מרחק האמינג: תהא X קבוצה אזי נגדיר $\Delta : X^n \times X^n \to \mathbb{N}$ כך $\Delta(x,y) = |\{i \in [m] \mid x_i \neq y_i\}|$.

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

קוד לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ אזי $\mathcal{C} \subseteq [q]^m$.

גודל האלפבית בקוד לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי q.

גודל הבלוק בקוד לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי m.

מרחק בקוד לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי $d[\mathcal{C}] = \min_{x \neq y} \Delta(x,y)$.

מימד/קצב בקוד לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי $r[\mathcal{C}] = \log_q |\mathcal{C}|$.

הערה: יהיו $q,m \in \mathbb{N}_+$ ויהי $\mathcal{C} \subseteq [q]^m$ קוד לתיקון שגיאות אזי נאמר כי $\mathcal{C}$ הינו קוד $[m, r[\mathcal{C}], d[\mathcal{C}], q]$ לתיקון שגיאות.

טענה: יהי $\mathcal{C}$ קוד $[m,r,d,q]$ לתיקון שגיאות יהי $w \in \mathcal{C}$ ויהי $w' \in [q]^m$ באשר $\Delta(w,w') \leq d-1$ אזי $w' \notin \mathcal{C}$.

טענה: יהי $\mathcal{C}$ קוד $[m,r,d,q]$ לתיקון שגיאות יהי $w \in \mathcal{C}$ ויהי $w' \in [q]^m$ באשר $\Delta(w,w') \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ אזי $\arg\min_{v \in \mathcal{C}} \Delta(v,w') = w$.

משפט חסם הסינגלטון: יהי $\mathcal{C}$ קוד $[m,r,d,q]$ לתיקון שגיאות אזי $r \leq m-d+1$.

קוד חזרות: יהיו $q,m,k \in \mathbb{N}_+$ אזי $\mathcal{C}_{k\text{-rep}} = \left\{ w \in [q]^{mk} \;\middle|\; \forall i \in [mk].\, w_i = w_{i \mod m} \right\}$.

טענה: יהיו $q,m,k \in \mathbb{N}_+$ אזי $\mathcal{C}_{k\text{-rep}}$ הינו קוד $[mk,m,k,q]$ לתיקון שגיאות.

קוד שארית: יהיו $q,m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}} = \left\{ w \in [q]^{m+1} \;\middle|\; w_{m+1} = \left(\sum_{i=1}^n w_i \mod q\right) \right\}$.

טענה: יהיו $q,m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}}$ הינו קוד $[m+1,m,2,q]$ לתיקון שגיאות.

קוד האמינג: יהי $m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hamming}} = \left\{ x \in \mathbb{F}_2^{2^m-1} \;\middle|\; \forall i \in [m].\, \left(\bigoplus_{\substack{k \in [2^m-1] \\ ((k)_2)_i = 1}} x_k = 0 \right) \right\}$.

טענה: יהי $m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{Hamming}}$ הינו קוד $[2^m-1, 2^m-m-1, 3, 2]$ לתיקון שגיאות.

טענה: יהיו $m,r,d,q \in \mathbb{N}_+$ עבורם קיים קוד $[m,r,d,q]$ לתיקון שגיאות אזי קיים $d' \geq d$ עבורו קיים קוד $[m\lceil \log(q) \rceil, r\log(q), d', 2]$ לתיקון שגיאות.

טענה: יהיו $m,r,d,q \in \mathbb{N}_+$ עבורם קיים קוד $[m,r,d,q]$ לתיקון שגיאות ויהי $\ell \in \mathbb{N}_+$ אזי קיים קוד $[\ell m, \ell r, d, q]$ לתיקון שגיאות.

טענה: יהי $d \in \mathbb{N}_{\text{odd}}$ ויהיו $m,r \in \mathbb{N}_+$ עבורם קיים קוד $[m,r,d,2]$ לתיקון שגיאות אזי קיים קוד $[m+1, r, d+1, 2]$ לתיקון שגיאות.

משפט האמינג: יהי $\mathcal{C}$ קוד $[m,r,d,q]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq q^m \cdot \left(\sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \left(\binom{m}{i} \cdot (q-1)^i \right) \right)^{-1}$.

למה פלוטקין: יהיו $d,q,m \in \mathbb{N}_+$ באשר $d \geq \left(1 - \frac{1}{q}\right) m$ ויהי $\mathcal{C}$ קוד $[m,r,d,q]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq \frac{d}{d + \frac{m}{q} - m}$.

טענה: יהיו $d,m \in \mathbb{N}_+$ באשר $d \leq \frac{m}{2}$ ויהי $\mathcal{C}$ קוד $[m,r,d,2]$ לתיקון שגיאות אזי $|\mathcal{C}| \leq d \cdot 2^{m-2d+2}$.

קוד לינארי לתיקון שגיאות: יהיו $q,m \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה אזי קוד לתיקון שגיאות $\mathcal{C} \subseteq \mathbb{F}_q^m$ המקיים כי $\mathcal{C}$ מרחב וקטורי.

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

מטריצה יוצרת: יהי $\mathcal{C}$ קוד לינארי $[m,r,d,q]$ לתיקון שגיאות ויהי $b_1 \ldots b_r \in \mathcal{C}$ בסיס אזי $M_{\mathcal{C}} \in \mathbb{F}_q^{m \times r}$ המוגדרת $C_i(M_{\mathcal{C}}) = b_i$ לכל $i \in [r]$.

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

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

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

טענה: יהיו $q,m \in \mathbb{N}_+$ אזי $\mathcal{C}_{\text{parity}}$ קוד לינארי לתיקון שגיאות.

מסקנה: יהיו $q,m \in \mathbb{N}_+$ אזי $M_{\mathcal{C}_{\text{parity}}} = \begin{pmatrix} I_m \\ \bar{1}^T \end{pmatrix} = \begin{pmatrix} I_m \\ (\bar{1})^T \end{pmatrix}$.

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

טענה: יהי $\mathcal{C}$ קוד לינארי $[m,r,d,q]$ לתיקון שגיאות אזי קיים קוד לינארי $[m,r,d,q]$ לתיקון שגיאות $\mathcal{D}$ עבורו קיימת $A \in \mathbb{F}_q^{(m-r) \times r}$ המקיימת $M_{\mathcal{D}} = \begin{pmatrix} I_r \\ A \end{pmatrix}$.

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

- לכל $V \subseteq \mathcal{C}$ באשר $\dim(V) = r-1$ מתקיים $|\{R_i(M_{\mathcal{C}}) \mid i \in [m]\} \cap V| \leq m-d$.
- קיים $V \subseteq \mathcal{C}$ המקיים $\dim(V) = r-1$ וכן $|\{R_i(M_{\mathcal{C}}) \mid i \in [m]\} \cap V| = m-d$.

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

משפט גרייסמר: יהי $\mathcal{C}$ קוד לינארי $[m,r,d,q]$ לתיקון שגיאות אזי $m \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil$.

למה: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $x \in \mathbb{F}_q^r \setminus \{0\}$ אזי לכל $b \in \mathbb{F}_q^m$ מתקיים $\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}}(Mx = b) = \frac{1}{q^m}$.

סימון: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $M \in \mathbb{F}_q^{m \times r}$ אזי $\mathcal{C}_M = \left\{M \cdot v \mid v \in \mathbb{F}_q^r\right\}$.

משפט: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה ויהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ אזי $\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}}(\mathcal{C}_M \text{ קוד לינארי}) \geq 1 - \frac{q^r - 1}{q^m(q-1)}$.

משפט: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה יהיו $m, r \in \mathbb{N}_+$ באשר $m > r$ ויהי $\delta \in (0, 1)$ אזי
$\mathbb{P}_{\substack{M \in \mathbb{F}_q^{m \times r} \\ \mathcal{C}_M \text{ קוד לינארי}}}\left(d\left[\mathcal{C}_M\right] \leq (1-\delta)\left(m - \frac{m}{q}\right)\right) \leq |\mathcal{C}_M| \cdot \exp\left(-\frac{\delta^2}{2}\left(m - \frac{m}{q}\right)\right)$.

הקוד הדואלי: יהי $\mathcal{C}$ קוד לינארי $[m, r, d, q]$ לתיקון שגיאות אזי $\mathcal{C}^\vee = \{w \in [q]^m \mid \forall c \in \mathcal{C}.\ \langle w, c \rangle = 0\}$.

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

מטריצת בדיקת שאריות: יהי $\mathcal{C}$ קוד לינארי לבדיקת שגיאות אזי $H_{\mathcal{C}} = M_{\mathcal{C}^\vee}$.

טענה: יהי $\mathcal{C}$ קוד לינארי לתיקון שגיאות אזי $\mathcal{C} = \ker\left(H_{\mathcal{C}}^T\right)$.

...

משפט האמינג: יהיו $d, m \in \mathbb{N}_+$ באשר $d \leq m$ ויהי $q \in \mathbb{P}$ אזי קיים קוד לינארי $[m, r, d, q]$ לתיקון שגיאות $\mathcal{C}$ המקיים $|\mathcal{C}| \geq q^m \cdot \left(\sum_{i=0}^{d-1}\left(\binom{m}{i} \cdot (q-1)^i\right)\right)^{-1}$.