```
\mathcal{C}\subseteq\left[q
ight]^m קוד לתיקון שגיאות: יהיו q,m\in\mathbb{N}_+ אזי
                                                                                            q,m\in\mathbb{N}_+ ויהי לתיקון לתיקון לתיקון אזי פודל אלפבית ויהי יהיו יהיו יהיו איזי אוודל האלפבית בקוד לתיקון איאות: יהיו
                                                                                                m אזי אזי לתיקון איאות אזי לתיקון ויהי q,m\in\mathbb{N}_+ ויהי אזי 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_q |\mathcal{C}| אזי לתיקון שגיאות אזי לתיקון ויהי q,m \in \mathbb{N}_+ ויהי יהיו לתיקון שגיאות אזי מימד/קצב בקוד לתיקון אייאות:
                             . הערה: [m,r\,[\mathcal{C}]\,,d\,[\mathcal{C}]\,,q] הינו קוד [m,r\,[\mathcal{C}]\,,d\,[\mathcal{C}]\,,q] הינו אזי נאמר כי [q,m\in\mathbb{N}_+] לתיקון שגיאות איי נאמר כי
                                                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} 
ight
vert באשר w' \in [q]^m ויהי w \in \mathcal{C} ויהי לתיקון שגיאות יהי
                                                                             (w,w) \leq \lfloor \frac{1}{2} \rfloor^{m} פשפט חסם הסינגלטון: יהי m,r,d,qן דור m,r,d,qן לתיקון שגיאות אזי m,r,d,qן לתיקון יהי m,r,d,qן אזי m,r,d,qן לתיקון שגיאות אזי m,r,d,qן לתיקון שגיאות. m,r,d,qן אזי m,r,d,qן אזי m,r,d,qן לתיקון שגיאות. m,r,d,qן אזי m,r,d,qן אזי m,r,d,qן אזי m,r,d,qן אזי m,r,d,qן לתיקון שגיאות. m,r,d,qן אזי m,r,d,q
                                                                                                          . טענה: יהיm \in \mathbb{N}_+ אזי \mathcal{C}_{\mathrm{Hamming}} הינו קוד \mathcal{C}_{\mathrm{Hamming}} אזי אזי אות.
                                                                טענה: יהיו d' \geq d עבורו אזי קיים שגיאות לתיקון [m,r,d,q] עבורו קיים קוד m,r,d,q \in \mathbb{N}_+ עבורו
                                                                                                                                                                                                                           . 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 m,r,d+1,2 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 אזי (m,r,d,q] לתיקון שגיאות אזי [m,r,d,q] לתיקון שגיאות אזי [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 לאר פלוטקין: יהיו d \geq \left(1-rac{1}{q}
ight)m באשר באשר לאר פוד d,q,m \in \mathbb{N}_+ לתיקון שגיאות אזי לאר באשר באשר באשר לאר פוד d,m \in \mathbb{N}_+ לתיקון שגיאות אזי לאר באשר באשר לאר פוד לאריקון שגיאות אזי לאריקון שגיאות אזי לאריקון פודי לאיי לאריקון פודי לאריקון 
                      . באשר \mathcal{C} מרחב המקיים כי \mathcal{C}\subseteq\mathbb{F}_q^m המיאות לינארי לתיקון שהיאות שבה אזי קוד אזי באשר באשר \mathbb{F}_q באשר שבה אזי קוד לינארי לתיקון שגיאות: יהיו
                                                                                                                                                            \dim\left(\mathcal{C}
ight)=r טענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות אזי
C_i\left(M_{\mathcal{C}}
ight)=b_i המוגדרת אזי איז בסיס איז בסיס לתיקון שגיאות ויהי לתיקון שגיאות [m,r,d,q] לתיקון שגיאות יוצרת: יהי
                                                                                                                                                                                                                                                                                                                    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
                                                                                                                                                                            טענה: יהיו q,m,k\in\mathbb{N}_+ אזי קוד לינארי לתיקון שגיאות. M_{\mathcal{C}_{k\text{-rep}}}=inom{I_m}{\vdots} אזי q,m,k\in\mathbb{N}_+ מסקנה: יהיו q,m,k\in\mathbb{N}_+
                                                                                                                                                                                  טענה: יהיו m\in\mathbb{N}_+ אזי \mathcal{C}_{\mathrm{parity}} קוד לינארי לתיקון שגיאות. M_{\mathcal{C}_{\mathrm{parity}}}=\left(egin{array}{c}I_m\\ \vec{\mathbf{l}}^T\end{array}
ight)=\left(egin{array}{c}I_m\\ \vec{\mathbf{l}}^T\end{array}
ight) 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
ight) איי שגיאות אזי ווי[m,r,d,q] לתיקון לינארי יהי
A \in \mathbb{F}_q^{(m-r) 	imes r} עבורו קיימת \mathcal{D} עבורו איימת (תיקון שגיאות איי קיים קוד לינארי [m,r,d,q] לתיקון שגיאות איימת [m,r,d,q]
                                                                                                                                                                                                                                                                                      M_{\mathcal{D}} = \left( \begin{smallmatrix} I_r \\ A \end{smallmatrix} \right) המקיימת
```

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

 $R\left(M
ight)=\left\{R_{i}\left(M
ight)\mid i\in\left[m
ight]
ight\}$  אזי  $M\in\mathbb{F}^{m imes n}$  ותהא  $m,n\in\mathbb{N}_{+}$  שדה יהיי שדה יהיי

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

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

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

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

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

```
m\geq\sum_{i=0}^{r-1}\left\lceil rac{d}{q^i}
ight
ceil לתיקון שגיאות אזי [m,r,d,q] לתיקור לינארי יהי c קוד לינארי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו שדה יהיו m>r באשר m,r\in\mathbb{N}_+ אזי לכל למה: יהי m>r באשר שדה יהיו לכל למה: יהי
                                                                                                                                                                                        \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} אזי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו m>r באשר m,r\in\mathbb{N}_+ שדה יהיו m>r באשר m,r\in\mathbb{N}_+ שדה ויהיו m>r באשר m,r\in\mathbb{N}_+ שדה ויהיו m>r באשר m,r\in\mathbb{N}_+ באשר m,r\in\mathbb{N}_+
                                                                               משפט: יהי m>r באשר m,r\in\mathbb{N}_+ שדה יהיו \mathbb{F}_q שדה יהי m>r באשר משפט: יהי באשר ק
                                             .\mathbb{P}_{\substack{M \in \mathbb{F}_q^m \times r \\ \mathcal{C}_M \text{ 'יהי'}}} \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 [q]^m \mid \forall c \in \mathcal{C}. \langle w, c \rangle = 0\} \text{ לתיקון שגיאות אזי } [m, r, d, q] 
. לעיקון שגיאות אזי קיים [m, m-r, d', q] הינו קוד לינארי איי קיים m, r, d, q לביות אזי קיים לענה: הי\mathcal{C}^\vee לבורו איי קוד לינארי
                                                                                                  H_{\mathcal{C}}=M_{\mathcal{C}^{ee}} אזי איאות שגיאות לבדיקת לינארי לינארי יהי יהי יהי מטריצת בדיקת אזי
                                                                                                                               \mathcal{C} = \ker\left(H_{\mathcal{C}}^{T}\right) יענה: יהי \mathcal{C} קוד לינארי לתיקון שגיאות אזי
                                                                               d=m-r+1 לתיקון שגיאות לתיקון פוד [m,r,d,q] קוד קוד שגיאות מקסימלי 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
                                                                                                                                     .(לכל A כי מתקיים מA \in \mathcal{P}_r\left(R\left(M\right)\right) בת"ל) שגיאות)
                                                        . טענה: יהי \mathcal{C} קוד לינארי מקסימלי לתיקון שגיאות אזי \mathcal{C}^{\vee} הינו קוד לינארי מקסימלי לתיקון שגיאות טענה:
משפט גילברט־וורשאמוב: יהיו d \leq m באשר באשר לינארי המקיים אזי קיים אזי ויהי ויהי שגיאות באשר לd \leq m באשר 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)} אוי קיים \sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k} עבורו עבורן k \leq m באשר באשר אויהי k \leq m באשר למה: יהי k \leq m באשר
                                                                                                                                              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)
אזי \sum_{i=0}^{d-2} \binom{m-1}{i} \left(q-1
ight)^i < q^{m-k} אזי עבורו q\in\mathbb{P} ויהי k\leq m באשר באשר k,m\in\mathbb{N}_+ יהיו k\leq m משפט גילברט־וורשאמוב: יהי k\leq m באשר
                                            |\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 	o Y^n אזי f:X 	o Y^n אזי f:X 	o Y^n עבורה f:X 	o Y^n אזי אזי אוי הי
                                    .g\left(f\left(s\right)_{p_{1}},\ldots,f\left(s\right)_{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\left[n
ight] ולכל s\in X אבורה לכל g:Y^{k-1}	o X מתקיים g:Y^{k-1}	o X
טענה: יהיו x_1\dots x_\ell\in\mathbb{F} שונים ונגדיר x_1\dots x_\ell\in\mathbb{F} יהי שדה סופי באשר שדה שדה \ell\leq k טענה: יהיו \ell\leq k באשר שדה שדה שדה סופי באשר
                                                                                                                                                                                                אזי \varphi(p) = (p(x_i))_{i=1}^{\ell}
                                                                                                            . איז פולינומי בזמן חשיבות \varphi, \varphi^{-1} וכן איז איזומורפיזם פולינומי \ell=k
                                                                                          k-\ell ממימד אפיני מרחב \varphi^{-1}\left(y\right)כי מתקיים y\in\mathbb{F}^{\ell} אז לכל \ell < k שם •
סכימת שמיר: f: \mathbb{F}_q 	imes (\mathbb{F}_q \setminus \{0\})^{k-1} 	o \left(\mathbb{F}_q^2\right)^n אזי k \in [n] ויהי n < q באשר n \in \mathbb{N}_+ שדה יהי \mathbb{F}_q שדה יהי \mathbb{F}_q באשר q \in \mathbb{N} אזי
      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 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 \in \mathbb{N} אזי סכימת שמיר הינה סכימת חלוקת סוד מושלמת. g \in \mathbb{N}
                                                  קוד ריד־סולומון: יהי lpha_1 \ldots lpha_m \in \mathbb{F}_q ויהיו r \in [m] יהי יהי שונים m \in [q] שונים אזי באשר ק
```

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

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

טענה: יהי  $\mathrm{RS}_q\left[m,r
ight]$  אזי  $lpha_1\ldotslpha_m\in\mathbb{F}_q$  יהי יהי  $m\in[q]$  שדה יהי שדה יהי באשר  $q\in\mathbb{N}$  יהי יהי לתיקון שגיאות. [m, r, m - r + 1, q]

 $(i,j)\in[m] imes[m]$  לכל  $\left(M_{\mathrm{RS}_q[m,r]}
ight)_{i,j}=lpha_i^{j-1}$  אזי  $lpha_1\ldotslpha_m\in\mathbb{F}_q$  ויהיו  $r\in[m]$  יהי  $m\in[q]$  שדה יהי  $m\in[q]$  שדה ויהי  $m\in[q]$  שדה ויהי  $m\in[q]$  שדה ויהי  $m\in[q]$  אזי  $m\in[q]$  אזי  $m\in[q]$  שדה ויהי  $m\in[q]$ 

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

אלגוריתם ברלקמפ־וולץ': ...

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

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

```
r\left[\mathrm{RM}_q\left[m,r
ight]
ight] = inom{m+r}{r} אזי r < q אזי m,r \in \mathbb{N}_+ שדה ויהיו \mathbb{F}_q שנה: יהי q \in \mathbb{N} אזי
                                            d\left[\mathrm{RM}_q\left[m,r
ight]
ight] = (q-r)\,q^{m-1} אזי r < q באשר m,r \in \mathbb{N}_+ שדה ויהיו \mathbb{F}_q שנה: יהי q \in \mathbb{N} 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]] = (q - b) q^{m-a-1}
                                                         \mathrm{RM}_a\left[m,r
ight]^ee = \mathrm{RM}_a\left[m,m-r-1
ight] אזי m,r\in\mathbb{N}_+ שדה ויהיו \mathbb{F}_a באשר q\in\mathbb{N} יהי מענה: יהי
                         \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\} איי m,r \in \mathbb{N}_{\geq 2} איי מענה: יהיי
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}' קוד לתיקון שגיאות אזי [m,r,d,q] לתיקון שגיאות אזי
                                                                                                                                    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'] קוד קוד לתיקון שגיאות היהי לתיקון שגיאות יהי
                                                                        \mathcal{C}\circ\mathcal{C}'\simeq\left\{h:[m]	imes[m']
ightarrow[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} המוגדרה: יהי S\subseteq\left[n
ight] אזי S\subseteq\left[n
ight] אזי מדרה: יהי S\subseteq\left[n
ight]
                                                                                             \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 היי היי אדמר: יהי
                                                                        . טענה: יהי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ הינו קוד לינארי n \in \mathbb{N}_+ לתיקון שגיאות.
                                                                                                                        \mathcal{C}_{	ext{Hadamard}} \simeq \{\chi_S \mid S \subseteq [n]\} אזי n \in \mathbb{N}_+ יהי הערה: יהי
                                                                                             .\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 יהי
                                                                                              \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 הי
                                                                                  . טענה: יהי [2^n,\log_2{(n)},2^{n-1},2] הינו קוד \mathcal{C}_{	ext{Dic}} לתיקון שגיאות הי יהי n\in\mathbb{N}_+
                                                                                                                                 \mathcal{C}_{\mathrm{Dic}} \simeq \{\chi_{\{i\}} \mid i \in [n]\} אזי n \in \mathbb{N}_+ הערה: יהי יהי
```