```
\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 אוית אזי לתיקון איאות אזי \mathcal{C}\subseteq [q]^m ויהי ויהי יהיו איאות: יהיו אגיאות: יהיו לתיקון אגיאות אזי אלפבית בקוד לתיקון א
                                                     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 ויהי 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 \mathcal{C} הינו לתיקון שגיאות לתיקון שגיאות ויהי q,m\in\mathbb{N}_{+} ויהי
                          w' \notin \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|\; \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}_+ האמינג: יהי m \in \mathbb{N}_+ אזי
                                   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.
. לתיקון שגיאות [m+1,r,d+1,2] ויהיו m,r\in\mathbb{N}_+ עבורם קיים קוד שגיאות [m,r,d,2] לתיקון שגיאות אזי קיים קוד שגיאות עבורם איים קיים קוד
                                     |\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} למה פלוטקין: יהיו [m,r,d,q] לויהי d \geq \left(1-rac{1}{q}
ight)m באשר באשר למה פלוטקין: יהיו
                                        ...|\mathcal{C}| \leq d \cdot 2^{m-2d+2} טענה: יהיו m,r,d, באשר שויהיd \leq \frac{m}{2} ויהיd \leq \frac{m}{2} ויהי ליהיו
            . פוטורי. מרחב \mathcal{C} כי מרחב המקיים כי המקיים לתיקון שגיאות קוד לינארי \mathbb{F}_q שדה אזי קוד לינארי q,m\in\mathbb{N}_+ יהיו הייו איים לינארי לתיקון לינארי לתיקון לינארי הייו
                                                                                      \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\} יסענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות יהי
                                        M\in\mathbb{F}^{m	imes n} אזי M\in\mathbb{F}^{m	imes n} תהא m,n\in\mathbb{N}_+ ויהי \mathbb{F} אזי \mathbb{F} אזי M\in\mathbb{F}^{m	imes n} מערכת משוואות 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) ערך של מערכת משוואות לינארית: תהא (M,t,\mathbb{F}) מערכת משוואות לינארית
	ext{CVP-code-search}\left((M,t,\mathbb{F})\,,arepsilon
ight)=v איי arepsilon>0 איי מערכת משוואות לינאריות משוואות לינאריות משוואות אויהי (M,t,\mathbb{F}) מערכת משוואות לינאריות ויהי
                                                                                                                                                         \|Mv - t\|_0 \le \varepsilon באשר
                                                                  .CVP-code = \{\langle (M,t,\mathbb{F})\,, \varepsilon \rangle \mid \mathrm{Val}\,((M,t,\mathbb{F})) \leq \varepsilon \} בעיית הוקטור הקרוב ביותר:
                                                                                               . טענה: יהיו לתיקון אזי אזי אזי אזי q,m,k\in\mathbb{N}_+ יהיו טענה: יהיו
                                                                                                M_{\mathcal{C}_{k	ext{-rep}}}=egin{pmatrix} I_m\\ I_m\\ \vdots\\ I_m \end{pmatrix} אזי q,m,k\in\mathbb{N}_+ אזי מסקנה: יהיו q,m\in\mathbb{N}_+ אזי \mathcal{C}_{	ext{parity}} קוד לינארי לתיקון שגיאות. \mathcal{C}_{	ext{parity}}=egin{pmatrix} I_m\\ I_T^{m} \end{pmatrix}=egin{pmatrix} I_m\\ I_T^{m} \end{pmatrix} אזי q,m\in\mathbb{N}_+ מסקנה: יהיו q,m\in\mathbb{N}_+ אזי q,m\in\mathbb{N}_+
                                                                          d = \min_{v \in \mathcal{C}} \Delta\left(v,0\right) יטענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי
                                                                  .SVP-code = \{\langle (M,0,\mathbb{F}), \varepsilon \rangle \mid \exists v \neq 0. \|Mv\|_0 \leq \varepsilon \} בעיית הוקטור הקצר ביותר:
```

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

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

```
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
                                                                                                                                                                                                                                                                                                                                                                                         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[m]
ight\} אזי M\in\mathbb{F}^{m	imes n} ותהא m,n\in\mathbb{N}_{+} שדה יהי \mathbb{F} שדה יהי שדה יהיו
                                                                                                                                                                                                                                                                        [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}}
ight)\cap V|=m-d וכן \dim\left(V
ight)=r-1 המקיים V\subseteq\mathcal{C} המקיים •
. לתיקון שגיאות אזי קיים [m-d,r-1,d',q] לתיקון שגיאות אזי קיים d'\geq \left[rac{d}{q}
ight] לתיקון שגיאות אזי קיים [m,r,d,q] לתיקון שגיאות.
                                                                       m\geq\sum_{i=0}^{r-1}\left\lceil rac{d}{q^i}
ight
ceil} משפט גרייסמר: יהי \mathcal C קוד לינארי [m,r,d,q] לתיקון שגיאות אזי m>r באשר m>r\in\mathbb R_q^m שדה יהיו m>r באשר m>r\in\mathbb N_q שדה יהיו m>r באשר m באשר
                                                                                                                                                                                                                                                                                                                                                                     \mathbb{P}_{M \in \mathbb{F}_q^m \times r} (Mx = b) = \frac{1}{q^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  $q\in\mathbb{N}_+$  אזי  $q\in\mathbb{N}_+$ 

משפט: יהי 
$$\delta\in(0,1)$$
 אזי  $m>r$  באשר  $m,r\in\mathbb{N}_+$  שדה יהיו  $\mathbb{F}_q$  שדה יהיו  $q\in\mathbb{N}_+$  אזי 
$$.\mathbb{P}_{M\in\mathbb{F}_q^{m\times r}}\left(d\left[\mathcal{C}_M\right]\leq (1-\delta)\left(m-\frac{m}{q}\right)\right)\leq |\mathcal{C}_M|\cdot\exp\left(-\frac{\delta^2}{2}\left(m-\frac{m}{q}\right)\right)$$
 
$$.\mathcal{C}^\vee=\{w\in\left[q\right]^m\mid\forall c\in\mathcal{C}.\langle w,c\rangle=0\}$$
 לתיקון שגיאות אזי  $\{m,r,d,q\}$  לתיקון שגיאות אזי יהי  $\mathcal{C}$  קוד לינארי  $\{m,r,d,q\}$ 

. לעיקון שגיאות [m, m-r, d', q] לינארי הינו  $\mathcal{C}^\vee$  עבורו לינארי  $\mathcal{C}^\vee$  עבורו איי קיים איי קיים  $\mathcal{C}^\vee$  לתיקון שגיאות איי קיים לינארי  $H_{\mathcal{C}}=M_{\mathcal{C}^{ee}}$  אזי אויי לינארי לתיקון איי יהי יהי אריות: יהי מטריצת בדיקת איי

 $\mathcal{C}=\ker\left(H_{\mathcal{C}}^{T}
ight)$  יטענה: 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 האטר m>r באשר  $m,r\in\mathbb{N}_+$  שדה יהיו קוד לינארי מקסימלי לתיקון  $A \in \mathcal{P}_r(R(M))$  בת"ל), שגיאות)

. טענה: יהי  $\mathcal{C}$  קוד לינארי מקסימלי לתיקון שגיאות אזי  $\mathcal{C}^\vee$  הינו אזי לתיקון שגיאות מקסימלי לתיקון שגיאות יהי

משפט גילברט־וורשאמוב: יהיו m באשר m באשר ש ויהי  $d \leq m$  ויהי לינארי היון שגיאות לתיקון שגיאות  $d \leq m$  באשר  $|\mathcal{C}| \ge q^m \cdot \left(\sum_{i=0}^{d-1} \left(\binom{m}{i} \cdot (q-1)^i\right)\right)^{-1}$ 

 $H \in \mathbb{F}_q^{m imes (m-k)}$  אזי קיים  $\sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k}$  עבורו  $q \in \mathbb{P}$  עבורו  $k \leq m$  באשר באשר אזי קיים  $k \leq m$  באשר למה: יהי 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  $\sum_{i=0}^{d-2} \binom{m-1}{i} \left(q-1
ight)^i < q^{m-k}$  אויהי  $q\in\mathbb{P}$  אויהי  $k\leq m$  באשר באשר  $k,m\in\mathbb{N}_+$  יהיו  $k\leq m$  באשר אמוב: יהי  $k\leq m$  יהיו  $|\mathcal{C}| \geq q^m \cdot \left(1 + \sum_{i=0}^{d-2} \left({m-1 \choose i} \cdot (q-1)^i\right)\right)^{-1}$  קיים קוד לינארי [m,k,d,q] לתיקון שגיאות  $f:X o Y^n$  אוי  $f:X o Y^n$  אוי  $f:X o Y^n$  אוי  $f:X o Y^n$  אוי אוי  $f:X o Y^n$  עבורה

 $g\left(f\left(s
ight)_{p_1},\ldots,f\left(s
ight)_{p_k}
ight)=s$  מתקיים  $g:Y^k o X$  מרקיים  $g:Y^k o X$  קיימת

 $.g\left(f\left(s\right)_{p_{1}},\ldots,f\left(s\right)_{p_{k-1}}
ight)=s$  מתקיים  $p_{1},\ldots,p_{k-1}\in\left[n
ight]$  ולכל ולכל  $s\in X$  עבורה לכל  $g:Y^{k-1} o X$  מתקיים  $g:Y^{k-1} o X$ arphi כך  $arphi: \mathbb{F}_{\leq k-1}[x] o \mathbb{F}^\ell$  יהי שונים ונגדיר  $x_1\dots x_\ell\in \mathbb{F}$  יהי שדה סופי באשר שדה  $\ell\leq k$  שונים ונגדיר  $\ell\leq k$  טענה: יהיו

אט פולינומי. איזומורפיזם וכן  $arphi, arphi^{-1}$  חשיבות איז איזומורפיזם פולינומי. • אס איזומורפיזם איזומורפיזם וכן

אזי  $\varphi(p) = (p(x_i))_{i=1}^{\ell}$ 

 $k-\ell$  ממימד אפיני ממימד  $arphi^{-1}\left(y
ight)$  מתקיים כי  $y \in \mathbb{F}^{\ell}$  אז לכל  $\ell < k$ 

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

מסקנה: יהי  $q \in \mathbb{N}$  באשר  $\hat{\mathbb{F}_q}$  שדה יהי  $n \in \mathbb{N}_+$  באשר  $n \in \mathbb{N}_+$  ויהי ויהי ויהי  $n \in \mathbb{N}_+$  אזי סכימת שמיר הינה סכימת חלוקת סוד מושלמת.

קוד ריד־סולומון: יהי  $lpha_1 \ldots lpha_m \in \mathbb{F}_q$  ויהיו  $r \in [m]$  יהי יהי שדה יהי שדה באשר  $q \in \mathbb{N}$  יהי יהי יהי  $.RS_{q}[m, r] = \left\{ (f(\alpha_{i}))_{i=1}^{m} \mid f \in (\mathbb{F}_{q})_{\leq r-1}[x] \right\}$ 

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

טענה: יהי  $\mathrm{RS}_q\left[m,r
ight]$  אזי  $lpha_1\ldotslpha_m\in\mathbb{F}_q$  ויהיו 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  $lpha_1\ldotslpha_m\in\mathbb{F}_q$  יהי  $m\in[q]$  לכל לכל ענה: יהי  $m\in[q]$  איזי איז  $q\in\mathbb{N}$  טענה: יהי  $\sum_{x\in\mathbb{F}_q}x^i=0$  אזי  $i\in\{0,\ldots,q-2\}$  שדה ויהי  $\mathbb{F}_q$  באשר באשר ענה: 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 q \in \mathbb{N} איזי q \in \mathbb{N}
                                                                                                                                                                   r\left[\mathrm{RM}_{2}\left[m,r
ight]
ight]=\sum_{i=0}^{r}inom{m}{i} אזי m,r\in\mathbb{N}_{+} יהיו
                                                         משפט: יהי r=a\,(q-1)+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}
                                                                                                                                              \mathrm{RM}_2\left[m,r
ight]^ee = \mathrm{RM}_2\left[m,m-r-1
ight] אזי m,r \in \mathbb{N}_+ יהיו
                                    \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
שרשור קודים לתיקון שגיאות: יהי \mathcal{C} קוד [m,r,d,q] לתיקון שגיאות ותהא [m,r,d,q] לתיקון שגיאות: יהי \mathcal{C} קוד קודים לתיקון שגיאות: יהי
                                                                                                                                                                   \mathcal{C} \circ \mathcal{C}' = \{(\rho(w_i))_{i=1}^m \mid w \in \mathcal{C}\} הפיכה אזי \rho: [q] \to \mathcal{C}'
                                 סענה: יהי \mathcal{C}\circ\mathcal{C}' אזי אזי לתיקון שגיאות אזי \left[m',\log_{q'}\left(q\right),d',q'\right] קוד קוד לתיקון שגיאות אזי לתיקון שגיאות ויהי
                                                                                                                                                                                         לתיקון שגיאות. \left[m \cdot m', r \cdot \log_{a'}(q), d \cdot d', q'\right]
הפיכה אזי 
ho:[q]	o \mathcal{C}' הות ותהא לתיקון שגיאות יהי [m',\log_{a'}(q)\,,d',q'] הוד קוד שגיאות היהי לתיקון שגיאות היהי לתיקון שגיאות היהי לתיקון שגיאות היהי
                                                                                                      \mathcal{C}\circ\mathcal{C}'\simeq\left\{h:[m]	imes[m']	o[q]\ \middle|\ \exists w\in\mathcal{C}.h\,(i,j)=(
ho\,(w_i))_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] אזי נהדרה: יהי n\in\mathbb{N}
                                                                                                     \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}_+ אזי n \in \mathbb{N}_+ הינו קוד לינארי n \in \mathbb{N}_+ לתיקון שגיאות. n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ הינו קוד לינארי
                                                                                                                                   \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}}\ \Big|\ i\in[n]
ight\} אזי n\in\mathbb{N}_{+} אזי היי n\in\mathbb{N}_{+} אזי הינו קוד \left[2^{n},\log_{2}\left(n
ight),2^{n-1},2
ight] לתיקון שגיאות. n\in\mathbb{N}_{+} אזי היי n\in\mathbb{N}_{+} אזי הינו קוד
                                                                                                                                                                                     \mathcal{C}_{	ext{Dic}} \simeq ig\{\chi_{\{i\}} \; ig| \; i \in [n]ig\} אזי n \in \mathbb{N}_+ יהי הערה: יהי
                                                                                               B_r(x)=\{y\in X\mid \Delta\left(x,y
ight)\leq r\} אזי x\in X ויהי ויהי r\in\mathbb{R}_+ איזי קבוצה יהי קבוצה יהי
|B_r\left(w
ight)\cap\mathcal{C}|\leq\ell מתקיים w\in[q]^m מתקיים שגיאות איי קוד ו[m,k,d,q] איי קוד איי קוד איי איי פוד ולתיקון שגיאות איי איי פוד וואיי קוד איי קוד וואיי קוד וואיי איי קוד מתקיים איי קוד וואיי פון דער איי קוד וואיי קוד וואיי קוד מתקיים איי קוד וואיי וואיי קוד וואיי וואייים וואיי וואיי
(m,k,d,q) איז m,k,r,\ell,q ויהי m,k,d,q לתיקון שגיאות רשימתי ויהי m,k,d,q הינו קוד 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
                                                                                                                                                                                                                                                              אלגוריתם סודן: ...
                                                                                                                    i\in[n] לכל \left(ec{1}
ight)_i=1 כך ec{1}\in\mathbb{F}^n אזי נגדיר n\in\mathbb{N}_+ לכל שדה ויהי \mathbb{F}
                                 	ext{NaxCut} = \left\{ \left\langle \left(M, ec{1}, \mathbb{F}_2 \right), arepsilon 
ight
angle \mid \left( orall i \left( w \left( R_i \left( M 
ight) 
ight) = 2 
ight) 
ight) \wedge \left( 	ext{Val} \left( \left(M, ec{1}, \mathbb{F} 
ight) 
ight) \leq arepsilon 
ight) 
ight\} בעיית החתך המקסימלי:
                                                                                                                    . פענה: קיים \operatorname{GAP}_{[\varepsilon,1-\varepsilon]}\operatorname{MaxCut} עבורו עבורו \varepsilon\in(0,1) הינה
                                                                                                                                                            . הינה \mathcal{NP}-קשה הינה \mathcal{C}\mathrm{VP\text{-}code}_{\varepsilon} עבורו \varepsilon \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 איי a,b \in [0,1] יהיי ביותר: יהיו לוקטור הקרוב ביותר:
                                                                   . הינה \mathcal{NP} הינה \mathrm{GAP}_{[arepsilon,1-arepsilon]} הינה שדה סופי \mathbb{F} עבורו עבורו \varepsilon>0 הינה arepsilon>0
                                                     \mathcal{P}=\mathcal{NP} אז CVP-code-search מסקנה: אם קיים אלגוריתם פולינומי A אשר מהווה אשר פולינומי
(M)_{i,j}=1 עבורו 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 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) אזי t \in \mathbb{F}^m מטריצת משחק מטריצת משחק ויהי M \in \mathbb{F}^{n 	imes m} שדה תהא
```

 $\mathrm{RM}_q\left[m,r
ight] = \left\{(f\left(lpha
ight))_{lpha \in \mathbb{F}_n^m} \mid f \in (\mathbb{F}_q)_{<_T}[x_1,\ldots,x_m]
ight\}$  אזי  $m,r \in \mathbb{N}_+$  שדה ויהיו  $\mathbb{F}_q$  שדה ויהיו  $q \in \mathbb{N}$  אזי  $q \in \mathbb{R}_q$ 

 $[q^m,r,d,q]$  אזי קיימים  $\mathrm{RM}_q[m,r]$  עבורם  $r,d\in\mathbb{N}_+$  אזי קיימים  $m,r\in\mathbb{N}_+$  שדה ויהיו שדה לינארי  $r,d\in\mathbb{N}_+$ 

 $\mathrm{RS}_{q}\left[q,r
ight]^{ee}=\mathrm{RS}_{q}\left[q,q-r
ight]$  אזי  $r\in\left[q
ight]$  שדה ויהי  $\mathbb{F}_{q}$  שדה באשר  $q\in\mathbb{N}$  יהי

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

 $r\left[\mathrm{RM}_q\left[m,r
ight]
ight] = inom{m+r}{r}$  אזי r < q איזי איזי  $m,r \in \mathbb{N}_+$  שדה ויהיו  $\mathbb{F}_q$  שדה יהי  $q \in \mathbb{N}$  איזי

אלגוריתם ברלקמפ־וולץ': ...

שגיאות.

```
\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 היחודיים: יהי
                                                      השערת המשחקים היחודיים: יהי arepsilon>0 אזי \mathrm{UG}\left(arepsilon
ight) אזי יהי פתוחה השערת המשחקים היחודיים: יהי
                              . 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 שדה יהי
                                                                                     אזי u,v\in\mathbb{F}^m אזי מטריצת משחק ויהיו M\in\mathbb{F}^{n	imes m} אזי הגדרה: יהי
                                                                                                    \operatorname{Val}_{2\to 1}\left(\left(M,\left\{u,v\right\},\mathbb{F}\right)\right) = \min_{t\in\operatorname{Interpol}(u,v)}\operatorname{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] יהיי יהיי על אחד: יהיי 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 אזי אזי
                                                                                                                \frac{1}{2}\mathrm{UG}\left(\varepsilon\right)=\mathrm{PCP}_{1\leftrightarrow1}\left[\frac{1}{2},1-arepsilon
ight] אזי arepsilon>0 אזי arepsilon>0
                                                                                                            -קשה. Promise-\mathcal{NP} הינה \frac{1}{2}\mathrm{UG}\left( arepsilon 
ight) אזי arepsilon > 0 אזי יהי
             A \in \mathbb{F}^{m 	imes n} ותהא A \in \mathbb{F}^{m 	imes n} ותהא A \in \mathbb{F}^{k 	imes m} ותהא אזי A \in \mathbb{F}^{k 	imes m} ותהא אזי A \in \mathbb{F}^{k 	imes m} ותהא
                                      \dots אזי B\in\mathbb{F}^{m	imes n} ותהא A\in\mathbb{F}^{k	imes m} אזי תהא k,m,n\in\mathbb{N}_+ שדה יהיי \mathbb{F} שדה שלגוריתם כפל מטריצות נאיבי: יהי
.\Theta\left(kmn
ight) הינה NaiveMatMul אזי סיבוכיות הריצה אל B\in\mathbb{F}^{m	imes n} ותהא ותהא אA\in\mathbb{F}^{k	imes m} הינה k,m,n\in\mathbb{N}_+ שדה יהי
                                                                                                                 אזי a,b\in \left\{0,1
ight\}^n ויהיו n\in \mathbb{N} אזי היי 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
```

```
... אזי A,B\in\mathbb{F}^{2^n	imes 2^n} ותהיינה n\in\mathbb{N} אזי שדה יהי \mathbb{F} אזי שלגוריתם סטרסן: יהי
                               A,B \in \mathbb{F}^{2^n \times 2^n} ותהיינה n \in \mathbb{N} שדה יהי n \in \mathbb{N} שדה יהי שדה יהי n \in \mathbb{N}
                                                                            \mathcal{O}\left(m^{\log_2(7)}
ight) הינה StrassenMatMul טענה: סיבוכיות הריצה של
                         \mathrm{MatInv}\left(\mathbb{F},A
ight)=A^{-1} הפיכה אזי A\in\mathbb{F}^{n	imes n} ותהא n\in\mathbb{N}_+ יהי \mathbb{F} שדה יהי \mathbb{F} שדה יהי \mathbb{F}
                         (T:\mathbb{N} \to \mathbb{N} \to \mathbb{N}) משפט: תהא אזי (בעיית T:\mathbb{N} \to \mathbb{N} חשיבה בזמן האמר 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}_{+} ותהא דטרמיננטה: יהי \mathbb{F} שדה יהי n\in\mathbb{N}_{+}
                        (T : \mathbb{N} \to \mathbb{N} \to \mathbb{N}) משפט: תהא אזי (בעיית MatMul משפט: תהא אזי (בעיית T : \mathbb{N} \to \mathbb{N}
                                                                                                                                                   בעיית פירוק LU: ...
                        משפט: תהא \mathbb{M} : \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{T}: \mathbb{N} \to \mathbb{N}
                                                                                                                   בעיית פתרון מערכת משוואות לינארית: ...
                     משפט: תהא \mathbb{M} אזי (בעיית MatMul חשיבה בזמן \mathbb{M}). משפט: תהא \mathbb{N} \to \mathbb{N} אזי (בעיית בימן \mathbb{N}).
                      \mathcal{L}_{\mathbb{F}|\mathcal{F}}[M] = \left\{ M \cdot x \mid x \in \mathcal{F}^k 
ight\} אזי M \in \mathbb{F}^{n 	imes k} ותהא n, k \in \mathbb{N}_+ יהיו \mathcal{F} \subseteq \mathbb{F} יהי שדה יהי
   \mathrm{dim}\left(\mathcal{L}_{\mathbb{F}|\mathcal{F}}[M]
ight)=k אזי M\in\mathbb{F}^{n	imes k} מדרגה M\in\mathbb{F}^{n	imes k} חוג יהיו n,k\in\mathbb{N}_+ חוג יהיו \mathcal{F}\subseteq\mathbb{F} חוג יהיו
\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 יהי\mathcal{F}\subseteq\mathbb{F} חוג יהי
                                                             \mathcal{L}\left[M
ight]=\mathcal{L}_{\mathbb{R}|\mathbb{Z}}\left[M
ight] יימון: יהיו n,k\in\mathbb{N}_{+} ותהא M\in\mathbb{R}^{n	imes k} ותהא
                                                                            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} לכל
```

- $\max\left\{|V|\mid (V\subseteq\mathcal{L})\wedge (\mathbb{Z} \text{ and } V)
  ight\}=k$ 
  - $B_r(0) \cap \mathcal{L} = \{0\}$  המקיים r > 0 היים •

 $\dim(\mathcal{L},k)=k$  מימד של סריג אבסטרקטי: יהיו  $k,n\in\mathbb{N}_+$  ותהא אות סריג באטרקטי אזי של סריג אבסטרקטי אזי נסמן  $\mathcal{L}=(\mathcal{L},k)$  הערה: יהי  $\mathcal{L}=(\mathcal{L},k)$  סריג אבסטרקטי אזי נסמן