Doubling method for self-dual linear codes

Jolanta Marzec-Ballesteros

(joint with Thanasis Bouganis)

36th Automorphic Forms Workshop
Oklahoma State University, 20-24.05.2024

Doubling method

- $\rightarrow$ Independently invented by Garrett and by Piatetski-Shapiro and Rallis in 1980s.
- $\rightarrow$ Used to construct L-functions, prove their analytic properties, algebraicity of special values and much more.

Doubling method

- → Independently invented by Garrett and by Piatetski-Shapiro and Rallis in 1980s.
- → Used to construct L-functions, prove their analytic properties, algebraicity of special values and much more.

$$\begin{array}{c} \text{integral of cuspform against} \\ \text{restriction of Siegel-type} \\ \text{Eisenstein series} \end{array} = \begin{array}{c} L\text{-function} \\ \text{attached to} \\ \text{cusp form} \end{array} \times \begin{array}{c} \text{cusp form or} \\ \text{Eisenstein series} \\ \text{att. to cusp form} \end{array}$$

$$\langle E(\left(\begin{smallmatrix} g & \\ & g' \end{smallmatrix}\right), s), f(g)\rangle = L(f, s) f(g'),$$

if $g, g' \in G$, $\mathrm{Re}\, s \gg 0$, f Hecke eigenform.

Doubling method

→ Independently invented by Garrett and by Piatetski-Shapiro and Rallis in 1980s.

→ Used to construct L-functions, prove their analytic properties, algebraicity of special values and much more.

integral of cuspform against restriction of Siegel-type Eisenstein series	=	L-function attached to cusp form	×	cusp form or Eisenstein series att. to cusp form

$$\langle E(\left(\begin{smallmatrix} g & \\ & g' \end{smallmatrix}\right), s), f(g)\rangle = L(f, s) f(g'),$$

if $g, g' \in G$, $\mathrm{Re}\, s \gg 0$, f Hecke eigenform.

→ Done for G symplectic, orthogonal, unitary over global field, also for congruence subgroups (G., P-S and R., Böcherer, Shimura), Jacobi group (Bouganis, M-B.).

Doubling method (overview)

f a cusp form on G, $\quad H$ such that $G \times G \hookrightarrow H$ exists

$E(h,s) = \sum_{\gamma \in P\backslash H} \phi(\gamma h, s)$ Eisenstein series on H,
e.g. $E(h,s) = \sum_{\gamma \in P\backslash H} \varphi(s)|_\gamma$

Doubling method (overview)

f a cusp form on G, H such that $G \times G \hookrightarrow H$ exists

$E(h,s) = \sum_{\gamma \in P\backslash H} \phi(\gamma h, s)$ Eisenstein series on H,
e.g. $E(h,s) = \sum_{\gamma \in P\backslash H} \varphi(s)|_\gamma$

$$\begin{aligned}
\langle E(\left(\begin{smallmatrix} g & \\ & g' \end{smallmatrix}\right), s), f(g)\rangle &= \sum_{\gamma \in P\backslash H} \langle \phi(\gamma \left(\begin{smallmatrix} g & \\ & g' \end{smallmatrix}\right), s), f(g)\rangle \\
&= \sum_{\gamma \in P\backslash H/(G\times G)} \sum_{(k,k')\in G\times G} \langle \phi(\gamma \begin{pmatrix} kg & \\ & k'g' \end{pmatrix}, s), f(g)\rangle \\
&= \ldots = \sum_{(k,k')\in G\times G} \langle \phi(\gamma_0 \begin{pmatrix} kg & \\ & k'g' \end{pmatrix}, s), f(g)\rangle \\
&= \sum_{\beta \in \gamma_0(G\times 1)} \psi(s) f|_\beta(g') = L(f,s) f(g')
\end{aligned}$$

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

$\langle\ ,\ \rangle : C \times C \to \mathbb{F}$ Euclidean inner product

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

$\langle\ ,\ \rangle : C \times C \to \mathbb{F}$ Euclidean inner product

C is self-dual if $C = C^{\perp} := \{v \in \mathbb{F}^{2n} : \forall_{c \in C}\, \langle v, c\rangle = 0\}$

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

$\langle\ ,\ \rangle : C \times C \to \mathbb{F}$ Euclidean inner product

C is self-dual if $C = C^{\perp} := \{v \in \mathbb{F}^{2n} : \forall_{c \in C}\, \langle v, c\rangle = 0\}$

Then (the length $2n$ is even and) $\dim C = n$.

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

$\langle\ ,\ \rangle : C \times C \to \mathbb{F}$ Euclidean inner product

C is self-dual if $C = C^{\perp} := \{v \in \mathbb{F}^{2n} : \forall_{c \in C}\, \langle v, c \rangle = 0\}$

Then (the length $2n$ is even and) $\dim C = n$.

The weight of a codeword $c = (c_1, \ldots, c_{2n}) \in C$ is

$$\mathrm{wt}\, c = \#\{i \in \{1, \ldots, 2n\} : c_i \neq 0\}.$$

Self-dual linear codes

A linear code of length $2n$ over a finite field $\mathbb{F}$ is $C \subset \mathbb{F}^{2n}$, a linear subspace.

$\langle\ ,\ \rangle : C \times C \to \mathbb{F}$ Euclidean inner product

C is self-dual if $C = C^{\perp} := \{v \in \mathbb{F}^{2n} : \forall_{c \in C}\ \langle v, c\rangle = 0\}$

Then (the length $2n$ is even and) $\dim C = n$.

The weight of a codeword $c = (c_1, \ldots, c_{2n}) \in C$ is

$$\mathrm{wt}\, c = \#\{i \in \{1, \ldots, 2n\} : c_i \neq 0\}.$$

Today: $\mathbb{F}$ means $\mathbb{F}_p$ with p prime.

Weight enumerators

... are certain homogeneous polynomials of degree $2n$ in variables from the set $V = \{x_\alpha : \alpha \in \mathbb{F}^g\}$, $g \in \mathbb{N}$ is a genus.

Weight enumerators

... are certain homogeneous polynomials of degree $2n$ in variables from the set $V = \{x_\alpha : \alpha \in \mathbb{F}^g\}$, $g \in \mathbb{N}$ is a genus.

The genus 1 weight enumerator of a code $C \subset \mathbb{F}_2^{2n}$ is a polynomial

$$W_1(C, (x_0, x_1)) = \sum_{c \in C} x_0^{2n - \mathrm{wt}\, c} x_1^{\mathrm{wt}\, c}$$

Weight enumerators

... are certain homogeneous polynomials of degree $2n$ in variables from the set $V = \{x_\alpha : \alpha \in \mathbb{F}^g\}$, $g \in \mathbb{N}$ is a genus.

The genus 1 weight enumerator of a code $C \subset \mathbb{F}_2^{2n}$ is a polynomial

$$W_1(C,(x_0,x_1)) = \sum_{c \in C} x_0^{2n-\mathrm{wt}\, c} x_1^{\mathrm{wt}\, c}$$

The genus g weight enumerator of a code $C \subset \mathbb{F}^{2n}$ is a polynomial

$$W_g(C,\mathbf{x}) = \sum_{(c^1,\ldots,c^g)\in C^g} \prod_{\alpha \in \mathbb{F}^g} x_\alpha^{w_\alpha(c^1,\ldots,c^g)}$$

of degree $2n$, where $\mathbf{x} = (x_\alpha)_{\alpha \in \mathbb{F}^g}$ and

$$w_\alpha(c^1,\ldots,c^g) = \#\{\text{rows } r \text{ in } \begin{pmatrix} c_1^1 & & c_1^g \\ \vdots & \ldots & \vdots \\ c_{2n}^1 & & c_{2n}^g \end{pmatrix} : r = \alpha\}$$

Weight enumerators

$$H_8 = \mathrm{span}_{\mathbb{F}_2}\left\{ \begin{pmatrix} 1\\0\\0\\1\\0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1\\0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\1\\0\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\1\\1\\1\\1 \end{pmatrix} \right\} \subset \mathbb{F}_2^8 \quad \text{(Hamming code)}$$

Weight enumerators

$$H_8 = \mathrm{span}_{\mathbb{F}_2}\{ \begin{pmatrix} 1\\0\\0\\1\\0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1\\0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\1\\0\\0\\1\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\0\\0\\1\\1\\1\\1 \end{pmatrix} \} \subset \mathbb{F}_2^8 \quad \text{(Hamming code)}$$

$$\begin{aligned} W_2(H_8, (x_{00}, x_{01}, x_{10}, x_{11})) &= \sum_{\alpha \in \mathbb{F}_2^2} x_\alpha^8 + 14 \sum_{\substack{\alpha_1, \alpha_2 \in \mathbb{F}_2^2 \\ \alpha_1 < \alpha_2}} x_{\alpha_1}^4 x_{\alpha_2}^4 + 168 x_{00}^2 x_{01}^2 x_{10}^2 x_{11}^2 \\ &= (8) + 14(4,4) + 168(2,2,2,2) \end{aligned}$$

Weight enumerators

$$H_8 = \mathrm{span}_{\mathbb{F}_2}\{ \begin{pmatrix}1\\0\\0\\1\\0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\\0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\\0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\0\\0\\1\\1\\1\\1\end{pmatrix} \} \subset \mathbb{F}_2^8 \quad \text{(Hamming code)}$$

$$\begin{aligned} W_2(H_8, (x_{00}, x_{01}, x_{10}, x_{11})) &= \sum_{\alpha \in \mathbb{F}_2^2} x_\alpha^8 + 14 \sum_{\substack{\alpha_1, \alpha_2 \in \mathbb{F}_2^2 \\ \alpha_1 < \alpha_2}} x_{\alpha_1}^4 x_{\alpha_2}^4 + 168 x_{00}^2 x_{01}^2 x_{10}^2 x_{11}^2 \\ &= (8) + 14(4,4) + 168(2,2,2,2) \end{aligned}$$

In general:

$$W_g(C) = \sum_A b_A \cdot (A),$$

where

$$A \in \{(a_0, \ldots, a_{2^g-1}) : \text{“admissible tuples”}, \quad \sum_{i=0}^{2^g-1} a_i = 2n\}.$$

Some analogies with modular forms

$W_g(C)$		modular form f of genus g
$\sum_A b_A \cdot (A)$	$\longleftrightarrow$	Fourier expansion
$(2n)$		constant term $a(0)$

Some analogies with modular forms

$W_g(C)$		modular form f of genus g
$\sum_A b_A \cdot (A)$	$\longleftrightarrow$	Fourier expansion
$(2n)$		constant term $a(0)$

Examples of cusp forms:

$$W_1(G_{24}) - W_1(H_8 \times H_8 \times H_8) = -42(20,4) + 168(16,8) - 252(12,12)$$

is a cusp form of genus 1.

Some analogies with modular forms

$W_g(C)$		modular form f of genus g
$\sum_A b_A \cdot (A)$	$\longleftrightarrow$	Fourier expansion
$(2n)$		constant term $a(0)$

Examples of cusp forms:

$$W_1(G_{24}) - W_1(H_8 \times H_8 \times H_8) = -42(20,4) + 168(16,8) - 252(12,12)$$

is a cusp form of genus 1.

$$\begin{aligned} & W_3(E_{16}) - W_3(H_8 \times H_8) = \\ & - 2688(9,1,1,1,1,1,1,1) + 1344(8,0,0,0,2,2,2,2) - 1344(6,2,2,2,4,0,0,0) \\ & + 5376(5,5,1,1,1,1,1,1) + 1344(4,4,4,0,4,0,0,0) + 2688(4,4,0,0,2,2,2,2) \\ & - 21504(3,3,3,3,1,1,1,1) + 96768(2,2,2,2,2,2,2,2) \end{aligned}$$

is a cusp form of genus 3.

Clifford-Weil group

Theorem (Runge, 1996; Nebe, Rains, Sloane, 2006)

$$\langle W_g(C) : C \text{ self-dual, over } \mathbb{F}\rangle = (\mathbb{C}[x_\alpha : \alpha \in \mathbb{F}^g])^{\mathcal{C}_g},$$

where $\mathcal{C}_g =< m_r, d_\phi, h_{\iota,u_\iota,v_\iota} : r \in \mathrm{GL}_g(\mathbb{F}), \phi, \iota >$ *with*

$$m_r : x_\alpha \mapsto x_{r\alpha}, \qquad d_\phi : x_\alpha \mapsto e^{2\pi i \phi(\alpha)} x_\alpha$$

$$h_{\iota,u_\iota,v_\iota} : x_\alpha \mapsto (\#\iota\mathbb{F}^g)^{-\frac{1}{2}} \sum_{w \in \iota\mathbb{F}^g} e^{\frac{2\pi i}{p}\langle w, v_\iota \alpha\rangle} x_{w+(1-\iota)\alpha},$$

$V = \{x_\alpha : \alpha \in \mathbb{F}^g\}$, $\operatorname{char}\mathbb{F} = p$, $\iota = u_\iota v_\iota \in \mathbb{F}^{g\times g}$ *symmetric idempotent.*

Clifford-Weil group

Theorem (Runge, 1996; Nebe, Rains, Sloane, 2006)

$$\langle W_g(C) : C \textit{ self-dual, over } \mathbb{F}\rangle = (\mathbb{C}[x_\alpha : \alpha \in \mathbb{F}^g])^{\mathcal{C}_g},$$

where $\mathcal{C}_g =< m_r, d_\phi, h_{\iota,u_\iota,v_\iota} : r \in \mathrm{GL}_g(\mathbb{F}), \phi, \iota >$ *with*

$$m_r : x_\alpha \mapsto x_{r\alpha}, \qquad d_\phi : x_\alpha \mapsto e^{2\pi i\phi(\alpha)}x_\alpha$$

$$h_{\iota,u_\iota,v_\iota} : x_\alpha \mapsto (\#\iota\mathbb{F}^g)^{-\frac{1}{2}} \sum_{w\in\iota\mathbb{F}^g} e^{\frac{2\pi i}{p}\langle w,v_\iota\alpha\rangle} x_{w+(1-\iota)\alpha},$$

$V = \{x_\alpha : \alpha \in \mathbb{F}^g\}$, $\mathrm{char}\,\mathbb{F} = p$, $\iota = u_\iota v_\iota \in \mathbb{F}^{g\times g}$ *symmetric idempotent.*

In fact:

- $\mathbb{F} = \mathbb{F}_p$, p odd: $\mathcal{C}_g \cong Z_{\gcd(p+1,4)} \times p_+^{1+2g}.\mathrm{Sp}_{2g}(\mathbb{F})$
- $\mathbb{F} = \mathbb{F}_2$, doubly even codes: $\mathcal{C}_g \cong Z_8 \times 2_+^{1+2g}.\mathrm{Sp}_{2g}(\mathbb{F})$
- $\mathbb{F} = \mathbb{F}_2$: $\mathcal{C}_g \cong 2_+^{1+2g}.\mathrm{O}_{2g}^+(\mathbb{F})$

Consider the mean polynomial ("Siegel-type Eisenstein series")

$$M_{2g}((2n)) = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} (2n)^{\gamma} = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} \sum_{\alpha \in \mathbb{F}^{2g}} ((x_\alpha)^{\gamma})^{2n}$$

$$= const. \sum_{\substack{C \subset \mathbb{F}^{2n} \\ \text{of fixed type}}} W_{2g}(C, \mathbf{x})$$

(second equality: Nebe, Rains, Sloane, 2000)

Consider the mean polynomial ("Siegel-type Eisenstein series")

$$M_{2g}((2n)) = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} (2n)^{\gamma} = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} \sum_{\alpha \in \mathbb{F}^{2g}} ((x_\alpha)^\gamma)^{2n}$$

$$= const. \sum_{\substack{C \subset \mathbb{F}^{2n} \\ \text{of fixed type}}} W_{2g}(C, \mathbf{x})$$

(second equality: Nebe, Rains, Sloane, 2000) and an inner product

$$\langle \prod_{\alpha \in \mathbb{F}^g} x_\alpha^{n_\alpha}, \prod_{\alpha \in \mathbb{F}^g} x_\alpha^{m_\alpha} \rangle = \begin{cases} \prod_{\alpha \in \mathbb{F}^g} n_\alpha!, & n_\alpha = m_\alpha \text{ for all } \alpha \\ 0, & \text{otherwise} \end{cases}.$$

Consider the mean polynomial ("Siegel-type Eisenstein series")

$$M_{2g}((2n)) = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} (2n)^{\gamma} = \sum_{\gamma \in P_{2g} \backslash \mathcal{C}_{2g}} \sum_{\alpha \in \mathbb{F}^{2g}} ((x_\alpha)^{\gamma})^{2n}$$
$$= const. \sum_{\substack{C \subset \mathbb{F}^{2n} \\ \text{of fixed type}}} W_{2g}(C, \mathbf{x})$$

(second equality: Nebe, Rains, Sloane, 2000) and an inner product

$$\langle \prod_{\alpha \in \mathbb{F}^g} x_\alpha^{n_\alpha}, \prod_{\alpha \in \mathbb{F}^g} x_\alpha^{m_\alpha} \rangle = \begin{cases} \prod_{\alpha \in \mathbb{F}^g} n_\alpha!, & n_\alpha = m_\alpha \text{ for all } \alpha \\ 0, & \text{otherwise} \end{cases}.$$

Theorem (Bouganis, M-B., 2024; in progress)

Let $\mathcal{T}$ be a family of self-dual codes of length $2n$ over a field $\mathbb{F}$: either $\mathrm{char}\,\mathbb{F}$ odd or $\mathbb{F} = \mathbb{F}_2$ and $C \in \mathcal{T}$ doubly-even; fix $g \in \mathbb{N}$. There exists an (explicit) constant C st. for a cusp form $f \in \mathcal{T}$ of genus r, $\deg f = 2n$:

$$\langle M_{2g}((2n))(\boldsymbol{xy}), f(\boldsymbol{x}) \rangle = \begin{cases} 0, & r < g \\ C \cdot f(\boldsymbol{y}), & r = g \end{cases}.$$

Theorem (Gleason, 1971)

If C is a self-dual doubly even code, then $W_1(C) \in \mathbb{C}[W_1(H_8), W_1(G_{24})]$.

Theorem (Hecke, 1937)

If Λ is a unimodular doubly even lattice, then $\theta_\Lambda(\tau) \in \mathbb{C}[E_4(\tau), \Delta_{12}(\tau)]$.

Theorem (Broué and Enguehard 1972, Duke 1993)

The map

$$\langle W_g(C) : C \text{ self-dual doubly even} \rangle \to \oplus_{4|k} \mathcal{M}_k(\mathrm{Sp}_g(\mathbb{Z}))$$

$$W_g(C, (x_\alpha)_{\alpha \in \mathbb{F}_2^g}) \mapsto W_g(C, \left(\sum_{b \in \mathbb{Z}^g} e^{2\pi i (b+\alpha/2)\tau(b+\alpha/2)^t} \right)_{\alpha \in \mathbb{F}_2^g})$$

$$= \sum_{l_1,\dots,l_g \in \Lambda(C)} e^{\pi i \mathrm{tr}(\tau G(l_1,\dots,l_g))}$$

is a homomorphism. It's an isomorphism for $g \in \{1, 2\}$.