Clifford-Weil groups of quotient representations.

Annika Günther and *Gabriele Nebe*

Lehrstuhl D für Mathematik, RWTH Aachen
52056 Aachen, Germany
annika.guenther@math.rwth-aachen.de, nebe@math.rwth-aachen.de

and

Eric M. Rains

Department of Mathematics, California Institute of Technology,
Pasadena, CA 91125, U.S.A.,
rains@caltech.edu

Abstract This note gives an explicit proof that the scalar subgroup of the Clifford Weil group remains unchanged when passing to the quotient representation filling a gap in [3].

1 Introduction

All notations in this paper are introduced in detail in [3] and we refer to this book for their definitions. One main goal of the book is to introduce a unified language to describe the Type of self-dual codes combining the different notions of self-duality and Types, that are well established in coding theory. The Type of a code is a finite representation $\rho = (V, \rho_M, \rho_\Phi, \beta)$ of a finite form ring $\mathcal{R} = (R, M, \psi, \Phi)$. The finite alphabet V is a left module for the ring R and the biadditive form $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ defines the notion of duality. A code C of length N is then an R-submodule of V^N and the dual code is

$$C^\perp = \{v \in V^N \mid \sum_{i=1}^{N} \beta(v_i, c_i) = 0 \ \forall c \in C\}.$$

Additional properties of codes of a given Type are encoded in the R-qmodule $\rho_\Phi(\Phi)$ which is a certain subgroup of the group of quadratic mappings $V \to \mathbb{Q}/\mathbb{Z}$. A code $C \leq V^N$ is *isotropic*, if $C \leq C^\perp$ and

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

Given a finite representation ρ, one associates a finite subgroup $\mathcal{C}(\rho)$ of $\mathrm{GL}(\mathbb{C}[V])$, called the associated Clifford-Weil group (see Section 2). For certain finite form rings (including direct products of matrix rings over finite Galois rings) it is shown in [3, Theorem 5.5.7] that the ring of polynomial invariants of $\mathcal{C}(\rho)$ is spanned by the complete weight-enumerators of self-dual isotropic codes of Type ρ. We conjecture that this theorem holds for arbitrary finite form rings. It is shown in [3, Theorem 5.4.13, 5.5.3] that in general the order of the scalar subgroup

$$\mathcal{S}(\mathcal{C}(\rho)) = \mathcal{C}(\rho) \cap \mathbb{C}^* \, \mathrm{id}_{\mathbb{C}[V]}$$

is exactly the least common multiple of the lengths of self-dual isotropic codes of Type ρ. The proof of this theorem uses the fact that the scalar subgroup of $\mathcal{C}(\rho)$ remains unchanged when passing to the quotient representation. The aim of the present note is to give a full proof of this statement, Theorem 1.

Throughout the note we fix an isotropic code $C \leq C^{\perp} \leq V$ in ρ. Then the quotient representation ρ/C is defined by

$$\rho/C := (C^{\perp}/C, \rho_M/C, \rho_{\Phi}/C, \beta/C),$$

where $(\rho_M/C(m))(v+C, w+C) = \rho_M(m)(v,w)$, $(\rho_{\Phi}/C(\phi))(v+C) = \rho_{\Phi}(\phi)(v)$, and $\beta/C(v+C, w+C) = \beta(v,w)$ for all $v, w \in C^{\perp}, m \in M, \phi \in \Phi$.

Theorem 1. *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a finite form-ring and let $\rho = (V, \rho_M, \rho_{\Phi}, \beta)$ be a finite representation of $\mathcal{R}$. Let C be an isotropic self-orthogonal code in ρ. Then*

$$\mathcal{S}(\mathcal{C}(\rho)) \cong \mathcal{S}(\mathcal{C}(\rho/C)).$$

2 Clifford-Weil groups and hyperbolic counitary groups

The Clifford-Weil group $\mathcal{C}(\rho)$ associated to the finite representation ρ acts linearly on the space $\mathbb{C}[V]$ with basis $[b_v : v \in V]$. It is generated by

$$\begin{array}{ll}
m_r : b_v \mapsto b_{rv} & \text{for } r \in R^* \\
d_{\phi} : b_v \mapsto \exp(2\pi i \rho_{\Phi}(\phi)(v)) b_v & \text{for } \phi \in \Phi \\
h_{e,u_e,v_e} : b_v \mapsto \frac{1}{|eV|^{1/2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)v} & e^2 = e \in R \text{ symmetric.}
\end{array}$$

Recall that the form-ring structure defines an involution ^{J} on R. Then an idempotent $e \in R$ is called *symmetric*, if eR and $e^J R$ are isomorphic as right R-modules, which means that there are $u_e \in eRe^J, v_e \in e^J Re$ such that $e = u_e v_e$ and $e^J = v_e u_e$.

The Clifford-Weil group $\mathcal{C}(\rho)$ is a projective representation of the hyperbolic counitary group

$$\mathcal{U}(R, \Phi) = U(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \mathrm{Mat}_2(R), \Phi_2).$$

The elements of $\mathcal{U}(R,\Phi)$ are of the form

$$X = \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \in \mathrm{Mat}_2(R) \times \Phi_2 \tag{1}$$

such that

$$\begin{pmatrix} \gamma^J \alpha & \gamma^J \beta \\ \delta^J \alpha - 1 & \delta^J \beta \end{pmatrix} = \psi_2^{-1} \begin{pmatrix} \lambda(\phi_1) & m \\ \tau(m) & \lambda(\phi_2) \end{pmatrix}.$$

A more detailed definition of $\mathcal{U}(R,\Phi)$ can be found in [3, Chapter 5.2].

It is shown in the book that $\mathcal{U}(R,\Phi)$ is generated by the elements

$$d((r,\phi)) = \left(\begin{pmatrix} r^{-J} & r^{-J}\psi^{-1}(\lambda(\phi)) \\ 0 & r \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi \end{pmatrix} \right)$$

with $r \in R^*, \phi \in \Phi$ and

$$H_{e,u_e,v_e} = \left(\begin{pmatrix} 1-e^J & v_e \\ -\epsilon^{-1} u_e^J & 1-e \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon e) \\ & 0 \end{pmatrix} \right),$$

where $e = u_e v_e$ runs through the symmetric idempotents of R.

Then the projective representation $p : \mathcal{U}(R,\Phi) \to \mathcal{C}(\rho)$ is defined on these generators by

$$p : \mathcal{U}(R,\Phi) \to \mathcal{C}(\rho); \quad d((r,\phi)) \mapsto m_r d_\phi, \quad H_{e,u_e,v_e} \mapsto h_{e,u_e,v_e} \tag{2}$$

and is clearly surjective since generators are mapped to generators.

It is shown in [3, Theorem 5.3.2] that this yields a projective representation. However the calculations there were omitted so we take the opportunity to give them here for completeness (also since there are a few typos in the proof there). As in Theorem 5.3.2 we define the associated Heisenberg group $\mathcal{E}(V) := V \times V \times \mathbb{Q}/\mathbb{Z}$ with multiplication

$$((z,x),q) \cdot ((z',x'),q') = ((z+z', x+x'), q+q'+\beta(x',z)).$$

Then $\mathcal{E}(V)$ acts linearly on $\mathbb{C}[V]$ by

$$((z,x),q) \cdot b_v = \exp(2\pi i(q + \beta(v,z)))b_{v+x}, \quad ((z,x),q) \in \mathcal{E}(V), \ v \in V.$$

This yields an absolutely irreducible faithful representation $\Delta : \mathcal{E}(V) \to GL_{|V|}(\mathbb{C})$. The hyperbolic counitary group $\mathcal{U}(R,\Phi)$ acts as group automorphisms on $\mathcal{E}(V)$ via

$$\begin{aligned} &\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) ((z,x),q) \\ &\quad = ((az+bx, cz+dx), q + \rho_\Phi(\phi_1)(z) + \rho_\Phi(\phi_2)(x) + \rho_M(m)(z,x)) \,. \end{aligned}$$

Also the associated Clifford Weil group $\mathcal{C}(\rho) \leq \mathrm{GL}(\mathbb{C}[V])$ acts on $\Delta(\mathcal{E}(V)) \cong \mathcal{E}(V)$ by conjugation.

Lemma 2. *For $r \in R^*, \phi \in \Phi$ and $(z, x, q) \in \mathcal{E}(V)$ we have*

$$\Delta(d(r, \phi)(z, x, q)) = (m_r d_\phi)\Delta((z, x, q))(m_r d_\phi)^{-1}.$$

Proof. The proof is an easy calculation.

$$d(r, \phi)(z, x, q) = (r^{-J} z + r^{-J}\psi^{-1}(\lambda(\phi))x, rx, q + \rho_\Phi(\phi)(x))$$

maps the basis element b_v $(v \in V)$ to

$$\exp(2\pi i(q + \rho_\Phi(\phi)(x) + \beta(v, r^{-J} z + r^{-J}\psi^{-1}(\lambda(\phi))x)))b_{v+rx}.$$

On the other hand

$$\begin{aligned}&(m_r d_\phi)\Delta((z, x, q))(m_r d_\phi)^{-1}(b_v) = m_r d_\phi \exp(2\pi i(q - \rho_\Phi(\phi)(r^{-1}v) + \beta(r^{-1}v, z))(b_{r^{-1}v+x}) = \\ &\exp(2\pi i(q - \rho_\Phi(\phi)(r^{-1}v) + \beta(r^{-1}v, z) + \rho_\Phi(\phi)(r^{-1}v + x)))(b_{v+rx}) = \\ &\exp(2\pi i(q + \beta(r^{-1}v, z) + \rho_M(\lambda(\phi))(r^{-1}v, x)))(b_{v+rx})\end{aligned}$$

which is the same as the above, since $\beta(r^{-1}v, z) = \beta(v, r^{-J} z)$ by definition of the involution J and

$$\rho_M(\lambda(\phi))(r^{-1}v, x) = \beta(r^{-1}v, \psi^{-1}(\lambda(\phi))x) = \beta(v, r^{-J}\psi^{-1}(\lambda(\phi))x).$$

□

Lemma 3. *For $e = u_e v_e$ a symmetric idempotent in R and $(z, x, q) \in \mathcal{E}(V)$*

$$\Delta(H_{e,u_e,v_e}(z, x, q)) = h_{e,u_e,v_e}\Delta((z, x, q))h^{-1}_{e,u_e,v_e}.$$

Proof. The group $\mathcal{E}(V)$ is generated by $(z, 0, 0), (0, x, 0), (0, 0, q)$ where $z \in e^J V \cup (1-e^J)V$, $x \in eV \cup (1 - e)V$, $q \in \mathbb{Q}/\mathbb{Z}$ and it is enough to check the lemma for these 5 types of generators. For $(0, 0, q)$ this is clear. Similarly, if $z \in (1 - e^J)V$ and $x \in (1 - e)V$, then both sides yield $\Delta((z, x, q))$ as one easily checks. For $z \in e^J V$, $x \in eV$, $q \in \mathbb{Q}/\mathbb{Z}$

$$H_{e,u_e,v_e}(z, x, q) = (v_e x, -\epsilon^{-1}u_e^J z, q + \beta(z, -\epsilon x)).$$

To calculate the right hand side, we note that according to the decomposition

$$V = eV \oplus (1 - e)V$$

the space $\mathbb{C}[V] = \mathbb{C}[eV] \otimes \mathbb{C}[(1 - e)V]$ is a tensor product and

$$h_{e,u_e,v_e} = (h_{e,u_e,v_e})_{\mathbb{C}[eV]} \otimes \mathrm{id}_{\mathbb{C}[(1-e)V]}\,.$$

Moreover the permutation matrix $\Delta((0, x, 0)) : b_v \mapsto b_{v+x}$ for $x \in eV$ is a tensor product $p_x \otimes \mathrm{id}$ and similarly the diagonal matrix $\Delta((z, 0, 0))$ for $z \in e^J V$ is a tensor product $d_z \otimes \mathrm{id}$.

It therefore is enough to calculate the action on elements of $\mathbb{C}[eV]$. For $z = e^J z \in e^J V$, $x = ex \in eV$ and $v = ev \in eV$ we get

$$\begin{aligned}
&h_{e,u_e,v_e} \circ \Delta((e^J z, 0, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = \\
&h_{e,u_e,v_e}(|eV|^{-1/2} \textstyle\sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J \epsilon v, w) + \beta(w, e^J z)))b_w) = \\
&|eV|^{-1} \textstyle\sum_{w' \in eV} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J \epsilon v, w) + \beta(w, e^J z) + \beta(w', v_e w)))b_{w'}.
\end{aligned}$$

Now $\beta(-\epsilon^{-1} v_e^J \epsilon v, w) + \beta(w, e^J z) + \beta(w', v_e w) = \beta(-\epsilon^{-1} v_e^J \epsilon v + \epsilon^{-1} z + \epsilon^{-1} v_e^J \epsilon w', w)$. Hence the sum over all w is non-zero, only if $-v_e^J \epsilon v + z + v_e^J \epsilon w' = 0$ which implies that $w' = v - \epsilon^{-1} u_e^J z$. Hence $h_{e,u_e,v_e} \circ \Delta((e^J z, 0, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = b_{v - \epsilon^{-1} u_e^J z}$. A similar calculation yields

$$\begin{aligned}
&h_{e,u_e,v_e} \circ \Delta((0, ex, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = \\
&h_{e,u_e,v_e}(|eV|^{-1/2} \textstyle\sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J \epsilon v, w)))b_{w+ex}) = \\
&h_{e,u_e,v_e}(|eV|^{-1/2} \textstyle\sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1} v_e^J \epsilon v, w - ex)))b_w) = \\
&h_{e,u_e,v_e} \circ h^{-1}_{e,u_e,v_e}(\exp(2\pi i(\beta(\epsilon^{-1} v_e^J \epsilon v, ex)))b_v) = \exp(2\pi i(\beta(v, v_e x)))b_v.
\end{aligned}$$

□

For the calculations in Section 5 we need the following lemma.

Lemma 4. *Let $X \in \mathcal{U}(R, \Phi)$ be as in (1). If $\delta^2 = \delta$ then $\iota := 1 - \delta$ is a symmetric idempotent of R.*

Proof. We define $u_\iota = -\iota \gamma^J \iota^J$, $v_\iota = \iota^J \beta \iota$ and calculate

$$\begin{aligned}
u_\iota v_\iota &= -(1-\delta)\epsilon^{-1}\gamma^J(1-\delta^J)\beta(1-\delta) \\
&= -(1-\delta)\epsilon^{-1} \underbrace{\gamma^J \beta}_{=\alpha^J \epsilon \delta - \epsilon} (1-\delta) + (1-\delta)\epsilon^{-1}\gamma^J \underbrace{\delta^J \beta}_{=\beta^J \epsilon \delta} (1-\delta) \\
&= (1-\delta)\epsilon^{-1}\epsilon(1-\delta) = 1 - \delta = \iota
\end{aligned}$$

and

$$\begin{aligned}
v_\iota u_\iota &= -(1-\delta^J)\beta(1-\delta)\epsilon^{-1}\gamma^J(1-\delta^J) \\
&= -(1-\delta^J) \underbrace{\beta \epsilon^{-1} \gamma^J}_{=\alpha \delta^J - 1} (1-\delta^J) + (1-\delta^J)\beta \underbrace{\delta \epsilon^{-1} \gamma^J}_{=\gamma \delta^J} (1-\delta^J) \\
&= -(1-\delta^J)(-1)(1-\delta^J) = 1 - \delta^J = \iota^J.
\end{aligned}$$

□

3 $\mathcal{S}(\mathcal{C}(\rho)) \leq \mathcal{S}(\mathcal{C}(\rho/C))$

The Clifford-Weil-group $\mathcal{C}(\rho/C)$ can be derived from $\mathcal{C}(\rho)$ by restricting the operation of $\mathcal{C}(\rho)$ to a submodule of $\mathbb{C}[V]$.

Lemma 5. *The group $\mathcal{C}(\rho)$ acts on a submodule of $\mathbb{C}[V]$ isomorphic to $\mathbb{C}[C^{\perp}/C]$. This yields a representation*

$$\mathrm{res} : \mathcal{C}(\rho) \to \mathrm{GL}(\mathbb{C}[C^{\perp}/C])$$

with the properties

(i) $\mathrm{res}(\mathcal{C}(\rho)) \leq \mathcal{C}(\rho/C)$,

(ii) if $p : \mathcal{U}(R, \Phi) \to \mathcal{C}(\rho)$ and $p/C : \mathcal{U}(R, \Phi) \to \mathcal{C}(\rho/C)$ denote the projective representations of $\mathcal{U}(R, \Phi)$ associated with ρ respectively ρ/C as defined (2)*, then*

$$\mathrm{res}(p(H_{e,u_e,v_e})) = p/C(H_{e,u_e,v_e})$$

and

$$\mathrm{res}(p(d((r, \phi)))) = p/C(d((r, \phi)))$$

for all $H_{e,u_e,v_e}, d((r, \phi)) \in \mathcal{U}(R, \Phi)$.

Proof. Let Rep denote a set of coset representatives of $C^{\perp}/C$. We define a subspace

$$U := \{ \sum_{v \in \mathrm{Rep}} \sum_{c \in C} a_v b_{v+c} \mid a_v \in \mathbb{C} \} \leq \mathbb{C}[V].$$

This subspace is isomorphic to $\mathbb{C}[C^{\perp}/C]$ via

$$f : \mathbb{C}[C^{\perp}/C] \to U, \ \sum_{v \in \mathrm{Rep}} a_v b_{v+C} \mapsto \sum_{v \in \mathrm{Rep}} \sum_{c \in C} a_v b_{v+c}.$$

So we have

$$\mathrm{res}(x) = f \circ x \circ f^{-1} \in GL(U)$$

for $x \in \mathcal{C}(\rho)$. Particularly, if $x = s \cdot \mathrm{id}_{\mathbb{C}[V]}$ then $\mathrm{res}(x) = s \cdot \mathrm{id}_{\mathbb{C}[C^{\perp}/C]}$. Consequently we will show that

$$f \circ p(H_{e,u_e,v_e}) \circ f^{-1} = p/C(H_{e,u_e,v_e})$$

and

$$f \circ p(d((r, \phi))) \circ f^{-1} = p/C(d((r, \phi))).$$

So we have $\mathrm{Im}(\mathrm{res}) \leq \mathcal{C}(\rho/C)$ and thus $\mathcal{S}(\mathcal{C}(\rho))$ is isomorphic to a subgroup of $\mathcal{S}(\mathcal{C}(\rho/C))$.

Now let $v+C \in C^\perp/C$ and let T denote a set of coset representatives of $eC^\perp/eC \cong eC^\perp/C$. Then

$$
\begin{aligned}
&f^{-1}\circ p(H_{e,u_e,v_e})\circ f(b_{v+C}) = f^{-1}\circ p(H_{e,u_e,v_e})(\textstyle\sum_{c\in C} b_{v+c}) = \\
&f^{-1}(\textstyle\sum_{c\in C} |eV|^{-\frac{1}{2}} \sum_{w\in eV} \exp(2\pi i\beta(w, v_e(v+c)))b_{w+(1-e)(v+c)}) = \\
&f^{-1}(|eV|^{-\frac{1}{2}}\ \textstyle\sum_{w\in eV} \exp(2\pi i\beta(w, v_e v)) \sum_{c'\in(1-e)C} \underbrace{\displaystyle\sum_{c\in eC} \exp(2\pi i\beta(w, v_e c))}_{=\begin{cases} |eC|, & w\in eC^\perp, \\ 0 & \text{else.}\end{cases}} b_{w+(1-e)(v+c')}) = \\
&f^{-1}(\tfrac{|eC|}{|eV|^{\frac{1}{2}}}\ \textstyle\sum_{w\in eC^\perp} \sum_{c'\in(1-e)C} \exp(2\pi i\beta(w, v_e v))b_{w+(1-e)(v+c')}) = \\
&f^{-1}(\tfrac{|eC|}{|eV|^{\frac{1}{2}}} \textstyle\sum_{w\in T} \sum_{c'\in(1-e)C} \sum_{c\in eC} \exp(2\pi i\beta(w, v_e v))b_{w+c+(1-e)(v+c')}) = \\
&f^{-1}(\tfrac{|eC|}{|eV|^{\frac{1}{2}}} \textstyle\sum_{w\in T} \exp(2\pi i\beta(w, v_e v)) \sum_{c\in C} b_{w+(1-e)v} + c) = \\
&|eC^\perp/C|^{-\frac{1}{2}} \textstyle\sum_{w\in eC^\perp/C} \exp(2\pi i\beta/C(w, v_e(v+C)))b_{w+(1-e)(v+C)} = p/C(H_{e,u_e,v_e})(b_{v+C}).
\end{aligned}
$$

Noting that $\rho_\Phi(\phi)(c) = 0$ for all $c\in C$ and for all $d((r,\phi))\in\mathcal{U}(R,\Phi)$, we get

$$
\begin{aligned}
&f^{-1}\circ p(d((r,\phi)))\circ f(b_{v+C}) = f^{-1}\circ p(d((r,\phi)))(\textstyle\sum_{c\in C} b_{v+c}) = \\
&f^{-1}(p(d((r,0)))\textstyle\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v+c))b_{v+c}) = f^{-1}(\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v))b_{rv+rc}) = \\
&f^{-1}(\textstyle\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v))b_{rv+c}) = \exp(2\pi i\rho_\Phi/C(\phi)(v+C))b_{r(v+C)}) = p/C(d((r,\phi)))(b_{v+C}).
\end{aligned}
$$

□

Since scalars acts as the same scalars on submodules, this shows the inclusion in the headline.

Corollary 6. $\ker(\mathrm{res})\cap\mathcal{S}(\mathcal{C}(\rho)) = \{1\}$ *and* $\mathcal{S}(\mathcal{C}(\rho))$ *is isomorphic to a subgroup of* $\mathcal{S}(\mathcal{C}(\rho/C))$.

4 The strategy.

Without loss of generality we now assume that ρ is faithful, that is,

$$\ker(\rho) = (\mathrm{Ann}_R(V), \ker(\rho_\Phi)) = (0,0)$$

and let $(I,\Gamma) = \ker(\rho/C)$. We then define $\overline{\mathrm{res}}:\mathcal{U}(R,\Phi)\to\mathcal{U}(R/I,\Phi/\Gamma)$ by

$$\overline{\mathrm{res}}(\left(\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}, \begin{pmatrix}\phi_1 & m\\ & \phi_2\end{pmatrix}\right)) = \left(\begin{pmatrix}\alpha+I & \beta+I\\ \gamma+I & \delta+I\end{pmatrix}, \begin{pmatrix}\phi_1+\Gamma & m+\psi(I)\\ & \phi_2+\Gamma\end{pmatrix}\right).$$

and the epimorphism

$$\nu:\mathcal{C}(\rho)\to\mathcal{U}(R,\Phi) \text{ by } \nu(m_r d_\phi) = d((r,\phi)),\ \ \nu(h_{e,u_e,v_e}) = H_{e,u_e,v_e}$$

for $r \in R^*, \phi \in \Phi$ and symmetric idempotents $e = u_e v_e \in R$. Similarly $\overline{\nu} : \mathcal{C}(\rho/C) \to \mathcal{U}(R/I, \Phi/\Gamma)$. Then $\nu \circ p = \mathrm{id}_{\mathcal{U}(R,\Phi)}$. The projective representation p comes from the action of $\mathcal{U}(R, \Phi)$ on the absolutely irreducible subgroup $\mathcal{E}(V) \leq \mathrm{GL}(\mathbb{C}[V])$ (see the proof of [3, Theorem 5.3.2]). This action coincides with the conjugation action of $\mathcal{C}(\rho)$ on $\mathcal{E}(V)$. Therefore the kernel of ν respectively $\overline{\nu}$ are precisely the scalars in the respective Clifford-Weil groups $\ker(\nu) = \mathcal{S}(\mathcal{C}(\rho))$ and $\ker(\overline{\nu}) = \mathcal{S}(\mathcal{C}(\rho/C))$.

We then have the following commutative diagram with exact rows and columns

$$\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & \\
 & & & & \downarrow & & \downarrow & & & & \\
 & & 1 & \to & \ker(\mathrm{res}) & \stackrel{\nu|_{\ker(\mathrm{res})}}{\to} & \ker(\overline{\mathrm{res}}) & \to & \mathcal{Y}' & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
1 & \to & \mathcal{S}(\mathcal{C}(\rho)) & \to & \mathcal{C}(\rho) & \stackrel{\nu}{\to} & \mathcal{U}(R,\Phi) & \to & 1 & & \\
 & & \downarrow & & \downarrow \mathrm{res} & & \downarrow \overline{\mathrm{res}} & & & & \\
1 & \to & \mathcal{S}(\mathcal{C}(\rho/C)) & \to & \mathcal{C}(\rho/C) & \stackrel{\overline{\nu}}{\to} & \mathcal{U}(R/I,\Phi/\Gamma) & \to & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
 & & \mathcal{Y} & & 1 & & 1 & & & & \\
 & & \downarrow & & & & & & & & \\
 & & 1 & & & & & & & &
\end{array}$$

To see that all sequences are exact, we note that $\nu_{|\ker(\mathrm{res})}$ is injective, since $\ker(\mathrm{res}) \cap \mathcal{S}(\mathcal{C}(\rho)) = 1$. The homomorphisms $\overline{\mathrm{res}}$ and res are surjective, since idempotents and units of R/I lift to idempotents and units of R. Moreover $\overline{\mathrm{res}} \circ \nu = \overline{\nu} \circ \mathrm{res}$ as one checks on the generators.

The claim of Theorem 1 is that $\mathcal{Y}$ is trivial. But this is fulfilled if and only if $\mathcal{Y}'$ is trivial, that is, if $\nu|_{\ker(\mathrm{res})}$ is an isomorphism since

$$|\mathcal{Y}| = \frac{|\mathcal{S}(\mathcal{C}(\rho/C))|}{|\mathcal{S}(\mathcal{C}(\rho))|} = \frac{|\mathcal{C}(\rho/C)| \cdot |\mathcal{U}(R,\Phi)|}{|\mathcal{U}(R/I,\Phi/\Gamma)| \cdot |\mathcal{C}(\rho)|} = \frac{|\ker(\overline{\mathrm{res}})|}{|\ker(\mathrm{res})|} = |\mathcal{Y}'|.$$

5 The surjectivity of $\nu|_{\ker(\mathrm{res})}$

During the proof of Theorem 1 some results on lifting symmetric idempotents are needed, which are stated in the next two lemmata.

Lemma 7. *Let R be an Artinian ring and I an ideal of R. If $e \in I + \mathrm{rad}\, R \subseteq R$ such that $e^2 \equiv e \mod \mathrm{rad}\, R$ then there exists an idempotent $e' \in I$ such that $e' \equiv e \mod \mathrm{rad}\, R$.*

Proof. We choose $x_0 \in \mathrm{rad}\, R$ such that $e_0 := e + x_0 \in I$. Then $e_0 + \mathrm{rad}\, R$ is an idempotent in $R/\mathrm{rad}\, R$. Since $\mathrm{rad}\, R$ is a nilpotent ideal of R [2, Theorem 4.9] constructs an idempotent $e' = f(e_0) \in I$ for some polynomial $f \in \mathbb{Z}[X]$ with $f(0) = 0$ such that $e' + \operatorname{rad} R = e_0 + \operatorname{rad} R$. $\square$

By [2, Theorem 4.5] applied to an idempotent $e \in R$, the right-modules eR and $e^J R$ are isomorphic, if and only if their quotients modulo $\operatorname{rad} R$ are isomorphic. Hence we find

Lemma 8. *Let $e + \operatorname{rad} R \in R/\operatorname{rad} R$ be a symmetric idempotent such that*

$$e + \operatorname{rad} R = u_e v_e + \operatorname{rad} R, \;\; e^J + \operatorname{rad} R = v_e u_e + \operatorname{rad} R,$$

$u_e + \operatorname{rad} R \in (eRe^J) + \operatorname{rad} R$, $v_e \in (e^J Re) + \operatorname{rad} R$. If $e \in R$ is an idempotent then e is symmetric as well. More precisely, there exist $\tilde{u_e} \in eRe^J$, $\tilde{v_e} \in e^J Re$ such that

$$e = \tilde{u_e}\tilde{v_e}, \; e^J = \tilde{v_e}\tilde{u_e}$$

and $\tilde{v_e} \equiv v_e \mod \operatorname{rad} R$.

For the rest of this note, let

$$X := \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \in \ker(\overline{\text{res}}) \tag{3}$$

and let $(I, \Gamma) := \ker(\rho/C)$. In particular, $\alpha, \delta \in 1 + I$, $\beta, \gamma \in I$, $\phi_1, \phi_2 \in \Gamma$ and $m \in \psi(I)$. We have to find some $x \in \ker(\text{res})$ such that $\nu(x) = X$.

Lemma 9. *We have $d(P(R, \Phi)) \cap \ker(\overline{\text{res}}) \subseteq \operatorname{Im}(\nu|_{\ker(\text{res})})$.*

Proof. Let $r \in R^*, \phi \in \Phi$ such that $d((r, \phi)) = \nu(m_r d_\phi) \in \ker(\overline{\text{res}})$. Then $r \in 1 + I$ and $\phi \in \Gamma$. In particular r acts as the identity on $C^\perp/C$ and $\rho_\Phi/C(\phi) = 0$. This implies that both m_r and $d_\phi \in \ker(\text{res})$. $\square$

Lemma 10. *Let δ be a unit. Then there exists $x \in \ker(\text{res})$ such that $\nu(x) = X$.*

Proof. Since $\ker(\text{res})$ is a normal subgroup of $\mathcal{C}(\rho)$ it suffices to show that X is contained in the normal subgroup of $\mathcal{U}(R, \Phi)$ generated by the elements $d(P(R, \Phi)) \cap \ker(\overline{\text{res}})$. We show that there is $\phi \in \Gamma$ such that

$$X = d((\delta, \phi_2)) H_{1,1,1} d(1, \phi)) H_{1,1,1}^{-1}.$$

We have $d(\delta, \phi_2) = \left(\begin{pmatrix} \delta^{-J} & \beta \\ 0 & \delta \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi_2 \end{pmatrix} \right)$ and hence

$$d((\delta, \phi_2))^{-1} \;\; = \;\; \left(\begin{pmatrix} \delta^J & -\delta^J \beta \delta^{-1} \\ 0 & \delta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & -\phi_2[\delta^{-1}] \end{pmatrix} \right).$$

We therefore find

$$d((\delta,\phi_2))^{-1}X = \left(\left(\begin{array}{cc} \delta^J\alpha-\delta^J\beta\delta^{-1}\gamma & 0 \\ \delta^{-1}\gamma & 1 \end{array}\right), \left(\begin{array}{cc} -\phi_2[\delta^{-1}\gamma]+\phi_1 & \tilde{m} \\ & 0 \end{array}\right)\right)$$

for some $\tilde{m}\in M$. Since the upper right entry in the first matrix of this element of $\mathcal{U}(R,\Phi)$ is 0 we obtain $\tilde{m}=0$ and similarly $\delta^J\alpha-\delta^J\beta\delta^{-1}\gamma=1$ and we get

$$d((\delta,\phi_2))^{-1}X = \left(\left(\begin{array}{cc} 1 & 0 \\ \delta^{-1}\gamma & 1 \end{array}\right), \left(\begin{array}{cc} -\phi_2[\delta^{-1}\gamma]+\phi_1 & 0 \\ & 0 \end{array}\right)\right)$$

Furthermore,

$$H_{1,1,1} = \left(\left(\begin{array}{cc} 0 & 1 \\ -\epsilon^J & 0 \end{array}\right), \left(\begin{array}{cc} 0 & \psi(-\epsilon) \\ & 0 \end{array}\right)\right),\ H_{1,1,1}^{-1} = \left(\left(\begin{array}{cc} 0 & -\epsilon \\ 1 & 0 \end{array}\right), \left(\begin{array}{cc} 0 & \psi(-\epsilon) \\ & 0 \end{array}\right)\right).$$

Then we have

$$(d((\delta,\phi_2))^{-1}X)^{H_{1,1,1}} = \left(\left(\begin{array}{cc} 1 & -\epsilon\delta^{-1}\gamma \\ 0 & 1 \end{array}\right), \left(\begin{array}{cc} 0 & m' \\ & \phi \end{array}\right)\right),$$

with some $m'\in M$ and

$$\phi = \{\!\!\{\psi(-\epsilon\delta^{-1}\gamma)\}\!\!\} - \phi_2[\delta^{-1}\gamma]+\phi_1 \in \Gamma,$$

since $-\epsilon\delta^{-1}\gamma\in I$ and $\phi_1,\phi_2\in\Gamma$. Again $m'=0$ since the lower left entry in the first matrix is 0. Hence

$$H_{1,1,1}^{-1}d((\delta,\phi_2))^{-1}XH_{1,1,1} = d((1,\phi)) \in \ker(\overline{\mathrm{res}})$$

as claimed. $\square$

We now conclude the proof of Theorem 1 by showing

Lemma 11. *The map $\nu|_{\ker(\mathrm{res})}$ is surjective, that is,* $\mathrm{Im}(\nu|_{\ker(\mathrm{res})}) = \ker(\overline{\mathrm{res}})$.

Proof. We show that there exists a symmetric idempotent $\iota\in I$ such that

$$X = \underbrace{\left(\left(\begin{array}{cc} \alpha' & \beta' \\ \gamma' & \delta' \end{array}\right), \left(\begin{array}{cc} \phi_1' & \mu' \\ & \phi_2' \end{array}\right)\right)}_{=:X'} H_{\iota,u_\iota,v_\iota}$$

and $\delta'\in R^*$. Since $\iota\in I=\ker(\rho/C)$ the set $\iota(C^\perp/C)=\{0\}$ and hence $h_{\iota,u_\iota,v_\iota}\in\ker(\mathrm{res})$. By Lemma 10 $X'\in\mathrm{Im}(\nu|_{\ker(\mathrm{res})})$, so the same holds for X.

Now let us construct ι. The ring $R/\operatorname{rad}R$ is a direct sum of matrix rings over skew fields. Thus there exist $u_1,u_2\in R^*$ such that $u_1\delta u_2$ is an idempotent modulo $\operatorname{rad}R$. After conjugating with u_2 we obtain an idempotent $\tilde{u}\delta + \operatorname{rad} R \in R/\operatorname{rad} R$ with $\tilde{u} \in R^*$. Since $\tilde{u}\delta + (I + \operatorname{rad} R) \in R/(I + \operatorname{rad} R)$ is an idempotent as well and $\delta \in 1 + I$ is a unit modulo $I + \operatorname{rad} R$, it follows that $\tilde{u} \in 1 + (I + \operatorname{rad} R)$. We can even assume that $\tilde{u} \in 1 + I$. If $\tilde{u} = 1 + i + r$ with $i \in I$ and $r \in \operatorname{rad} R$ then $(1+i)\delta = (\tilde{u} - r)\delta$ is an idempotent mod $\operatorname{rad} R$. Additionally, from $\tilde{u} \in R^*$ we get $1 + i \in R^*$, so we can assume $\tilde{u} = 1 + i$. Now $d((\tilde{u}, 0)) \in \ker(\overline{\mathrm{res}})$, thus

$$\begin{aligned} X \in \ker(\overline{\mathrm{res}}) \quad &\Leftrightarrow \quad d((\tilde{u},0))X \in \ker(\overline{\mathrm{res}}) \\ &\Leftrightarrow \quad \left(\begin{pmatrix} \tilde{u}^{-J}\alpha & \tilde{u}^{-J}\beta \\ \tilde{u}\gamma & \tilde{u}\delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right) \in \ker(\overline{\mathrm{res}}) \end{aligned}$$

Thus we can assume that $\delta + \operatorname{rad} R \in R/\operatorname{rad} R$ is an idempotent.

In the hyperbolic counitary group $\mathcal{U}(R/\operatorname{rad} R, \Phi/\tilde{\Gamma})$ there is

$$\tilde{X} := \left(\begin{pmatrix} \alpha + \operatorname{rad} R & \beta + \operatorname{rad} R \\ \gamma + \operatorname{rad} R & \delta + \operatorname{rad} R \end{pmatrix}, \begin{pmatrix} \phi_1 + \tilde{\Gamma} & \mu + \psi(\operatorname{rad} R) \\ & \phi_2 + \tilde{\Gamma} \end{pmatrix} \right)$$

Lemma 4 says that $e := (1 - \delta) + \operatorname{rad} R$ is a symmetric idempotent of $R/\operatorname{rad} R$; more precisely, we may write $e = u_e v_e$ with

$$\begin{aligned} u_e &= -e\epsilon^{-1}\gamma^J e^J + \operatorname{rad} R, \\ v_e &= e^J \beta e^J + \operatorname{rad} R. \end{aligned}$$

By Lemma 7 we obtain a symmetric idempotent

$$\iota := e + x = 1 - \delta + x \in I$$

with $x \in \operatorname{rad} R \cap I$. We calculate the projection on the first component

$$\pi(XH^{-1}_{\iota,u_\iota,v_\iota}) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \delta^J - x^J & -v_\iota^J \epsilon \\ u_\iota^J & \delta - x \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

with $\delta' = -\gamma v_\iota^J \epsilon + \delta - \delta x$. It remains to show that $\delta' \in R^*$. Lemma 8 gives $v_\iota \equiv (1 - \delta^J)\beta(1 - \delta) \mod \operatorname{rad} R$. Also $\delta x \in \operatorname{rad}(R)$, so it remains to show that

$$\widetilde{\delta'} := -\gamma(1 - \delta^J)\beta^J \epsilon(1 - \delta) + \delta \in R^*.$$

We observe that $\widetilde{\delta'}\delta = -\gamma(1-\delta^J)\beta^J\epsilon \underbrace{(1-\delta)\delta}_{=0} + \delta^2 = \delta$ and

$$\begin{aligned} (1-\delta)\widetilde{\delta'} \quad &= \quad -(1-\delta)\gamma(1-\delta^J)\beta^J\epsilon(1-\delta) = \\ -(1-\delta)\gamma\beta^J\epsilon(1-\delta) + \underbrace{(1-\delta)\gamma\delta^J\beta^J\epsilon(1-\delta)}_{=0,\text{ since } \gamma\delta^J = \delta\epsilon^J\gamma^J} \quad &= \quad -(1-\delta)\gamma\beta^J\epsilon + (1-\delta)\gamma \underbrace{\beta^J\epsilon\delta}_{=\delta^J\beta} = \\ -(1-\delta) \underbrace{\gamma\beta^J\epsilon}_{=\delta\epsilon^J\alpha^J\epsilon - 1} + \underbrace{(1-\delta)\gamma\delta^J\beta}_{=0} \quad &= \quad 1 - \delta. \end{aligned}$$

Particularly, $(1-\delta)(2-\widetilde{\delta}')=1-\delta$. Now we see that $\widetilde{\delta}'$ is a unit since

$$\widetilde{\delta}'(2-\widetilde{\delta}')=\widetilde{\delta}'(\delta+(1-\delta))(2-\widetilde{\delta}')=\widetilde{\delta}'-\delta\widetilde{\delta}'+\delta=1-\delta+\delta=1.$$

$\square$

References

[1] A. Günther, *Self-dual group ring codes.* PhD Thesis, Aachen, in preparation

[2] H. Nagao, Y. Tsushima, *Representations of finite groups.* Academic Press (1988)

[3] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-dual codes and invariant theory.* Springer (2006)