

Clifford-Weil groups.

Gabriele Nebe, RWTH Aachen University

Vlora, April 29, 2008

- Introduce Clifford-Weil group $\mathcal{C}(T)$.
- Complete weight enumerators of codes of Type T are invariant under $\mathcal{C}(T)$.
- In many (conjecturally all) situations the invariant ring of $\mathcal{C}(T)$ is generated by the cwe_C for C of Type T
- Symmetrized weight enumerators and symmetrized Clifford-Weil groups.
- Higher weight enumerators and higher Clifford-Weil groups.

Recall that a **Type** $T = (R, V, \beta, \Phi)$ consists of
 a ring R with involution J , a left R -module V ,
 an ϵ -Hermitian form $\beta : V \times V \rightarrow \mathbb{Q}/\mathbb{Z}$
 an R -qmodule $\Phi \leq \text{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$
 containing $x \mapsto \beta(x, rx)$ for all $r \in R$
 such that for all $\phi \in \Phi$ there is $r_\phi \in R$ with
 $\lambda(\phi) : (x, y) \mapsto \phi(x + y) - \phi(x) - \phi(y) = \beta(x, r_\phi y)$

A **code** C is an R -submodule $C \leq V^N$ and the
dual code is $C^\perp = \{v \in V^N \mid \sum_{i=1}^N \beta(v_i, c_i) = 0 \text{ for all } c \in C\}$
 C is **isotropic** if $\sum_{i=1}^N \phi(c_i) = 0$ for all $\phi \in \Phi$, $c \in C$.
 A self-dual isotropic code is a **code of Type** T .

Complete weight enumerators,

For $c = (c_1, \dots, c_N) \in V^N$ and $v \in V$ put

$$a_v(c) := |\{i \in \{1, \dots, N\} \mid c_i = v\}|.$$

Then

$$\text{cwe}_C := \sum_{c \in C} \prod_{v \in V} x_v^{a_v(c)} \in \mathbb{C}[x_v : v \in V]$$

is called the **complete weight enumerator of the code C** .

The tetracode.

$$t_4 := \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{array} \right] \leq \mathbb{F}_3^4$$

$$\text{cwe}_{t_4}(x_0, x_1, x_2) = x_0^4 + x_0x_1^3 + x_0x_2^3 + 3x_0x_1^2x_2 + 3x_0x_1x_2^2.$$

$$\text{hwe}_{t_4}(x, y) = \text{cwe}_{t_4}(x, y, y) = x^4 + 8xy^3.$$

Clifford-Weil groups.

Let $T := (R, V, \beta, \Phi)$ be a Type. Then the **associated Clifford-Weil group** $\mathcal{C}(T)$ is a subgroup of $\mathrm{GL}_{|V|}(\mathbb{C})$

$$\mathcal{C}(T) = \langle m_r, d_\phi, h_{e, u_e, v_e} \mid r \in R^*, \phi \in \Phi, e = u_e v_e \in R \text{ symmetric idempotent} \rangle$$

Let $(e_v \mid v \in V)$ denote a basis of $\mathbb{C}^{|V|}$. Then

$$m_r : e_v \mapsto e_r v, \quad d_\phi : e_v \mapsto \exp(2\pi i \phi(v)) e_v$$

$$h_{e, u_e, v_e} : e_v \mapsto |eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) e_{w + (1-e)v}$$

Type I codes (2_I)

$$R = \mathbb{F}_2 = V, \beta(x, y) = \frac{1}{2}xy, \Phi = \{\varphi : x \mapsto \frac{1}{2}x^2 = \beta(x, x), 0\}$$

$$\mathcal{C}(I) = \langle d_\varphi = \text{diag}(1, -1), h_{1,1,1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = h_2 \rangle = G_I$$

Type II codes (2_{II}).

$$R = \mathbb{F}_2 = V, \beta(x, y) = \frac{1}{2}xy, \Phi = \{\phi : x \mapsto \frac{1}{4}x^2, 2\phi = \varphi, 3\phi, 0\}$$

$$\mathcal{C}(II) = \langle d_\phi = \text{diag}(1, i), h_2 \rangle = G_{II}$$

Type III codes (3).

$$R = \mathbb{F}_3 = V, \quad \beta(x, y) = \frac{1}{3}xy, \quad \Phi = \{\varphi : x \mapsto \frac{1}{3}x^2 = \beta(x, x), 2\varphi, 0\}$$

$$\mathcal{C}(\text{III}) = \langle m_2 = \begin{pmatrix} 100 \\ 001 \\ 010 \end{pmatrix}, d_\varphi = \text{diag}(1, \zeta_3, \zeta_3), h_{1,1,1} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix} \rangle$$

Type IV codes (4^H).

$$R = \mathbb{F}_4 = V, \quad \beta(x, y) = \frac{1}{2} \text{trace}(x\bar{y}), \quad \Phi = \{\varphi : x \mapsto \frac{1}{2}x\bar{x}, 0\}$$

where $\bar{x} = x^2$.

$$\mathcal{C}(\text{IV}) = \langle m_\omega = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix}, d_\varphi = \text{diag}(1, -1, -1, -1), h_{1,1,1} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \rangle$$

Theorem.

Let $C \leq V^N$ be a self-dual isotropic code of Type T . Then cwe_C is invariant under $\mathcal{C}(T)$.

Proof.

Invariance under m_r ($r \in R^*$) because C is a code.

Invariance under d_ϕ ($\phi \in \Phi$) because C is isotropic.

Invariance under h_{e,u_e,v_e} because C is self dual.

The main theorem.(N., Rains, Sloane (1999-2006))

If R is a direct product of matrix rings over chain rings, then

$$\text{Inv}(\mathcal{C}(T)) = \langle \text{cwe}_C \mid C \text{ of Type } T \rangle.$$

Symmetrizations.

Let (R, J) be a ring with involution.

Then the **central unitary group** is

$$\text{ZU}(R, J) := \{g \in Z(R) \mid gg^J = g^J g = 1\}.$$

Theorem. Let $T = (R, V, \beta, \Phi)$ be a Type and

$$U := \{u \in \text{ZU}(R, J) \mid \phi(uv) = \phi(v) \text{ for all } \phi \in \Phi, v \in V\}.$$

Then $m(U) := \{m_u \mid u \in U\}$ is in the center of $\mathcal{C}(T)$.

Let $U \leq \text{ZU}(R, J)$ and X_0, \dots, X_n be the U -orbits on V .
 The U -**symmetrized Clifford-Weil group** is

$$\mathcal{C}^{(U)}(T) = \{g^{(U)} \mid g \in \mathcal{C}(T)\} \leq \text{GL}_{n+1}(\mathbb{C})$$

If

$$g\left(\frac{1}{|X_i|} \sum_{v \in X_i} e_v\right) = \sum_{j=0}^n a_{ij} \left(\frac{1}{|X_j|} \sum_{w \in X_j} e_w\right)$$

then

$$g^{(U)}(x_i) = \sum_{j=0}^n a_{ij} x_j.$$

Remark. The invariant ring of $\mathcal{C}^{(U)}(T)$ consists of the U -symmetrized invariants of $\mathcal{C}(T)$. In particular, if the invariant ring of $\mathcal{C}(T)$ is spanned by the complete weight enumerators of self-dual codes in T , then the invariant ring of $\mathcal{C}^{(U)}(T)$ is spanned by the U -symmetrized weight-enumerators of self-dual codes in T .

Let U permute the elements of V and let $C \leq V^N$. Let X_0, \dots, X_n denote the orbits on U on V and for $c = (c_1, \dots, c_N) \in C$ and $0 \leq j \leq n$ define

$$a_j(c) = |\{1 \leq i \leq N \mid c_i \in X_j\}|$$

Then the U -**symmetrized weight-enumerator** of C is

$$\text{cwe}_C^{(U)} = \sum_{c \in C} \prod_{j=0}^n x_j^{a_j(c)} \in \mathbb{C}[x_0, \dots, x_n]$$

.

Gleason's Theorem revisited.

For Type I,II,III,IV the central unitary group $ZU(R, J)$ is transitive on $V - \{0\}$, so there are only two orbits:

$$x \leftrightarrow \{0\}, \quad y \leftrightarrow V - \{0\}$$

and the symmetrized weight enumerators are the Hamming weight enumerators.

$$\mathcal{C}(\text{III}) = \langle m_2 = \begin{pmatrix} 100 \\ 001 \\ 010 \end{pmatrix}, d_\varphi = \text{diag}(1, \zeta_3, \zeta_3), h_{1,1,1} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix} \rangle$$

yields the symmetrized Clifford-Weil group $G_{\text{III}} = \mathcal{C}^{(U)}(\text{III})$

$$\mathcal{C}^{(U)}(\text{III}) = \langle m_2^{(U)} = I_2, d_\varphi^{(U)} = \text{diag}(1, \zeta_3), h_{1,1,1}^{(U)} = h_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \rangle$$

$$\mathcal{C}(\text{IV}) = \langle m_\omega = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix}, d_\varphi = \text{diag}(1, -1, -1, -1), h_{1,1,1} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \rangle$$

yields the symmetrized Clifford-Weil group $G_{\text{IV}} = \mathcal{C}^{(U)}(\text{IV})$

$$\mathcal{C}^{(U)}(\text{IV}) = \langle m_\omega^{(U)} = I_2, d_\varphi^{(U)} = \text{diag}(1, -1), h_{1,1,1}^{(U)} = h_4 = \frac{1}{2} \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \rangle$$

Hermitian codes over \mathbb{F}_9

$$(9^H) : R = V = \mathbb{F}_9, \beta(x, y) = \frac{1}{3} \text{trace}(x\bar{y}), \Phi = \{\varphi : x \mapsto \frac{1}{3}x\bar{x}, 2\varphi, 0\}.$$

Let α be a primitive element of \mathbb{F}_9 and put $\zeta = \zeta_3 \in \mathbb{C}$. Then with respect to the \mathbb{C} -basis

$$(0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$$

of $\mathbb{C}[V]$, the associated Clifford-Weil group $\mathcal{C}(9^H)$ is generated by $d_\varphi := \text{diag}(1, \zeta, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2)$,

$$m_\alpha := \begin{pmatrix} 100000000 \\ 000000001 \\ 010000000 \\ 001000000 \\ 000100000 \\ 000010000 \\ 000001000 \\ 000000100 \\ 000000010 \end{pmatrix}, \quad h := \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1\zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 \\ 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 \\ 1 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 \\ 1 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 \\ 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta \\ 1\zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta & \zeta^2 & 1 \\ 1 & 1 & \zeta & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta \\ 1\zeta^2 & 1 & \zeta^2 & \zeta^2 & \zeta & 1 & \zeta & \zeta \end{pmatrix}$$

$\mathcal{C}(9^H)$ is a group of order 192 with Molien series

$$\frac{\theta(t)}{(1-t^2)^2(1-t^4)^2(1-t^6)^3(1-t^8)(1-t^{12})}$$

where

$$\begin{aligned}\theta(t) := & 1 + 3t^4 + 24t^6 + 74t^8 + 156t^{10} + 321t^{12} + 525t^{14} + 705t^{16} \\ & + 905t^{18} + 989t^{20} + 931t^{22} + 837t^{24} + 640t^{26} + 406t^{28} \\ & + 243t^{30} + 111t^{32} + 31t^{34} + 9t^{36} + t^{38},\end{aligned}$$

So the invariant ring of $\mathcal{C}(9^H)$ has at least

$$\theta(1) + 9 = 6912 + 9 = 6921$$

generators and the maximal degree (=length of the code) is 38.

What about Hamming weight enumerators ?

$$U := \text{ZU}(9^H) = \{x \in \mathbb{F}_9^* \mid x\bar{x} = x^4 = 1\} = (\mathbb{F}_9^*)^2$$

has 3 orbits on $V = \mathbb{F}_9$:

$$\{0\} = X_0, \quad \{1, \alpha^2, \alpha^4, \alpha^6\} =: X_1, \quad \{\alpha, \alpha^3, \alpha^5, \alpha^7\} =: X_2$$

$$\mathcal{C}^{(U)}(9^H) = \langle d_\varphi^{(U)} := \text{diag}(1, \zeta, \zeta^2), \quad m_\alpha^{(U)} := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad h^{(U)} := \frac{1}{3} \begin{pmatrix} 1 & 4 & 4 \\ 1 & 1-2 \\ 1-2 & 1 \end{pmatrix} \rangle$$

of order $\frac{192}{4} = 48$ of which the invariant ring is a polynomial ring spanned by the U -symmetrized weight enumerators

$$q_2 = x_0^2 + 8x_1x_2, \quad q_4 = x_0^4 + 16(x_0x_1^3 + x_0x_2^3 + 3x_1^2x_2^2)$$

$$q_6 = x_0^6 + 8(x_0^3x_1^3 + x_0^3x_2^3 + 2x_1^6 + 2x_2^6) \\ + 72(x_0^2x_1^2x_2^2 + 2x_0x_1^4x_2 + 2x_0x_1x_2^4) + 320x_1^3x_2^3$$

of the three codes with generator matrices

$$\begin{bmatrix} 1 & \alpha \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & \alpha & 2\alpha & 0 & 1 & 2 \end{bmatrix}.$$

Their Hamming weight enumerators are

$$r_2 = q_2(x, y, y) := x^2 + 8y^2,$$

$$r_4 = q_4(x, y, y) := x^4 + 32xy^3 + 48y^4,$$

$$r_6 = q_6(x, y, y) := x^6 + 16x^3y^3 + 72x^2y^4 + 288xy^5 + 352y^6.$$

The polynomials r_2, r_4 and r_6 generate the ring $\text{Ham}(9^H)$ spanned by the Hamming weight enumerators of the codes of Type 9^H .

$\text{Ham}(9^H) = \mathbb{C}[r_2, r_4] \oplus r_6\mathbb{C}[r_2, r_4]$ with the syzygy

$$r_6^2 = \frac{3}{4}r_2^4r_4 - \frac{3}{2}r_2^2r_4^2 - \frac{1}{4}r_4^3 - r_2^3r_6 + 3r_2r_4r_6.$$

Note that $\text{Ham}(9^H)$ is **not** the invariant ring of a finite group.

Higher genus complete weight enumerators.

Let $c^{(i)} := (c_1^{(i)}, \dots, c_N^{(i)}) \in V^N$, $i = 1, \dots, m$, be m not necessarily distinct codewords. For $v := (v_1, \dots, v_m) \in V^m$, let

$$a_v(c^{(1)}, \dots, c^{(m)}) := |\{j \in \{1, \dots, N\} \mid c_j^{(i)} = v_i \text{ for all } i \in \{1, \dots, m\}\}|.$$

The **genus- m complete weight enumerator** of C is

$$\text{cwe}_m(C) := \sum_{(c^{(1)}, \dots, c^{(m)}) \in C^m} \prod_{v \in V^m} x_v^{a_v(c^{(1)}, \dots, c^{(m)})} \in \mathbb{C}[x_v : v \in V^m].$$

$$\begin{array}{cccccc}
 c_1^{(1)} & c_2^{(1)} & \dots & c_j^{(1)} & \dots & c_N^{(1)} \\
 c_1^{(2)} & c_2^{(2)} & \dots & c_j^{(2)} & \dots & c_N^{(2)} \\
 \vdots & \vdots & \dots & \vdots & \dots & \vdots \\
 c_1^{(m)} & c_2^{(m)} & \dots & c_j^{(m)} & \dots & c_N^{(m)} \\
 & & & \uparrow & & \\
 & & & v \in V^m & &
 \end{array}$$

$C = i_2 = \{(0, 0), (1, 1)\}$, then $\text{cwe}_2(C) = x_{00}^2 + x_{11}^2 + x_{01}^2 + x_{10}^2$.

$$C = e_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

$$\begin{aligned} \text{cwe}_2(e_8) &= x_{00}^8 + x_{01}^8 + x_{10}^8 + x_{11}^8 + 168x_{00}^2x_{01}^2x_{10}^2x_{11}^2 + \\ &14(x_{00}^4x_{01}^4 + x_{00}^4x_{10}^4 + x_{00}^4x_{11}^4 + x_{01}^4x_{10}^4 + x_{01}^4x_{11}^4 + x_{10}^4x_{11}^4) \end{aligned}$$

For $C \leq V^N$ and $m \in \mathbb{N}$ let

$$C(m) := R^{m \times 1} \otimes C = \{(c^{(1)}, \dots, c^{(m)})^{\text{Tr}} \mid c^{(1)}, \dots, c^{(m)} \in C\} \leq (V^m)^N$$

Then

$$\text{cwe}_m(C) = \text{cwe}(C(m)).$$

Moreover if C is a self-dual isotropic code of Type $T = (R, V, \beta, \Phi)$, then $C(m)$ is a self-dual isotropic code of Type

$$T^m = (R^{m \times m}, V^m, \beta^{(m)}, \Phi^{(m)})$$

and hence

$$\text{cwe}_m(C) \text{ is invariant under } \mathcal{C}_m(T) := \mathcal{C}(T^m)$$

the genus- m Clifford-Weil group.

Example: $\mathcal{C}_2(\text{I})$.

$$R = \mathbb{F}_2^{2 \times 2}, R^* = \text{GL}_2(\mathbb{F}_2) = \langle a := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, b := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \rangle$$

$$V = \mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}, \text{ symmetric idempotent } e = \text{diag}(1, 0)$$

$$\mathcal{C}_2(\text{I}) = \langle m_a = \begin{pmatrix} 1000 \\ 0010 \\ 0100 \\ 0001 \end{pmatrix}, m_b = \begin{pmatrix} 1000 \\ 0001 \\ 0100 \\ 0010 \end{pmatrix},$$

$$h_{e,e,e} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, d_{\phi e} = \text{diag}(1, -1, 1, -1) \rangle$$

$$\mathcal{C}_2(\text{II}) = \langle m_a, m_b, h_{e,e,e}, d_{\phi e} = \text{diag}(1, i, 1, i) \rangle.$$

$$\mathcal{C}_2(\text{II}) = \langle m_a, m_b, h_{e,e,e}, d_{\phi e} = \text{diag}(1, i, 1, i) \rangle.$$

$\mathcal{C}_2(\text{II})$ has order 92160 and Molien series

$$\frac{1 + t^{32}}{(1 - t^8)(1 - t^{24})^2(1 - t^{40})}$$

where the generators correspond to the degree 2 complete weight enumerators of the codes:

$$e_8, g_{24}, d_{24}^+, d_{40}^+, \text{ and } d_{32}^+$$

$\mathcal{C}_2(\text{II})$ has a reflection subgroup of index 2, No. 31 on the Shephard-Todd list.

Higher genus Clifford-Weil groups for Type I, II, III, IV.

$$\mathcal{C}_m(\text{I}) = 2_+^{1+2m} \cdot O_{2m}^+(\mathbb{F}_2)$$

$$\mathcal{C}_m(\text{II}) = Z_8 Y 2^{1+2m} \cdot \text{Sp}_{2m}(\mathbb{F}_2)$$

$$\mathcal{C}_m(\text{III}) = Z_4 \cdot \text{Sp}_{2m}(\mathbb{F}_3)$$

$$\mathcal{C}_m(\text{IV}) = Z_2 \cdot U_{2m}(\mathbb{F}_4)$$

Higher genus Clifford-Weil groups for the classical Types of codes over finite fields.

$$\mathcal{C}_m(T) = S.(\ker(\lambda) \times \ker(\lambda)).\mathcal{G}_m(T)$$

$$\lambda(\phi) : (x, y) \mapsto \phi(x + y) - \phi(x) - \phi(y)$$

R	J	ϵ	$\mathcal{G}_m(T)$
$\mathbb{F}_q \oplus \mathbb{F}_q$	$(r, s)^J = (s, r)$	1	$\mathrm{GL}_{2m}(\mathbb{F}_q)$
\mathbb{F}_{q^2}	$r^J = r^q$	1	$U_{2m}(\mathbb{F}_{q^2})$
\mathbb{F}_q, q odd	$r^J = r$	1	$\mathrm{Sp}_{2m}(\mathbb{F}_q)$
\mathbb{F}_q, q odd	$r^J = r$	-1	$O_{2m}^+(\mathbb{F}_q)$
\mathbb{F}_q, q even	doubly even		$\mathrm{Sp}_{2m}(\mathbb{F}_q)$
\mathbb{F}_q, q even	singly even		$O_{2m}^+(\mathbb{F}_q)$