```
\Delta\left(x,y
ight)=|\{i\in[m]\mid x_i
eq y_i\}| ברחק האמינג: תהא X קבוצה אזי נגדיר X
                                                                                 .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
                                                                                                               \mathcal{C}\subseteq \left[q
ight]^m אזי q,m\in\mathbb{N}_+ הייו שגיאות: לתיקון שגיאות:
                                                  q,m\in\mathbb{N}_+ ויהי לתיקון שגיאות לתיקון אזי פוד לתיקון ויהי ויהי אזי אוודל האלפבית בקוד לתיקון איאות אזי וודל האלפבית בקוד לתיקון איאות
                                                    m אזי אויהי לתיקון לתיקון איאות: יהיו q,m\in\mathbb{N}_+ ויהי אוי לתיקון איאות אזי \mathcal{C}\subseteq[q]^m 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\left[\mathcal{C}
ight] = \log_q |\mathcal{C}| אזי אויאי לתיקון שגיאות אזי \mathcal{C} \subseteq \left[q
ight]^m ויהי q,m \in \mathbb{N}_+ יהיו איזי שגיאות בקוד לתיקון איאות מימד/קצב בקוד לתיקון איי
               . 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 א\Delta\left(w,w'
ight) \leq d-1 באשר באשר w' \in \left[q
ight]^m ויהי שניהו לתיקון שגיאות יהי שגיאות יהי 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\lfloor rac{d-1}{2} 
ight
vert באשר w' \in [q]^m באשר שגיאות יהי w \in \mathcal{C} לתיקון שגיאות יהי
                                                                    r \leq m-d+1 משפט חסם הסינגלטון: יהי \mathcal C קוד קוד [m,r,d,q] לתיקון שגיאות אזי משפט
                                                       \mathcal{C}_{k	ext{-rep}} = \left\{w \in [q]^{mk} \ \middle| \ orall i \in [mk] \ .w_i = w_i \mod m 
ight\} אזי q,m,k \in \mathbb{N}_+ אהירות: יהיו
                                                     טענה: יהיו [w, m, k, q] אזי [w, m, k, q] הינו קוד [w, m, k, q] לתיקון שגיאות. [w, m, k, q] הינו [w, m, k, q] אזי [w, m, k] אזי [w, m, k] אזי [w, m, k] הינו קוד [w, m, k] לתיקון שגיאות. [w, m, k] הינו קוד [w, m, k] לתיקון שגיאות.
                                             \mathcal{C}_{	ext{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\} אזי m \in \mathbb{N}_+ אזי m \in \mathbb{N}_+ אזי m \in \mathbb{N}_+ אזי
                                                             . איי אוי אוי איי אוי הינו קוד \mathcal{C}_{\mathsf{Hamming}} הינו קוד \mathcal{C}_{\mathsf{Hamming}} איי איי אוי איי איי איי איי איי אוי הינו קוד
                                   עבורו קיים קוד d' \geq d עבורו אזי קיים [m,r,d,q] לתיקון שגיאות עבורם m,r,d,q \in \mathbb{N}_+ עבורו קיים קוד
                                                                                                                       לתיקון שגיאות. [m \lceil \log(q) \rceil, r \log(q), d', 2]
 . טענה: יהיו \ell m, \ell r, d, q עבורם קיים קוד [m, r, d, q] לתיקון שגיאות ויהי m, r, d, q \in \mathbb{N}_+ אזי קיים קוד שגיאות.
. שניאות [m+1,r,d+1,2] איים קוד [m,r,d,2] לתיקון שגיאות אזי קיים קוד אות. עבורם קיים קוד m,r\in\mathbb{N}_+ ויהיו והיי לתיקון שגיאות.
                                     |\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 [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 אוהי 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 d \leq \frac{m}{2} ויהיd \leq \frac{m}{2} קוד וואיאות אזי
            . באשר \mathcal{C} באשר \mathbb{F}_q שדה אזי קוד לתיקון שגיאות: יהיו יהיו q,m\in\mathbb{N}_+ באשר באשר פוד לינארי לתיקון איישות: יהיו יהיו q,m\in\mathbb{N}_+ באשר
                                                                                     \dim\left(\mathcal{C}\right)=r יסענה: יהי \mathcal{C} קוד לינארי [m,r,d,q] לתיקון שגיאות יהי
C_i\left(M_{\mathcal{C}}
ight)=b_i המוגדרת אזי M_{\mathcal{C}}\in\mathbb{F}_q^{m	imes r} בסיס אזי היי b_1\dots b_r\in\mathcal{C} לתיקון שגיאות ויהי
```

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

. טענה: יהיו לתיקון אזי אזי אזי אזי  $q,m,k\in\mathbb{N}_+$  יהיו טענה: יהיו

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

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

 $A \in \mathbb{F}_q^{(m-r) imes r}$  עבורו קיימת  $\mathcal{D}$  עבורו אזי קיים קוד לינארי [m,r,d,q] לתיקון שגיאות אזי קיים קוד לינארי (ווארי [m,r,d,q] לתיקון שגיאות אזי קיים קוד לינארי  $M_{\mathcal{D}} = \left( \begin{smallmatrix} I_r \\ A \end{smallmatrix} \right)$  המקיימת

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

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

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

. אניאות (m-d,r-1,d',q לתיקון שגיאות אזי קיים מענה: היי  $d'\geq \left\lceil \frac{d}{q} \right\rceil$  לתיקון שגיאות אזי לתיקון שגיאות (m,r,d,q) איי קיים קוד לינארי  $m \geq \sum_{i=0}^{r-1} \left\lceil rac{d}{q^i} 
ight
ceil$  משפט גרייסמר: יהי  $\mathcal C$  קוד לינארי [m,r,d,q] לתיקון שגיאות אזי למה: יהי  $x\in\mathbb{F}_q^m$  אזי לכל m>r באשר  $m,r\in\mathbb{N}_+$  שדה יהיו  $\mathbb{F}_q$  שדה יהיו m>r באשר  $m,r\in\mathbb{N}_+$  שדה יהיו  $\mathbb{F}_q$  שדה יהיו  $\mathbb{F}_q$  באשר  $\mathbb{F}_q^m\times r$  (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  $q\in\mathbb{N}_+$  שדה יהיו m>r באשר  $m,r\in\mathbb{N}_+$  אזי m>r באשר  $m,r\in\mathbb{N}_+$  באשר  $m,r\in\mathbb{N}_+$  באשר  $m,r\in\mathbb{N}_+$  באשר m>r באשר  $m,r\in\mathbb{N}_+$  ויהי m>r באשר  $m,r\in\mathbb{N}_+$  שדה יהיו m>r באשר  $m,r\in\mathbb{N}_+$  ויהי יהי m>r באשר  $m,r\in\mathbb{N}_+$  ויהי יהי m>r באשר  $m,r\in\mathbb{N}_+$  ויהי יהי m>r באשר  $m,r\in\mathbb{N}_+$  באשר  $m,r\in\mathbb{N}_+$  שדה יהיו

 $\mathbb{P}_{\substack{M \in \mathbb{F}_q^{m \times r} \\ \mathcal{C}_M \text{ in the then } }} \left( d\left[\mathcal{C}_M\right] \leq (1-\delta) \left(m-\frac{m}{q}\right) \right) \leq |\mathcal{C}_M| \cdot \exp\left(-\frac{\delta^2}{2} \left(m-\frac{m}{q}\right)\right)$  קוד לינארי

 $\mathcal{C}^ee = \{w \in [q]^m \mid orall c \in \mathcal{C}. \langle w,c 
angle = 0\}$  לתיקון שגיאות אזי וואלי: יהי  $\mathcal{C}$  קוד לינארי ווארי [m,r,d,q] לתיקון איי

טענה: יהי  $\mathcal{C}^\vee$  קוד לינארי [m, r, d, q] לתיקון שגיאות אזי קיים  $d' \in \mathbb{N}_+$  עבורו שגיאות אזי [m, r, d, q] לתיקון שגיאות.  $H_\mathcal{C} = M_{\mathcal{C}^\vee}$  איים שגיאות אזי לנארי לבדיקת שגיאות אזי יהי  $\mathcal{C}$  קוד לינארי לבדיקת שגיאות אזי

 $\mathcal{C} = \ker \left( H_{\mathcal{C}}^T 
ight)$  יטענה: 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 m>r באשר  $m,r\in\mathbb{N}_+$  שדה יהיו m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r באשר אזי (לכל m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r מתקיים כי m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r באשר מקיים כי m>r באשר  $m,r\in\mathbb{N}_+$  מתקיים כי m>r באשר מקיים בי m>r באשר מקר מיים בי מיים בי

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

 $H\in \mathbb{F}_q^{m imes(m-k)}$  אזי קיים  $\sum_{i=0}^{d-2} {m-1\choose i} \left(q-1
ight)^i < q^{m-k}$  עבורו לכל  $k\leq m$  באשר באשר איי קיים  $k\leq m$  באשר באיר איי למה:  $k\leq m$  באשר איי קיים  $k\leq m$  באשר איי קיים  $k\leq m$  באשר איי קיים  $k\leq m$  בת"ל.

משפט גילברט־וורשאמוב: יהי  $q \in \mathbb{R}^{d-2}$  יהיו  $k \leq m$  באשר בשר  $k, m \in \mathbb{N}_+$  יהיו  $k \leq m$  יהיו  $k \leq m$  המקיים קוד לינארי  $k \leq m$  המקיים  $k \leq m$  המקיים