

Weight polynomials of linear codes

Frank Bower

Definition : Let \mathbb{F}_q be a finite field.

- 1) Hamming weight: $wt(x) := \#\{i \in \{1, \dots, n\} | x_i \neq 0\}$, $x \in \mathbb{F}_q^n$
- 2) $C \subset \mathbb{F}_q^n$ (linear) code: $\iff C$ \mathbb{F}_q – linear subspace
- 3) C $[n,k,d]$ -Code : $\iff C \subset \mathbb{F}_q^n$ linear Code of dimension k and minimum weight $d = \min_{x \in C \setminus \{0\}} wt(x)$

- 4) Generator matrix :

$$\Omega(C) = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{kn} \end{pmatrix}$$

where $b_1, \dots, b_k \in C$ basis

- 5)

$$C \approx C' : \iff \text{i) } \exists \pi \in S_n, A := \begin{pmatrix} a_1 & & 0 \\ & \dots & \\ 0 & & a_n \end{pmatrix},$$

$$a_1, \dots, a_n \in \mathbb{F}_q \setminus \{0\} :$$

$$A \cdot P(\pi) \cdot x \in C' \quad \forall x \in C$$

$$\text{ii) } \#C = \#C'$$

[8, 4, 4]-binary Hamming-code H_8 :

$$\Omega(H_8) = \left(\begin{array}{ccc|cccc} 1 & & 0 & 0 & 1 & 1 & 1 \\ & 1 & & 1 & 0 & 1 & 1 \\ & & 1 & 1 & 1 & 0 & 1 \\ 0 & & & 1 & 1 & 1 & 0 \end{array} \right)$$

$$\#H_8 = 2^{\dim H_8} = 2^4 = 16$$

$$\mathbb{I} := (1, 1, 1, 1, 1, 1, 1, 1) \in H_8$$

$$W_{H_8}(X_0, X_1) = X_0^8 + 14 \cdot X_0^4 X_1^4 + X_1^8$$

$$\begin{aligned} P_2(H_8)(X_0, X_1, X_2, X_3) = & X_0^8 + X_1^8 + X_2^8 + X_3^8 \\ & + 14 \cdot (X_0^4 X_1^4 + X_0^4 X_2^4 + X_0^4 X_3^4 \\ & \quad + X_1^4 X_2^4 + X_1^4 X_3^4 + X_2^4 X_3^4) \\ & + 168 \cdot X_0^2 X_1^2 X_2^2 X_3^3 \end{aligned}$$

Hamming weight enumerator

$C \subset \mathbb{F}_q^n$ $[n, k, d]$ -code

$$\begin{aligned} W_C(X_0, X_1) &= \sum_{\beta \in C} X_0^{n-wt(\beta)} X_1^{wt(\beta)} \\ &= \sum_{i=0}^n A_i \cdot X_0^{n-i} X_1^i \end{aligned}$$

where $A_i := \#\{x \in C \mid wt(x) = i\}$

Properties :

- 1) $W_C(X_0, X_1)$ homogeneous of degree n
- 2) $W_{C_1 \times C_2}(X_0, X_1) = W_{C_1}(X_0, X_1) \cdot W_{C_2}(X_0, X_1)$
- 3) $W_C(1, 1) = \#C$
- 4) $W_C(X_0, X_1) = X_0^n + A_d \cdot X_0^{n-d} X_1^d + \sum_{j=d+1}^n A_j \cdot X_0^{n-j} X_1^j$
- 5) $C \approx C' \Rightarrow W_C(X_0, X_1) = W_{C'}(X_0, X_1)$
 $\not\Leftarrow$

Higher weight polynomials

$C \subset \mathbb{F}_2^n$ $[n, k, d]$ -code

$$P_g(C)(X_0, X_1, \dots, X_{2^g-1}) := \sum_{\beta_1, \dots, \beta_g \in C} \prod_{a \in \mathbb{F}_2^g} X_a^{\epsilon_a(\beta_1, \dots, \beta_g)}$$

where $\epsilon_a(\beta_1, \dots, \beta_g) := \#\{i \mid 1 \leq i \leq n, a = (\beta_{1i}, \dots, \beta_{gi})\}$

$$\begin{aligned} \{0, 1, 2, \dots, 2^g - 1\} &\xrightarrow{\cong} \mathbb{F}_2^g \\ 0 &\mapsto (0, \dots, 0, 0, 0) \\ 1 &\mapsto (0, \dots, 0, 0, 1) \\ 2 &\mapsto (0, \dots, 0, 1, 0) \\ &\vdots \\ 2^g - 1 &\mapsto (1, \dots, 1, 1, 1) \end{aligned}$$

$$\begin{pmatrix} \beta_{11} & \dots & \beta_{1i} & \dots & \beta_{1n} \\ \vdots & & \vdots & & \vdots \\ \beta_{g1} & \dots & \beta_{gi} & \dots & \beta_{gn} \end{pmatrix}$$

$\xrightarrow{\text{scanning}}$

Example : $g=2$.

$$P_2(H_8)(X_0, X_1, X_2, X_3) = ???$$

$$\beta_1 = (1, 1, 1, 0, 0, 0, 0, 1)^T \in H_8$$

$$\beta_2 = (1, 0, 0, 1, 1, 0, 0, 1)^T \in H_8$$



$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$X_0 \leftrightarrow (0, 0)^T$$

$$X_1 \leftrightarrow (0, 1)^T$$

$$X_2 \leftrightarrow (1, 0)^T$$

$$X_3 \leftrightarrow (1, 1)^T$$

$$\epsilon_0(\beta_1, \beta_2) = 2$$

$$\epsilon_1(\beta_1, \beta_2) = 2$$

$$\epsilon_2(\beta_1, \beta_2) = 2$$

$$\epsilon_3(\beta_1, \beta_2) = 2$$

$$P_g(C)(X_0, \dots, X_{2^g-1}) = \sum_{\beta_1, \dots, \beta_g \in C} \prod_{a \in \mathbb{F}_2^g} X_a^{\epsilon_a(\beta_1, \dots, \beta_g)}$$

Properties of $P_g(C)$:

- 1) $P_1(C)(X_0, X_1) = W_C(X_0, X_1)$
- 2) $P_g(C)$ homogeneous of degree n
- 3) $P_g(C_1 \times C_2) = P_g(C_1) \cdot P_g(C_2)$
- 4) $P_g(C)(X_0, 0, X_2, 0, \dots, X_{2^g-2}, 0) = P_{g-1}(C)(X_0, X_2, X_4, \dots, X_{2^g-2})$

$$\varphi : P_g(C)(X_0, X_1, \dots, X_{2^g-1}) \mapsto P_{g-1}(C)(X_0, X_1, \dots, X_{2^{g-1}-1})$$

$$X_a \mapsto \begin{cases} X_{a/2} & a \equiv 0(2) \\ 0 & a \equiv 1(2) \end{cases}$$

- 5) $C \approx C' \Rightarrow P_g(C) = P_g(C')$
- 6) $C, C' [n, k] - \text{codes and } P_k(C) = P_k(C') \Rightarrow C \approx C'$

Remark :

$$s : \mathbb{F}_2^m \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$$

$$(x, y) \longmapsto \sum_{i=1}^n x_i y_i$$

s is a symmetric bilinear form

C $[n, k]$ -code.

$$C^\perp := \{y \in \mathbb{F}_2^m \mid s(x, y) = 0 \forall x \in C\} \text{ dual code of } C$$

Definition :

- 1) C selfdual $\iff C = C^\perp$
- 2) C doubly-even $\iff 4 \mid wt(x) \forall x \in C$

MacWilliams-Identity :

$$P_g(C) = W \cdot P_g(C),$$

$$\text{where } W := \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} W_1 & & 0 \\ & \ddots & \\ 0 & & W_1 \end{pmatrix}, \quad W_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and

$$M_n(\mathbb{C}) \times \mathbb{C}[X_a]_{a \in \mathbb{F}_2^g} \longrightarrow \mathbb{C}[X_a]_{a \in \mathbb{F}_2^g}$$

$$(A, p(X_0, \dots, X_{2^g-1})) \longmapsto A \cdot p(X_0, \dots, X_{2^g-1}) := p((X_0, \dots, X_{2^g-1}) \cdot A^T)$$

$$G_g := \langle W, E, AGL(g) \rangle \subset GL(2^g, \mathbb{C}), \quad E := \text{Diag}(1, i, \dots, 1, i)$$

Theorem : (Runge)

$$CP_g := \mathbb{C}[X_a]_{a \in \mathbb{F}_2^g}^{G_g}$$

is generated by the polynomials $P_g(C)$ of sdde codes C .

Example : $g=1$.

$$G_1 = \left\langle \frac{1}{\sqrt{2}}W_1, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle, \quad AGL(1) = \Sigma_2.$$

Theorem : (Gleason)

$$CP_1 = \mathbb{C}[W_{H_8}(X_0, X_1), W_{G_{24}}(X_0, X_1)]$$

$$\begin{array}{ccc}
\mathbb{Z}^n & & \Gamma_C := \frac{1}{\sqrt{2}} \cdot \pi^{-1}(C) \subset \mathbb{R}^n \\
\downarrow \pi = \text{mod } 2 & & \uparrow \\
\mathbb{F}_2^n & \supset & C
\end{array}$$

$$C \text{ code} \mapsto \vartheta_{\Gamma_C}(z) := \sum_{x \in \Gamma_C} e^{\pi i(x|x) \cdot z}$$

$$\vartheta_{\Gamma_C} : \mathbb{H} \longrightarrow \mathbb{C}$$

Well known : C code $\implies \vartheta_{\Gamma_C}$ elliptic modular form

$$\begin{aligned}
Th_1 : CP_1 &\xrightarrow{\cong} \bigoplus_{4|k} [\Gamma_1, k] = \mathbb{C}[g_4, g_6^2] \\
X_0 &\mapsto f_0 \\
X_1 &\mapsto f_1
\end{aligned}$$

$$Th_1(W_{H_8}(X_0, X_1)) = g_4$$

$$Th_1(W_{\mathcal{G}_{24}}(X_0, X_1)) = \frac{11}{18}g_4^3 + \frac{7}{18}g_6^2$$

Elliptic modular forms

$\Gamma_1 := Sl_2(\mathbb{Z})$ modular group

$f : \mathbb{H} \longrightarrow \mathbb{C}$ holomorphic

f modular form of weight k :

$$\Leftrightarrow 1) f((az + b) \cdot (cz + d)^{-1}) = (cz + d)^k \cdot f(z) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl_2(\mathbb{Z})$$

2) f has a power series expansion in $q := e^{2\pi iz}$

Siegel modular forms

$$\mathbb{H} \rightsquigarrow \mathbb{H}_g := \{Z = X + iY \in \mathbb{C}^{n \times n} \mid Z = Z^T, Y = \text{Im}Z > 0\}$$

$$\Gamma_1 = Sl_2(\mathbb{Z}) \rightsquigarrow \Gamma_g := Sp(2g, \mathbb{Z})$$

Theorem: (Duke / Runge)

$$\begin{aligned} Th_g : CP_g &\longrightarrow \bigoplus_{4|k} [\Gamma_g, k] \\ X_a &\longmapsto f_a(Z) \end{aligned}$$

$g = 1, 2 :$

$$CP_g \cong \bigoplus_{4|k} [\Gamma_g, k]$$

Commuting diagram

$$\begin{array}{ccc} CP_g & \xrightarrow{Th_g} & \bigoplus_{4|k} [\Gamma_g, k] \\ \downarrow \varphi & & \downarrow \Phi \\ CP_{g-1} & \xrightarrow{Th_{g-1}} & \bigoplus_{4|k} [\Gamma_{g-1}, k] \end{array}$$