סימון: יהי $\mathbb{F}$ שדה ויהיו $m,n\in\mathbb{N}_+$ אזי $\mathbb{F}^{m\times n}=M_{m\times n}\left(\mathbb{F}\right)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: יהיו $d,m\in\mathbb{N}_+$ באשר $d\le\frac{m}{2}$ ויהי $\mathcal{C}$ קוד $\left[m,r,d,2\right]$ לתיקון שגיאות אזי $\left|\mathcal{C}\right|\le d\cdot2^{m-2d+2}$.

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 $\left[m,r,d,q\right]$ לתיקון שגיאות אזי $\dim\left(\mathcal{C}\right)=r$.

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

טענה: יהי $\mathcal{C}$ קוד לינארי $\left[m,r,d,q\right]$ 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 $M_{\mathcal{C}_{\text{parity}}}=\begin{pmatrix}I_m\\ \vec{1}^T\end{pmatrix}=\begin{pmatrix}I_m\\ \left(\vec{1}\right)^T\end{pmatrix}$.

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

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

סימון: יהי $\mathbb{F}$ שדה יהיו $m,n\in\mathbb{N}_+$ ותהא $M\in\mathbb{F}^{m\times n}$ אזי $R\left(M\right)=\left\{R_i\left(M\right)\mid i\in\left[m\right]\right\}$.

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

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

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

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

למה: יהי $q \in \mathbb{N}_+$ באשר $\mathbb{F}_q$ שדה יהיו $m,r \in \mathbb{N}_+$ באשר $m > r$ ויהי $x \in \mathbb{F}_q^r \backslash \{0\}$ 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 $\mathbb{P}_{M \in \mathbb{F}_q^{m \times r}}(\text{קוד לינארי } \mathcal{C}_M) \ge 1 - \frac{q^r - 1}{q^m (q-1)}$.

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

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 $\mathcal{C} = \ker\left(H_{\mathcal{C}}^T\right)$.

קוד מקסימלי לתיקון שגיאות: קוד $[m,r,d,q]$ לתיקון שגיאות המקיים $d = m - r + 1$.

טענה: 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 ($\mathcal{C}_M$ קוד לינארי מקסימלי לתיקון שגיאות)$\Longleftrightarrow$(לכל $A \in \mathcal{P}_r(R(M))$ מתקיים כי A בת"ל).

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

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

למה: יהי $d \in \mathbb{N}_{\ge 2}$ יהיו $k,m \in \mathbb{N}_+$ באשר $k \le m$ ויהי $q \in \mathbb{P}$ עבורו $\sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k}$ אזי קיים $H \in \mathbb{F}_q^{m \times (m-k)}$ עבורו לכל $A \in \mathcal{P}_{d-1}(R(M))$ מתקיים כי A בת"ל.

משפט גילברט־וורשאמוב: יהי $d \in \mathbb{N}_{\ge 2}$ יהיו $k,m \in \mathbb{N}_+$ באשר $k \le m$ ויהי $q \in \mathbb{P}$ עבורו $\sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i < q^{m-k}$ אזי קיים קוד לינארי $[m,k,d,q]$ לתיקון שגיאות $\mathcal{C}$ המקיים $|\mathcal{C}| \ge q^m \cdot \left(1 + \sum_{i=0}^{d-2} \left(\binom{m-1}{i} \cdot (q-1)^i \right) \right)^{-1}$.

סכימת חלוקת סוד מושלמת: תהיינה X,Y קבוצות יהי $n \in \mathbb{N}_+$ ויהי $k \in [n]$ אזי $f : X \to Y^n$ עבורה

- קיימת $g : Y^k \to X$ עבורה לכל $s \in X$ ולכל $p_1, \ldots, p_k \in [n]$ מתקיים $g\left(f(s)_{p_1}, \ldots, f(s)_{p_k} \right) = s$.
- לא קיימת $g : Y^{k-1} \to X$ עבורה לכל $s \in X$ ולכל $p_1, \ldots, p_{k-1} \in [n]$ מתקיים $g\left(f(s)_{p_1}, \ldots, f(s)_{p_{k-1}} \right) = s$.

טענה: יהיו $\ell, k \in \mathbb{N}_+$ באשר $\ell \le k$ יהי $\mathbb{F}$ שדה סופי באשר $|\mathbb{F}| \ge k$ יהיו $x_1 \ldots x_\ell \in \mathbb{F}$ שונים ונגדיר $\varphi : \mathbb{F}_{\le k-1}[x] \to \mathbb{F}^\ell$ כך $\varphi(p) = (p(x_i))_{i=1}^\ell$ אזי

- אם $\ell = k$ אז φ איזומורפיזם וכן φ, φ^{-1} חשיבות בזמן פולינומי.
- אם $\ell < k$ אז לכל $y \in \mathbb{F}^\ell$ מתקיים כי $\varphi^{-1}(y)$ מרחב אפיני ממימד $k - \ell$.

סכימת שמיר: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ באשר $n < q$ ויהי $k \in [n]$ אזי $f : \mathbb{F}_q \times (\mathbb{F}_q \backslash \{0\})^{k-1} \to \left(\mathbb{F}_q^2\right)^n$ המוגדרת $f(s,a) = \left(\left(s_i, s + \sum_{j=1}^{k-1} a_j s_i^j \right) \right)_{i=1}^n$ באשר $s_1 \ldots s_n \in \mathbb{F}_q \backslash \{0\}$ שונים.

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

קוד ריד־סולומון: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ שונים אזי $\mathrm{RS}_q[m,r] = \left\{ (f(\alpha_i))_{i=1}^m \mid f \in (\mathbb{F}_q)_{\le r-1}[x] \right\}$.

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

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ אזי $\mathrm{RS}_q[m,r]$ הינו קוד לינארי מקסימלי $[m,r,m-r+1,q]$ לתיקון שגיאות.

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $m \in [q]$ יהי $r \in [m]$ ויהיו $\alpha_1 \ldots \alpha_m \in \mathbb{F}_q$ אזי $\left(M_{\mathrm{RS}_q[m,r]}\right)_{i,j} = \alpha_i^{j-1}$ לכל $(i,j) \in [m] \times [r]$.

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $i \in \{0, \ldots, q-2\}$ אזי $\sum_{x \in \mathbb{F}_q} x^i = 0$.

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

אלגוריתם ברלקמפ־וולץ': ...

קוד ריד־מיולר: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r \in \mathbb{N}_+$ אזי $\mathrm{RM}_q[m,r] = \left\{ (f(\alpha))_{\alpha \in \mathbb{F}_q^m} \mid f \in (\mathbb{F}_q)_{\le r}[x_1, \ldots, x_m] \right\}$.

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

טענה: יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r \in \mathbb{N}_+$ אזי קיימים $r,d \in \mathbb{N}_+$ עבורם $\mathrm{RM}_q[m,r]$ הינו קוד לינארי $[q^m,r,d,q]$ לתיקון שגיאות.

טענה: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r\in\mathbb{N}_+$ באשר $r<q$ אזי $r\left[\mathrm{RM}_q\left[m,r\right]\right]=\binom{m+r}{r}$.

טענה: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r\in\mathbb{N}_+$ באשר $r<q$ אזי $d\left[\mathrm{RM}_q\left[m,r\right]\right]=\left(q-r\right)q^{m-1}$.

טענה: יהיו $m,r\in\mathbb{N}_+$ אזי $r\left[\mathrm{RM}_2\left[m,r\right]\right]=\sum_{i=0}^{r}\binom{m}{i}$.

משפט: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r,a,b\in\mathbb{N}_+$ באשר $r=a\left(q-1\right)+b$ חלוקה עם שארית אזי $d\left[\mathrm{RM}_q\left[m,r\right]\right]=\left(q-b\right)q^{m-a-1}$.

טענה: יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $m,r\in\mathbb{N}_+$ אזי $\mathrm{RM}_q\left[m,r\right]^{\vee}=\mathrm{RM}_q\left[m,m-r-1\right]$.

טענה: יהיו $m,r\in\mathbb{N}_{\ge2}$ אזי $\mathrm{RM}_2\left[m,r\right]=\left\{\left(u,u+v\right)\mid\left(u\in\mathrm{RM}_2\left[m-1,r\right]\right)\wedge\left(v\in\mathrm{RM}_2\left[m-1,r-1\right]\right)\right\}$.

שרשור קודים לתיקון שגיאות: יהי $\mathcal{C}$ קוד $\left[m,r,d,q\right]$ לתיקון שגיאות יהי $\mathcal{C}'$ קוד $\left[m',\log_{q'}\left(q\right),d',q'\right]$ לתיקון שגיאות ותהא $\rho:\left[q\right]\to\mathcal{C}'$ הפיכה אזי $\mathcal{C}\circ\mathcal{C}'=\left\{\left(\rho\left(w_i\right)\right)_{i=1}^{m}\mid w\in\mathcal{C}\right\}$.

טענה: יהי $\mathcal{C}$ קוד $\left[m,r,d,q\right]$ לתיקון שגיאות ויהי $\mathcal{C}'$ קוד $\left[m',\log_{q'}\left(q\right),d',q'\right]$ לתיקון שגיאות אזי $\mathcal{C}\circ\mathcal{C}'$ הינו קוד $\left[m\cdot m',r\cdot\log_{q'}\left(q\right),d\cdot d',q'\right]$ לתיקון שגיאות.

הערה: יהי $\mathcal{C}$ קוד $\left[m,r,d,q\right]$ לתיקון שגיאות יהי $\mathcal{C}'$ קוד $\left[m',\log_{q'}\left(q\right),d',q'\right]$ לתיקון שגיאות ותהא $\rho:\left[q\right]\to\mathcal{C}'$ הפיכה אזי $\mathcal{C}\circ\mathcal{C}'\simeq\left\{h:\left[m\right]\times\left[m'\right]\to\left[q\right]\;\middle|\;\exists w\in\mathcal{C}.h\left(i,j\right)=\left(\rho\left(w_i\right)\right)_j\right\}$.

הגדרה: יהי $n\in\mathbb{N}$ ותהא $S\subseteq\left[n\right]$ אזי $\chi_S:\mathbb{F}_2^n\to\mathbb{F}_2$ המוגדרת $\chi_S\left(x\right)=\sum_{i\in S}x_i$.

קוד אדמר: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Hadamard}}=\left\{\left(\chi_S\left(x\right)\right)_{x\in\mathbb{F}_2^n}\;\middle|\;S\subseteq\left[n\right]\right\}$.

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Hadamard}}$ הינו קוד לינארי $\left[2^n,n,2^{n-1},2\right]$ לתיקון שגיאות.

הערה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Hadamard}}\simeq\left\{\chi_S\mid S\subseteq\left[n\right]\right\}$.

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Hamming}}=\left\{\left(\chi_S\left(x\right)\right)_{x\in\mathbb{F}_2^n\backslash\{0\}}\;\middle|\;S\subseteq\left[n\right]\right\}^{\vee}$.

קוד דיקטטורות: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Dic}}=\left\{\left(\chi_{\{i\}}\left(x\right)\right)_{x\in\mathbb{F}_2^n}\;\middle|\;i\in\left[n\right]\right\}$.

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Dic}}$ הינו קוד $\left[2^n,\log_2\left(n\right),2^{n-1},2\right]$ לתיקון שגיאות.

הערה: יהי $n\in\mathbb{N}_+$ אזי $\mathcal{C}_{\mathrm{Dic}}\simeq\left\{\chi_{\{i\}}\;\middle|\;i\in\left[n\right]\right\}$.