THE INVOLUTION MODULE OF $\text{PSU}_3(2^{2^f})$

LARS PFORTE

(Received May 10, 2013, revised January 29, 2014)

Abstract

For any group $G$ the involutions $I$ in $G$ form a $G$-set under conjugation. The corresponding $kG$-permutation module $kI$ is known as the involution module of $G$, with $k$ an algebraically closed field of characteristic two. In this paper we discuss the involution module of the projective special unitary group $\text{PSU}_3(4^f)$.

1. Introduction

Let $I$ be the set of all involutions in a group $G$, that is, the group elements of order two. Then $G$ acts on $I$ by conjugation. The corresponding $kG$-permutation module $kI$ is known as the involution module of $G$. Here $k$ denotes an algebraically closed field of characteristic two. The involution module has been studied in general by G.R. Robinson [8] and J. Murray [4], [5]. Furthermore the author studied the involution module of the special linear group $\text{SL}_2(2^f)$ in [6] and the general linear group $\text{GL}_n(2^f)$ in [7].

In this paper we investigate the involution module of the projective special unitary group $\text{PSU}_3(2^{2^f})$. In the following we introduce this group. For details see [3] and [2]. Let $q := 2^f$, for some $f \geq 2$. Then $\mathbb{F}_{q^2}$ is the finite field with $q^2$ elements. For any element $x \in \mathbb{F}_{q^2}$ we define $N(x) := x^{q+1}$ and $\text{tr}(x) := x + x^q$, called norm and trace of $x$, respectively. As is standard $\text{GL}_3(q^2)$ denotes the general linear group, that is, the group of invertible $3 \times 3$-matrices with entries in $\mathbb{F}_{q^2}$. The elements in $\text{GL}_3(q^2)$ with determinant one form the special linear group $\text{SL}_3(q^2)$. Let $A \in \text{GL}_3(q)$. Then $A$ denotes the matrix obtained from $A$ by raising each entry of $A$ to the power $q$. Moreover $A^T$ is the transpose of $A$. Finally $A$ is called hermitian matrix if $A^T = A$.

Let $A \in \text{GL}_3(q^2)$ be hermitian. The set of all $X \in \text{GL}_3(q^2)$ so that $X^T A X = A$ form the unitary group $U_3(q^2)$. Its kernel under the determinant map is the special unitary group $\text{SU}_3(q^2)$. We have $|\text{SU}_3(q^2)| = q^3(q^2 - 1)(q^3 + 1)$. If $Z(\text{SU}_3(q^2))$ denotes the center of $\text{SU}_3(q^2)$, then we obtain the projective unitary group $\text{PSU}_3(q^2) \cong \text{SU}_3(q^2)/Z(\text{SU}_3(q^2))$. This group is simple, and thus makes an interesting object of study. Even though our main interest lies in $\text{PSU}_3(q^2)$ we work with $\text{SU}_3(q^2)$ in this paper, as all results can be transferred back via the canonical epimorphism $\text{SU}_3(q^2) \twoheadrightarrow \text{PSU}_3(q^2)$.

---

2010 Mathematics Subject Classification. 20G40.
Up to isomorphism this construction of $SU_3(q^2)$ is independent of the choice of the Hermitian form $A$. In the following we set

$$A := \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 \\ 1 \end{pmatrix},$$

and for the remainder of the paper let $G = \{ X \in SL_3(q^2) : X^T A X = A \}$.

In Section 2 we take a first look at the involution module of $G$ and show that there is one conjugacy class of involutions. We briefly present the irreducible $kN$ and $kG$-modules in Sections 3 and 4, respectively, where $N$ is the normalizer of the centralizer of an involution of $G$. In Section 5 we determine the components of $kI$ and finally in Section 6 we study the composition factors of $kI$. In Theorem 6.6 provides a formula to calculate the multiplicity of each irreducible $kG$-module in $kI$. In the remainder of Section 6 we look at a combinatorial method to determine the numbers involved in Theorem 6.6.

2. Local subgroups and involutions in $SU_3(q^2)$

Let $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ such that $\alpha \neq 0$. Then

$$M(\alpha, \beta, \gamma) := \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha^q & \alpha^{q^{-1}} & \alpha^{-1} \beta^q \\ \alpha^{-q} & \beta^{-q} & \alpha^{-\gamma} \end{pmatrix}$$

lies in $SL_3(q^2)$. Furthermore let $L := \{ M(\alpha, \beta, \gamma) : \alpha \in \mathbb{F}_{q^2}^*, \beta, \gamma \in \mathbb{F}_{q^2} \}$. Since

(1) \hspace{1cm} M(\alpha, \beta, \gamma) \cdot M(\alpha', \beta', \gamma') = M(\alpha \alpha', \alpha \beta' + \beta \alpha'^{-1}, \alpha \gamma' + \alpha^{-1} \beta \beta'^{-1} + \gamma \alpha^{-q})

it follows that $L$ is a subgroup of $SL_3(q^2)$. Also it is a straightforward exercise to show that $M(\alpha, \beta, \gamma) \in G$ if and only if $\text{tr}(\alpha \gamma^q) = N(\beta)$. In particular

$$N := G \cap L = \{ M(\alpha, \beta, \gamma) : \alpha \in \mathbb{F}_{q^2}^*, \beta, \gamma \in \mathbb{F}_{q^2}, \text{ tr}(\alpha \gamma^q) = N(\beta) \}.$$ 

Let us fix elements $\alpha \neq 0$ and $\beta$ in $\mathbb{F}_{q^2}$. Then there are exactly $q$ different $x \in \mathbb{F}_{q^2}$ such that $\text{tr}(x) = N(\beta)$. As for each such $x$ there is a unique $\gamma \in \mathbb{F}_{q^2}$ such that $\alpha \gamma^q = x$, we get that $|N| = q^3(q^2 - 1)$.

Next we present two homomorphisms on $N$. First consider the map

(2) \hspace{1cm} \varphi_1 : N \rightarrow N : M(\alpha, \beta, \gamma) \mapsto M(\alpha, 0, 0).

Then $\varphi_1$ is a homomorphism by (1). Moreover the kernel of $\varphi_1$ is given by

$$S := \{ M(1, \beta, \gamma) : \beta, \gamma \in \mathbb{F}_{q^2}, \text{ tr}(\gamma) = N(\beta) \}.$$
Therefore $N/C \cong C_{q-1}$ and $|C| = q^3(q + 1)$.

As is common let $N_G(U)$ denote the normalizer of $U$ in $G$, if $U \leq G$.

**Lemma 2.1.** Let $g \in G$. Then $S \cap g S g^{-1} = 1_G$ if and only if $g \in G \setminus N$. In particular, $N = N_G(S)$.

Proof. Since $S$ is normal in $N$ it is enough to show that $S \cap g S g^{-1} \neq 1_G$ implies $g \in N$. So let $g = (a_i) \in G$ such that $S \cap g S g^{-1} \neq 1_G$. Then there exists $1_G \neq M(1, \beta, \gamma) \in S \cap g S g^{-1}$. As $N(\beta) = \text{tr}(\gamma)$ it follows that $\gamma \neq 0$. Furthermore there is $1_G \neq M(1, \beta', \gamma') \in S$ such that $M(1, \beta, \gamma) \cdot g = g \cdot M(1, \beta', \gamma')$. By comparing the first and second columns on either side we see that $g$ is an upper triangular matrix. Now $g \in N$ can be derived from the fact that $g^T A \overline{g} = A$. (Note that $a_{11}a_{22}a_{33} = 1$) \hfill \Box

One can show that also $N = N_G(C)$. However we do not require this result and omit a proof here. The following result is a consequence of $G$ having a BN-pair (for details see [1]), where our $N$ and the group generated by the matrix $A$ make up the pair.

**Lemma 2.2.** There are two $(N, N)$-double cosets in $G$, which are $N$ and $NAN$. Furthermore $N \cap ANA^{-1} = \{M(\alpha, 0, 0) : \alpha \in \mathbb{F}_q^*\}$.

Next we count the involutions in $G$. Let $M(1, \beta, \gamma) \in S$. Then $M(1, \beta, \gamma)^2 = M(1, 0, N(\beta))$, by (1). Note that $N(\beta) = \text{tr}(\gamma) = 0$ iff $\beta = 0$ and $\gamma \in \mathbb{F}_q$. Hence $\{M(1, 0, \gamma) : \gamma \in \mathbb{F}_q^*\}$ are all involutions in $S$. Next take $\gamma, \gamma' \in \mathbb{F}_q^*$ and let $\alpha \in \mathbb{F}_q^*$ such that $N(\alpha) = \gamma' \gamma^{-1}$. Note that such an $\alpha$ always exists. Then $M(\alpha, 0, 0) \cdot M(1, 0, \gamma') \cdot M(\alpha, 0, 0)^{-1} = M(1, 0, \gamma')$, by (1). Hence all involutions in $S$ are $G$-conjugate, and thus all involutions in $G$ lie in the same conjugacy class. Moreover Lemma 2.1 implies that two different Sylow-2-subgroups of $G$ intersect trivially. As there are $|G : N_G(S)| = |G : N| = q^3 + 1$ Sylow-2-subgroups of $G$ we conclude that there are $(q^3 + 1)(q - 1)$ involutions forming one conjugacy class.

We consider the involution $T := M(1, 0, 1)$. As usual let $C_G(T)$ denote its centralizer in $G$ and $\text{Cl}_G(T)$ its conjugacy class in $G$.

**Lemma 2.3.** We have $I = \text{Cl}_G(T)$ and $C = C_G(T)$. In particular $kI \cong k_C \uparrow^G$.

Proof. It remains to show that $C = C_G(T)$. Using (1) it follows easily that $C \leq C_G(T)$. As $|C_G(T)| = |G|/|\text{Cl}_G(T)| = q^3(q + 1)$ the proof is complete. \hfill \Box
Note that since $S$ is a trivial intersection group and normal in $C$, every component of $kI$ is either projective or has vertex $S$.

Finally observe that $Z(G) = \{ \alpha \cdot 1 : \alpha \in \mathbb{F}_{q^2}, \alpha^2 = 1 = \alpha^{q+1} \}$. Therefore $|Z(G)| = \varepsilon$ and $|\text{PSU}(3, q^2)| = q^3(q^2 - 1)(q^3 + 1)/\varepsilon$, where $\varepsilon := \gcd(3, q + 1)$. In particular $Z(G)$ is of odd size. As the $Z(G)$ acts trivially on the involutions by conjugation it follows that the involution module of $G$ is the inflation of the involution module of $\text{PSU}_3(q^2)$, w.r.t. the canonical epimorphism $\text{SU}(3, q^2) \to \text{PSU}_3(q^2)$. Hence in order to understand the latter it is sufficient to study the former.

3. The irreducible $kN$-modules

Recall that $S$ is normal in $N$. By Clifford theory the irreducible $kN$-modules are inflated from the irreducible $kN/S$-module w.r.t. the epimorphism $N \to N/S$ induced by $\varphi_1$ as given in (2). Since $N/S \cong H := \{ M(\alpha, 0, 0) : \alpha \in \mathbb{F}_{q^2} \}$ is cyclic of order $q^2 - 1$ we can describe the irreducible $kN$-modules as follows.

For $j \in \{0, 1, \ldots, q^2 - 2\}$ let $V_j$ be a one-dimensional $k$-vector space where

\begin{equation}
M(\alpha, \beta, \gamma) \cdot \omega = M(\alpha, 0, 0) \cdot \omega := \alpha^j \cdot \omega,
\end{equation}

for all $M(\alpha, \beta, \gamma) \in N$ and $\omega \in V_j$. The various $V_j$ give all irreducible $kN$-modules.

Often we use an alternative representation of the irreducible $kN$-modules. Let $F := \{0, 1, \ldots, 2f - 1\}$. Then for $I \subseteq F$ we define

\begin{equation}
n(I) := \sum_{i \in I} 2^i.
\end{equation}

Note the bijection $I \leftrightarrow n(I)$, between the subsets $I$ of $F$ and $\{0, 1, \ldots, q^2 - 1\}$. We define $V_I := V_{n(I)}$, for all $J \subseteq F$. Since $n(F) \equiv 0 \mod (q^2 - 1)$, we have $V_F = V_0 = k_N$. Overall the irreducible $kN$-modules are given by $V_J := V_{n(J)}$, for all $J \subseteq F$.

Let $\tau_J$ or $\tau_{n(J)}$ denote the Brauer character and $V_J^*$ the dual of $V_J$. Observe that $V_J \otimes V_{F \setminus J} \cong k_N$, and thus

\begin{equation}
V_J^* \cong V_{\overline{J}}, \quad \text{where } \overline{J} := F \setminus J.
\end{equation}

4. The irreducible $kG$-modules

In this section we focus on the irreducible $kG$-modules. They are described in detail in [2]. Still let $F := \{0, 1, \ldots, 2f - 1\}$ and take $t \in F$. Let $M \cong k^3$ with the natural $G$-structure. Next we define $M_{t} \cong k^3$ as the $kG$-module, where $X$ acts on $M_{t}$ as $X^{(t)}$ acts on $M$. By $X^{(t)}$ we denote the matrix that derives from $X$ by raising each entry to the power $2^t$. Next, for $t = 0, \ldots, f - 1$, we have

\begin{equation}
M_{t} \otimes M_{t+f} \cong k_G \oplus M_{(t,t+f)}, \quad \text{as } kG\text{-modules},
\end{equation}

where $k_G$ is the Brauer character.
where $M_{(t,t+f)}$ is irreducible and has dimension 8.

For every $I \subseteq F$ we define the sets

\[
\begin{align*}
I_p & := \{ t \in \{0, 1, \ldots, f-1\} : t, t + f \in I \}, \\
I_s & := \{ t \in I : t + f \notin I \}, \\
f(I) & := \{ t + f : t \in I \}, \\
R(I) & := \{ t \in F : t \in I \text{ or } t + f \in I \}.
\end{align*}
\]

It helps to think of $F$ as two rows, with the top row ranging from 0 to $f-1$ and the bottom row ranging from $f$ to $2f-1$. Given $I \subseteq F$ the set $I_p$ contains those integers $t$ from the top row whose counterpart $t + f$ in the bottom row also belongs to $I$. Hence \{t, t + f\} form a “pair” in $I$. On the other hand the set $I_s$ gives the “single” elements in $I$, that is, those integers $t$ in both rows where $t + f$ is not contained in $I$. Here $t + f$ is to be taken modulo $2f$. Furthermore $f(I)$ is the set of all counterparts of elements in $I$, whereas $R(I)$ is the union of $I$ and $f(I)$.

Set $M_\emptyset := k_G$, and for $I \neq \emptyset$ we define

\[
M_I := \bigotimes_{t \in I_p} M_{(t,t+f)} \otimes \bigotimes_{t \in I_s} M_t.
\]

As explained in [2] this gives all $q^2$ irreducible, pairwise non-isomorphic $kG$-modules.

Recall that the involution module of $G$ is inflated from the involution module of $\overline{G} := G/Z(G)$. Hence if $M_I$ appears in $k\overline{I}$ then $Z(G)$ acts trivially on $M_I$. So let $\alpha \cdot I \in Z(G) = \{ \alpha \cdot I : \alpha \in \mathbb{F}_{q^2}, \alpha^3 = 1 = \alpha^{q+1} \}$. Then $(\alpha \cdot I) \cdot \omega = \alpha^2 \cdot \omega$, for $\omega \in M_I$, and $(\alpha \cdot I) \cdot \omega = \alpha^2 \cdot \omega$, for $\omega \in M_{(t,t+f)}$. Hence, if we use $n(I)$ as defined in (4), we obtain

**Corollary 4.1.** Let $I \subseteq F$ such that $M_I$ appear in the involution module $k\overline{I}$. Then $\varepsilon | n(I)$, where $\varepsilon = \gcd(3, q + 1)$.

Let $\varphi_I$ denote the Brauer character of $M_I$, for $I \subseteq F$, and for every $t \in F$ set $\varphi_t := \varphi_{\{t\}}$. We aim to express $\varphi_t \downarrow N$ as a linear combination of the irreducible Brauer characters $\{\tau_J : J \subseteq F\}$ of $N$. With respect to the basis $\{e_1, e_2, e_3\}$ the action of any $M(\alpha, \beta, \gamma) \in N$ on $M_t$ is given by

\[
\begin{pmatrix}
\alpha^{2^t} & \beta^{2^t} & \gamma^{2^t} \\
(\alpha^{q^2} - 1)^2 & (\alpha^{-1} \beta^q)^2 & (\alpha^{-3})^2 \\
\end{pmatrix}.
\]

Hence

\[
\varphi_t \downarrow N = \tau_{2^t} + \tau_{2^{t+f} - 2} + \tau_{-2^{t+f}}.
\]
Also one checks easily that the socle of \( M_i \downarrow_N \) coincides with \( V_{(t)} \). This leads to

**Lemma 4.2.** Let \( I \subseteq F \). Then \( M_i \downarrow_N \) has \( V_I \) in its socle.

Finally let \( M^* \) denote the dual of some \( kG \)-module \( M \). Then for every \( t \in F \), we have

\[
M_t^* \cong M_{t+f} \quad \text{and} \quad M_{(t,t+f)}^* \cong M_{(t,t+f)}.
\]

**5. The components of \( kI \)**

In this section we provide a complete decomposition of the involution module \( kI \) of \( G \). By Lemma 2.3 we have \( kI \cong kC \uparrow^G \). Furthermore recall that \( C \) is normal in \( N \), where \( N/C \) is a cyclic group of order \( q - 1 \). Hence \( kC \uparrow^N \cong kN/C \) is a direct sum of all irreducible \( kN \)-modules on which \( C \) acts trivially.

In Section 3 we described the irreducible \( kN \)-modules. By (3) we know that \( M(\alpha, \beta, \gamma) \cdot \omega = \alpha^{n(J)} \cdot \omega \), for all \( M(\alpha, \beta, \gamma) \in C \) and \( \omega \in V_J \). Hence \( C \) acts trivially on \( V_J \) if \( J_s = \emptyset \), as then \( n(J) = \sum_{i \in J} 2^i = (q + 1) \cdot \sum_{i \in J} 2^i \). Since there are exactly \( q - 1 \) different \( J \subsetneq F \) with \( J_s = \emptyset \) we conclude that \( kC \uparrow^N \cong \bigoplus_{J \subseteq F, J_s = \emptyset} V_J \). In particular

\[
kC \uparrow^G \cong \bigoplus_{J \subseteq F, J_s = \emptyset} V_J \uparrow^G.
\]

Moreover we have \( V_0 \uparrow^G = kN \uparrow^G = kG \oplus X \), where \( X \) is a \( q^3 \)-dimensional \( kG \)-module. Hence there are at least \( q \) indecomposable summands in \( kC \uparrow^G \). Furthermore observe that \( k_N \) appears in the socle of \( M_F \downarrow_N \), by Lemma 4.2. Hence \( M_F \) appears in the head of \( kN \uparrow^G \). Consequently \( X = M_F \). Using Lemma 2.2 we see that \( M_F \downarrow_N = k_H \uparrow^N \), where \( H = \{ M(\alpha, 0, 0); \alpha \in F_q^* \} \). Since \( H \) is a \( 2^t \)-group we know that \( k_H \uparrow^N \) is projective. Then, as \( N \) contains a Sylow-2-subgroup of \( G \), we conclude that \( M_F \) is projective. In fact \( M_F \) is known as the Steinberg module.

In the following we show that our \( q \) summands of \( kI \) are all indecomposable.

**Lemma 5.1.** Let \( J \subsetneq F \) so that \( J_s = \emptyset \). Then \( \text{Hom}_{kG}(V_J \uparrow^G, V_J \uparrow^G) \) is one-dimensional, unless \( J = \emptyset \) in which case it is two-dimensional. In particular, \( V_J \uparrow^G \) is indecomposable if \( J \neq \emptyset \), and \( V_0 \uparrow^G \cong kG \oplus M_F \).

**Proof.** By Lemma 2.2 we know that the \( (N, N) \)-double cosets in \( G \) are given by \( \{N, NAN\} \), and furthermore \( N \cap ANA^{-1} = H = \{ M(\alpha, 0, 0); \alpha \in F_q^* \} \). Now let \( J \subsetneq F \). Then, by Mackey’s lemma,

\[
(V_J \uparrow^G) \downarrow_N = \bigoplus_{s \in N \backslash G/N} (s(V_J)_{N \cap sN A^{-1}}) \uparrow^N = V_J \oplus (A \cdot V_J)_H \uparrow^N.
\]
We claim that $A \cdot V_J \cong V_T$ as $kH$-modules, where $\overline{J} := F \setminus J$. Let $\omega \in A \cdot V_J$ and $\alpha \in F_q^*$. Then

$$M(\alpha, 0, 0) \cdot \omega = (A \cdot M(\alpha^{-q}, 0, 0) \cdot A^{-1}) \cdot \omega = \alpha^{-qn(J)} \cdot \omega,$$

since $-qn(J) = -q \sum_{i \in J} 2^i = \sum_{i \in J} 2^{i+j} \equiv n(\overline{J}) \mod (q^2 - 1)$. Therefore

$$(10) \quad (V_J \uparrow^G \downarrow_N) = V_J \oplus (V_T^H \uparrow^N).$$

Next let $I \subsetneq F$ such that $V_I$ appears in the socle of $(V_T^H \uparrow^N)$. Then by Frobenius reciprocity it follows that $V_T \cong V_I$, as $kH$-modules, and thus as $kN$-modules. Therefore

$$(11) \quad \text{soc}((V_T^H \uparrow^N) = V_T.$$

As $\dim_k \text{Hom}_{kG}(V_J \uparrow^G, V_J \uparrow^G) = \dim_k \text{Hom}_{kN}(V_J, (V_J \uparrow^G) \downarrow_N)$ the statement follows from (10) and (11).

The following proposition summarizes the complete decomposition of $kC \uparrow^G$ into indecomposable modules.

**Proposition 5.2.** The involution module $k\mathcal{I}$ has $q$ components and its decomposition is

$$k\mathcal{I} \cong kC \uparrow^G \cong k_G \oplus M_F \oplus \bigoplus_{\emptyset \neq J \subsetneq F, J \neq \emptyset} V_J \uparrow^G.$$

Next we want to investigate the structure of the head and socle of $V_J \uparrow^G$, for $\emptyset \neq J \subsetneq F$ such that $J_s = \emptyset$.

**Proposition 5.3.** For every $\emptyset \neq J \subsetneq F$ so that $J_s = \emptyset$ we have $\text{hd}(V_J \uparrow^G) = M_J$ and $\text{soc}(V_J \uparrow^G) = M_T$.

Proof. Assume $M_I$, for $I \subsetneq F$, appears in the socle of $V_J \uparrow^G$. Then $\text{soc}(M_I \downarrow_N)$ is a direct summand of $\text{soc}((V_J \uparrow^G) \downarrow_N)$. The latter equals $V_J \oplus V_T$ by (10) and (11). Now it follows from Lemma 4.2 that $I = J$ or $I = \overline{J}$. Furthermore $M_I$ appears exactly once in the socle of $V_J \uparrow^G$.

We claim that $M_I \downarrow_N$ is indecomposable. Since $I_s = \emptyset$ we have $M_I \otimes M_T = M_F$. Then $M_I \downarrow_N \otimes M_T \downarrow_N = M_F \downarrow_N$ and therefore it is enough to show that $M_F \downarrow_N$ is indecomposable. But $M_F \downarrow_N \cong k_H \uparrow^N$, whose socle is $k_N$, by (11). That proves the claim.

As $(V_J \uparrow^G) \downarrow_N = V_J \oplus (V_T^H \uparrow^N)$, by (10), it follows that $M_I \downarrow_N$ appears in $(V_T^H \uparrow^N)$. However that forces $I = \overline{J}$ and thus $\text{soc}(V_J \uparrow^G) = M_T$.

The statement about the head follows from $\text{hd}(V_J \uparrow^G) = (\text{soc}(V_J^* \uparrow^G))^*$ and the facts $M_J = M_J$ and $V_J^* = V_T$, given by (8) and (5), respectively. \qed
6. The composition factors of \( k \mathcal{I} \)

In this section we investigate the composition factors of \( k \mathcal{I} \). In Theorem 6.6 we present a formula to calculate the multiplicity of each irreducible \( kG \)-module in \( k \mathcal{I} \). Finally we study a combinatorial method to determine the numbers involved in Theorem 6.6.

First we look at the components of the projective module \( M_F \otimes M_I \), for \( I \subseteq F \). In [2] Burkhardt determines these components. Consider the following properties (P1)–(P5).

Let \( I, J \subseteq F \) and set \( X := f(I) \cap f(J) \):

(P1) \( f(I) \cup J = F \),
(P2) \( X_s \neq \emptyset \),
(P3) \( R(X) = F \),
(P4) between any two elements of \( X_s \) there is an even number of elements in \( R(X_p) \),
(P5) between any element of \( X_s \) and any element of \( f(X_s) \) there is an odd number of elements in \( R(X_p) \).

**Definition 6.1.** Let \( I, J \subseteq F \). We say \( J \) is of type \( I \), if \( I \) and \( J \) satisfy the properties (P1)–(P5). Furthermore by \( \mathcal{T}(I) \) we mean the set of all sets \( J \subseteq F \) that are of type \( I \).

**Lemma 6.2.** Let \( I, J \subseteq F \) such that \( J \) is of type \( I \). Then

(Q1) \( R(I) = F = R(J) \),
(Q2) \( R(I_s) \subseteq J \),
(Q3) \( I \neq F \) or \( J \neq F \),
(Q4) \( |(f(I) \cap J)_p| \) is odd.

Proof. Observe that (P3) implies (Q1). As \( I_s \subseteq J \), by (P1) and \( f(I_s) \subseteq J \), by (P3), we obtain (Q2). Next (Q3) follows from (P2), and (Q4) is a consequence of (P2) and (P5). \( \square \)

Before we present Burkhardt's result on the components of \( M_F \otimes M_I \), we need the following lemma. For \( I \subseteq F \) we define \( N(I) := \overline{R(I)} \), that is, \( N(I) = \{ t \in F : t, t + f \not\in I \} \).

**Lemma 6.3.** Let \( I, J \subseteq F \). Then \( f(I) \cup J = F \) and \( (f(I) \cap J)_s = \emptyset \) if and only if there is some \( A \subseteq I_p \) such that \( J = I_s \cup N(I) \cup R(A) \). Also in this case \( A = I_p \cap J_p \).

Proof. Observe that \( F \) is the disjoint union of \( I_s \), \( f(I_s) \), \( R(I_p) \) and \( N(I) \). Also note that \( f(I) \cup J = F \) implies \( I_s \cup N(I) \subseteq J \). Since \( \emptyset = (f(I) \cap J)_s = (f(I_s) \cap J)_s \cup (R(I_p) \cap J)_s = (f(I_s) \cap J) \cup (R(I_p) \cap J) \) we obtain \( f(I_s) \cap J = \emptyset \) and \( R(I_p) \cap J_s = \emptyset \). The former gives \( J = I_s \cup N(I) \cup (R(I_p) \cap J) \), while the latter implies that \( R(I_p) \cap J = R(I_p) \cap R(J_p) = R(I_p \cap J_p) \). Overall we get \( J = I_s \cup N(I) \cup R(A) \), where \( A := I_p \cap J_p \).
Now suppose that \( J = I_{t} \cup N(I) \cup R(A) \), for some \( A \subseteq I_{t} \). Then clearly \( f(I) \cup J = F \), and since \( f(I) \cap J = R(A) \), we obtain \( (f(I) \cap J)_{s} = \emptyset \).

For any \( I \subseteq F \), let \( P_{I} \) denote the projective cover of \( M_{I} \). Then the following corollary is a consequence of \([2, (31)]\) and Lemma 6.3.

**Corollary 6.4.** Let \( I \subseteq F \). Then
\[
M_{F} \otimes M_{I} = \bigoplus_{A \subseteq I_{p}} 2^{|A|} \pi_{L(I) \cup N(I) \cup R(A)} \oplus \bigoplus_{J \in T(I)} 2^{\left|I_{p} \cap J_{p}\right|} \pi_{J},
\]
\[
M_{F} \otimes M_{F} = m \cdot M_{F} \oplus \bigoplus_{A \subseteq F_{p}} 2^{|A|} \pi_{R(A)} \oplus \bigoplus_{J \in T(F)} 2^{\left|J_{p}\right|} \pi_{J}
\]
where \( m = 1 \) if \( f \) is even and \( m = 2^{f+1} + 1 \) if \( f \) is odd.

For \( I \subseteq F \) we define the Brauer character \( \alpha_{I} := \varphi_{I} \downarrow_{N} \). Then for \( t \in F \), we have \( \alpha_{t} := \alpha_{t_{0}} = \tau_{t}^t + \tau_{t+1}^{t+1} + \tau_{t-1}^{t-1} \), by \( (7) \), and \( \alpha_{t,t+1} := \alpha_{t+1,t} = \alpha_{t} \cdot \alpha_{t+1} - \tau_{0} \), by \( (6) \). Hence the multiplicity of \( \tau_{0} \) in \( \alpha_{t,t+1} \) equals 2, and thus we can define \( \beta_{t} := \alpha_{t,t+1} - 2\tau_{0} \). For non-empty \( I \subseteq F_{p} \) we define \( \beta_{I} := \prod_{t \in I_{p}} \beta_{t} \), while \( \beta_{\emptyset} := \tau_{0} \). Then
\[
(\varphi_{F} \varphi_{I}) \downarrow_{N} = \alpha_{F} \cdot \alpha_{I} \cdot \prod_{t \in I_{p}} (\beta_{t} + 2\tau_{0}) = \sum_{A \subseteq I_{p}} 2^{\left|A\right|} \cdot \alpha_{F} \cdot \alpha_{I} \cdot \beta_{I_{p}\setminus A}.
\]

Furthermore, for every \( I \subseteq F \), we denote the Brauer character of \( P_{I} \downarrow_{N} \) by \( \chi_{I} \).

**Lemma 6.5.** Let \( \emptyset \neq I \subseteq F \). Then
\[
\chi_{I} = \alpha_{F} \cdot \alpha_{I} \cdot \beta_{N(I)_{p}} - \sum_{J \in T(I_{p} \cup N(I))} 2^{\left|J_{p}\cap I_{p}\right|} \cdot \chi_{J},
\]
\[
\chi_{\emptyset} = \alpha_{F} \cdot \beta_{F_{p}} - m \cdot \chi_{F} - \sum_{J \in T(F)} 2^{\left|J\right|} \cdot \chi_{J},
\]
where \( m = 1 \) if \( f \) is even and \( m = 2^{f+1} + 1 \) if \( f \) is odd.

**Proof.** Let \( \emptyset \neq I \subseteq F \). Then
\[
\left( \sum_{A \subseteq N(I)_{p}} 2^{|A|} \cdot \chi_{I \cup R(A)} \right) + \chi_{I} = \sum_{J \in T(I_{p} \cup N(I))} 2^{\left|J_{p}\cap I_{p}\right|} \cdot \chi_{J}
\]
\[
= (\varphi_{F} \cdot \varphi_{L_{I} \cup N(I)}) \downarrow_{N} = \sum_{A \subseteq N(I)_{p}} 2^{|A|} \cdot \alpha_{F} \cdot \alpha_{I} \cdot \beta_{N(I)_{p}\setminus A},
\]
where the equalities follows from Corollary 6.4 and \( (12) \), respectively. Next take \( \emptyset \neq A \subseteq N(I)_{p} \), and let \( X := I_{t} \cup N(I) \setminus R(A) \). Then \( X_{p} = N(I)_{p}\setminus A \), \( X_{s} = I_{t} \) and \( N(X) = \)
This proves the first part of the lemma. The second part is proven similarly.

For two characters $\varphi_1$ and $\varphi_2$ let $\#(\varphi_1, \varphi_2)$ denote the multiplicity of $\varphi_1$ in $\varphi_2$. Likewise for modules $M_1$ and $M_2$ let $\#(M_1, M_2)$ denote the multiplicity of $M_1$ in $M_2$. For $I \subseteq F$ we define

$$m_I := \sum_{K \subseteq F, K \cap I = \emptyset} \#(K, \alpha_I, \beta_I).$$

**Theorem 6.6.** Let $\emptyset \neq I \subseteq F$ and $m = 1$ if $f$ is even and $m = 2^{f+1} + 1$ if $f$ is odd. Then

$$\#(M_I, k_{C \uparrow F}^G) = m_{L \cup N(I)} - \sum_{J \in T(I \cup N(I))} 2^{[N(I)_p \cap J_1]} \cdot m_J,$$

$$\#(M_{\emptyset}, k_{C \uparrow F}^G) = m - \sum_{J \in T(F)} 2^{[J_1]} \cdot m_J.$$  

Proof. First let $J \subseteq F$ be of some type $L \subseteq F$. We claim that $\chi_J = \alpha_F \cdot \alpha_J$. By (Q1) we have $R(J) = F$. Hence $N(J) = \emptyset$ and $J \neq \emptyset$. Also $T(J \cup N(J)) = \emptyset$. This is true since $J \cup N(J) = J$ and $(f(J) \cap K)_p = \emptyset$, for any $K \subseteq F$, which then violates property (Q4). Overall the claim now follows from Lemma 6.5.

Next let $\emptyset \neq I \subseteq F$. By Lemma 6.5 and the above paragraph we obtain

$$\chi_I = \alpha_F \cdot \left( \alpha_I \cdot \beta_{N(I)_p} - \sum_{J \in T(I \cup N(I))} 2^{[N(I)_p \cap J_1]} \cdot \alpha_J \right),$$

$$\chi_\emptyset = \alpha_F \cdot \left( \beta_{I_0} - m \cdot \tau_0 - \sum_{J \in T(F)} 2^{[J_1]} \cdot \alpha_J \right).$$

Now let $K \subseteq F$ so that $K_s = \emptyset$. Then $\#(M_K, V_K \uparrow F^G)$ coincides with the dimension of $\text{Hom}_{kG}(V_K \uparrow F^G, P_I) \cong \text{Hom}_{kN}(V_K, P_I \downarrow N)$. As $M_F \downarrow N \otimes V_K$ is the projective cover of $V_K$.
we get that \( \#(M_I, V_K \uparrow^G) \) equals the multiplicity of \( M_{F \downarrow N} \otimes V_K \) as a direct summand of \( P_I \downarrow N \). The Brauer character of \( M_{F \downarrow N} \otimes V_K \) is given by \( \alpha_F \cdot \tau_K \), and thus we obtain

\[
\#(M_I, V_K \uparrow^G) = \left( \tau_K, \alpha_I, \cdot \beta_{\mathcal{N}(I)} \right) = \sum_{J \in T(F) \cup \mathcal{N}(I)} 2^{I(F) \cap \mathcal{N}(I)} \cdot \alpha_J,
\]

\[
\#(M_{\emptyset}, V_K \uparrow^G) = \left( \tau_K, \beta_{\emptyset} - m \cdot \tau_{\emptyset} - \sum_{J \in T(F)} 2^{I(F) \cap \mathcal{N}(I)} \cdot \alpha_J.\right).
\]

As \( \#(M_I, k_C \uparrow^G) = \sum_{K \subseteq F, K \neq \emptyset} \#(M_I, V_K \uparrow^G) \) the proof is complete. \( \square \)

In the following we wish to calculate the number \( m_I \) combinatorially.

**Definition 6.7.** Let \( I \subseteq F \). A map \( \varsigma: I \rightarrow \{1, 2, 3\} \) is called a **solution** of \( I \) if

1. \( I_1 \cap f(I_3) = I_2 \cap f(I_3) = I_3 \cap f(I_1) = \emptyset \),
2. \( \sum_{t \in I_1 \cup I_2} 2^t + \sum_{t \in I_3} 2^{t+i} \equiv 0 \mod (q + 1) \),

where \( I_j := \{ t \in I : \varsigma(t) = j \} \), for \( j = 1, 2, 3 \).

Furthermore a solution \( \varsigma \) of \( I \) with \( I_3 = \emptyset \) is called a **basic solution** of \( I \).

Let \( I \subseteq F \). Every solution \( \varsigma \) of \( I \) can be associated to a basic solution of \( I \), by composing \( \varsigma \) with the map \( \tau: \{1, 2, 3\} \rightarrow \{1, 2, 3\} \) such that \( \tau(1) = 1 = \tau(3) \) and \( \tau(2) = 2 \). Note that two solutions \( \varsigma_1 \) and \( \varsigma_2 \) of \( I \) are associated to the same basic solution if and only if \( \varsigma_1 \) and \( \varsigma_2 \) map the same elements of \( I \) onto 2.

Now we can also determine how many solutions of \( I \) are associated to a given basic solution \( \varsigma \) of \( I \). Note that every time we change certain 1’s in the image of \( \varsigma \) to 3’s we obtain a new solution, as long as we make sure to treat pairs \( \{ t, t + f \} \subseteq I \) that are both mapped onto 1 equally. Hence if we define \( T_\varsigma := \{ t \in \{0, 1, \ldots, f - 1\} : \{ t, t + f \} \cap I_1 \neq \emptyset \} \), then for every subset \( P \subseteq T_\varsigma \) we obtain a solution of \( I \) that is associated to \( \varsigma \). Overall a basic solution \( \varsigma \) has \( 2^{|P|} \) solutions associated to it.

**Lemma 6.8.** Let \( I \subseteq F \). Then \( m_I \) equals the number of solutions of \( I \), that is,

\[
m_I = \sum 2^{|P|},
\]

where the sum is taken over all basic solutions \( \varsigma \) of \( I \).

Proof. It is enough to show that \( m_I \) equals the number of solutions of \( I \), as the rest of the statement then follows from the previous paragraph.

By definition \( m_I \) counts the occurrences of characters of the form \( \tau_K \) in \( \alpha_I, \beta_{\mathcal{N}(I)} \), where \( K \subseteq F \) so that \( K_0 = \emptyset \). Recall that \( \alpha_0 = \tau_0 + \tau_{2^t} + \tau_{2^{t+f}} + \tau_{2^{t+2f}} \) and \( \beta_0 = \alpha_0 \alpha_0 - \tau_0 \), for \( t \in F \). In particular note that in \( \alpha_0 \alpha_0 \) the three occurrences of the trivial characters \( \tau_0 \), derive from multiplying the first summand of \( \alpha_0 \) with the third...
The third summand of $K$ we are only interested in those that are congruent modulo $(q+1)$. These correspond to the solutions of $I$. Hence we have confirmed Corollary 4.1. Let $\varepsilon = \gcd(3, q+1)$ and suppose $M_I$ appears in $kC \uparrow^G I$. Then by Theorem 6.6, we have $m_{I, \cup N(I)} \geq 1$. Thus by Lemma 6.8 there is a basic solution of $I_3 \cup N(I)$. But now Lemma 6.9 (ii) implies that $\varepsilon$ divides $n(I_3)$. As $n(I)$ and $n(I_3)$ are congruent modulo $q+1$, they are also congruent modulo $\varepsilon$. Consequently $\varepsilon \mid n(I)$, which is the statement of Corollary 4.1.
In the following we explain how to find all basic solution for a given \( I \subseteq F \) using Lemma 6.9. For instance let \( f = 5 \), and consider \( F \) as two rows

\[
\begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 \\
5 & 6 & 7 & 8 & 9
\end{array}
\]

Next let \( I = \{0, 1, 2, 3, 4, 5, 8, 9\} \), which is given by

\[
\begin{array}{cccccc}
0 & 1 & 2 & 3 & 4 \\
5 & . & . & . & 8 & 9
\end{array}
\]

By Lemma 6.9 our aim is to find subsets \( I_2 \) of \( I \) such that \( \sum_{i \in I_2} 2^i \equiv 3 \cdot \sum_{i \in I_2} 2^i \mod (q + 1) \), where \( I_2 \) contains from each column at most one element. Since in our example \( \sum_{i \in I_2} 2^i = 2 + 2^3 = 6 \), we are looking for solutions of the linear congruence \( 6 \equiv 3x \mod 33 \). The following image shows the powers of 2 modulo \( q + 1 \) that can be obtained

\[
\begin{array}{cccccc}
2^0 & 2^1 & 2^2 & 2^3 & 2^4 \\
-2^0 & . & . & -2^3 & -2^4
\end{array}
\]

As \( x \) is the sum of at most one entry from each column, we get the upper bound \( M = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 31 \) and the lower bound \( m = -2^0 - 2^3 - 2^4 = -25 \) for \( x \). One checks easily that \( 6 \equiv 3x \mod 33 \) has five solutions between \(-25\) and \(31\), which are \(-20, -9, 2, 13\) and \(24\). However it is difficult to see if we have found all possibilities of writing, say \(-20\), as a sum of the available powers of two. Thus we propose the following technique.

We start by allocating all entries of the lower row to \( I_2 \), that is, \( \{5, 8, 9\} \) in our case. Then \( x = -25 \), which is not what we want. Now every time we remove an entry from \( I_2 \) we have to add the respective power of 2 to \(-25\). For instance if we remove 9 we have to add \( 2^4 \). Likewise we may include entries form the first row. For instance 2, which means we have to add \( 2^2 \). We could also wish to include 4. As this would also force us to remove 9 first we have to add \( 2^4 \) for the removal of 9 and \( 2^4 \) for the inclusion of 4, that is, \( 2^5 \) altogether. The following table shows the change we cause to \( x \) by including elements of the top row or removing elements from the bottom row.

\[
\begin{array}{cccccc}
2^1 & 2^1 & 2^2 & 2^4 & 2^4 \\
2^0 & . & . & 2^3 & 2^4
\end{array}
\]

So let us start with \( x_0 = -20 \). Initially we have \( I_2 = \{5, 8, 9\} \). In order to get form \(-25\) to \(-20\) we need to add \( 5 = 2^0 + 2^2 \). Observe that the only way to get \( 2^0 \) is to remove 5 from \( I_2 \), (and not include 0). Now the only way to get \( 2^2 \) is by including 2. We get \( I_2 = \{2, 8, 9\} \), which we represent as follows

\[
\begin{array}{cccccc}
1 & 1 & 2 & 1 & 1 \\
1 & . & . & 2 & 2
\end{array}
\]
Next let \( x_0 = -9 \). The difference \( 16 = 2^4 \) can be obtained in three different ways. Firstly by including 3, which involves the removal of 8. Secondly by removing 9 and thirdly by removing 8 and including 0, 1, 2, since \( 2^4 = 2^3 + 2^2 + 2^1 + 2^1 \). Overall we have three basic solutions as follows

\[
\begin{array}{cccc}
1 & 1 & 1 & 2 \\
2 & \cdot & \cdot & 1 \\
\end{array}
\quad
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
2 & \cdot & \cdot & 2 \\
\end{array}
\quad
\begin{array}{cccc}
2 & 2 & 2 & 1 \\
1 & \cdot & \cdot & 1 \\
\end{array}
\]

Now let \( x_0 = 2 \). Then \( | -25 - 2 | = 27 = 2^0 + 2^1 + 2^3 + 2^4 \). Here there is only one basic solution, which is

\[
\begin{array}{cccc}
1 & 2 & 1 & 1 \\
1 & \cdot & \cdot & 1 \\
\end{array}
\]

For \( x_0 = 13 \) we have \( | -25 - 13 | = 38 = 2^1 + 2^2 + 2^5 \). There are two possibilities of \( 2^1 \). Also with one \( 2^1 \) gone there is only one possibility to obtain \( 2^2 \). Finally \( 2^5 = 2^4 + 2^4 \) can be obtained in two different ways, leading to the four basic solutions

\[
\begin{array}{cccc}
2 & 1 & 2 & 1 \\
1 & \cdot & \cdot & 2 \\
\end{array}
\quad
\begin{array}{cccc}
2 & 1 & 2 & 1 \\
1 & \cdot & \cdot & 1 \\
\end{array}
\quad
\begin{array}{cccc}
1 & 2 & 2 & 1 \\
2 & \cdot & \cdot & 1 \\
\end{array}
\quad
\begin{array}{cccc}
1 & 2 & 2 & 1 \\
2 & \cdot & \cdot & 1 \\
\end{array}
\]

Finally let \( x_0 = 24 \). Then \( | -25 - 24 | = 49 = 2^0 + 2^4 + 2^5 \). There is only one way to obtain this sum and we get

\[
\begin{array}{cccc}
1 & 1 & 1 & 2 \\
1 & \cdot & \cdot & 1 \\
\end{array}
\]

Hence we have found all basic solutions of \( I \). Finally the number of solutions associated to each basic solution depends on the number of columns that contain a 1, as in each such column all the \( I \)'s may be changed to \( 3 \)'s. Going through all basic solutions given above we obtain

\[
(14) \quad m_I = 2^4 + 2^5 + 2^5 + 2^3 + 2^4 + 2^4 + 2^3 + 2^3 + 2^5 = 184.
\]

In the above example we have \( I_s = \{ 1, 2 \} \). Next let \( I' \subseteq F \) such that \( I'_s = \{ 1, 2 \} \). Note that then \( I' \subseteq I \). We can use the above results to calculate \( m_{I'} \). Take for instance \( I' = \{ 0, 1, 2, 5 \} \). A basic solution for \( I' \) becomes a basic solution for \( I \), by sending all elements in \( I \setminus I' \) onto one. The only basic solution for \( I \) where \( \{ 3, 4, 8, 9 \} \) is mapped onto one is when \( x = 2 \). Hence the only basic solution for \( I' \) is

\[
\begin{array}{cccc}
1 & 2 & 1 & \cdot \\
1 & \cdot & \cdot & \cdot \\
\end{array}
\]
Consequently we have \( m_1 = 2^2 = 4 \).

Finally let us characterize those sets \( I \subseteq F \) that have a basic solution.

**Definition 6.10.** Let \( U \subseteq F \). We call \( U \) a U-form
1. of length zero, if \( U = \{ t, t + f \} \), for some \( t \in F \),
2. of length one, if \( U = \{ t, t + 1 \} \), for some \( t \in F \),
3. of length \( n \geq 2 \), if there is \( H \subseteq H(t, n) \setminus \{ t \} \), for some \( t \in F \), such that \( U = (H(t, n) \setminus H) \cup (f(H) - 1) \) is a disjoint union, where \( H(t, n) = \{ t, t + n \} \cup \{ t + 1 + f, \ldots, t + n - 1 + f \} \).

**Theorem 6.11.** Let \( I \subseteq F \). Then \( I \) has a basic solution if and only if \( I \) is the disjoint union of U-forms.

Proof. First suppose that \( I \) has a basic solution \( \xi \). We argue by induction on \( |I| \)
that \( I \) is a disjoint union of U-forms. This is clear if \( |I| = 0 \), and thus in the following let \( |I| \geq 1 \).

Define \( X := I_1 \cup (f(I_2) + 1) \) and \( Y := I_1 \cap (f(I_2) + 1) \). By property (S2) there is some \( K \subseteq F \), such that \( K_x = \emptyset \) and

\[
\sum_{i \in K} 2^i = \sum_{i \in I_1} 2^i + \sum_{i \in I_2} 2^{i+1+f} \equiv \sum_{i \in X} 2^i + \sum_{i \in Y} 2^i \mod (q^2 - 1).
\]

First suppose that \( Y = \emptyset \). Then \( X = K \). If \( I_2 = \emptyset \), then there is some \( t \in I_1 \) so that \( U = \{ t, t + f \} \subseteq I \). If \( I_2 \neq \emptyset \), then there is some \( t \in I_2 \) such that \( t + 1 \in K \). Note that by (S1) we have \( t + 1 \in I_1 \) and thus \( U = \{ t, t + 1 \} \subseteq I \). In both cases \( U \) is a U-form such that \( \xi \) is a basic solution on \( I \setminus U \). Now by induction \( I \setminus U \) is a disjoint union of U-forms, and thus so is \( I \). Hence we may assume that \( Y \neq \emptyset \).

Set \( T := f(Y) - 1 = \{ t_1, \ldots, t_r \} \), that is, \( T \) contains all \( t \in I_2 \) such that \( t + 1 + f \in I_1 \).

For each \( i \in \{ 1, \ldots, r \} \) let \( n_i \geq 2 \) be maximal such that \( \{ t_i + 2 + f, \ldots, t_i + n_i - 1 + f \} \subseteq X \setminus Y \). We set \( S_i := \{ t_i + 1 + f, \ldots, t_i + n_i - 1 + f \} \). Then \( S_i \subseteq X \).

Next we claim that \( S_i \cap S_j = \emptyset \), for all \( i \neq j \). Assume otherwise. Then there is \( a \in S_i \cap S_j \) so that \( a - 1 \in (S_i \cup S_j) \setminus (S_i \cap S_j) \). Without loss of generality let \( a - 1 \in S_j \setminus S_i \). Then \( t_j = a - 1 + f \) and thus \( a \in Y \), contradicting \( a \in S_i \). That proves the claim.

Let \( S = \bigcup_{i=1}^r S_i \). Since \( 2^{i+1+f} + \sum_{i \in S} 2^i \equiv 2^{i+n_i + f} \mod (q^2 - 1) \), we get

\[
\sum_{i \in K} 2^i = \sum_{i \in I_1 \setminus S} 2^i + \sum_{i \in f(I_2) + 1 \setminus S} 2^i + \sum_{i=1}^r 2^{i+n_i + f} \mod (q^2 - 1).
\]

Note that the maximality of \( T \) ensures that the first two sums have no power of 2 in common, and the maximality of \( n_i \) ensures that the last sum has no power of 2 in common with the first two sums. Hence \( t_1 + n_1 + f \in K \), and thus \( a := t_1 + n_1 \in K \).
Assume $a \not\in X$. Then $a = t_1 + n_1 + f$, for some $i \in \{2, \ldots, r\}$. Note that $n_1 \neq n_i$, as otherwise $t_1 = t_i + f \in I_2 \cap f(I_2)$, in contradiction to (S1). If $n_1 < n_i$, then $t_1 = t_i + n_1 - n_i + f$. As $n_1 \geq 2$, we have $t_1 + 1 \in S_i \subseteq X$. But $t_1 + 1 \not\in f(I_2) + 1$, by (S1), and thus $t_1 + 1 \in I_1$. Hence $U = \{t_1, t_1 + 1\}$ is a $U$-form such that $\zeta$ is a basic solution on $I \setminus U$. Likewise if $n_i < n_1$, then $t_i + 1 \in I_1$ and $U = \{t_i, t_i + 1\}$ is a $U$-form such that $\zeta$ is a basic solution on $I \setminus U$. Hence in the following we may assume that $t_1 + n_1 \in X$.

Now let $t = t_1$ and $n = n_1$. Set $H := (H(t, n) \setminus \{t, t + 1 + f\}) \cap (f(I_2) + 1)$. Then $H \subseteq H(t, n) \setminus \{t\}$. We claim that $(H(t, n) \setminus H) \cap (f(H) - 1) = \emptyset$. Note that $f(H) - 1 = I_2 \cap \{t + 1, \ldots, t + n - 2, t + n - 1 + f\}$. Hence $t + n - 1 + f$ is the only possible element in $H(t, n) \cap (f(H) - 1)$. In this case we have $t + n + f \not\in I_2$. In particular $t + n + f \not\in I_1$ and so $t + n - 1 + f \neq t + f + 1$. Also recall that $t + n - 1 + f \not\in X \setminus Y$. Hence $t + n - 1 + f \not\in f(I_2) + 1$. Therefore $t + n - 1 + f \in H$, which proves the claim.

Thus $U = (H(t, n) \setminus H) \cup (f(H) - 1)$ is a $U$-form. Also $U \subseteq I$, which is clear since all $x \in H(t, n) \setminus \{t\}$ either belong to $I_1$ or to $f(I_2) + 1$. Finally $U \cap I_1 = H(t, n) \setminus (H \cup \{t\})$ and $U \cap I_2 = (f(H) - 1) \cup \{t\}$. Since

$$
\sum_{k \in I_1 \cap U} 2^k + \sum_{k \in I_2 \cap U} 2^{k+1+f} = 2^{t+1+f} + \sum_{k \in H(t, n) \setminus (H \cup \{t\})} 2^k + \sum_{k \in f(H) - 1} 2^{k+1+f} \\
\equiv 2^{t+1+f} + \sum_{k \in H(t, n) \setminus \{t\}} 2^k \equiv 2^{t+n} + 2^{t+n+f} \equiv 0 \mod (q + 1),
$$

we see that $\zeta$ is still a basic solution on $I \setminus U$. Thus, by induction, $I$ is a disjoint union of $U$-forms.

Now suppose that $I = U_1 \cup \cdots \cup U_r$ is a disjoint union of $U$-forms. We define a map $\zeta$ on each $U_i$. If $U_i = \{t, t + f\}$ is of length zero, then set $\zeta(t) = 1 = \zeta(t + f)$. If $U_i = \{t, t + 1\}$ is of length one, then $\zeta(t) = 2$ and $\zeta(t + 1) = 1$. Finally, if $U_i$ is of length $n \geq 2$, that is, $U_i = (H(t, n) \setminus H) \cup (f(H) - 1)$, for some $H \subseteq H(t, n) \setminus \{t\}$, then $\zeta(x) = 1$, for all $x \in H(t, n) \setminus (H \cup \{t\})$ and $\zeta(x) = 2$, for all $x \in \{(t) \cup (f(H) - 1)\}$. We claim that in each case property (S2) is satisfied on $U_i$. This is straightforward if $U$ is of length zero or one. So let $U$ be of length $n \geq 2$. Then

$$
\sum_{k \in I_1 \cap U_i} 2^k + \sum_{k \in I_2 \cap U_i} 2^{k+f+1} \\
\equiv \sum_{k \in H(t, n) \setminus (H \cup \{t\})} 2^k + \sum_{k \in f(H) - 1 + f} 2^k \\
\equiv 2^{t+f+1} + \sum_{k \in H(t, n) \setminus \{t\}} 2^k \equiv 2^{t+f+n} + 2^{t+n} \equiv 0 \mod (q + 1).
$$

Hence (S2) holds on each $U_i$, and thus on $I$. 

However note that \( I_2 \cap f(I_2) \) may not be empty, and thus property (S1) fails to hold. Thus for each \( t \in I_2 \cap f(I_2) \) we set \( \zeta(t) = 1 = \zeta(t + f) \). Since \( 2' + 2^{t+f} \equiv 2^{t+1} + 2^{t+f+1} \mod (q + 1) \), this does not effect the validity of property (S2). In particular we have constructed a basic solution of \( I \).  

We can now construct irreducible \( M_I \) that have basic solutions. Take for instance \( f = 13 \) and consider the union of the following \( U \)-forms of 
(a) length zero,
(b) length one,
(c) length four, with \( H = \emptyset \) and
(d) length five, with \( H \) containing the two \( d' \).

<table>
<thead>
<tr>
<th>a</th>
<th>c</th>
<th>b</th>
<th>b</th>
<th>c</th>
<th>·</th>
<th>·</th>
<th>d</th>
<th>·</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>·</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>·</td>
<td>·</td>
<td>d</td>
<td>d'</td>
<td>d'</td>
</tr>
</tbody>
</table>

In particular \( M_{\{0,1,2,3,5,8,11,13,15,16,17,20,21,22,25\}} \) has basic solutions.

We conclude this paper by calculating the multiplicity of certain irreducible modules in the involution module of \( \text{PSU}_3(q^2) \). Let \( f = 5 \) and take \( I = \{1, 2\} \). We use Theorem 6.6. Observe that \( K := I_s \cup N(I) = \{0, 1, 2, 3, 4, 5, 8, 9\} \), and \( m_K = 184 \), by (14). It remains to calculate \( m_{J_s} \), for all \( J \in \mathcal{T}(K) \). So let \( J \) be of type \( K \). Then \( R(K_s) = \{1, 2, 6, 7\} \subseteq J \), by (Q2). Next set \( X := f(K) \cap J \). Observe that \( X_p \subseteq \{0, 3, 4\} \), Moreover by (Q4) we know that \( |X_p| \) is odd. This either implies \( |X_p| = 3 \), in which case \( J = F \) and thus \( m_{J_s} = 0 \), or \( |X_p| = 1 \), in which case \( J_s \) contains exactly two elements. Assuming \( m_{J_s} \neq 0 \), it follows from Theorem 6.11 that \( J_s \) is a union of \( U \)-forms. Hence \( J_s \) is a \( U \)-form of length one, and thus it is one the four possible sets \( \{3, 4\}, \{4, 5\}, \{8, 9\} \) and \( \{0, 9\} \). Since \( X_s = f(K_s) \cup J_s = \{6, 7, 17\} \cup J_s \), we conclude from (P4) and (P5) that \( J_s = \{8, 9\} \) or \( J_s = \{4, 5\} \). One checks easily that \( m_{J_s} = 2 \) in either case. Furthermore \( |N(I)_p \cap J_s| = |X_p| = 1 \). Overall we get

\[
#(M_I, k_C \uparrow^G) = m_K - 2 \cdot m_{\{8,9\}} - 2 \cdot m_{\{4,5\}} = 184 - 2 \cdot 2 - 2 \cdot 2 = 176.
\]

Hence \( M_{\{1,2\}} \) appears 176 times in the involution module of \( \text{PSU}_3(4^5) \).

Next we choose \( I = \{1, 2, 3, 4, 8, 9\} \). Then \( I_s \cup N(I) = \{0, 1, 2, 5\} \). Since \( R(I_s \cup N(I)) \neq F \), there is no set of type \( I_s \cup N(I) \). Hence \( #(M_I, k_C \uparrow^G) = m_{\{0,1,2,5\}} \). Before Definition 6.10 we found that \( m_{\{0,1,2,5\}} = 4 \). Hence \( M_{\{1,2,3,4,8,9\}} \) appears 4 times in the involution module of \( \text{PSU}_3(4^5) \).

ACKNOWLEDGEMENTS. I wish to thank the anonymous referee for some very constructive input towards the final version of this paper.
References


Department of Mathematics
National University of Ireland, Maynooth
Co. Kildare,
Ireland
e-mail: lars.pforte@nuim.ie