Codes and invariant theory.

Gabriele Nebe

Lehrstuhl für Algebra und Zahlentheorie

Clifford Weil Groups and Symmetrizations

Complete weight enumerators,

Let V be a finite abelian group (e.g. $V = \mathbb{F}_q$) and $C \subseteq V^N$. For $c = (c_1, \ldots, c_N) \in V^N$ and $v \in V$ put

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

Then

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

is called the complete weight enumerator of C.

The tetracode.

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

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

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

Clear. $\mathrm{hwe}_C(x, y) = \mathrm{cwe}_C(x, y, \ldots, y)$

A formal notion of a Type of a code.

Definition of Type, part I

A Type is a quadrupel (R, V, Φ, β) with

- R is a finite ring (with 1) and $^J : R \to R$ an involution of R.
  $(ab)^J = b^J a^J$ and $(a^J)^J = a$ for all $a, b \in R$
- V a finite left R-module.
- $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ regular, ϵ-hermitian:
  $\beta(rv, w) = \beta(v, r^J w)$ for $r \in R, v, w \in V$,
  $v \mapsto \beta(v, \cdot) \in \mathrm{Hom}(V, \mathbb{Q}/\mathbb{Z})$ isomorphism,
  $\epsilon \in Z(R)$, $\epsilon\epsilon^J = 1$ $\beta(v, w) = \beta(w, \epsilon v)$ for $v, w \in V$.
- $\Phi \subset \mathrm{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ a set of quadratic mappings on V.

and certain additional properties.

Codes of a given Type.

Let (R, V, Φ, β) be a Type.

Definition.

- A code C over the alphabet V is an R-submodule of V^N.
- The dual code (with respect to β) is

$$C^{\perp} := \{x \in V^N \mid \beta^N(x, c) = \sum_{i=1}^{N} \beta(x_i, c_i) = 0 \text{ for all } c \in C\} .$$

  C is called self-dual (with respect to β) if $C = C^{\perp}$.
- Then C is called isotropic (with respect to Φ) if

$$\phi^N(c) := \sum_{i=1}^{N} \phi(c_i) = 0 \text{ for all } c \in C \text{ and } \phi \in \Phi.$$

A formal notion of a Type of a code.

Definition

The quadruple (R, V, Φ, β) as above is called a Type if

- $\Phi \leq \mathrm{Quad}_0(V, \mathbb{Q}/\mathbb{Z})$ is a subgroup and for all $r \in R$, $\phi \in \Phi$ the mapping $\phi[r] : x \mapsto \phi(rx)$ is again in Φ.
  Then Φ is an R-qmodule.
- For all $\phi \in \Phi$ there is some $r_\phi \in R$ such that

  $$\lambda(\phi)(v, w) = \phi(v + w) - \phi(v) - \phi(w) = \beta(v, r_\phi w) \text{ for all } v, w \in V.$$

- For all $r \in R$ the mapping

  $$\phi_r : V \to \mathbb{Q}/\mathbb{Z}, v \mapsto \beta(v, rv) \text{ lies in } \Phi.$$

Type I,II,III,IV in the new language.

Type I codes (2_{I})

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

Type II code (2_{II}).

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

Type III codes (3).

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

Type IV codes (4^H).

$$R = \mathbb{F}_4 = V,\ \beta(x,y) = \frac{1}{2}\operatorname{tr}(x\overline{y}),\ \Phi = \{\varphi : x \mapsto \frac{1}{2}x\overline{x}, 0\}$$

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

The Clifford-Weil group associated to a Type.

Definition.

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

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

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

$$m_r : e_v \mapsto e_{rv}, \quad d_\phi : e_v \mapsto \exp(2\pi i \phi(v)) e_v$$

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

Invariance of complete weight enumerators.

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

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

The Clifford-Weil groups for Type I and II.

Type I codes (2_{I})

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

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

Type II codes (2_{II}).

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

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

The Clifford-Weil groups for Type III and IV.

Type III codes (3).

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

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

Type IV codes (4^H).

$$R = \mathbb{F}_4 = V,\ \beta(x,y) = \frac{1}{2}\mathrm{tr}(x\overline{y}),\ \Phi = \{\varphi : x \mapsto \frac{1}{2}x\overline{x}, 0\}$$

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

Symmetrizations.

Definition

Let (R, J) be a ring with involution. Then the central unitary group is

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

Theorem.

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

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

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

Example.

$R = \mathbb{F}_2$ or $R = \mathbb{F}_3$ then $\mathrm{ZU}(R, \mathrm{id}) = R - \{0\}$.
If $R = \mathbb{F}_4$ then $\mathrm{ZU}(R, \mathrm{id}) = \{1\}$, but $\mathrm{ZU}(R, ^-) = R - \{0\}$.

Symmetrized Clifford-Weil groups.

Definition.

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

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

If

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

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 $\mathcal{C}(T)$.

Symmetrized weight enumerators.

Definition.

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

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

.

Remark.

If the invariant ring of $\mathcal{C}(T)$ is spanned by the complete weight enumerators of self-dual codes of Type T, then the invariant ring of $\mathcal{C}^{(U)}(T)$ is spanned by the U-symmetrized weight-enumerators of self-dual codes of Type T.

Gleason's Theorem revisited.

Remark

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

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

and the symmetrized weight enumerators are the Hamming weight enumerators.

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

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

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

The symmetrized Clifford-Weil group of Type IV.

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

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

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

Hermitian codes over $\mathbb{F}_9$

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

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 $d_\varphi := \operatorname{diag}(1, \zeta, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2, \zeta, \zeta^2)$,

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

Hermitian codes over $\mathbb{F}_9$

$\mathcal{C}(9^H)$ 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

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

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 ?

Hermitian codes over $\mathbb{F}_9$

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

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

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

$$\mathcal{C}^{(U)}(9^H) = \langle d_\varphi^{(U)} := \mathrm{diag}(1, \zeta, \zeta^2),\ m_\alpha^{(U)} := \begin{pmatrix} 100 \\ 001 \\ 010 \end{pmatrix},\ h^{(U)} := \frac{1}{3}\begin{pmatrix} 1 & 4 & 4 \\ 1 & 1 & \text{-}2 \\ 1 & \text{-}2 & 1 \end{pmatrix} \rangle$$

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

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

$$\begin{array}{l} q_6 = x_0^6 + 8(x_0^3x_1^3 + x_0^3x_2^3 + 2x_1^6 + 2x_2^6) \\ +72(x_0^2x_1^2x_2^2 + 2x_0x_1^4x_2 + 2x_0x_1x_2^4) + 320x_1^3x_2^3 \end{array}$$

of the three codes with generator matrices

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

Hermitian codes over $\mathbb{F}_9$

Their Hamming weight enumerators are

$$\begin{aligned} r_2 = q_2(x,y,y) \quad &:= x^2 + 8y^2 \,, \\ r_4 = q_4(x,y,y) \quad &:= x^4 + 32xy^3 + 48y^4 \,, \\ r_6 = q_6(x,y,y) \quad &:= x^6 + 16x^3y^3 + 72x^2y^4 + 288xy^5 + 352y^6 \,. \end{aligned}$$

The polynomials r_2, r_4 and r_6 generate the ring $\mathrm{Ham}(9^H)$ spanned by the Hamming weight enumerators of the codes of Type 9^H.
$\mathrm{Ham}(9^H) = \mathbb{C}[r_2, r_4] \oplus r_6\mathbb{C}[r_2, r_4]$ with the syzygy

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

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