Curs 5 STLS II

$K \leq E$ corp finit $\left(\mathbb{F}_{p^\alpha} \leq \mathbb{F}_{p^\beta} \quad \alpha \mid \beta \right)$

trace (urmă) $Tr_{E/K} : E \to K$

$$Tr_{E/K}(a) = \sum_{\gamma \in G} \gamma(a) = a + a^q + a^{q^2} + \dots + a^{q^{n-1}}$$

G = automorfismul lui E care pe K fixează pe K pointwise

unde $n = [E:K]$ și $q = |K|$

A grup abelian $\chi : A \to \mathbb{C}^\times$ morfism

$\chi(a+b) = \chi(a)\chi(b)$

caracter de grup

$\chi \equiv 1$ caracter trivial

χ caracter $\Rightarrow \overline{\chi}$ caracter

$|\chi(a)| = 1 \qquad \chi(-a) = \frac{1}{\chi(a)} = \overline{\chi}(a)$

~~caracteristica~~ $Ch(A)$ = grupul caracterelor $\simeq A$

cu:

$K = \mathbb{F}_q$, $F = \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ $\varepsilon \in \mathbb{C}$ p-rădăcină complexă a unității

V = spațiu finit dimensional peste K (de exemplu E) *1

$V^* = Hom_K(V, K)$

$Ch(V) = \{\chi_f \mid f \in V^*\}$

$\chi_f(v) = \varepsilon^{Tr_{K/F}(f(v))}$

A multime finită $\quad \mathbb{C}^A = \{f : A \to \mathbb{C}\}$

$$\boxed{\langle f, g\rangle = \frac{1}{|A|}\sum_{x\in A} f(x)\,\overline{g}(x)}$$ produs hermitian

A grup abelian $\quad \chi, \psi$ caractere ale lui A $\quad \langle \chi, \psi\rangle = \begin{cases} 0, & \text{dacă } \chi = \psi \\ 1, & \text{altfel} \end{cases}$

$Ch(A)$ "

Caracterele lui A formează o bază ortogonală pt. $\mathbb{C}^A$.

Th Mac Williams

C cod de lungime n, $A_i = |\{v \in C \mid wt(v) = i\}|$ (card)

$$A_C = \sum_{i=0}^{n} A_i z^i \in \mathbb{Z}[z]$$ ($\mathbb{N}$) polinomul ponderilor (Weight polynomial)

C $[n,k]$ cod peste K, $|K| = q$;

$C^\perp$ complementul ortogonal

$C \leftrightarrow A(z)$, $A^\perp(z) \leftrightarrow C^\perp$

Atunci: $A^\perp(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right)$

Lem. Fie χ caracter netrivial al grupului $(K,+,0)$

$u \in K^n$ $\quad g_u(z) = \sum_{v\in K^n} \chi(\langle u, v\rangle)\cdot z^{wt(v)}$ polinom în z.

$$\sum_{c\in C} g_c(z) = \sum_{c\in C}\sum_{v\in K^n} \chi(\langle c, v\rangle)\cdot z^{wt(v)} =$$

$$= \sum_{v\in K^n} f(v)\, z^{wt(v)} \quad \text{unde } f(v) = \sum_{c\in C} \chi(\langle c, v\rangle)$$

$c \rightsquigarrow \chi(\langle c, v\rangle)$ caracter χ_v al lui C

este 1_C (trivial) $\rightsquigarrow v \in C^\perp$

$$f(v) = \sum_{c \in C} \chi(\langle c, v\rangle) = |C| \langle \chi_v, 1_C \rangle =$$

$$= \begin{cases} |C|, & v \in C^\perp \\ 0, & v \notin C^\perp \end{cases}$$

$$\sum_{c \in C} g_c(z) = \sum_{c^\perp \in C^\perp} |C| z^{wt(c^\perp)} = |C| A^\perp(z)$$

(Tim alt mod)

ponderea unui elem. 0 dacă elem = 0, 1 altfel

Fie $c = (c_1, \dots, c_n) \in C$

$$g_c(z) = \sum_{v \in K^n} z^{wt(v)} \chi(\langle c, v\rangle) = \sum_{(a_1, \dots, a_n) \in K^n} z^{\sum_{i=1}^n wt(a_i)} \cdot \chi\left(\sum_{i=1}^n c_i a_i\right) =$$

$$= \sum_{(a_1, \dots, a_n) \in K^n} \prod_{i=1}^n z^{wt(a_i)} \chi(c_i a_i) =$$

$$= \prod_{i=1}^n \sum_{a_i \in K}^* z^{wt(a_i)} \chi(c_i a_i)$$

$(p-1)! \equiv -1 \bmod p$

$$\chi \neq 1 \Rightarrow \sum_{a \in K^*} \chi(a) = -1$$

$$\sum_{a_i \in K} z^{wt(a_i)} \chi(c_i a_i) = \begin{cases} \sum_{a_i \in K} z^{wt(a_i)} = 1 + (q-1)z & \{ c_i = 0 \\ 1 + z \sum_{a \in K^*} \chi(a) = 1 - z & \{ c_i \neq 0 \end{cases}$$

$v_1 \in$

v_2

$$g_c(z) = (1-z)^{wt(c)} (1+(q-1)z)^{n-wt(c)}$$

$$A^{\perp}(z) = |C|^{-1} \sum_{c \in C} g_c(z) = q^{-k}(1+(q-1)z)^n \cdot \sum_{c \in C} \left(\frac{1-z}{1+(q-1)z}\right)^{wt(c)}$$

$|C| = q^k$

$$= q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right) \quad \square$$

Exemplu $\mathrm{Sim}_q(K)$: $A(z) = 1 + (q^k - 1) z^{q^{k-1}}$

$\mathbb{F}_2$ $\mathrm{Sim}_2(k)$ simplex $\quad \overset{A(x)}{1 + (2^k - 1) x^{2^{k-1}}}$ polinomul ponderilor

$[2^k - 1, n-k, 3]$ $\quad A^{\perp}(x) = \frac{1}{2^k}\left[(1+x)^n + n(1-x)^2 \cdot (1+x)^{2^{k-1}-1}\right] =$

$\mathrm{Ham}_2(k)$

$$= \frac{1}{n+1}\left[(1+x)^n + n(1-x)(1-x^2)^{\frac{n-1}{2}}\right]$$

$$A_i^{\perp} = \begin{cases} \frac{1}{n+1}\left[\binom{n}{i} + n(-1)^{i/2}\binom{\frac{n-1}{2}}{\frac{i}{2}}\right], & i = 2\Delta \text{ (par)} \\ \frac{1}{n+1}\left[\binom{n}{i} + n(-1)^{\frac{i+1}{2}}\binom{\frac{n-1}{2}}{\frac{i-1}{2}}\right], & i = 2\Delta + 1 \end{cases}$$

Ex! $\quad n \geq 1$

$$C_1 = \{(a_1, \ldots, a_n) \in \mathbb{F}_2^n \mid wt(a_1, \ldots, a_n) = 2\Delta, \Delta \in \mathbb{N}\}$$

C liniar; parametrii lui? $\quad C / \mathbb{F}_2$

$v_1 \in C$ $\quad wt(v_1) = k_1$ par

$v_2 \in C$ $\quad wt(v_2) = k_2$ par

un nr de Δ se suprapun $\Rightarrow wt(v_1 + v_2) = (k_1 - \Delta) + (k_2 - \Delta) = k_1 + k_2 - 2\Delta$

$v_1 + v_2 \in C$ par

$\rightarrow$ q.e.d.

$v = (c_1, c_2, \dots, c_n) \in C \iff c_1 + c_2 + \dots + c_n = 0$

$\Rightarrow H = (1\ 1\ 1\ \dots\ 1)$ matricea de control

$$(1\ 1\ \dots\ 1)\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = 0$$

$d(C) = 2$ (nr. de 1 necesari pt. a cuv. din cod să nu fie identic 0)

param.: $[n, n-1, 2]$

deci $|C| = 2^{n-1}$ (cardinalitatea corpului la puterea dimensiunii matricii)

caut apl. $G: \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ injectiv liniară

al. $C = G(\mathbb{F}_2^{n-1})$

element generic

$(x_1, x_2, \dots, x_{n-1}, x_1 + x_2 + \dots + x_{n-1}) = G(x_1, \dots, x_{n-1})$

$G = \left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \\ & & & 1 \end{matrix} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array}\right)$ ($n-1$ linii, $n-1$ coloane)

matr. generatoare: n col., $n-1$ lin.

$(x_1, \dots, x_n) = (x_1, \dots, x_{n-1})\,G$

Ex

$C_2 = \{(0,0,\dots,0), (1,1,\dots,1)\} \subseteq \mathbb{F}_2^n / \mathbb{F}_2$ lungime n

param., matr. control, matr. generatoare

$[n, 1, n]$

$G: \{0,1\} \to \{0,1\}^n$

$G(x) = xG$

$G = (1\ 1\ \dots\ 1)$

matr. verif. dacă de elem. din cod

$$H: \begin{cases} x_1 = x_n \\ x_2 = x_n \\ \dots \\ x_{n-1} = x_n \end{cases} \iff \begin{cases} x_1 + x_n = 0 \\ x_2 + x_n = 0 \\ \dots \\ x_{n-1} + x_n = 0 \end{cases} \iff H = \left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{array}\right)$$

$C_2 = C_1^{\perp}$

$A(x) = 1 + x^n$ codul cu repetiție

Din MacWilliams se poate face polinomul codului din ex. anterior.

Ex $U_n \in \mathcal{M}_{2^n \times 2^n}(\mathbb{F}_2)$ $\quad U_n = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 \end{pmatrix}$

$H_0 = (0) \in \mathcal{M}_{2^0 \times 2^0}(\mathbb{F}_2)$ $\quad H_{n+1} = \begin{pmatrix} H_n & H_n \\ H_n & H_n + U_n \end{pmatrix} \in \mathcal{M}_{2^{n+1} \times 2^{n+1}}(\mathbb{F}_2)$

Liniile lui H_n = RM $(1, n)$ (Reed-Muller)

$H_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad H_2 = \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$

inducție $n \rightsquigarrow n+1$

H_{n+1}, două linii

caz I: $(x, x) + (y, y) = (x+y, x+y)$ — linie din jum. I a lui H_n.
x, y linii în H_{n-1} $\quad x+y$ linie în H_{n-1}

cat II: $(x, \vec{1}+x) + (y, \vec{1}+y) = (x+y, x+y)$
linie din jum. I a lui H_n.

cat III: $(x, x) + (y, \vec{1}+y) = (x+y, \vec{1} + (x+y))$
linie din jum. II a lui H_n.

$\forall v \in H_n$ linie v conține nr. egal de 0 și de 1.
$\Leftrightarrow Sim_2(n)$. distanță minimă 2^{n-1}