+ יהי הי שדה יהי \mathbb{F} שדה יהי \mathbb{F} שדה יהי n \in \mathbb{N}_+ ותהא היפוך מטריצה: יהי
                                            (T איי (בעיית \mathrm{MatInv} חשיבה בזמן \mathrm{MatMul} חשיבה בזמן \mathrm{T}:\mathbb{N}\to\mathbb{N} משפט: תהא
                                         \operatorname{MatDet}\left(\mathbb{F},A\right)=\det\left(A\right) הפיכה אזי A\in\mathbb{F}^{n	imes n} ותהא n\in\mathbb{N}_{+} שדה יהי \mathbb{F} שדה יהי n\in\mathbb{N}_{+}
                                           (T:\mathbb{N} \to \mathbb{N} ) חשיבה בזמן MatDet משפט: תהא אזי (בעיית T:\mathbb{N} \to \mathbb{N} חשיבה בזמן השיבה מוער.).
```

בעיית פירוק $\mathbb{L}U$ חשיבה בזמן M משפט: תהא $\mathbb{N} \to \mathbb{N}$ אזי (בעיית $\mathbb{N} \to \mathbb{N}$ חשיבה בזמן $\mathbb{N} \to \mathbb{N}$ השיבה בזמן $\mathbb{N} \to \mathbb{N}$ חשיבה בזמן $\mathbb{N} \to \mathbb{N}$ חשיבה בזמן $\mathbb{N} \to \mathbb{N}$ הא משפט: תהא $\mathbb{N} \to \mathbb{N}$ אזי (בעיית $\mathbb{N} \to \mathbb{N}$ חשיבה בזמן $\mathbb{N} \to \mathbb{N}$ היי $\mathbb{N} \to \mathbb{N}$ אזי (בעיית $\mathbb{N} \to \mathbb{N}$ חשיבה בזמן $\mathbb{N} \to \mathbb{N}$ הוע $\mathbb{N} \to \mathbb{N}$ אזי $\mathbb{N} \to \mathbb{N}$ היי $\mathbb{N} \to \mathbb{N}$ הוע $\mathbb{N} \to \mathbb{N}$ אזי $\mathbb{N} \to \mathbb{N}$ הוע \mathbb{N} הו

- $x-y\in\mathcal{L}$ מתקיים $x,y\in\mathcal{L}$ •
- $\max\{|V|\mid (V\subseteq\mathcal{L})\land (\mathbb{Z})$ מעל מעל בת"ל קבוצה ע $V)\}=k$

```
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 אבר באשר (\mathcal{L},k) סריג אבסטרקטי: יהיו יהיא
                                                                                                                                             \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 k מדרגה k מדרגה k מדרגה k אזי k בורה k אזי ((\mathcal{L},k)) הינו סריג אבסטרקטי)
                                        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.i.a}:\mathbb{R}^{n	imes n}	o\mathbb{R}^{n	imes n} אזי נגדיר עמודות: יהי n\in\mathbb{N}_+ יהיו שונים ויהי i,j\in[n] שונים יהי
                                                                                                                                                                                .\Phi_{i,j,a}^{+}\left(M\right) = M + a \cdot \left(C_{j}\left(M\right) \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 n\in\mathbb{N}_+ 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} איי נגדיר i\in[n] איי ויהי i\in\mathbb{N}_+ יהי יהי
                        \left\{\Phi_{i,j,a}^+ \ \middle| \ \left(egin{array}{c} i,j\in[n] \ i
eq j \end{array}
ight) \wedge (a\in\mathbb{Z})
ight\} \cup \left\{\Phi_{i,j}^+ \ \middle| \ i,j\in[n] \ i\neq j \end{array}
ight\} \cup \left\{\Phi_i^- \ \middle| \ i\in[n]
ight\} איז n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ הפיכה ותהא n\in\mathbb{N}_+ טרנספורמציה אלמנטרית איז n\in\mathbb{N}_+ תהא n\in\mathbb{N}_+ הפיכה ותהא n\in\mathbb{N}_+ טרנספורמציה אלמנטרית איז n\in\mathbb{N}_+
משפט: יהי m\in\mathbb{N}_+ וקיימות טרנספורמציות אלמנטריות איי הפיכות אזי A,B\in\mathbb{R}^{n	imes n} ותהיינה n\in\mathbb{N}_+ ותהיינה אלמנטריות אלמנטריות
                                                                                                                                                                       (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} \} סריג דואלי: יהי \mathcal{L} סריג דואלי
                                                                                                                                                                      . טענה: יהי \mathcal{L} סריג ממשי אזי \mathcal{L}^{\vee} סריג ממשי
                                                                                                                                                                           \left(\mathcal{L}^ee
ight)^ee = \mathcal{L} טענה: יהי \mathcal{L} סריג ממשי אזי
                                                                                                          M^ee = M^{-T} מטריצה דואלית: יהיn \in \mathbb{N}_+ ותהא ותהא n \in \mathbb{N}_+ מטריצה דואלית: יהי
                                                                                                                              M \in \mathbb{R}^{n 	imes n} ותהא M \in \mathbb{R}^{n 	imes n} ותהא n \in \mathbb{N}_+ יהי יהי יהי
                                                                                                                    \mathcal{L}\left[M
ight]^ee=\mathcal{L}\left[M^ee
ight] אזי הפיכה 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 יהי סריג ממשי ויהי
                                                                                                   (q\cdot\mathcal{L}[M]=\mathcal{L}[q\cdot M] אזי (k,n\in\mathbb{N}_+) מדרגה (k,n\in\mathbb{N}_+) ותהא (k,n\in\mathbb{N}_+) מדרגה איזי
                                                                                                                              (q\cdot\mathcal{L})^ee=q^{-1}\cdot\mathcal{L}^ee אזי q\in\mathbb{R}_{>0} אויהי ממשי ויהי סריג ממשי ויהי
                               \mathrm{MatInd} = ig\{\langle \mathbb{F}, M 
angle \mid (שדה) \wedge (n, k \in \mathbb{N}_+) \wedge (M \in \mathbb{F}^{n 	imes k}) \wedge (k מדרגה M) ig\} שדה M
                \text{LatIn} = \left\{ \langle M, v \rangle \mid (n, k \in \mathbb{N}_+) \land \left(M \in \mathbb{R}^{n \times k}\right) \land (k \text{ atras } M) \land \left(v \in \mathcal{L}\left[M\right]\right) \right\} \text{ .} \text{LatInc} = \left\{ \langle A, B \rangle \mid (n, k, m \in \mathbb{N}_+) \land \left( \substack{A \in \mathbb{R}^{n \times k} \\ B \in \mathbb{R}^{n \times m}} \right) \land \left( \substack{k \text{ atras } A \\ B \text{ atras } B} \right) \land \left(\mathcal{L}\left[A\right] \subseteq \mathcal{L}\left[B\right]\right) \right\} \text{ atras } B \in \mathbb{R}^{n \times m} \text{LatInc} = \left\{ \langle A, B \rangle \mid (n, k, m \in \mathbb{N}_+) \land \left( \substack{A \in \mathbb{R}^{n \times k} \\ B \in \mathbb{R}^{n \times m}} \right) \land \left( \substack{k \text{ atras } B \text{ atras } B \text{ atras } B} \right) \land \left(\mathcal{L}\left[A\right] \subseteq \mathcal{L}\left[B\right]\right) \right\} \text{ atras } B \in \mathbb{R}^{n \times m} \text{LatInc} = \left\{ \langle A, B \rangle \mid (n, k, m \in \mathbb{N}_+) \land \left( \substack{A \in \mathbb{R}^{n \times k} \\ B \in \mathbb{R}^{n \times m}} \right) \land \left( \substack{k \text{ atras } B \text{ atras } B \text{ atras } B} \right) \land \left( \substack{k \text{ atras } B \text{ atras } B} \right) \right\}
                                                                                                                                                              .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}\left[0,1
ight)}\left[M
ight] אזי M\in\mathbb{R}^{n	imes k} ותהא n,k\in\mathbb{N}_{+} אזי יהיו
                           M\cdot a|_{\mathcal{P}[M]}=M\cdot \lfloor a \rfloor אזי אזי a\in \mathbb{R}^k מדרגה k ויהי M\in \mathbb{R}^{n	imes k} תהא n,k\in \mathbb{N}_+ עיגול לפי המקבילון היסודי: יהיו
                                         \|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 n,k\in\mathbb{N}_+
              (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 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}_+ יהיו n,k\in\mathbb{N}_+ אזי
         \mathcal{L}[A] = \mathcal{L}[B] \iff (\mathcal{P}[B] \cap \mathcal{L}[A] = \{0\}) אזי \mathcal{L}[B] \subseteq \mathcal{L}[A] הפיכות באשר A, B \in \mathbb{R}^{n \times n} ותהיינה n \in \mathbb{N}_+ יהי
                                                                                                      \operatorname{Vol}\left(\mathcal{P}\left[M
ight]
ight)=\left|\det\left(M
ight)
ight| הפיכה אזי M\in\mathbb{R}^{n	imes n} ותהא n\in\mathbb{N}_{+} יהי יהי
                                                    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 וותהיינה מסקנה: יהי
                                                                      \det\left(\mathcal{L}\left[M
ight]
ight)=\operatorname{Vol}\left(\mathcal{P}\left[M
ight]
ight) הפיכה אזי M\in\mathbb{R}^{n	imes n} ותהא n\in\mathbb{N}_{+} יהי של סריג: 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 n\in\mathbb{N}_{+} יהי יהי
                                                                                                                                                                                                                  AatDet \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})} איזי משטי אזי סענה: יהי
```

 $\lambda_i\left[\mathcal{L}
ight]=\inf\left\{r\geq 0\mid \dim \mathrm{span}\left(B_r\left(0
ight)\cap\mathcal{L}
ight)\geq i
ight\}$ איז $i\in[k]$ איז $i\in[k]$ סריג ממשי מדרגה k ויהי $k\in\mathbb{N}_+$ איז איז יהי

אורתונורמליזציה: יהי $u_1^\perp,\dots,u_n^\perp\in\mathbb{R}^n$ ויהיו וויהיו באשר $u_1\dots u_n\in\mathbb{R}^n$ בסיס אזי אורתונורמליזציה: יהי

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

```
. בסיס אורתונורמלי. בסיס \{u_1^\perp,\ldots,u_n^\perp\}
```

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

 $u_1\dots u_n$ בטיס אזי קיימת ויחידה אורתונורמליזציה של $u_1\dots u_n$ באשר באיר בטיס א $u_1\dots u_n\in\mathbb{R}^n$ ויהיו $n\in\mathbb{N}_+$ יהי

לכל $C_i\left(M^\perp\right)=C_i\left(M^\perp\right)^\perp$ המקיימת $M^\perp\in\mathbb{R}^{n imes n}$ הפיכה אזי הפיכה $M\in\mathbb{R}^{n imes n}$ ותהא ותהא $n\in\mathbb{N}_+$ יהי יהי

 $\lambda_1\left[\mathcal{L}\left[M
ight]
ight] \geq \min_{i \in [n]}\left|\left\langle C_i\left(M
ight), C_i\left(M^\perp
ight)
ight
angle
ight|$ הפיכה אזי $M \in \mathbb{R}^{n imes n}$ ותהא $n \in \mathbb{N}_+$ יהי

n מדרגה $\mathcal{L}\subseteq\mathbb{R}^n$ אזי סריג ממשי $n\in\mathbb{N}_+$ יהי יהי מלאה: יהי

 $u_i \in [n]$ טענה: יהי $n \in \mathbb{N}_+$ ויהי $n \in \mathbb{N}_+$ סריג מדרגה מלאה n אזי קיימים $n \in \mathbb{N}_+$ בת"ל המקיימים $n \in \mathbb{N}_+$ ויהי

 $i\in[n]$ אאי לכל $i\in[n]$ אאי לכל איי לכל ויהיי $u_i=\lambda_i$ איי המקיימים $u_i=\lambda_i$ המקיימים ויהיי ויהיי $u_i=1$ איי לכל מסקנה: יהי $B_{\lambda_{i+1}[\mathcal{L}]}(0) \cap \mathcal{L} \subseteq \operatorname{span}(u_1 \dots u_i)$ מתקיים

 $\|C_i\left(M
ight)\|=\lambda_i\left[\mathcal{L}
ight]$ וכן $\mathcal{L}=\mathcal{L}\left[M
ight]$ וכן $M\in\mathbb{R}^{n imes n}$ אזי סריג \mathcal{L} מדרגה מלאה מלאה $n\in\mathbb{R}^n$ עבורו קיימת $i \in [n]$ לכל

. טענה: יהי \mathcal{L} אינו סריג סטנדרטי מדרגה באשר n באשר איים סריג סטנדרטי יהי $n \in \mathbb{N}_{>5}$

טענה: יהי $n \in [4]$ ויהי \mathcal{L} סריג מדרגה מלאה n אזי $n \in [4]$

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

 $u,v\in S$ משפט בליכפלדט: יהי $n\in\mathbb{N}_+$ יהי \mathcal{L} סריג מדרגה מלאה n ותהא ותהא $S\subseteq\mathbb{R}^n$ מדידה באשר יהי $n\in\mathbb{N}_+$ אזי קיימים $.u-v\in\mathcal{L}$ שונים עבורם

S=-S המקיימת $S\subseteq\mathbb{R}^n$ אזי קבוצה קמורה $n\in\mathbb{N}_+$ יהי יהי לראשית: יהי

משפט הגוף הקמור של מינקובסקי: יהי $n\in\mathbb{N}_+$ יהי יהי $S\subseteq\mathbb{R}^n$ ותהא מלאה n ביחס לראשית יהי יהי יהי יהי יהי יהי אוויה מינקובסקי: יהי יהי יחס לראשית $\mathcal{L} \cap S \neq \{0\}$ אזי $\operatorname{Vol}(S) > 2^n \cdot \det(\mathcal{L})$ באשר

אליפסואיד של סריג: יהי $\|u_i\|=\lambda_i[\mathcal{L}]$ יהי אליפסואיד של סריג: יהי $n\in\mathbb{N}_+$ יהי יהי $n\in\mathbb{N}_+$ אזי אליפסואיד אליפסואיד אליפסואיד איזי

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

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

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

 $\widehat{f+g}=\widehat{f}+\widehat{g}$ אזי $f,g\in L^{1}\left(\mathbb{R}^{n}
ight)$ ותהיינה $n\in\mathbb{N}_{+}$ אזי $n\in\mathbb{N}_{+}$

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

סענה: יהי $h\left(x
ight)=f\left(x+z
ight)$ כך $h:\mathbb{R}^{n} o\mathbb{R}$ כן נגדיר $z\in\mathbb{R}^{n}$ יהי $f\in L^{1}\left(\mathbb{R}^{n}
ight)$ אזי לכל $n\in\mathbb{N}_{+}$ יהי $n\in\mathbb{N}_{+}$ $\widehat{h}(\omega) = e^{2\pi i \cdot \langle w, z \rangle} \cdot \widehat{f}(\omega)$

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 $f\in L^1\left(\mathbb{R}^n
ight)$ אזי לכל $n\in\mathbb{N}_+$ מתקיים $\widehat{h}(\omega) = \frac{1}{\sqrt{n}} \cdot \widehat{f}(\frac{\omega}{\lambda})$

טענה: יהי $h\left(x
ight)=\prod_{i=1}^{n}f_{i}\left(x_{i}
ight)$ כך $h:\mathbb{R}^{n} o\mathbb{R}$ אזי לכל $f_{1}\dots f_{n}\in L^{1}(\mathbb{R})$ אזי לכל $n\in\mathbb{R}_{+}$ מתקיים $n\in\mathbb{R}_{+}$ $\hat{h}(\omega) = \prod_{i=1}^{n} \hat{f}_i(\omega_i)$

 $\mathcal{N}_n\left[\sigma
ight](x) = rac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$ כך $\mathcal{N}_n\left[\sigma
ight](x) = \frac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$ כך $\mathcal{N}_n\left[\sigma
ight](x) = \frac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$ כך $\mathcal{N}_n\left[\sigma
ight](x) = \frac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$ כך $\mathcal{N}_n\left[\sigma
ight](x) = \frac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$ כך $\mathcal{N}_n\left[\sigma
ight](x) = \frac{1}{(2\pi)^{rac{n}{2}} \cdot \sigma^n} \cdot e^{-rac{1}{2\sigma^2} \cdot \|x\|^2}$

 $\widehat{\mathcal{N}_n\left[\sigma
ight]} = \left(rac{\sqrt{2\pi}}{\sigma}
ight)^n\cdot\mathcal{N}_n\left[rac{1}{\sigma}
ight]$ איזי $n\in\mathbb{N}_+$ יהי $n\in\mathbb{N}_+$ יהי $n\in\mathbb{N}_+$ איזי $n\in\mathbb{N}_+$ יהי $n\in\mathbb{N}_+$ יהיו $n\in\mathbb{N}_+$ יהיו $n\in\mathbb{N}_+$ ותהא $n\in\mathbb{N}_+$ איזי $n\in\mathbb{N}_+$ איזי $n\in\mathbb{N}_+$ יהיו $n\in\mathbb{N}_+$ יהיו

 $\mathcal{S}\left(\mathbb{R}^{n},A
ight)=\left\{f\in C^{\infty}\left(\mathbb{R}^{n},A
ight)\ \middle|\ orall lpha,eta\in\mathbb{N}^{n}:\left\Vert f
ight\Vert _{lpha,eta}<\infty
ight\}$ אזי $A\subseteq\mathbb{C}$ אזי $n\in\mathbb{N}_{+}$ יהי שוורץ: יהי $n\in\mathbb{N}_{+}$ יהי

nטענה נוסחאת הסכימה של פואסון: יהי $n \in \mathbb{N}_+$ תהא $n \in \mathbb{N}$ ויהי n סריג מדרגה מלאה n אזי

 $\sum_{v \in \mathcal{L}} f(v) = \frac{1}{\det(\mathcal{L})} \cdot \sum_{v \in \mathcal{L}^{\vee}} \hat{f}(v)$

משפט: יהי $n\in\mathbb{R}$ היים $r\in\mathbb{R}$ אזי קיים arepsilon>0 המקיים מדרגה מלאה $n\in\mathbb{R}$ היהי

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

 $\pi_{\perp u}\left(v
ight)=\pi_{\perp u}:\mathbb{R}^n o\mathbb{R}^n$ אזי נגדיר $u\in\mathcal{L}$ אזי מדרגה מלאה n יהי \mathcal{L} סריג מדרגה מלאה $n\in\mathbb{N}_+$ אזי נגדיר $v - \frac{\langle u, v \rangle}{\|u\|^2} \cdot u$

```
\mathcal{L}_{\perp u} = \{\pi_{\perp u}\left(v
ight) \mid v \in \mathcal{L}\} אזי u \in \mathcal{L} אזי סריג ממשי מדרגה מלאה יהי סריג על וקטור: יהי \mathcal{L} סריג ממשי מדרגה מלאה ויהי
                                                                                   n-1 טענה: יהי \mathcal{L}_{\perp u} סריג מדרגה מלאה n ויהי n\in\mathbb{N}_+ אזי יהי n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+
                                                                               המקיימת M\in\mathbb{R}^{n\times n} אזי מדרגה מלאה n ויהי \mathcal{L} סריג ויהי n\in\mathbb{N}_+ המקיימת המקיימת
                                                                                                                                                                                                                                                                               \mathcal{L} = \mathcal{L}[M] \bullet
                                                                                                                                                                                                                                                         ||C_1(M)|| = \lambda_1[\mathcal{L}] \bullet
                                                                              \mathcal{L}_{\perp C_{1}(M)} עבור עבור 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
ight| מתקיים i\in\left[n\right] לכל
                                                                                                                                                                              \mathcal{L}ל \mathrm{KZ} לים בסיס ליים מלאה אזי קיים מדרגה מדרגה מדרגה משפט: יהי
טענה: יהי \mathcal L סריג מדרגה מלאה M\in\mathbb R^{n	imes n} באשר M\in\mathbb R^{n	imes n} של \mathcal L של בסיס אזי n\in\mathbb N_+ יהי n\in\mathbb N_+ יהי n\in\mathbb N_+
                                                                                                                                                                                                                                                                                                     מתקיימים
                         .\langle C_{i}\left(M\right),C_{i}\left(M^{\perp}\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\}\text{ מתקיים }i\in\left[n\right]לכל •
                                                                               \left.\left|\left\langle C_{i}\left(M\right),C_{j}\left(M^{\perp}\right)\right
ight
angle
ight| \leq rac{1}{2}\left|\left\langle C_{j}\left(M\right),C_{j}\left(M^{\perp}\right)
ight
angle
ight| מתקיים j< i באשר j \in [n] לכל
                                                                                                           M\in\mathbb{R}^{n	imes n} טענה: יהי M\in\mathbb{R}^{n	imes n} יהי מדרגה מלאה n\in\mathbb{N}_+ יהי ויהי n\in\mathbb{N}_+
                                                                                                                                                                       \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\right),C_{i}\left(M^{\perp}\right)\right
ight
angle 
ight|\leq\left\|C_{l}\left(M
ight)
ight\| מתקיים j\geq i באשר i,j\in\left[n\right] לכל •
                                                                                           .rac{1}{\sqrt{rac{i-1}{4}+1}}\cdot\|C_i\left(M
ight)\|\leq \lambda_i\left[\mathcal{L}
ight]\leq \sqrt{rac{i-1}{4}+1}\cdot\|C_i\left(M
ight)\| מתקיים i\in[n] מתקיים אזי מרך של סריג: יהי \mathbb{F} שדה יהי \mathcal{F}\subseteq\mathbb{F} יהי m\in\mathbb{N}_+ תהא הפיכה ויהי m\in\mathbb{F}^n אזי אזי של סריג: יהי \mathbb{F}
                                                                                                                                                                                                  .Val-lattice (M, t, \mathbb{F}, \mathcal{F}) = \min_{x \in \mathcal{F}^n} \|Mx - t\|
בעיית חיפוש הוקטור הקרוב ביותר בסריג: יהי \mathbb{F} שדה יהי \mathcal{F}\subseteq\mathbb{F} יהי תהא m\in\mathbb{F}^{n	imes n} הפיכה יהי הפיכה t\in\mathbb{F}^n ויהי
                                                                                                                                                       \|Mv - t\| \le \varepsilon באשר CVP-lattice-search ((M, t, \mathbb{F}, \mathcal{F}), \varepsilon) = v
                                                                  .CVP-lattice = \{\langle M, t, \mathbb{F}, \mathcal{F}, \varepsilon \rangle \mid \text{Val-lattice}(M, t, \mathbb{F}, \mathcal{F}) < \varepsilon \} בעיית הוקטור הקרוב ביותר בסריג:
                                                                   המקיימת M\in\mathbb{R}^{n	imes n} אזי \delta>0 ויהי ווהי n\in\mathbb{N}_+ יהי המקיימת לנסטרה־לנסטרה־לנסטרה־לובאס ויהי
                              \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 מתקיים j< i מתקיים j< i באשר j\in[n] באשר •
\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]
                                                                                טענה: יהי \delta > 0 אזי לכל \delta = n-1 מצומצמת אזי לכל \delta = n-1 מתקיים יהי \delta > 0 יהי ותהא יהי \delta > 0
                                                                                                                                                              \langle C_{i+1}(M), C_{i+1}(M^{\perp}) \rangle \ge \sqrt{\delta - \frac{1}{4} \cdot \langle C_i(M), C_i(M^{\perp}) \rangle}
                                    \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} אא \delta-LLL מענה: יהי n\in\mathbb{N}_+ יהי \delta>0 ותהא \delta>0 ותהא M\in\mathbb{R}^{n	imes n} הפיכה אזי ... M\in\mathbb{N}_+ יהי n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+ יהי n\in\mathbb{N}_+ יהי ווייים ווייים אלגוריתם מערכת מדיר און איני ווייים וויים ווייים וויים ווייים וויים ווייים ווייים ווייים ווייים ווייים ווייים ווייים ווייים וויי
                                                               \mathcal{D}\mathcal{D}\left[M
ight] = \prod_{i=1}^{n} \left|\left\langle C_{i}\left(M
ight), C_{i}\left(M^{\perp}
ight)
ight
angle \right|^{n-i+1} כך \mathcal{D}\mathcal{D}: \mathbb{Z}^{n 	imes n} 	o \mathbb{N} אזי נגדיר n \in \mathbb{N}_{+} יהי יהי n \in \mathbb{N}_{+} יהי
                                                                                               1\leq\mathcal{DD}\left[M
ight]\leq\left(\max_{i\in[n]}\left\|C_{i}\left(M
ight)
ight\|
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}_{+}
                                                                                                 \mu\left(\mathcal{L}
ight)=\max_{t\in\mathbb{R}^n}\mathrm{dist}\left(t,\mathcal{L}
ight) אזי n\in\mathbb{N}_+ ויהי n\in\mathbb{N}_+ ויהי סריג מדרגה מלאה מ
                                                                                                                                              -rac{1}{2}\lambda_n\left[\mathcal{L}
ight] \leq \mu\left(\mathcal{L}
ight) אזי n\in\mathbb{N}_+ טענה: יהי n\in\mathbb{N}_+ ויהי n\in\mathbb{N}_+ סריג מדרגה מלאה
                                                                              ... אזי t\in\mathbb{R}^n ויהי \delta	ext{-LLL} מצומצמת מצומצמת M\in\mathbb{R}^{n	imes n} תהא \delta>0 יהי n\in\mathbb{N}_+ יהי
                                                                       O\left(n^2
ight) הינה NaiveMatMul איז סיבוכיות הריצה איז n\in\mathbb{N}_+ הינה n\in\mathbb{N}_+ הינה \mu\left(\mathcal{L}\left[M
ight]\right)\leq rac{1}{2}\sqrt{\sum_{i=1}^{n}\left\langle C_i\left(M
ight),C_i\left(M^\perp
ight)
ight
angle^2} הפיכה איז M\in\mathbb{R}^{n	imes n} ותהא n\in\mathbb{N}_+ ותהא הפיכה איז היי
                                                                                                                                     \mu\left(\mathcal{L}
ight) \leq rac{\sqrt{n}}{2} \lambda_n\left[\mathcal{L}
ight] אזי n \in \mathbb{N}_+ ויהי n \in \mathbb{N}_+ ויהי מסקנה: יהי
\|t-\operatorname{Babai}\left(M,t
ight)\|\leq 2^{rac{n}{2}-1}\left|\left\langle C_{n}\left(M
ight),C_{n}\left(M^{\perp}
ight)
ight
angle אזי t\in\mathbb{R}^{n} אזי t\in\mathbb{R}^{n} מצומצמת M\in\mathbb{R}^{n	imes n} מצומצמת M\in\mathbb{R}^{n	imes n}
                                                                                                                               	ext{CVP-lattice-search} מסקנה: Babai \circ \frac{3}{4}-LLL מסקנה: Babai \circ \frac{3}{4}-LLL
                                         \mathrm{GAP}_{[T,S]}\mathrm{CVP}=\mathrm{GAP}_{[T,S]}\mathrm{Val\text{-lattice}} אזי איי תהיינה תהיינה בסריג: תהיינה בסריג: תהיינה אוי
                                                                                                                         \mathrm{GAP\text{-}CVP}_T=\mathrm{GAP}_{[r,r\cdot T]}\mathrm{CVP} אזי איזי T:\mathbb{N}	o\mathbb{N} הגדרה: תהא
             .\mathrm{Val\text{-}lattice}_0\left(M,\mathbb{F},\mathcal{F}\right)=\min_{x\in\mathcal{F}^n\setminus\{0\}}\|Mx\| הפיכה אזי M\in\mathbb{F}^{n\times n} ותהא ותהא n\in\mathbb{N}_+ יהי \mathcal{F}\subseteq\mathbb{F} יהי שדה יהי \mathcal{F}\subseteq\mathbb{F} יהי
```