Symmetries of weight enumerators

Martino Borello

Université Paris 8 - LAGA

Fq13

Introduction

"One of the most remarkable theorems in coding theory is Gleason's 1970 theorem about the weight enumerators of self-dual codes."

N. Sloane

Properties of codes
(or of families of codes)

$\leftrightsquigarrow$

Symmetries of their weight enumerators

M. Borello, O. Mila. **On the Stabilizer of Weight Enumerators of Linear Codes**. arXiv:1511.00803.

Background

q a prime power.

- A q-**ary linear code** $\mathcal{C}$ of **length** n is a subspace of $\mathbb{F}_q^n$.
- If $c = (c_1, \dots, c_n) \in \mathcal{C}$ (**codeword**), the (Hamming) **weight** of c is

$$\mathrm{wt}(c) := \#\{i \in \{1, \dots, n\} \mid c_i \neq 0\}$$

  $(\mathrm{wt}(\mathcal{C}) := \{\mathrm{wt}(c) \mid c \in \mathcal{C}\})$.
- If $\mathcal{C} = \mathcal{C}^{\perp}$, the code $\mathcal{C}$ is called **self-dual**.
- $\mathcal{C} \subseteq \mathbb{F}_q^n \rightsquigarrow w_{\mathcal{C}}(x, y) := \sum_{c \in \mathcal{C}} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$
  with $A_i := \#\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}$ (**weight enumerator** of $\mathcal{C}$).

$\mathcal{C}$ **binary** linear code.

Divisibility conditions

- **Even**: $\mathrm{wt}(\mathcal{C}) \subseteq 2\mathbb{Z} \Rightarrow w_{\mathcal{C}}(x, y) = w_{\mathcal{C}}(x, -y)$.
- **Doubly-even**: $\mathrm{wt}(\mathcal{C}) \subseteq 4\mathbb{Z} \Rightarrow w_{\mathcal{C}}(x, y) = w_{\mathcal{C}}(x, iy)$.

MacWilliams' identities

- **Self-dual** $\Rightarrow w_{\mathcal{C}}(x, y) = w_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$.

Group action

- $\mathrm{GL}_2(\mathbb{C}) \circlearrowleft \mathbb{C}[x, y]$: $p(x, y)^{\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]} := p(ax + by, cx + dy)$.
- For $G \leqslant \mathrm{GL}_2(\mathbb{C})$, the **invariant ring** of G is

$$\mathbb{C}[x, y]^G := \{p(x, y) \mid p(x, y)^A = p(x, y)\ \forall A \in G\}.$$

- **Notation**: for $p(x, y) \in \mathbb{C}[x, y]$, $S(p(x, y)) := \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{C})}(p(x, y))$.

Gleason's Theorem

Theorem (Gleason '70)

Let $\mathcal{C}$ be a binary linear code which is self-dual and doubly-even. Then

$$w_{\mathcal{C}}(x,y) \in \mathbb{C}[f_1, f_2]$$

where $f_1 := w_{\hat{\mathcal{H}}_3}(x,y)$ and $f_2 := w_{\mathcal{G}_{24}}(x,y)$.

- $\mathcal{C}$ self-dual $\Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$,
- $\mathcal{C}$ doubly-even $\Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}(x, iy)$,
- $G := \left\langle \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \right\rangle \Rightarrow \mathbb{C}[x,y]^G = \mathbb{C}[f_1, f_2]$.

$\mathcal{C} \subseteq \mathbb{F}_2^n$ self-dual and doubly-even.

Consequences

- $8 \mid n$ (Gleason '71).
- $\mathrm{d}(\mathcal{C}) \leqslant 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$ (Mallows and Sloane '73).

If the bound is achieved $\mathcal{C}$ is called **extremal**.

- extremal and doubly-even $\Rightarrow n \leqslant 3928$ (Zhang '99).
- **Is there an extremal self-dual code of length 72?** (Sloane '73).
- $\underbrace{24 \mid n \text{ and extremal}}_{\Downarrow}$

  all codewords of given weight support a **5-design** (Assmus and Mattson '69)

Questions

Many generalization of Gleason's theorem.

G. Nebe, E.M. Rains, N.J.A. Sloane. **Self-dual codes and invariant theory**. Vol. 17. Berlin: Springer, 2006.

What if MacWilliams' identities do not give a symmetry?

Our questions

- Which are the possible groups of symmetries?
- Given a weight enumerator of a code, which are its symmetries?
- Are they shared by the whole family of this code?
- Can we determine with these methods unknown weight enumerators?

Possible symmetries

For $p(x,y) \in \mathbb{C}[x,y]_h$ (h=homogeneous), denote

$$V(p(x,y)) := \{(x:y) \in \mathbb{P}^1(\mathbb{C}) \mid p(x,y) = 0\}.$$

$\pi : S(p(x,y)) \leqslant \mathrm{GL}_2(\mathbb{C}) \mapsto \overline{S}(p(x,y)) \leqslant \mathrm{PGL}_2(\mathbb{C})$.

$$\begin{array}{ccc} \mathrm{PGL}_2(\mathbb{C}) & \circlearrowright & \mathbb{P}^1(\mathbb{C}) \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, (x:y)\right) & \mapsto & (ax+by : cx+dy) \end{array}$$

simply 3-transitive

induces

$$\overline{S}(p(x,y)) \circlearrowright V(p(x,y)).$$

Theorem (B.,Mila)

$$\#S(p(x,y)) < \infty \Leftrightarrow \#V(p(x,y)) \geqslant 3.$$

Theorem (Blichfeldt 1917)

If $H \leqslant \mathrm{PGL}_2(\mathbb{C})$ is finite, then H is conjugate to one of the following:

- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_m \end{smallmatrix}\right] \right\rangle \simeq C_m$ for a certain $m \in \mathbb{N}$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_m \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \right\rangle \simeq D_m$ for a certain $m \in \mathbb{N}$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right] \right\rangle \simeq A_4$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right] \right\rangle \simeq S_4$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & -\omega \\ \omega & -2 \end{smallmatrix}\right] \right\rangle \simeq A_5$ where $\omega = (1-\sqrt{5})i - (1+\sqrt{5})$.

Corollary

If $\#V(p(x,y)) \geqslant 3$, then $\exists A \in \mathrm{GL}_2(\mathbb{C})$ s.t. $S(p(x,y))^A$ is a **central extension** of one of the **groups listed above**.

The algorithm

Input: $p(x,y) \in \mathbb{C}[x,y]_h$ of degree n s.t. $p(1,0) \neq 0$.

1. $G := \varnothing$.
2. $V :=$RootsOf$(p(x,1)) = \{x_1, \dots, x_m\}$.
3. If $m < 3$, then print("Infinite group") and break; else
   $V_3 := \{$all ordered 3-subsets of $V\}$.
4. For $\{x_1', x_2', x_3'\} \in V_3$:

   4a. Solve $\begin{cases} x_1 a + b - x_1' x_1 c - x_1' d = 0 \\ x_2 a + b - x_2' x_2 c - x_2' d = 0 \\ x_3 a + b - x_3' x_3 c - x_3' d = 0 \end{cases}$ (the unknowns are a, b, c, d).

   Call $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ one of the ∞^1 solutions.

   4b. If $\left\{ \frac{\underline{a}x+\underline{b}}{\underline{c}x+\underline{d}} \mid x \in V \right\} = V$, then

   4bi. $A := \begin{bmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{bmatrix}$.

   4bii. $\lambda := \frac{p(\underline{a},\underline{c})}{p(\mathbf{1},\mathbf{0})}$. $B := \lambda^{-1/n} A$.

   4biii. If $p(x,y)^B = p(x,y)$, then $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C}$ s.t. $\zeta_n^n = 1\}$.

Output: $G = S(p(x,y))$.

The algorithm

`Input`: $p(x,y) \in \mathbb{C}[x,y]_h$ of degree n s.t. $p(1,0) \neq 0$.

1. $G := \emptyset$.
2. $V :=$`RootsOf`$(p(x,1)) = \{x_1, \dots, x_m\}$. (Where?)
3. `If` $m < 3$, `then print`("Infinite group") `and break; else` $V_3 := \{$all ordered 3-subsets of $V\}$. ($\#V_3 = m^3 - 3m^2 + 2m$)
4. `For` $\{x_1', x_2', x_3'\} \in V_3$:

   4A. `Solve` $\begin{cases} x_1 a + b - x_1' x_1 c - x_1' d = 0 \\ x_2 a + b - x_2' x_2 c - x_2' d = 0 \\ x_3 a + b - x_3' x_3 c - x_3' d = 0 \end{cases}$ (the unknowns are a, b, c, d).

   Call $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ one of the ∞^1 solutions. (simply 3-transitive)

   4B. `If` $\left\{ \frac{\underline{a}x + \underline{b}}{\underline{c}x + \underline{d}} \mid x \in V \right\} = V$, `then`

   4BI. $A := \begin{bmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{bmatrix}$.

   4BII. $\lambda := \frac{p(\underline{a},\underline{c})}{p(1,0)}$. $B := \lambda^{-1/n} A$. (to fix the polynomial, not only the roots)

   4BIII. `If` $p(x,y)^B = p(x,y)$, `then` $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C} \text{ s.t. } \zeta_n^n = 1\}$.

`Output`: $G = S(p(x,y))$.

Reed-Muller codes

- $\mathcal{RM}_q(r,m) := \{(f(\underline{a}))_{\underline{a}\in\mathbb{F}_q^m} \mid f \in \mathbb{F}_q[x_1,\dots,x_m] \text{ of degree } \leqslant r\} \subseteq \mathbb{F}_q^{q^n}$.

Dimension and minimum distance known.

Weight enumerator of a $\mathcal{RM}_q(r,m)$ code	$\leftrightsquigarrow$	**Counting $\mathbb{F}_q$-rational points** of hypersurfaces in $\mathbb{A}^m(\mathbb{F}_q)$

N. Kaplan. **Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory**. 2013. Thesis (Ph.D.) - Harvard University

Remark

$\mathcal{RM}_2(r,2r+1)$ self-dual and doubly-even $\Rightarrow \overline{S}(w_{\mathcal{RM}_2(r,2r+1)}(x,y)) \simeq S_4$.

Theorem (B.,Mila)

If one of the following holds

- $q=2$ and $m \geqslant 3r+1$,
- $q \in \{3,4,5\}$ and $m \geqslant 2r+1$,
- $q>5$ and $m \geqslant r+1$,

then $\overline{S}(w_{\mathcal{RM}_q(r,m)}(x,y))$ and $\overline{S}(w_{\mathcal{RM}_q(m(q-1)-r-1,m)}(x,y))$ are cyclic or dihedral.

Theorem (B.,Mila)

$$\overline{S}(w_{\mathcal{RM}_4(1,1)}(x,y)) = \left\langle \begin{bmatrix} 3-\sqrt{-15} & 6+2\sqrt{-15} \\ -4 & \sqrt{-15}-3 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 1 & -1 \end{bmatrix} \right\rangle \simeq V_4$$

so that $w_{\mathcal{RM}_4(1,1)}(x,y) \in \mathbb{C}[f_1,f_2]$, where
$f_1 := 2x^2+(3+\sqrt{-15})xy+(3-\sqrt{-15})y^2$, $f_2 := 53x^4-36x^3y-18x^2y^2+636xy^3+213y^4$.

Table: $\overline{S}(w_{\mathcal{RM}_2(r,m)}(x,y))$

r \ m	1	2	3	4	5	6	7
0	∞	D_4	D_8	D_{16}	D_{32}	D_{64}	D_{128}
1	∞	D_4	S_4	D_8	D_{16}	D_{32}	D_{64}
2	∞	∞	D_8	D_8	S_4	D_4	D_8
3	∞	∞	∞	D_{16}	D_{16}	D_4	S_4
4	∞	∞	∞	∞	D_{32}	D_{32}	D_8
5	∞	∞	∞	∞	∞	D_{64}	D_{64}
6	∞	∞	∞	∞	∞	∞	D_{128}

Table: $\overline{S}(w_{\mathcal{RM}_3(r,m)}(x,y))$

r \ m	1	2	3	4
0	D_3	D_9	D_{27}	D_{81}
1	D_3	C_3	C_9	C_{27}
2	∞	C_3	C_3	C_3
3	∞	D_9	C_3	?
4	∞	∞	C_9	?
5	∞	∞	D_{27}	C_3
6	∞	∞	∞	C_{27}
7	∞	∞	∞	D_{81}

Table: $\overline{S}(w_{\mathcal{RM}_4(r,m)}(x,y))$

r \ m	1	2	3
0	D_8	D_{16}	D_{64}
1	V_4	C_4	C_{16}
2	D_8	$\{\mathrm{Id}\}$	C_4
3	∞	$\{\mathrm{Id}\}$	$\{\mathrm{Id}\}$
4	∞	C_4	?
5	∞	D_{16}	$\{\mathrm{Id}\}$
6	∞	∞	C_4
7	∞	∞	C_{16}
8	∞	∞	D_{64}

Open problem

Understand the **general behavior** and deduce properties and **new weight enumerators**.

Thank you very much for the attention!

At most two roots

- $\mathcal{C} \subseteq \mathbb{F}_q^n$ s.t. $\#V(w_{\mathcal{C}}(x,y)) < 3$.

Theorem (B.,Mila)

One of the following holds:

- $\mathcal{C} = \{\underline{0}\}$;
- $\mathcal{C} = \mathbb{F}_q^n$;
- n is even and $\mathcal{C}$ is equivalent to $\bigoplus_{i=1}^{n/2}[1,1]$;
- n is even, $q = 2$ and $w_{\mathcal{C}}(x,y) = (x^2 + y^2)^{n/2}$.

Open problem

Is it possible to classify all the **binary** codes of **even length** n with **weight enumerator** $(x^2 + y^2)^{n/2}$?

$$\mathcal{M} := \{\text{binary codes of length } n \text{ and weight enumerator } (x^2+y^2)^{n/2} \mid n \in 2\mathbb{N}\}/\sim,$$

Lemma

$(\mathcal{M}, \oplus)$ is a semigroup.

- the $[2,1,2]$ code $\mathcal{X}_1$ with generator matrix $[1,1]$;
- the $[6,3,2]$ code $\mathcal{X}_2$ with generator matrix

$$\begin{bmatrix} 1&0&0&1&1&1 \\ 0&1&0&1&1&1 \\ 0&0&1&1&1&1 \end{bmatrix};$$

- three $[14,7,2]$ codes, $\mathcal{X}_3, \mathcal{X}_4$ and $\mathcal{X}_5$, with generator matrices $[I|X_3]$,$[I|X_4]$ and $[I|X_5]$ respectively, where

$$X_3 := \begin{bmatrix} 1&1&1&0&0&0&0 \\ 1&1&1&0&0&0&0 \\ 1&1&1&0&0&0&0 \\ 1&0&0&1&1&1&1 \\ 1&0&0&1&1&1&1 \\ 1&0&0&1&1&1&1 \\ 1&0&0&0&0&0&0 \end{bmatrix}, \quad X_4 := \begin{bmatrix} 1&1&1&1&1&0&0 \\ 1&1&1&1&1&0&0 \\ 1&1&1&1&1&0&0 \\ 1&1&1&1&1&0&0 \\ 1&1&1&1&0&1&0 \\ 1&1&1&1&0&1&0 \\ 1&1&1&1&1&1&1 \end{bmatrix}, \quad X_5 := \begin{bmatrix} 1&0&1&0&1&0&0 \\ 1&0&1&0&1&0&0 \\ 1&0&1&0&1&0&0 \\ 1&0&1&0&1&0&0 \\ 1&1&1&0&1&0&1 \\ 1&1&1&0&1&0&1 \\ 1&1&1&1&1&1&1 \end{bmatrix}$$

and I is the 7×7 identity matrix.

Minimal set of generators? Infinitely many?

Another open problem

Examples

- $[n, 1, n]$ repetition code with $n > 3$:

$$w_{\mathcal{C}}(x, y) = x^n + y^n \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x, y)) \simeq D_n.$$

- $[12, 6, 6]_3$ ternary Golay code:

$$w_{\mathcal{C}}(x, y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12} \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x, y)) \simeq A_4.$$

- $[8, 4, 4]$ extended Hamming code:

$$w_{\mathcal{C}}(x, y) = x^8 + 14x^4y^4 + y^8 \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x, y)) \simeq S_4.$$

Open problem

Is there a code $\mathcal{C}$ such that $\overline{S}(w_{\mathcal{C}}(x, y)) \simeq A_5$?