Symmetries of Weight Enumerators

Martino Borello

Université Paris 8 - LAGA

Trento, 16.11.2016

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.

Basic definitions

- 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 $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ is the standard **inner product**,

$$\mathcal{C}^\perp := \{v \in \mathbb{F}_q^n \mid \langle v, c \rangle = 0, \text{ for all } c \in \mathcal{C}\} \quad (\textbf{dual} \text{ of } \mathcal{C}).$$

- If $\mathcal{C} = \mathcal{C}^\perp$, the code $\mathcal{C}$ is called **self-dual**.

Weight enumerator

$$\mathcal{C} \subseteq \mathbb{F}_q^n \rightsquigarrow w_{\mathcal{C}}(x,y) := \sum_{c \in \mathcal{C}} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

with $A_i := \#\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}$.

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

Remark: self-dual $\Rightarrow$ even.

Group action

$\mathrm{GL}_2(\mathbb{C}) \circlearrowleft \mathbb{C}[x,y]$:

$$\left(A := \begin{bmatrix} a & b \\ c & d \end{bmatrix}, p(x,y)\right) \mapsto p(x,y)^A := p(ax+by, cx+dy).$$

For $G \leqslant \mathrm{GL}_2(\mathbb{C})$, denote

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

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

$$S(p(x,y)) := \{A \in \mathrm{GL}_2(\mathbb{C}) \mid p(x,y)^A = p(x,y)\} \leqslant \mathrm{GL}_2(\mathbb{C}).$$

Example

$$G := \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle \Rightarrow \mathbb{C}[x,y]^G = \mathbb{C}[x,y^2].$$

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).
- $d := \min_{c \in \mathcal{C} - \{\underline{0}\}} \mathrm{wt}(c) \leqslant 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$ (Mallows and Sloane '73).

If the bound is achieved $\mathcal{C}$ is called **extremal**.
A length n is called **jump length** if $24 \mid n$.

- extremal and doubly-even $\Rightarrow n \leqslant 3928$ (Zhang '99).

Other results

- jump length and extremal $\Rightarrow$ doubly-even (Rains '98)

$\Downarrow$

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.

Idea:
properties of families of (self-dual) codes $\rightsquigarrow$ **symmetries** of weight enumerators $\rightsquigarrow$ new **properties**.

Our questions

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

Possible symmetries

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

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

This is a set of $N \leqslant \deg(p(x,y)) + 1$ points.

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

$$\begin{array}{ccc} \mathrm{PGL}_2(\mathbb{C}) & \circlearrowright & \mathbb{P}^1(\mathbb{C}) \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, (x:y)\right) & \mapsto & (ax+by : cx+dy) \end{array} \qquad \textbf{simply 3-transitive}$$

induces

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

- $p(x, y) \in \mathbb{C}[x, y]_h$ of degree n.

Remark 1

We have

$$p(x, y) = p(\lambda x, \lambda y) \Leftrightarrow \lambda^n = 1.$$

Then

$$\overline{S}(p(x, y)) = S(p(x, y)) \Big/ \left\langle \begin{bmatrix} \zeta_n & 0 \\ 0 & \zeta_n \end{bmatrix} \right\rangle ,$$

where $\zeta_n \in \mathbb{C}$ is a primitive n-th root of unity.

If $\overline{S}(p(x, y)) < \infty$, then

$$\#S(p(x, y)) = n \cdot \#\overline{S}(p(x, y)).$$

Remark 2

For all $A \in \mathrm{GL}_2(\mathbb{C})$, we have

$$S(p(x, y)^A) = S(p(x, y))^A.$$

Theorem (B.,Mila)

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

Proof:

$\Leftarrow$) $V(p(x,y)) = \{P_1, P_2, P_3, \ldots, P_m\}$.
$\forall \{i,j,k\} \subseteq \{1,\ldots,m\}$ there is at most one element $A \in \overline{S}(p(x,y))$ s.t.

$$P_1^A = P_i, \quad P_2^A = P_j, \quad P_3^A = P_k.$$

Then $\overline{S}(p(x,y)) \leqslant m \cdot (m-1) \cdot (m-2)$.

$\Rightarrow$) If $\#V(p(x,y)) < 3$, then $\#\overline{S}(p(x,y)) = \infty$.

□

In particular, if $\#V(p(x,y)) \geqslant 3$, then $\#S(p(x,y)) \leqslant n^4$.

Theorem (Blichfeldt 1917)

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

- $\left\langle \begin{bmatrix} 1 & 0 \\ 0 & \zeta_m \end{bmatrix} \right\rangle \simeq C_m$ for a certain $m \in \mathbb{N}$.
- $\left\langle \begin{bmatrix} 1 & 0 \\ 0 & \zeta_m \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \simeq D_m$ for a certain $m \in \mathbb{N}$.
- $\left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & i \\ 1 & -1 \end{bmatrix} \right\rangle \simeq A_4$.
- $\left\langle \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} i & i \\ 1 & -1 \end{bmatrix} \right\rangle \simeq S_4$.
- $\left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & i \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 2 & -\omega \\ \omega & -2 \end{bmatrix} \right\rangle \simeq A_5$ 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**.

- $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Proposition

$$\begin{bmatrix} 1 & 0 \\ 0 & \zeta_m \end{bmatrix} \in S(w_{\mathcal{C}}(x,y)) \Leftrightarrow \mathrm{wt}(\mathcal{C}) \subseteq m\mathbb{Z} \text{ (divisibility)}.$$

In particular, if $m > 5$,

$$\mathrm{wt}(\mathcal{C}) \subseteq m\mathbb{Z} \Rightarrow \overline{S}(w_{\mathcal{C}}(x,y)) \simeq C_{m'} \text{ or } \overline{S}(w_{\mathcal{C}}(x,y)) \simeq D_{m'} \ (m|m').$$

Lemma

If $q = 2$,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in S(w_{\mathcal{C}}(x,y)) \Leftrightarrow \underline{1} = (1,1,\dots,1) \in \mathcal{C}.$$

Example (Repetition code)

$\mathcal{C}$ the $[12,2,6]$ binary code with generator matrix

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

$w_{\mathcal{C}}(x,y) = x^{12} + 2x^6y^6 + y^{12} \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x,y)) \simeq D_6$.

MacWilliams identities.

Example (ternary Golay code)

$\mathcal{C}$ the $[12,6,6]_3$ ternary code with generator matrix

$$\begin{bmatrix} 1&0&0&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&0&0&1&0&1&2&2&1\\ 0&0&1&0&0&0&1&1&0&1&2&2\\ 0&0&0&1&0&0&1&2&1&0&1&2\\ 0&0&0&0&1&0&1&2&2&1&0&1\\ 0&0&0&0&0&1&1&1&2&2&1&0 \end{bmatrix}$$

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

Example (Hamming code)

$\mathcal{C}$ the $[8,4,4]$ binary code with generator matrix

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

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

Example

$f_1(x,y) := x^{20} + 228x^{15}y^5 + 494x^{10}y^{10} - 228x^5y^{15} + y^{20};$
$f_2(x,y) := x^{30} - 522x^{25}y^5 - 10005x^{20}y^{10} - 10005x^{10}y^{20} + 522x^5y^{25} + y^{30}.$

$$p(x,y) \in \mathbb{C}[f_1(x,y), f_2(x,y)] \Rightarrow \overline{S}(p(x,y)) \simeq A_5.$$

Open problem

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

Extensive search in $\mathbb{C}[f_1(x,y)^A, f_2(x,y)^A]$ for $A \in \mathrm{GL}_2(\mathbb{C})$ of $p(x,y)$ s.t.

- its coefficients are positive;
- $p(1,0) = 1$;
- $p(1,1)$ is a prime power.

Not yet found.

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$(p(x,1)) = \{x_1, \ldots, x_m\}$.
3. If $m < 3$, then print("Infinite group") and break; else $V_3 := \{\text{all ordered 3-subsets of } V\}$.
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. $\lambda := \frac{p(\underline{a},\underline{c})}{p(1,0)}$. $B := \lambda^{-1/n} A$.
     - 4biii. If $p(x,y)^B = p(x,y)$, then $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C} \text{ s.t. } \zeta_n^n = 1\}$.

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. $G := \varnothing$.
2. $V :=$ RootsOf$(p(x,1)) = \{x_1, \ldots, x_m\}$. (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 $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C}$ s.t. $\zeta_n^n = 1\}$.

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

- $\mathcal{C} \subseteq \mathbb{F}_q^n$ linear code.

Remark 1

$$\underline{0} \in \mathcal{C} \Rightarrow w_{\mathcal{C}}(x, y) = x^n + \dots \Rightarrow (1:0) \notin V(w_{\mathcal{C}}(x, y)).$$

Remark 2

$$w_{\mathcal{C}}(x, y) \in \mathbb{Z}[x, y] \Rightarrow \text{the roots of } w_{\mathcal{C}}(x, 1) \text{ are in } \overline{\mathbb{Z}}.$$

In the algorithm, roots in K s.t. $[K : \mathbb{Q}] < \infty$ (splitting field).

Remark 3

If we consider roots in $\mathbb{C}$, we have to deal with approximations.

Reed-Muller codes

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

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

Theorem (Ax '64)

Let $\Delta := q^{\lfloor \frac{m-1}{r} \rfloor}$. Then

$$\mathrm{wt}(\mathcal{RM}_q(r,m)) \subseteq \Delta\mathbb{Z}.$$

Lemma

If $r < m(q-1)$, then

$$\mathcal{RM}_q(r,m)^\perp = \mathcal{RM}_q(m(q-1)-r-1, m).$$

Remark

$$\mathcal{RM}_q(r,m) \text{ self-dual } \Leftrightarrow \begin{cases} q \text{ power of } 2, \\ m \text{ is odd}, \\ r = \frac{m(q-1)-1}{2}. \end{cases}$$

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

Ax's theorem implies:

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 $\overline{S}(w_{\mathcal{RM}_q(r,m)}(x, y))$ is either cyclic or dihedral.

Proof

$\begin{bmatrix} 1 & 0 \\ 0 & \zeta_\Delta \end{bmatrix} \in \overline{S}(w_{\mathcal{RM}_q(r,m)}(x, y))$ of order > 5 (ζ_Δ primitive Δ-th root of unity). □

By the algorithm we get:

Theorem (B.,Mila)

If $m \geqslant 2$, then

$$\begin{bmatrix} u & u-1 \\ u-1 & u \end{bmatrix} \in \overline{S}(w_{\mathcal{RM}_2(m-1,m)}(x,y)),$$

with $u := \frac{\zeta+1}{2}$ (ζ primitive 2^m-th root of unity).

Theorem (B.,Mila)

Let $\mathcal{C} \in \{\mathcal{RM}_4(2,2), \mathcal{RM}_4(3,2), \mathcal{RM}_5(2,2)\}$, then

$$\overline{S}(w_{\mathcal{C}}(x,y)) = \{\mathrm{Id}\}.$$

Open problem

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

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?

Thank you very much for the attention!