A Characterization of $U_3(q)$*

MICHAEL E. O'NAN

Department of Mathematics, Rutgers University, New Brunswick, New Jersey 08903

Communicated by Walter Feit

Received February 23, 1971

INTRODUCTION

We prove the following theorem:

**THEOREM.** Let $G$ be a doubly-transitive group on a set $X$ where $|X| = 1 + q^3$ and $q$ is the power of some odd prime number $p$. Suppose $\infty$ and 0 are points of $X$, $H$ is the subgroup of $G$ fixing $\infty$, and $K$ is the subgroup of $G$ fixing 0 and $\infty$. Suppose further

1. $H$ has a normal subgroup $Q$, regular on $X - \infty$.
2. $K$ is cyclic of order $(q^3 - 1)/(q + 1, 3)$.

Then, $G$ is isomorphic to $U_3(q)$, the three-dimensional projective special unitary group over the field with $q$ elements.

This theorem was obtained by Suzuki [8] when $q + 1 \equiv 0 \pmod{3}$. It was obtained by Harada [2] when $q = 5$.

In an earlier paper [6] we showed that $U_3(q)$ satisfies the hypotheses of the foregoing theorem. In addition it was shown that there is on the set $X$ a block design $\mathcal{A}$ preserved by $U_3(q)$, in which all blocks have $1 + q$ points. This unitary block design, $\mathcal{A}$, also has the property that every two-element subset of $X$ belongs to a unique block of $\mathcal{A}$. In the reference cited above it was shown that the automorphism group of $\mathcal{A}$ is the group $P\Gamma U(3, q)$. From this it follows quickly that any subgroup of $\text{aut}(\mathcal{A})$, doubly-transitive on $X$ and having the same order as $U_3(q)$, is $U_3(q)$.

We use a geometric approach in the proof of the foregoing theorem. To the set $X$ we attach a block design $\mathcal{B}$ preserved by the group $G$. We use the properties of $G$ in the hypotheses of the theorem to show that the block design $\mathcal{B}$ enjoys many of the properties of $\mathcal{A}$, the unitary block design of

* The material herein was presented to Princeton University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Copyright © 1972 by Academic Press, Inc.
All rights of reproduction in any form reserved.
We begin Section 4 by studying the action of \( H \) on the blocks of \( \mathcal{B} \). Since \( \mathcal{Q} \) is regular on \( X - \infty \), we may identify the points of \( X - \infty \) with \( \mathcal{Q} \), \( 1 \in \mathcal{Q} \) corresponding to 0 \( \in X - \infty \). If we set \( P = C(\mathcal{Q} \mathcal{W}) \) and use this identification, it turns out that each block containing \( \infty \) is of the form \( \infty \cup hP \), \( h \in \mathcal{Q} \). Furthermore, we show that \( X - \Delta \) (which corresponds to \( \mathcal{Q} - P \)) is the disjoint union of blocks fixed by \( W \). Using this fact we eliminate the possibility that \( \mathcal{Q} \) is abelian. In the case in which \( 1 + q \equiv 0 \pmod{3} \), it follows quickly that \( \mathcal{B} = \mathcal{A} \), completing the proof of the theorem. If, on the other hand, \( 1 + q \not\equiv 0 \pmod{3} \), and if \( \omega \) denotes a primitive \((q + 1)\)-st root of unity in \( E \), we show that there is a block in \( \mathcal{B} \) of the form

\[
\{(\omega^{3i}, -\frac{1}{2}), (\lambda \omega^{3i+1}, -\frac{1}{2} + u), (\eta \omega^{3i+2}, -\frac{1}{2} + v)\}, \quad 0 \leq i < (q + 1)/3
\]

where \( \lambda, \eta, u, \) and \( v \) are elements of \( E \) which must be determined. We note that if \( \lambda = 1, \eta = 1, u = 0, \) and \( v = 0 \), it follows from Lemma 2.8 of [6] that \( \mathcal{B} = \mathcal{A} \).
In Section 5 we relate the block design $\mathcal{A}$ associated with $U_3(q)$ to the block design $\mathcal{B}$ associated with $G$. The two block designs are compared by means of a local isomorphism around the block $\Delta$, which is a member of both the block designs $\mathcal{A}$ and $\mathcal{B}$. A local isomorphism is a permutation $f$ of $X$ such that if $A \in \mathcal{A}$ and $A \cap \Delta \neq \emptyset$, then $f(A) \in \mathcal{B}$, and conversely. The existence of such a function forces many of the properties of the block design $\mathcal{A}$ to propagate to $\mathcal{B}$.

In our determination of the automorphism group of the block design $\mathcal{A}$ in [6], a concept of central importance is that of the system of circles $\mathcal{C}$ associated with the block design $\mathcal{A}$. Inquiring no further into this topic of the moment, we shall content ourselves with pointing out that an analogous system of circles $\mathcal{D}$ may be associated with the block design $\mathcal{B}$. In the same manner in which the local isomorphism correlates many of the properties of $\mathcal{A}$ and $\mathcal{B}$, so too, using it, we may obtain many of the properties of the system of circles $\mathcal{D}$ from those of $\mathcal{C}$. This program is carried out in Section 6.

In Section 7, by using the qualitative properties of the system $\mathcal{D}$ derived in Section 6, we obtain numerical relations of the quantities $\lambda$ and $\eta$ of Section 4. In particular, with $x = \lambda^{(q+1)/3}$ and $y = \eta^{(q+1)/3}$, we find

$$x^3y + 2xy^2 + x^2y - y^3 - 3xy + 2x^2 + y^2 + 4y - 5x - 2 = 0,$$
$$xy^3 + 2x^2y + xy^2 - x^3 - 3xy + 2y^2 + x^2 + 4x - 5y - 2 = 0.$$

In Section 8 similar numerical relations are derived for $u$ and $v$. Solving the equations obtained implies that $\mathcal{A} = \mathcal{B}$, yielding our theorem.

We note that by the theorem of Harada [2], the case $q = 5$ may be excluded. Although the same procedure can be used in this case, for technical reasons which will become apparent in Section 4 and Section 7 considerably more calculation is involved. For these reasons we assume when necessary that $q \neq 5$.

1. General Results on Permutation Groups and Block Designs

If $G$ is a permutation group on a set $X$, and $B \subseteq G$, we shall use $F_B$ to denote the set of fixed points of $B$. If $Y \subseteq X$, $G_Y$ will mean the subgroup of $G$ fixing all points of $Y$. $G_Y^*$ will be the subgroup fixing the set $Y$. If $B \subseteq G_Y^*$, $R | Y$ will denote the permutation group obtained by restricting $B$ to $Y$.

In the following all groups and sets will be finite.

If $X$ is a set and $\mathcal{B}$ a family of subsets of $X$, we shall say that $\mathcal{B}$ is a block design on $X$ if the following conditions hold:

(i) If $B_1, B_2 \in \mathcal{B}$, $| B_1 | = | B_2 |$. 

O'NAN
(ii) Every two element subset of $X$ is contained in precisely one member of $\mathcal{B}$.

The elements of $\mathcal{B}$ are called blocks. We say that $\mathcal{B}$ is proper if for $B \in \mathcal{B}$, $2 < |B| < |X|$. If $\alpha \in X$, $\mathcal{B}_\alpha$ denotes the family of blocks of $\mathcal{B}$ which contains the point $\alpha$. $\mathcal{B}_\alpha'$ denotes the family of blocks of $\mathcal{B}$ which do not contain $\alpha$.

**Lemma 1.1.** Let $\mathcal{B}$ be a proper block design on $X$. Suppose $|X| = 1 + n$ and each block of $\mathcal{B}$ has $1 + s$ points. Then,

1. $\mathcal{B}$ has $(1 + n)n/(1 + s)s$ blocks.
2. Each point of $X$ is contained in exactly $n/s$ blocks.
3. $n \geq s + s^2$.

**Proof.** (i) Let $t$ be the number of blocks. Since $X$ has $1 + n$ points, there are $(1 + n)n/2$ two element subsets of $X$. Since each two element subset is contained in a unique block, and each block has $(1 + s)s/2$ two element subsets, $(1 + n)n/2 = (1 + s)s/2 \cdot t$, and (i) follows.

(ii) If $\beta \in X - \alpha$, $\beta$ lies in a unique block $B$ containing $\alpha$. Since $|X - \alpha| = n$ and $|B - \alpha| = s$, (ii) follows.

(iii) Since $\mathcal{B}$ is a proper block design, if $\alpha \in X$, there is some block $B$ not containing $\alpha$. Then each $\beta \in B$ belongs to a block $C$ containing $\alpha$ and $B \cap C = \{\beta\}$. Therefore, $|\mathcal{B}_\alpha| \geq |B|$; so $n/s \geq 1 + s$.

Two block designs $\mathcal{B}_1$ and $\mathcal{B}_2$ are isomorphic if there is a permutation $f$ of $X$ such that $f(B_1) \in \mathcal{B}_2$ if and only if $B_1 \in \mathcal{B}_1$. If $f(B) \in \mathcal{B}$ whenever $B \in \mathcal{B}$, we say $f$ is an automorphism of $\mathcal{B}$. We denote the group of all automorphisms of a block design $\mathcal{B}$ by $\text{aut}(\mathcal{B})$. If $G$ is a permutation group on $X$, we say that $G$ preserves $\mathcal{B}$ if $G \subseteq \text{aut}(\mathcal{B})$.

The concept of a local isomorphism will be useful in what follows. If $\mathcal{B}_1$ and $\mathcal{B}_2$ are block designs on $X$ and $\Delta$ is a block of both $\mathcal{B}_1$ and $\mathcal{B}_2$, we shall say that $\mathcal{B}_1$ and $\mathcal{B}_2$ are locally isomorphic around $\Delta$ if there is a permutation $f$ of $X$ such that

1. $f$ fixes all points of $\Delta$.
2. If $B_1 \in \mathcal{B}_1$ and $B_1 \cap \Delta \neq \phi$, then $f(B_1) \in \mathcal{B}_2$.
3. If $B_2 \in \mathcal{B}_2$ and $B_2 \cap \Delta \neq \phi$, then $f^{-1}(B_2) \in \mathcal{B}_1$.

We note that if $\Delta$ is a block of $\mathcal{B}_1$ and $\mathcal{B}_2$, two block designs on $X$, and if $f$ is a permutation satisfying (i) and (ii), then $f$ also satisfies (iii). Indeed, since $\mathcal{B}_1$ and $\mathcal{B}_2$ have a common block, the blocks of $\mathcal{B}_1$ are the same size as those of $\mathcal{B}_2$ and each point of $X$ is, by Lemma 1.1, contained in the same number of blocks in $\mathcal{B}_1$ and $\mathcal{B}_2$. Since $f$ carries $(\mathcal{B}_1)_\Delta$ in a one-one manner into $(\mathcal{B}_2)_\Delta$, (iii) follows.
We note:

**Lemma 1.2.** Let $G$ be a doubly-transitive group on $X$ preserving a block design $\mathcal{B}$. If $B \in \mathcal{B}$, $G_B^* \mid B$ is doubly-transitive.

Most frequently we shall obtain block designs from the following lemma.

**Lemma 1.3** (Witt, [9]). Let $G$ be a doubly-transitive group on a set $X$. Let $\alpha, \beta \in X$, and suppose $W$ is a weakly-closed subgroup of $G_{\alpha\beta}$, with $W \neq 1$. Then,

(i) $W$ has a unique conjugate $W_{\nu\delta}$ in $G_{\nu\delta}$, $\nu, \delta \in X$, $\nu \neq \delta$.

(ii) If $W$ fixes three or more points, the fixed point sets $F_{W_{\nu\delta}}$ form a proper block design on $X$.

(iii) If $\Delta = F_W$, $G_\alpha^* = N_G(W)$.

The following will prove to be of value.

**Lemma 1.4.** Let $G$ be a doubly-transitive group on a set $X$, $|X| = 1 + q$, with $q$ the power of some odd prime number. Suppose $\alpha, \beta \in X$, $\alpha \neq \beta$. Suppose $G_\alpha$ has a normal subgroup $Q_\alpha$, regular on $X - \alpha$ and $G_{\alpha\beta}$ is cyclic of order divisible by $q - 1$ and $(|G_{\alpha\beta}|, q) = 1$. Then,

(i) $|G_{\alpha\beta}| = q - 1$;

(ii) $G = \text{PGL}(2, q)$.

**Proof.** We prove that $G$ is a Zassenhaus group whose two-point stabilizer is of even order and invoke the classification of such Zassenhaus groups.

[10].

We begin by taking a chief series $Q_0 \subset Q_1 \subset \cdots \subset Q_k = Q_\alpha$, for $Q_\alpha$ and suppose $|Q_{i+1} : Q_i| = p^{a_i}$. Then $G_{\alpha\beta}$ acts irreducibly on $Q_{i+1}/Q_i$. Since $G_{\alpha\beta}$ is cyclic, it acts without fixed points on $Q_{i+1}/Q_i$, and thus, it induces on $Q_{i+1}/Q_i$ an automorphism group whose order divides $p^{a_i} - 1$. Since $(|G_{\alpha\beta}|, q) = 1$, if $f \in G_{\alpha\beta}$ centralizes each of the factor groups $Q_{i+1}/Q_i$, then $f = 1$. Therefore, $|G_{\alpha\beta}| = (p^{a_0} - 1) \cdots (p^{a_{k-1}} - 1)$, and $p^{a_0} \cdots p^{a_{k-1}} = q$. Since $q - 1$ divides $|G_{\alpha\beta}|$, it follows that $k = 1$ and $|G_{\alpha\beta}| = q - 1$. Thus, $G_{\alpha\beta}$ acts irreducibly on $Q_\alpha$ and thus without fixed points. By Zassenhaus [10], $G = \text{PGL}(2, q)$.

2. **Permutation Group Structure of $G$**

We assume that $G$ satisfies the hypotheses of our main theorem, i.e., $G$ is a doubly-transitive group on a set $X$, $|X| = 1 + q^3$, with $q = p^n$ and $p$ an odd prime. We take $\infty, 0 \in X, \infty \neq 0$, set $H = G_\infty$ and $K = G_0\infty$. 
A CHARACTERIZATION OF $U_d(q)$

$Q < H$ and $Q$ is regular on $X - \infty$. $K$ is cyclic of order $(q^2 - 1)/(q + 1, 3)$.
We let $j$ be the unique involution of $K$ and $j'$ be some conjugate of $j$ inter-changing 0 and \(\infty\). We set $\Delta = F_j$, $\Delta' = F_{j'}$, $W = G_\Delta$, and $W' = G_{\Delta'}$. We take $1 + s = |\Delta|$.

Since $Q$ is regular on $X - \infty$, we may identify $Q$ with $X - \infty$, $1 \in Q$ corresponding to $0 \in X - \infty$. Then the action of $K$ as an automorphism group of $Q$ corresponds to its action on $X - \infty$. We take $P = C_\Delta(j)$. Then $P$ is transitive on $\Delta - \infty$ and $s = p^a$ for some integer $a$, $a > 0$.

Since \(\langle j \rangle\) is weakly closed in $K$, the fixed point sets of conjugates of $j$, by Lemma 1.3, form a block design on $X$ which we call $\mathcal{B}$. Also, by Lemma 1.3, $C_\Delta(j) = G_\Delta = N_\Delta(W)$. We set $L = C_\Delta(j)$.

**Lemma 2.1.** If $M \subseteq K$ and $M$ fixes three or more points, then, with $\Gamma = F_M$,

(i) $N_\Delta(M) = G_{\Gamma^*}$ is doubly-transitive on $\Gamma$;

(ii) $N_\Delta(M) = C_\Delta(M)$;

(iii) $M \subseteq C_K(j')$.

**Proof.** (i) follows from Lemma 1.3(iii).
To prove (ii), note that $K \subseteq C_\Delta(M)$ and $N_H(M) = KN_\Delta(M)$. Since $Q < H$, $N_\Delta(M) = C_\Delta(M)$. Thus, $N_H(M) = C_H(M)$. Since aut($M$) is abelian, as $M$ is cyclic, and $|\Gamma| \geq 3$, $C_\Delta(M)/\Gamma \neq 1$. Thus, $C_\Delta(M)$ is transitive on $\Gamma$. Thus, $N_\Delta(M) = C_\Delta(M)$.

(iii). Since $j'$ interchanges 0 and $\infty$, $j'$ normalizes $K = G_{0,\infty}$. Since $K$ is cyclic, $j'$ normalizes $M$. Since $N_\Delta(M) = C_\Delta(M)$, by (ii), $j'$ centralizes $M$; so $M \subseteq C_K(j')$.

**Lemma 2.2.** $\Delta \cap \Delta' = \phi$.

**Proof.** Since $G_{\Delta^*} = C_\Delta(j)$, and $j' \in C_\Delta(j)$, $j'$ fixes $\Delta$. Since $j'$ is an involution and $|\Delta| = 1 + p^a$ is even, if $j'$ fixes one point on $\Delta$, it fixes at least two points on $\Delta$, and $|\Delta \cap \Delta'| \geq 2$. Since $\mathcal{B}$ is a block design, $\Delta, \Delta' \in \mathcal{B}$, $\Delta = \Delta'$. Then $j'$ fixes 0 and $\infty$, contrary to its definition. Therefore, $j'$ fixes no points of $\Delta$ and $F_{j'} \cap \Delta = \Delta' \cap \Delta = \phi$.

**Lemma 2.3.** $\langle K, j' \rangle - K$ has one $K$-class of involutions if the Sylow 2-subgroups of $\langle K, j' \rangle$ are quasi-dihedral or modular. $\langle K, j' \rangle - K$ has two $K$-classes of involutions if the Sylow 2-subgroups of $\langle K, j' \rangle$ are abelian or dihedral.

**Proof.** This follows readily from the classification of 2-groups having a cyclic subgroup of index 2.
Henceforth, we let $\epsilon$ be the number of $K$-classes of involutions in $\langle K, j' \rangle - K$ fused to $j$ in $G$. By Lemma 2.3, $\epsilon = 1$ or $2$.

**Lemma 2.4.** $q^3 = s + \epsilon s(1 + s) | K | | C_K(j')|.$

**Proof.** To prove this we count the number of conjugates of $j$ in $G, H$, and $G - H$. Since $|G| = (1 + q^3)q^3 | K |$, $|C_G(j)| = (1 + s)s | K |$, $|H| = q^3 | K |$, and $|C_H(j)| = s | K |$, $j$ has $(1 + q^3)q^3/s(1 + s)$ conjugates in $G$ and $q^3/s$ conjugates in $H$. Now each conjugate of $j$ in $G - H$ is the conjugate under $H$ of some involution $t$ interchanging 0 and 00. Since $C_H(t) = C_K(t) = C_K(j')$, $t$ has $q^3 | K | | C_K(j')|$ $H$-conjugates in $G - H$. Thus, $j$ has $\epsilon q^3 | K | | C_K(j')|$ conjugates in $G - H$. Then, $(1 + q^3)q^3/s(1 + s) = q^3/s + \epsilon q^3 | K | | C_K(j')|$ implies (i).

**Lemma 2.5.** $\epsilon$ is the number of orbits of $H$ on the blocks of $\mathcal{B}_\alpha'$.

**Proof.** The involutions of $G - H$ conjugate to $j$ are in a natural one-one correspondence with the blocks of $\mathcal{B}_\alpha'$. Conjugation of involutions under $H$ corresponds to translation of blocks. Since there are $\epsilon H$-classes of involutions in $G - H$ fused to $j$, there are $\epsilon$ orbits of $H$ on $\mathcal{B}_\alpha'$.

**Corollary.** The stabilizer in $H$ of a block of $\mathcal{B}_\alpha'$ is a conjugate of $C_K(j')$.

**Lemma 2.6.** $s = q$.

**Proof.** By Lemma 2.3, $q^3 = s + \epsilon s(1 + s) | K | | C_K(j')|$ with $\epsilon = 1$ or $2$. Thus, $(1 + s) | (1 + q^3)$. Since $s = p^\alpha$ and $q^3 = p^{3n}$, $\alpha | 3n$. If $\alpha > n$, then $\alpha = (3n)/2$. Then, $q^3 = s^2$, in contradiction to Lemma 1.1(iii).

Thus, $\alpha \leq n$. Suppose that $\alpha < n$. Let $d = |K| | C_K(t)|$. Then, $q^3 = s + \epsilon s(1 + s)d$, so $d | (q^3 - s)$. Also, $d | | K |$, so $d | (q^2 - 1)$. Therefore, $d | (q - s)$. Since $q - s = p^\alpha - p^\alpha$ and $(p, d) = 1$, $d | (p^{n-\alpha} - 1)$. Since $\alpha < n$, $d < q - 1$. Also, $s \leq q/p$.

Thus, $q^3 < q/p + \epsilon(q/p)(q/p + 1)(q - 1) < 3(q/p)(q^2 - 1)$, as $\epsilon = 1$ or $2$. Thus, $3q/p < (3/p - 1)q^3$. So $3/p - 1 > 0$, or $p < 3$, a contradiction. It follows that $s = q$.

**Lemma 2.7.** $W$ is semiregular on $X - \Delta$.

**Proof.** Suppose $U \subseteq W$, $U \neq 1$, fixes $v \in X - \Delta$ and set $\Gamma = F_U$. Then, the translates of $\Delta$ form a block design on $\Gamma$, so by Lemma 1.1(iii), $|\Gamma| - 1 \geq q + q^2$. Also, the translates of $\Gamma$ form a block design on $X$, so $q^3 \geq (|\Gamma| - 1)(|\Gamma| - 1)^2$. Then, $q^3 \geq q^4$, a contradiction.

**Lemma 2.8.** $|W| \geq (q + 1)/(q + 1, 3)$. 
Proof. By Lemma 2.1(iii), $W \subseteq C_K(j')$. Thus $W$ fixes the set $\Delta'$. By Lemma 2.2 $\Delta \cap \Delta' = \emptyset$. Since $W$ is semiregular on $X - \Delta$, by Lemma 2.7, $| W | \mid | \Delta' |$. By Lemma 2.6, $| W | \mid (1 + q)$. Since also

$$| W | \mid (q^2 - 1)/(q + 1, 3), \quad | W | \mid (q + 1)/(q + 1, 3).$$

LEMMA 2.9. $L \mid \Delta = PGL(2, q), | W | = (q + 1)/(q + 1, 3)$.

Proof. $L \mid \Delta$ is a doubly-transitive group satisfying the hypotheses of Lemma 1.4. It follows then that $L \mid \Delta = PGL(2, q)$ and $| K \mid \Delta | = q - 1$. Since $W = G_{\Delta}$, $| W | = (q + 1)/(q + 1, 3)$.

LEMMA 2.10. $W = C_K(j')$.

Proof. Since, by Lemma 2.9, $j'$ inverts $K/W$, $| C_K(j') : W | \leq 2$. Also $C_K(j')$ fixes $\Delta'$ and $\Delta \cap \Delta' = \emptyset$.

We claim $C_K(j') \mid \Delta'$ is semiregular.

Indeed, if this is not the case, some element $f \in C_K(j')$ of prime order fixes some point in $\Delta'$. However, $W$ contains all elements of prime order of $C_K(j')$ and $W$ is semiregular on $\Delta' \subset X - \Delta$, by Lemma 2.7. Thus, $C_K(j') \mid \Delta'$ is, in fact, semiregular.

Therefore, $| C_K(j') | \mid | \Delta' |$. Thus, $| C_K(j') | \mid (1 + q)$. Since also

$$| C_K(j') | \mid (q^2 - 1)/(q + 1, 3), \quad | C_K(j') | \mid (1 + q)/(q + 1, 3).$$

Since $K$ is cyclic, $C_K(j') \subseteq W$.

LEMMA 2.11. $K$ is semiregular on $X - \Delta$.

Proof. Suppose $U \subset K$ fixes $v \in X - \Delta$. By Lemma 2.1(iii), $U \subset C_K(j')$. By Lemma 2.10, $C_K(j') = W$, and $W$ is, by Lemma 2.7, semiregular on $X - \Delta$. Therefore, $U = 1$.

LEMMA 2.12. If $q = 1 (\text{mod } 4)$, a Sylow 2-subgroup of $\langle K, j' \rangle$ is a Sylow 2-subgroup of $G$ and is quasi-dihedral.

Proof. $| G : \langle K, j' \rangle | = (1 + q^2)q^3/2 \equiv 1 (\text{mod } 2)$, if $q = 1 (\text{mod } 4)$. Thus, a Sylow 2-subgroup of $\langle K, j' \rangle$ is a Sylow 2-subgroup of $G$.

Since $\langle K, j' \rangle \mid \Delta$ is dihedral of order divisible by 8, a Sylow 2-subgroup of $\langle K, j' \rangle$ is dihedral or quasi-dihedral.

By Schur [7], $[L, L]$ is PSL(2, $q$) or SL(2, $q$), and if $[L, L]$ is PSL(2, $q$), $L$ has a subgroup of index 2 isomorphic to PSL(2, $q$) × $W$. In this case, $G$ is not of 2-rank 2, in contradiction to the previous paragraph. Thus, $[L, L]$ is SL(2, $q$) and the Sylow 2-subgroup of $G$ contains a generalized quaternion subgroup. Therefore, it is quasi-dihedral.
Lemma 2.14. If $q = 3 \pmod{4}$, the Sylow 2-subgroup of $\langle K, t \rangle$ is modular and the Sylow 2-subgroup of $G$ is wreathed, i.e., $\mathbb{Z}_q \wr \mathbb{Z}_2$, where $2'$ is the 2-part of $q + 1$.

Proof. Since $C_K(j') = W$, the Sylow 2-subgroup of $\langle K, j' \rangle$ is modular. Since $|G| = (1 + q^3)q^q(q^q - 1)(q + 1, 3)$, the Sylow 2-subgroup of $G$ is of order $2^{2f+1}$. Let $a$ generate the Sylow 2-subgroup of $W$, $b$, the Sylow 2-subgroup of $W'$. Then, $|a| = |b| = 2'$.

Since $j \in C_G(j')$, by Lemma 2.1, $j \in C_G(W')$. Thus, $W' \subseteq C_G(j) = C_G(W)$. Since $\Delta \cap \Delta' = \phi$, by Lemma 2.2, and $W$ is semiregular on $X - \Delta$, by Lemma 2.7, $W \cap W' = 1$. Thus, $\langle a, b \rangle$ is an abelian subgroup of type $(2', 2')$.

Since $L \mid \Delta = \text{PGL}(2, q)$, $b \mid \Delta$ is inverted by some fix-point free involution $d$ of $L \mid \Delta$. Since all fix-point free involutions of $\text{PGL}(2, q)$ are conjugate and $j' \mid \Delta$ is fix-point free, there is some involution $c \in G$ such that $c \mid \Delta = d$. Then, $cac^{-1} = a$ and $cbc^{-1} = b^{-1}a^\alpha$, for some integer $\alpha$.

We claim: $\alpha$ is odd.

For suppose $\alpha$ is even. Then $(a^\alpha b^\nu)^{2'} = 1$ and $(a^\alpha b^\nu c)(a^\alpha b^\nu c) = a^{2\nu + \alpha}$; so $(a^\alpha b^\nu c)^{2'} = 1$. Thus, the Sylow 2-subgroup of $G$ is of exponent $2'$, in contradiction to the fact that $K$ has an element of order $2^{f+1}$. Thus, $\alpha$ is odd.

Then, $\langle a, b, c \rangle = \langle b, b^{-1}a^\nu, c \rangle$ is $\mathbb{Z}_q \wr \mathbb{Z}_2$.

Lemma 2.15. $e = 1$ and $G$ has a single class of involutions.

Proof. From Lemmas 2.13 and 2.14, $\langle K, j' \rangle - K$ has a single $K$-class of involutions.

Lemma 2.16. $[L, L] = \text{SL}(2, q)$.

Proof. By Schur [7], $[L, L] = \text{SL}(2, q)$ or $\text{PSL}(2, q)$. In the last case, $L$ has a subgroup of index 2 isomorphic to $\text{PSL}(2, q) \times W$. Then, $G$ is not of 2-rank 2, in contradiction to Lemmas 2.14 and 2.15.

Lemma 2.17. $L$ is transitive on $X - \Delta$.

Proof. Let $\nu \in X - \Delta$ and set $M = L_\nu$. Then $M$ fixes a block $\Delta$ and a point $\nu$ off $\Delta$. By the corollary to Lemma 2.5, $M$ is conjugate to $C_K(j') = W$, (by Lemma 2.10). Since $|L : M| = |L : W| = q^q - q = |X - \Delta|$, $L$ is transitive on $X - \Delta$.

Lemma 2.18. $[L, L]$ is regular on $X - \Delta$.

Proof. Let $\nu \in X - \Delta$ and set $M = L_\nu$. Since $|[L, L]| = q^q - q = |X - \Delta|$, it suffices to show that $L_\nu \cap [L, L] = 1$. As in Lemma 2.17, $L_\nu$ is conjugate to $W$ in $G$. 
By Lemma 2.1, if $R \subseteq L_r$, $N_0(R) = C_0(R)$. Now, as $[L, L] = \text{SL}(2, q)$, any element of $[L, L]$ of order dividing $q + 1$ is inverted by some element of $[L, L]$. It follows that $L_r \cap [L, L] \subseteq \langle j \rangle$. Also, $j$ fixes no elements of $X - \Delta$, so $L_r \cap [L, L] = 1$.

**Lemma 2.19.** $H$ is transitive on $B_\infty'$. 

*Proof.* This is immediate from Lemmas 2.5 and 2.15.

**Lemma 2.20.** $X - \Delta$ is the disjoint union of blocks fixed by $W$.

*Proof.* Using Lemma 2.19, we consider $H$ as a transitive permutation group on $B_\infty'$. By the corollary to Lemma 2.5 and Lemma 2.10, $W$ is the stabilizer in $H$ of a block $B \in B_\infty'$. Then, the number of blocks of $B_\infty'$ fixed by $W$ is $|N_H(W) : W| = q(q - 1)$.

We claim: if $j$ fixes a block $B$ of $B_\infty'$, $j$ fixes no points on $B$. Indeed, suppose $j$ fixes $v \in B$. Since $|B|$ is even, $j$ fixes two points of $B$. Since $\Delta = F_j$ is a block and $|\Delta \cap B| \geq 2$, $B = \Delta$. Therefore, $\infty \in B$, in contradiction to $B \in B_\infty'$.

We also claim: if $B_1$ and $B_2$ are distinct blocks of $B_\infty'$ fixed by $j$, $B_1 \cap B_2 = \emptyset$. Indeed, since $B_1$ and $B_2$ are distinct, $|B_1 \cap B_2| = 1$. Since $j$ fixes $B_1$ and $B_2$, $j$ fixes $B_1 \cap B_2$. Since $j$ fixes no points on $B_1$, by the previous paragraph, $B_1 \cap B_2 = \emptyset$.

Since $j \in W$, the $q(q - 1)$ blocks of $B_\infty'$ fixed by $W$ are pairwise disjoint and contained in $X - \Delta$. Since each block has $1 + q$ points and $|X - \Delta| = q^3 - q$, $X - \Delta$ is the disjoint union of these blocks.

### 3. Structure of $H$

In this section we determine explicitly the structure of $H$. Recall that $P = C_Q(j) = C_Q(W)$. Since $K$ is semiregular on $X - \Delta$ (Lemma 2.11), $K$ is semiregular on $Q - P$. Also, by Lemma 2.9, $K/W$ acts transitively and without fixed points on $P - 1$. It follows that $P$ is elementary abelian of order $q$.

**Lemma 3.1.** $P \subseteq Z(Q)$.

*Proof.* Suppose $P \nsubseteq Z(Q)$. Since $K$ acts transitively on $P - 1$, $P \cap Z(Q) = 1$. Since $K$ is semiregular on $Q - P$, $K$ is semiregular on $Z(Q)$. Since $|P| = q$, $|Q| = q^3$, $|Z(Q)| \leq q^2$. Since $|K| = (q^3 - 1)/(q + 1, 3)$, $|Z(Q)| = q^2$. Since $P$ is abelian and $P \cdot Z(Q) = Q$, $Q$ is abelian, contrary to $P \nsubseteq Z(Q)$. Therefore, $P \subseteq Z(Q)$. 

481/22/2-5
Lemma 3.2. Either $Q$ is abelian, or $P = Z(Q) = [Q, Q] = \Phi(Q)$, and $P$ is a maximal characteristic subgroup of $Q$.

Proof. Since $P \subseteq Z(Q)$, $P \triangleleft Q$ and $|Q/P| = q^2$. Since $K$ is semiregular on $Q - P$, $K$ acts without fixed points on $Q/P$. Since $|K| = (q^2 - 1)/(q + 1, 3)$, $K$ acts irreducibly on $Q/P$. Thus, if $Q$ is not abelian, $P = Z(Q)$ and $P$ is maximal characteristic. Since $Q/P$ is elementary abelian, the remaining statements follow.

Lemma 3.3. $Q$ is of exponent $p$.

Proof. Since $P$ is elementary abelian, $P \subseteq \Omega_1(Q)$. Since $P$ is maximal characteristic, either $P = \Omega_1(Q)$ or $\Omega_2(Q) = Q$. Since $Q$ is a $p$-group of class two, $p$ odd, in the latter case $Q$ is of exponent $p$.

Consider then the mapping $\sigma$, with $\sigma(x) = x^p$. Since $Q$ is a $p$-group of class two, $p$ odd, $\sigma$ is a homomorphism, [1, p. 183]. Since $Q/P$ is elementary abelian, $\sigma$ is a homomorphism from $Q$ into $P$. Since $|Q| = q^3$, $|P| = q$, $P \subseteq \ker \sigma$. Thus, $P \subseteq \Omega_1(Q)$. Therefore, $Q = \Omega_1(Q)$.

We now take $F$ a field with $q$ elements, $E$, a quadratic extension of $F$. Then, $E$ has $q^2$ elements and an automorphism $x \rightarrow x^a - x$. $F$ is the field of fixed elements of this automorphism.

Lemma 3.4. If $Q$ is abelian, we may take $Q$ to be $E \oplus F$ (considered as an additive group) and describe the action of $K$ on $Q$ as follows. There is a \( \lambda \in E \), \( |\lambda| = (q^2 - 1)/(q + 1, 3) \), and an integer \( \ell \), \( (\ell, q - 1) = 1 \), such that $K = \langle k_\lambda \rangle$, where

\[
(x, y) \xrightarrow{k_\lambda} (\lambda x, (\lambda^\ell)y), \quad x \in E, \quad y \in F.
\]

Proof. Since $Q$ is abelian and $(|K|, p) = 1$, by Maschke's theorem, $Q = P \oplus R$, where $R$ is a $K$-invariant complement to $P$. Since $K$ acts semiregularly on $Q - P$, $K$ acts semiregularly on $R - 1$. Since $|R| = q^2$, $K$ acts irreducibly on $R$. Since $K$ is cyclic, its action on $P$ and $R$ is given by a field multiplication. We may then identify $R$ with $E$, $P$ with $F$, and the action with the one given.

We now consider the case in which $Q$ is nonabelian. Since $|Q/P| = q^2$, we may identify $Q/P$ with $E$. Likewise, we may identify $P$ with $F$. Since $K$ acts without fixed points and irreducibly on $Q/P$, there is a $\lambda \in E$, \( |\lambda| = (q^2 - 1)/(q + 1, 3) \), such that $K = \langle k_\lambda \rangle$ and $k_\lambda$ induces on $Q/P$ the automorphism $x \rightarrow \lambda x$. There is also a $\zeta \in F$ with $k_\lambda$ inducing on $P$ the automorphism $x \rightarrow \zeta x$. Then we may take as $Q$, the ordered pairs, $(x, y)$, $x \in E$ and $y \in F$. 
Since $Q$ is a class two group of exponent $p$, there is an alternate biadditive function $b : E \times E \to F$ such that

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + b(x_1, x_2)).$$

From the action of $K$ on $Q$, it follows that $b(\lambda x_1, \lambda x_2) = \zeta b(x_1, x_2)$. Therefore, we determine the alternate bi-additive functions $b$ from $E \times E$ into $F$, satisfying $b(\lambda x_1, \lambda x_2) = \zeta b(x_1, x_2)$, for $\lambda \in E$, $|\lambda| = |K|$, $\zeta \in F$, $|\zeta| = q - 1$.

We begin by studying the space of all such bilinear functions. We let $I$ be the vector space over $E$ of all alternate bi-additive functions from $E \times E$ into $E$. Let $I^*$ denote the vector space over the prime field $Z_p$ of all alternate bi-additive functions from $E \times E$ into $Z_p$. Clearly, $I = E \otimes Z_p, I^*$. Also, by [3, p. 221], the dimension of $I$ as a vector space over $E$ is just the dimension of $I^*$ as a vector space over $Z_p$.

**Lemma 3.5.** $\dim_{E}(I) = (2n)(2n - 1)/2$.

**Proof.** Since $|E| = q^2 = p^{2n}$, $\dim_{Z_p}(E) = 2n$. Then, by [5, p. 426], the dimension of the space of alternate bilinear functions from $E \times E$ into $Z_p$ is $(2n)(2n - 1)/2$. By the remark preceding the lemma, the result follows.

We now take a certain basis for $I$. If $\phi, \psi \in \text{aut}(E)$, we define an alternate bi-additive function $\tau_{\phi, \psi}$ from $E \times E$ into $E$ as follows: $\tau_{\phi, \psi}(x_1, x_2) = \phi(x_1) \psi(x_2) - \psi(x_1) \phi(x_2)$, $(x_1, x_2) \in E \times E$. Then, $\tau_{\phi, \psi} = 0$ and $\tau_{\phi, \psi} = -\tau_{\psi, \phi}$.

From the two ordered pairs $(\phi, \psi)$, $(\psi, \phi)$, $\phi \neq \psi$, $\phi, \psi \in \text{aut}(E)$, we pick one ordered pair and collect our choices into an index set $I$. We intend to show that the set $\{\tau_{\phi, \psi}\}_{(\phi, \psi) \in I}$ forms a basis for $I$. This will follow from:

**Lemma 3.6.** The family of functions $\{\sigma_{\phi, \psi}\}_{(\phi, \psi) \in \text{aut}(E) \times \text{aut}(E)}$, where

$$\sigma_{\phi, \psi}(x_1, x_2) = \phi(x_1) \psi(x_2), \quad (x_1, x_2) \in E \times E,$$

is a linearly independent set of functions from $E \times E$ into $E$.

**Proof.** Suppose there are scalars $\alpha_{\phi, \psi} \in E$, such that $\sum_{(\phi, \psi)} \alpha_{\phi, \psi} \sigma_{\phi, \psi} = 0$. Fix $x_1 \in E$. Then, for all $x_2 \in E$,

$$\sum_{\phi} \left(\sum_{\psi} \alpha_{\phi, \psi} \phi(x_1)\right) \psi(x_2) = 0.$$

We now use a theorem of Dedekind [4]: If $E$ is a field, $\psi_1, \psi_2, ..., \psi_k$ distinct automorphisms of $E$, then $\psi_1, \psi_2, ..., \psi_k$ are linearly independent as functions from $E$ into $E$. 
From this theorem, then, it follows,

$$\sum_{\phi} \alpha_{\phi, \psi} \phi(x_1) = 0$$

for all $x_1 \in E$ and all $\psi \in \text{aut}(E)$.

Applying the theorem again, we find that $\alpha_{\phi, \psi} = 0$ for all

$$(\phi, \psi) \in \text{aut}(E) \times \text{aut}(E),$$

and Lemma 3.6 follows.

**Lemma 3.7.** The family of functions $\{\tau_{\phi, \psi}\}_{(\phi, \psi) \in I}$ is a basis for $\Gamma$.

**Proof.** From Lemma 3.6 and the fact that $\tau_{\phi, \psi} = \sigma_{\phi, \psi} - \sigma_{\phi, \psi}$, it follows that the functions $\tau_{\phi, \psi}$, $(\phi, \psi) \in I$, are linearly independent. Since there $(2n)(2n - 1)/2$ such functions and $\dim_{\mathbb{F}}(\Gamma) = (2n)(2n - 1)/2$, the result follows.

**Lemma 3.8.** Let $p$ be an odd prime, $s$, $r$, and $n$ integers, satisfying $0 < s < r < 2n$.

If $(1 + p^n)/(1 + p^n, 3) \mid p^n + p^r$, then $r = n + s$.

**Proof.** If $n = 1$, $0 < s < r < 2$, so we must have $s = 0$ and $r = 1$, and the result follows. Accordingly, we assume $n > 1$.

From the hypothesis, it follows that $(1 + p^n)/(1 + p^n, 3) \mid (1 + p^{r-s})$. It is readily shown that $(1 + p^n)/(1 + p^n, 3) > 1 + p^{s-1}$, and so $n < r - s$. By hypothesis, $0 < s < r < 2n$, and so $r - s < 2n$. Setting $t = r - s$, $n < t < 2n$.

If $t > n$, we have

$$\frac{1 + p^n}{(1 + p^n, 3)} \mid (p^t - p^n)$$

and so

$$\frac{1 + p^n}{(1 + p^n, 3)} \mid (p^{t-n} - 1),$$

with $0 < t - n < n$, a contradiction. Thus, $t = n$.

We can now prove:

**Lemma 3.9.** Let $b(\ , \ )$ be an alternate, nondegenerate, biadditive function from $E \times E$ into $E$. Suppose that $b(\lambda x_1, \lambda x_2) = \zeta b(x_1, x_2)$, where $\lambda \in E$, $|\lambda| = (q^a - 1)/(q + 1, 3)$, $\zeta \in F$, $|\zeta| = q - 1$. Then, there is a $\theta \in \text{aut}(E)$ and $\delta \in F$, such that $b(x_1, x_2) = \delta b(x_1 x_2, x_1 x_2)$.

**Proof.** By Lemma 3.7 there are $m_{\phi, \psi} \in E$, such that $b(x_1, x_2) = \sum m_{\phi, \psi}(\phi(x_1) \psi(x_2) - \phi(x_2) \psi(x_1))$, for all $(x_1, x_2) \in E \times E$. Since

$$b(\lambda x_1, \lambda x_2) = \zeta b(x_1, x_2), \quad \phi(\lambda) \psi(\lambda)m_{\phi, \psi} = \zeta m_{\phi, \psi}.$$

Since $b$ is nonzero, for some $(\phi, \psi)$, $m_{\phi, \psi} \neq 0$, and so $\phi(\lambda) \psi(\lambda) = \zeta$. Then,
there are integers $0 \leq s < r < 2n$, such that $\phi(x) = x^{p^s}$, $\psi(x) = x^{p^r}$, $s < r$, since $\phi \neq \psi$. Then $\lambda^{p^s + p^r} = \zeta$. Thus, $\lambda^{(q-1)(p^s + p^r)} = 1$. It follows that $(p^n + 1)(p^n + 1, 3) | p^r + p^s$. By Lemma 3.8, $r = n + s$. Thus, $\psi(x) = \phi(x)$.

Thus, $\phi(x_1)\psi(x_2) - \phi(x_2)\psi(x_1) = \phi(x_1 x_2 - x_1 x_2)$. Thus, $\psi(x_1) = \phi(x_2)$.

Thus, $b(x_1, x_2) = \sum m_\phi(x_1 x_2 - x_1 x_2)$, for $m_\phi \in E$, $\phi \in \text{aut}(E)$. If $m_\phi \neq 0$, then $\phi(\lambda) = \zeta$. If $m_\phi \neq 0$ as well, then $(\psi^{-1}\phi')(\zeta) = \zeta$. Since $\zeta$ generates $F$, $\phi | F = \psi | F$. Thus, either $\phi = \psi$ or $\phi(x) = \phi(x)$. In any case, it follows that

$$b(x_1, x_2) = \delta\theta(x_1 x_2 - x_1 x_2), \quad \text{for some } \theta \in \text{aut}(E), \quad \delta \in E.$$ 

**Corollary.** Let $b(\cdot, \cdot)$ be an alternate, nondegenerate biadditive function from $E \times E$ into $F$, satisfying the hypotheses of Lemma 3.9. Then, there is a $\theta \in \text{aut}(E)$ and $\delta \in E$ with $\delta = -\delta$, such that $b(x_1, x_2) = \delta\theta(x_1 x_2 - x_1 x_2)$.

**Proof.** By Lemma 3.9, $b(x_1, x_2) = \delta\theta(x_1 x_2 - x_1 x_2)$ for some $\delta \in E$. Since $b(x_1, x_2) \in F$ and $b$ is nondegenerate, there is some $(x_1, x_2) \in E \times E$ such that $b(x_1, x_2)$ is a nonzero element of $F$. Then, $\delta\theta(x_1 x_2 - x_1 x_2) = \delta\theta(x_1 x_2 - x_1 x_2)$. Thus, $\delta = -\delta$.

We have now determined all possibilities for the form $b(\cdot, \cdot)$. We show that the groups $Q$ which the various forms give rise to are isomorphic.

**Lemma 3.10.** Let $\theta$ be an automorphism of the field $F$, $e_1, e_2 \in E$, $\tilde{e}_1 = -e_1$, $\tilde{e}_2 = -e_2$. Let $b(x_1, x_2) = e_1(x_1 x_2 - x_1 x_2)$ and $b'(x_1, x_2) = \theta(e_2(x_1 x_2 - x_1 x_2))$.

Let $Q$ be the group with the multiplication rule

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 + y_2 + b(x_1, x_2)),$$

and $Q'$ be the group with the multiplication rule

$$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 + y_2 + b'(x_1, x_2)).$$

Then, $Q_1$ and $Q'$ are isomorphic.

**Proof.** Choose $\mu \in E$ so that $\mu\tilde{e}_1 = e_1/\theta(e_2)$. As noted in [6], Lemma 3.8, this is possible if $e_1/\theta(e_2) \in F$. However, $e_1/\theta(e_2)$ does belong to $F$, for $e_1/\theta(e_2) = \tilde{e}_1/\theta(e_2) = -e_1/\theta(e_2) = e_1/\theta(e_2)$.

Now, consider the mapping $\tau : Q \rightarrow Q'$, defined by $\tau((x, y)) = (\theta^{-1}(\mu x), y)$. One verifies that $b(x_1, x_2) = b'(\theta^{-1}(\mu x_1), \theta^{-1}(\mu x_2))$. From this it follows that $\tau$ is an isomorphism.

It follows therefore that if $Q$ is not abelian, its structure is uniquely determined. Moreover, as $b(\lambda x_1, \lambda x_2) = \zeta b(x_1, x_2)$ implies $\lambda \tilde{\lambda} = \zeta$, the action of $K$ on $Q$ is uniquely determined. It follows from [6], Section 1, that $\Omega K$ is isomorphic to the subgroup fixing a point in $U_d(q)$. 

4. **Action of \( H \) on \( \mathcal{B} \)**

We retain the notation of earlier sections.

**Lemma 4.1.** Let \( N \) be a subgroup of \( H \) of order \( q \mid K \). Then, \( N \) is conjugate in \( H \) to \( PK \).

**Proof.** By replacing \( N \) by one of its conjugates in \( H \), if necessary, we may assume \( K \subset N \). Then, the Sylow \( p \)-subgroup \( P' \) of \( N \) is of order \( q \), and \( P' = N \cap Q \). Thus, \( P' \triangleleft N \). Since \( K \) is semiregular on \( Q \) and \( P' \) is a \( K \)-invariant subgroup of order less than \( |K| \), \( P' = P \).

**Lemma 4.2.** The following statements are equivalent.

(i) \( B \in \mathcal{B}_\infty \).

(ii) \( B \) is the union of \( \infty \) and an orbit of \( P \).

(iii) \( B = \infty \cup hP, h \in Q \).

**Proof.** It is clear that (ii) and (iii) are equivalent, since by Lemma 3.1, \( P \subset Z(Q) \) and \( Q \) is regular on \( X - \infty \).

We show that (i) implies (ii). Since \( H \) is transitive on \( X - \infty \), \( H \) is transitive on \( \mathcal{B}_\infty \). By Lemma 1.1(ii) and Lemma 2.6, \( |\mathcal{B}_\infty| = q^2 \). It follows that the stabilizer in \( H \) of some block \( B \in \mathcal{B}_\infty \) is of order \( q \mid K \). By Lemma 4.1, then, \( P \cdot K \) fixes some block of \( \mathcal{B}_\infty \). Since \( P \triangleleft H \), \( P \) fixes all blocks of \( \mathcal{B}_\infty \). By Lemma 2.6 each block has \( 1 + q \) points and all orbits of \( P \) are of length \( q \). Thus, each block is the union of \( \infty \) and an orbit of \( P \).

Since \( |\mathcal{B}_\infty| = q^2 \) and \( P \) has \( q^2 \) orbits on \( X - \infty \), (ii) implies (i).

**Lemma 4.3.**

(i) \( H \) is transitive on \( \mathcal{B}_\infty' \).

(ii) The stabilizer in \( H \) of a block of \( \mathcal{B}_\infty' \) is a conjugate in \( H \) of \( W \).

(iii) \( X - \Delta \) is the disjoint union of blocks fixed by \( W \) and \( W \) is semiregular on each of these fixed blocks.

This lemma is merely a restatement of Lemmas 2.7, 2.19, and 2.20.

In the remainder of this paper \( \omega \) is a primitive \((q + 1)\)-st root of unity in \( E \). Then, \( \omega \bar{\omega} = 1 \).

**Lemma 4.4.** \( Q \) is not abelian.

**Proof.** By the theorem of Harada, [2], we may assume that \( q \neq 5 \).

We treat two cases according as \( q + 1 \equiv 0 \pmod{3} \) or \( q + 1 \equiv 0 \pmod{3} \).

By Lemma 3.4, \( Q = E \oplus F \) and the action of \( K \) on \( Q \) is given by \((x, y) \rightarrow \lambda x, (\lambda x, y) \), \( x \in E, y \in F, (\ell, q - 1), \lambda \in E, \) and

\[
|\lambda| = (q^2 - 1)/(q + 1, 3).
\]
First, suppose \( q + 1 \neq 0 \) (mod 3). Let \( A \) be a block of \( B_\infty \) containing \((1,0)\in O\) and fixed by \( W \). By Lemma 4.3(iii), such a block exists. Since \((q + 1, 3) = 1\), \(|W| = q + 1\). \( W \) is generated by the transformation \( k_\omega, (x,y) \rightarrow k_\omega (\omega x, y) \), with \( \omega \), a primitive \((q + 1)\)-st root of unity. Since \((1,0)\in A, (\omega^i,0)\in A\), for all integers \( i \). Since \(|A| = q + 1\),

\[
A = \{(\omega^i,0) : 0 \leq i \leq q\}.
\]

We apply to \( A \) the transformation \( k_{(1+\omega)} \). Since \(|\lambda| = q^2 - 1\), \( 1 + \omega \in \langle \lambda \rangle \), and the transformation \( k_{(1+\omega)} \in K \). Thus, \( \{(\omega^i + \omega^{i+1},0) : 0 \leq i \leq q\} \) is a block. Translating by \((-\omega,0)\in O\), we obtain the block

\[
B = \{(\omega^i + \omega^{i+1} - \omega,0) : 0 \leq i \leq q\}.
\]

Then, \((1,0)\in B\) and \((\omega^i,0)\in B\). Thus, \( A = B \). It follows that the transformation \((-\omega,0)k_{(1+\omega)}\) fixes \( A \). Since \( W \) is the subgroup of \( H \) fixing \( A \) and \((-\omega,0)k_{(1+\omega)} \notin W \), this is impossible. Thus, \( Q \) cannot be abelian.

Next, suppose \( q + 1 \equiv 0 \) (mod 3). The procedure in this case is basically the same. Let \( A \) be a block of \( B_\infty \) containing \((1,0)\in Q\) and fixed by \( W \). Since \((q + 1, 3) = 3\), \(|W| = (q + 1)/3\). \( W \) is generated by the transformation \( k_\omega, (x,y) \rightarrow k_\omega (\omega x, y) \). Since \((1,0)\in A\), \((\omega^{3i},0)\in A\), for all integers \( i \). Thus, \( \{(\omega^{3i},0) : 0 \leq i < (q + 1)/3\} \subseteq A \).

We apply to \( A \) the transformation \( k_{(1+\omega^3)} \), where

\[
(x,y) \rightarrow ((1 + \omega^3)x, (1 + \omega^3)(1 + \omega^3)^i y).
\]

To do this, we must first show that \( k_{(1+\omega^3)} \in K \), i.e., \( 1 + \omega^3 \in \langle \lambda \rangle \), if \(|\lambda| = (q^2 - 1)/3\). It suffices to show that \( (1 + \omega^3)^{(q^2-1)/3} = 1 \).

Now

\[
(1 + \omega^3)^{(q^2-1)/3} = ((1 + \omega^3)^{(q-1)/3})^{(q+1)/3} = \left(1 + \omega^6\right)^{(q+1)/3} = (\omega^3)^{(q+1)/3} = 1.
\]

Therefore, \( \{(\omega^{3i} + \omega^{3i+3},0) : 0 \leq i < (q + 1)/3\} \) is contained in the block \( k_{(1+\omega^3)}(A) \). Translating by \((-\omega^3,0)\), we find that \((-\omega^3,0)k_{(1+\omega^3)}(A) \) is a block containing the set \( \{(\omega^{3i} + \omega^{3i+3} - \omega^3,0) : 0 \leq i < (q + 1)/3\} \). It follows that this block contains \((1,0)\) and \((\omega^6,0)\). If \( q \neq 5 \), as we are assuming, \( \omega^6 \neq 1 \). Thus \((-\omega^3,0)k_{(1+\omega^3)}(A) = A \), since the two blocks contain in common the points \((1,0)\) and \((\omega^6,0)\). Since \((-\omega^3,0)k_{(1+\omega^3)} \notin W \), and \( W \) is the subgroup fixing \( A \), a contradiction results. Therefore, \( Q \) is not abelian.

From Lemma 4.4 and the previous section it follows now that the structure of \( H \) is uniquely determined. \( H \) is, in fact, the subgroup fixing \( \infty \) in \( U_9(q) \). Therefore, we may and do assume that \( U_9(q) \) and \( G \) contain the subgroup \( H \) in common. Now, as in [6], \( \mathcal{A} \) is the block design associated with \( U_9(q) \).
From the characterization of blocks containing \( \infty \) given in Lemma 4.2 and since \( G_\infty = (U_\infty(q))_\infty \), it follows that \( \mathcal{A}_\infty = \mathcal{B}_\infty \). In order then to show that \( \mathcal{A} = \mathcal{B} \), it follows from Lemma 4.3(i), we need only show that \( \mathcal{A}_\infty' \) and \( \mathcal{B}_\infty' \) have a common block. We state this as a lemma.

**Lemma 4.5.** \( \mathcal{A} = \mathcal{B} \) if and only if \( \mathcal{A}_\infty' \) and \( \mathcal{B}_\infty' \) have a common block.

Henceforth, \( Q \) will be taken as the family of ordered pairs \( (\alpha, \beta) \in E \times E \) with \( \beta + \beta + \omega \bar{\alpha} = 0 \), as in [6]. The group operation on \( Q \) is given by \( (\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2 - \alpha_2 \bar{\alpha}) \). \( K = \langle k_\mu \rangle \), \( \mu \in E - 0 \), and \( (\alpha, \beta) \rightarrow k_\mu (\mu^3/\bar{\mu} \alpha, \mu \bar{\beta}) \). This follows from the structure of \( H \) given in [6].

**Lemma 4.6.** If \( q + 1 \equiv 0 \pmod{3} \), \( \mathcal{A} = \mathcal{B} \) and \( G = U_3(q) \).

**Proof.** Take \( A \) a block in \( \mathcal{A} \) (or \( \mathcal{B} \)) containing \( (1, -1/2) \in Q \) and fixed by \( W \). By Lemma 4.3(iii) such a block exists. We shall show that \( A \) is uniquely determined.

Since \( q + 1 \equiv 0 \pmod{3} \), \( |W| = q + 1 \). Now \( W \) is generated by the transformation \( k_\omega \) with \( \omega \) a primitive \( (q + 1) \)-st root of unity. Since \( W \) fixes \( A \) and \( (1, -1/2) \in A \), \( \{ (\omega^i, -1/2) : 0 \leq i \leq q \} \) is contained in \( A \). Since \( |A| = 1 + q \), \( A = \{ (\omega^i, -1/2) : 0 \leq i \leq q \} \). Thus, \( A \) is uniquely determined and \( A \in \mathcal{A} \cap \mathcal{B} \). By Lemma 4.5 \( \mathcal{A} = \mathcal{B} \). By [6], Section 5, \( \mathcal{A} = \mathcal{B} \).

The main theorem is a consequence of Lemma 4.6 when \( q + 1 \equiv 0 \pmod{3} \). Accordingly in the remainder of this paper we assume that \( q + 1 \equiv 0 \pmod{3} \). Then, \( |K| = (q^2 - 1)/3 \) and \( |W| = (q + 1)/3 \). Henceforth, we take \( A \) to be a block containing \( (1, -1/2) \in Q \) and fixed by \( W \).

Since \( W = \langle k_\omega \rangle \) and \( (\alpha, \beta) \rightarrow k_\omega (\omega^3 \alpha, \beta) \), \( A \) contains the set

\[ \{ (\omega^{3i}, -1/2) : 0 \leq i < (q + 1)/3 \}. \]

By choosing as representatives of the other orbits of \( W \) in \( A \) the points \( (\lambda, -1/2 + \mu) \) and \( (\eta, -1/2 + \nu) \in Q \), we have

\[ A = \{ (\omega^{3i}, -1/2) : 0 \leq i < (q + 1)/3 \} \cup \{ (\lambda \omega^{3i}, -1/2 + \mu) : 0 \leq i < (q + 1)/3 \}
\cup \{ (\eta \omega^{3i}, -1/2 + \nu) : 0 \leq i < (q + 1)/3 \}. \]

We shall eventually show that \( \lambda = \omega \) and \( \mu = 0 \), \( \eta = \omega^2 \) and \( \nu = 0 \). By [6], Lemma 2.8, and Lemma 4.5, it follows then that \( \mathcal{A} = \mathcal{B} \).

In [6], Section 3, it was found useful to consider the family of circles \( \mathcal{C} \) associated with the block design \( \mathcal{A} \). We shall now define a system of circles \( \mathcal{D} \) associated with the block design \( \mathcal{B} \) exactly the same way that \( \mathcal{C} \) is associated to \( \mathcal{A} \). In fact, when \( G = U_3(q) \) and \( \mathcal{B} = \mathcal{A} \), then \( \mathcal{D} \) will be the family of circles \( \mathcal{C} \).
We consider the quotient map \( \sigma : Q \to E \) defined by \( \sigma((x, \beta)) = \alpha \). If \( B \) is a block containing \( \infty \), then \( B - \infty \) is a coset of \( P \) in \( Q \), by Lemma 4.2. Also, \( P = \ker \sigma \). It follows then that \( \sigma \) collapses \( B - \infty \) to a point of \( E \).

It will be useful to consider the images of blocks of \( \mathcal{B}_\infty \) under the mapping \( \sigma \). We say that a set \( D \subseteq E \) is a circle if \( D = \sigma(B) \) for some \( B \in \mathcal{B}_\infty \). The family of all circles is denoted by \( \mathcal{D} \). Thus, \( \mathcal{D} = \{ \sigma(B) : B \in \mathcal{B}_\infty \} \). We say that a permutation \( f \) on \( E \) is circle-preserving if \( f(D) \in \mathcal{D} \) whenever \( D \in \mathcal{D} \).

We note:

**Lemma 4.7.** If \( f \in H \), then \( f \) induces a mapping \( \tau(f) \) on \( E \) such that

(i) The following diagram commutes.

\[
\begin{array}{ccc}
Q & \xrightarrow{\sigma} & E \\
\downarrow f & & \downarrow \tau(f) \\
Q & \xrightarrow{\sigma} & E
\end{array}
\]

(ii) \( \tau(f) \) is circle-preserving.

(iii) The mapping \( f \to \tau(f) \) is a homomorphism.

**Proof.** (i) Since \( f \in H \), \( f \) permutes blocks containing \( \infty \) into blocks containing \( \infty \). By Lemma 4.2 such blocks are just the union of \( \infty \) and a coset of \( P \) in \( Q \). Since \( \sigma \) collapses cosets of \( P \) in \( Q \) to points in \( E \), (i) follows.

(ii) Since \( f \in H \), \( f \) carries blocks not containing \( \infty \) to blocks not containing \( \infty \). Thus, \( \tau(f) \) carries circles to circles.

**Lemma 4.8.** (i) \( \tau(Q) \) consists of the transformations \( z \to z + a \), \( a \in E \).

(ii) \( \tau(K) \) consists of the transformations \( z \to (\lambda^3 / \lambda)z \), \( \lambda \in E - 0 \).

(iii) \( \sigma(A) \) is the circle \( C = \{ \omega^3 i, \lambda \omega^{3i}, \eta \omega^{3i} \}, 0 \leq i < (q + 1)/3 \).

**Lemma 4.9.** All circles of \( \mathcal{D} \) can be obtained by applying the transformations of \( \tau(H) \) to the circle \( C \).

**Proof.** This follows immediately from the fact that \( H \) is transitive on \( \mathcal{B}_\infty \) (Lemma 4.3(i)).

**Lemma 4.10.** Each circle of \( \mathcal{D} \) has \( 1 + q \) points.

**Proof.** If \( |\sigma(B)| < |B| \), then there are points \( x_1, x_2 \in B \), with \( x_1 \neq x_2 \), and \( \sigma(x_1) = \sigma(x_2) \). Since \( \infty \cup \sigma^{-1}(\sigma(x_1)) \) is a block containing \( \infty \) (by Lemma 4.2), \( B \) has two points in common with some block containing \( \infty \); so \( \infty \in B \). Thus, if \( B \in \mathcal{B}_\infty \), \( |\sigma(B)| = |B| = 1 + q \). Since each circle of \( \mathcal{D} \) is the \( \sigma \)-image of some block of \( \mathcal{B}_\infty \), the result follows.
Lemma 4.11. If $D$ is a circle containing 0, there is a block $B \in B_\infty$ containing $(0, 0)$, such that $\sigma(B) = D$.

Proof. Since $D \in \mathcal{D}$, there is a block $B \in B_\infty$ such that $\sigma(B) = D$. Since $0 \in D$, $\sigma(x) = 0$, for some $x \in B$. If $\sigma(x) = 0$, then $x \in P$. Then, $\sigma(x^{-1}B) = \sigma(x^{-1}) \sigma(B) = \sigma(B)$. Thus, $(0, 0) \in x^{-1}B$ and $\sigma(x^{-1}B) = D$.

5. Local Isomorphism and Its Consequences

In this section, we derive a local isomorphism between $A$ and $B$ and examine some of the implications of its existence. Since $A_\infty = B_\infty$, the block $A$ containing both 0 and $\infty$ belongs to both $A$ and $B$. We let $L_u$ be the subgroup of $U(q)$ fixing $A$. $L$ is, of course, the subgroup of $G$ fixing $A$. Both $[L, L]$ and $[L_u, L_u]$ are isomorphic to $SL(2, q)$ (Lemma 2.16) and the restriction of each of these groups to $A$ is $PSL(2, q)$. Moreover, each group is regular on $X - A$ (Lemma 2.18). Henceforth $T$ will be the subgroup of $K$ of order $q - 1$. Since $H \subseteq U(q) \cap G$, $P \cdot T \subseteq [L_u, L_u] \cap [L, L]$.

Lemma 5.1. There is a permutation $c$ of $X$ such that $c[L_u, L_u]c^{-1} = [L, L]$.

Proof. This follows quickly from the fact that $[L_u, L_u] \mid A$ and $[L, L] \mid A$ is the permutation group $PSL(2, q)$ (Lemma 2.9) and that $[L_u, L_u] \mid X - A$ and $[L, L] \mid X - A$ is the regular representation of $SL(2, q)$ (Lemma 2.18).

Lemma 5.2. There is a permutation $c$ of $X$ such that

(i) $c$ centralizes $P \cdot T$.
(ii) $c \mid A = 1$.
(iii) $c[L_u, L_u]c^{-1} = [L, L]$.

Proof. By Lemma 5.1, there is a permutation $c$ of $X$ such that $c[L_u, L_u]c^{-1} = [L, L]$.

By composing $c$ with a suitable inner automorphism of $[L, L]$ we may suppose that $c[L_u, L_u]c^{-1} = [L, L]$ and $cP \cdot Tc^{-1} = P \cdot T$. (Recall that $P \cdot T \subseteq [L_u, L_u] \cap [L, L]$). Now given any automorphism of $P \cdot T$ there is an element in the normalizer of $[L_u, L_u]$ in the symmetric group on $X$ which normalizes $P \cdot T$ and induces this automorphism on $[L_u, L_u]$ [6, Corollary 2.9b]. Thus, we may assume that $c[L_u, L_u]c^{-1} = [L, L]$ and $c$ centralizes $P \cdot T$. Clearly, $c$ fixes the sets $A$ and $X - A$. Since $c \mid A$ centralizes the stabilizer of a point in $PSL(2, q)$, $c \mid A = 1$. 
Lemma 5.3. There is a local isomorphism \( c \) of the block design \( \mathcal{A} \) and \( \mathcal{B} \) around the block \( \Delta \), such that \( c \) centralizes \( T \).

Proof. Take \( c \) to be the permutation of Lemma 5.2. Then \( c \) centralizes \( T \) and fixes all points of \( \Delta \). It only remains to show that if \( B \in \mathcal{A} \) and \( B \cap \Delta \neq \emptyset \), then \( c(B) \in \mathcal{B} \).

Let \( P_\alpha \) be the Sylow \( p \)-subgroup of \( [L, L] \) fixing the point \( \alpha \) of \( \Delta \). By Lemma 4.2 each block of \( \mathcal{B}_\alpha \) is the union of \( \infty \) and an orbit of \( P \). By conjugating it follows that each block of \( \mathcal{B}_\alpha \) is the union of \( \alpha \) and an orbit of \( P_\alpha \). The same reasoning holds for the Sylow \( p \)-subgroups of \([L_u, L_u]\). Since \( c \) fixes each \( \alpha \in \Delta \), \( c \) carries orbits of the Sylow \( p \)-subgroup of \([L_u, L_u]\) fixing the point \( \alpha \) into orbits of the Sylow \( p \)-subgroup of \([L, L]\) fixing the point \( \alpha \). Thus, \( c \) carries blocks of \( \mathcal{A} \) which intersect \( \Delta \) into blocks of \( \mathcal{B} \) which intersect \( \Delta \).

We now use the local isomorphism \( c \) to relate the family of circles \( \mathcal{G} \) to the family of circles \( \mathcal{D} \). This is facilitated by the following lemma.

Lemma 5.4. There is a permutation \( d \) on \( E \) such that

1. \( d(0) = 0 \).
2. \( C \) is a circle of \( \mathcal{G} \) containing \( 0 \) if and only if \( d(C) \) is a circle of \( \mathcal{D} \) containing \( 0 \).
3. \( d(\lambda x) = \lambda d(x) \) for all \( x \in E \) and \( \lambda \) in \( F \).

Proof. We take \( c \) to be the local isomorphism of Lemma 5.3. Since \( c \) carries the blocks of \( \mathcal{A}_\alpha \) to blocks of \( \mathcal{B}_\alpha \) and since \( \mathcal{A}_\alpha = \mathcal{B}_\alpha \), \( c \) induces a mapping \( d \) on \( E \) such that the following diagram commutes:

\[
\begin{array}{ccc}
Q & \xrightarrow{c} & E \\
\downarrow & & \downarrow d \\
Q & \xrightarrow{c} & E
\end{array}
\]

Since \( c \) commutes with \( T \) and \( T \) induces on \( E \) the mappings \( z \rightarrow \lambda z \), \( \lambda \in F \), \( d(\lambda x) = \lambda d(x) \), \( x \in E \) and \( \lambda \in F \).

Suppose \( C \) is a circle of \( \mathcal{G} \) containing \( 0 \). Then, by Lemma 4.11, there is a block \( B \) in \( \mathcal{A} \) containing \( (0, 0) \) such that \( \sigma(B) = C \). Then, \( d(C) = \sigma(c(B)) \). Since \( c \) is a local isomorphism, \( c(B) \) is a block of \( \mathcal{B} \) containing \( (0, 0) \). Thus \( d(C) \) is a circle containing \( 0 \). Since \( d \) has an inverse, the converse follows.

We can now use the function \( d \) to force many of the properties of the system of circles \( \mathcal{G} \) to propagate to the system \( \mathcal{D} \).
In this section and the next we shall show that $\mathcal{C} = \mathcal{D}$. In this section we shall show that the qualitative properties of the systems $\mathcal{D}$ and $\mathcal{C}$ are the same. We begin by abstracting the properties of $\mathcal{D}$ necessary to obtain these results. We say then that a family of subsets $\mathcal{D}$ of $E$ is an abstract system of circles (which we promptly abbreviate to system of circles or family of circles) if

(i) The group of transformations $z \rightarrow (\lambda^2/\lambda)z + a$, $\lambda \in E - 0$, $a \in E$, is transitive on $\mathcal{D}$. We call this group $M$.

(ii) There is a permutation $d$ of $E$ such that

(a) $d(0) = 0$.

(b) If $C$ is a circle of $\mathcal{C}$ containing $0$, then $d(C) \in \mathcal{D}$, and conversely.

(c) $d(\lambda x) = \lambda d(x)$, $\lambda \in F$, $x \in E$.

By Lemmas 4.9 and 5.4 the system of circles $\mathcal{D}$ associated with the block design $\mathcal{B}$ has these properties.

In this and the following section $\mathcal{D}$ will be a system of circles in the above sense. We begin by noting:

**Lemma 6.1.** Each $D \in \mathcal{D}$ has $1 + q$ points.

**Proof.** This follows from the existence of the function $d$ of (ii), the fact that each element of $\mathcal{C}$ has $1 + q$ points [6, Section 3], and the transitivity of $M$ on $\mathcal{D}$.

**Lemma 6.2.** If $\mu \in E - 0$, let $\phi_\mu$ be the transformation of $E$ defined by $\phi_\mu(z) = \mu z$. If $\mathcal{D}$ is an abstract system of circles, so is $\phi_\mu(\mathcal{D})$.

**Proof.** This follows from the fact that $\phi_\mu$ preserves the circles of $\mathcal{C}$ [6, Section 3] and normalizes the group $M$.

**Lemma 6.3.** No two distinct circles of $\mathcal{D}$ have three common points.

**Proof.** Suppose $D_1, D_2 \in \mathcal{D}$ have three common points. By translating, if necessary, we may suppose that $0 \in D_1 \cap D_2$. Let $C_1, C_2 \in \mathcal{C}$ such that $d(C_1) = D_1$ and $d(C_2) = D_2$. By (ii) above this is possible. Since $d$ is a permutation, $C_1$ and $C_2$ have three common points. By Lemma 3.11 of [6], $C_1 = C_2$. Therefore, $D_1 = D_2$.

Let $D_1$ and $D_2$ be two circles of $\mathcal{D}$ which intersect at a point $a$. We say that $D_1$ and $D_2$ are tangent at $a$ if either $D_1 = D_2$ or $D_1$ and $D_2$ intersect at $a$ alone.
Theorem 6.1. Tangency of circles is an equivalence relation on the circles which contain a given point.

Proof. By translating it suffices to prove the statement for the circles of $\mathcal{D}$ containing 0. This however follows from the existence of the function $d$ and a similar statement in $\mathcal{C}$ [6, Corollary 3.10a].

Corollary. $d$ carries the tangency classes of $\mathcal{C}$ at 0 into the tangency classes of $\mathcal{D}$ at 0.

Theorem 6.2. If $D$ is a circle of $\mathcal{D}$ containing 0, the tangency class of $D$ at 0 consists of the circles $\lambda D$, $\lambda \in F - 0$. Moreover, $\lambda D \neq \mu D$ if $\lambda \neq \mu$.

Proof. Let $C \in \mathcal{C}$ be a circle such that $d(C) = D$. Since $d$ preserves the relation of tangency at 0, $d$ carries the tangency class of $C$ into the tangency class of $D$. By Corollary 3.10c of [6], Theorem 6.2 holds in $\mathcal{C}$. Thus, the tangency class of $C$ at 0 consists of the $q - 1$ circles $\lambda C$, $\lambda \in F - 0$. Since $d(\lambda x) = \lambda d(x)$ for $\lambda \in F$, a similar statement holds in $\mathcal{D}$.

This theorem may be restated as follows: The transformation $z + \lambda z$, $\lambda \in F - 0$, fixes each tangency class at 0 while permuting the circles of a given tangency class transitively among themselves.

Theorem 6.3. Let $x_1, x_2, \ldots, x_q$ be the $q$ nonzero points of the circle $D \in \mathcal{D}$, where $D$ contains 0. Then, $x_1, x_2, \ldots, x_q$ span distinct subspaces of $E$ regarded as a vector space over $F$.

Proof. Let $\ell$ be a line through 0. We must show that $\ell$ and $D$ intersect at no more than one nonzero point. Since $\ell$ is just a one-dimensional subspace of $E$ over $F$, the mapping $x \mapsto \mu x$, $\mu \in F - 0$, fixes $\ell$.

Suppose $|\ell \cap (D - 0)| \geq 2$. Then, $|\ell \cap \lambda(D - 0)| \geq 2$ for all $\lambda \in F - 0$.

By Theorem 6.2, as $\lambda$ runs through the nonzero elements of $F$, $\lambda D$ runs through the distinct members of the tangency class of $\mathcal{D}$ at 0. Thus, if $\lambda \neq \mu$, $\lambda(D - 0) \cap \mu(D - 0) = \emptyset$. It follows then that $|\ell| \geq 2(q - 1) + 1$, a contradiction, as $|\ell| = q$. Theorem 6.3 follows.

Since $F$ has $1 + q$ one-dimensional subspaces over $F$, there are $1 + q$ lines through 0. Thus, given any circle $D \in \mathcal{D}$ containing 0, there is a unique line $\ell$ intersecting $D$ only at 0. We call this line the tangent line of $D$ at 0.

Theorem 6.4. $\mathcal{D}$ has $q^4(q - 1)$ circles.

Proof. From the existence of the function $d$ and Corollary 3.10b of [6], it follows that $q^2 - 1$ circles of $\mathcal{D}$ contain 0. Since $M$ is transitive on the points of $E$, each point of $E$ is contained in $q^2 - 1$ circles. Let $r$ be the number of circles. Using the fact that each circle contains $1 + q$ points
and counting in two ways the number of pairs \((a, D), a \in E, D \in \mathcal{D},\) and \(a \in D,\) it follows that \(r(1 + q) = q^2(q^2 - 1).\) Thus, \(r = q^2(q - 1).\)

**Lemma 6.8.** The subgroup of \(M\) fixing a single circle of \(\mathcal{D}\) is of order \((q + 1)/3.\)

**Proof.** \(M\) is transitive on \(\mathcal{D},\) \(|M| = q^2(q^2 - 1)/3,\) and \(|\mathcal{D}| = q^2(q - 1).\)

Any subgroup of \(M\) of order \((q + 1)/3\) is conjugate to the group generated by the transformation \(z \to \omega^3z,\) where \(\omega\) is a primitive \((q + 1)\text{-st}\) root of unity of \(E.\) We call this group \(W.\)

**Lemma 6.9.** \(E - 0\) is the disjoint union of circles fixed by \(W.\)

**Proof.** Let \(D\) be a circle fixed by \(W.\) Since \(W\) is semiregular on \(E - 0,\) \(0 \not\in D.\) Thus \(D \subseteq E - 0.\)

Since \(M\) is transitive on \(\mathcal{D},\) the number of circles fixed by \(W\) is \(|N_M(W)| = q - 1.\) If \(D_1\) and \(D_2\) are two circles fixed by \(W\) and \(D_1 \cap D_2 \neq \phi, D_1\) and \(D_2\) intersect in an orbit of \(W.\) Since \(q > 5, (q + 1)/3 > 2;\) so \(D_1 = D_2\) by Lemma 6.3. Thus, the circles fixed by \(W\) are pairwise disjoint subsets of \(E - 0, q - 1\) in number. Since each circle has \(1 + q\) points, the result follows.

Let \(C\) be a circle of \(\mathcal{D}\) fixed by \(W\) and containing \(1.\) By Lemma 6.9, such a circle exists. Let \(\lambda\) and \(\eta\) be representatives of the other orbits of \(W\) on \(C.\)

Then, \(C = \{\omega^{3i}, \lambda\omega^{3i}, \eta\omega^{3i}\}, 0 \leq i < (q + 1)/3.\)

**Lemma 6.10.** \(1, \lambda, \eta\) belong to different cosets in \(E - 0\) of the subgroup of the multiplicative group of \(E - 0\) of order \((q^2 - 1)/3.\)

**Proof.** Since \(N_M(W)\) is transitive on the circles fixed by \(W,\) it follows from Lemma 6.9 that \(E - 0 = \cup \mu C,\) where \(\mu\) ranges over the multiplicative subgroup of \(E - 0\) of order \((q^2 - 1)/3\) (i.e., \(\mu\) ranges through elements of the form \(\lambda^{3\mu}, \) with \(\lambda \in E - 0).\) Clearly this is not possible if, in \(C = \{\omega^{3i}, \lambda\omega^{3i}, \eta\omega^{3i}\},\) two of the elements \(1, \lambda, \eta\) belong to the same coset of the subgroup of order \((q^2 - 1)/3.\)

Henceforth, we let \(C = \{\omega^{3i}, \lambda\omega^{3i+1}, \eta\omega^{3i+2}\}, 0 \leq i < (q + 1)/3,\) where \(\lambda^{(q^2-1)/3} = \eta^{(q^2-1)/3} = 1.\) This is possible by Lemma 6.10.

7. **Calculation of \(\lambda\) and \(\eta\)**

In this section by calculating \(\lambda\) and \(\eta\) we show that \(C = \mathcal{D}.\) We recall the circle \(C = \{\omega^{3i}, \lambda\omega^{3i+1}, \eta\omega^{3i+2}\}, 0 \leq i < (q + 1)/3\) of Section 6. All other circles of \(\mathcal{D}\) can be determined by applying the transformations of \(M\) to the circle \(C.)\)
We note that replacing $\lambda$ by $\lambda \omega^{3j}$ for some integer $j$ does not change the set $C$. An analogous remark holds for $\eta$. Accordingly the quantities of real interest are not so much $\lambda$ and $\eta$, as $\lambda^{(q+1)/3}$ and $\eta^{(q+1)/3}$. Thus, we define $x = \lambda^{(q+1)/3}$ and $y = \eta^{(q+1)/3}$. Clearly the set $C$ depends only on the quantities $x$ and $y$ for the determination of its members.

**Lemma 7.1.** $x, y \in F$, $x \neq 0$, $y \neq 0$.

**Proof.** By the definitions of $\lambda$ and $\eta$ following Lemma 6.10 $\lambda^{(q^2-1)/3} = \eta^{(q^2-1)/3} = 1$. Therefore, $x^{q-1} = y^{q-1} = 1$. It follows that $x \neq 0$, $y \neq 0$, and $x = x$, $y = y$. Thus, $x, y \in F$.

We say that $(\lambda, \eta)$ is an admissible pair if the circle $C$ belongs to some abstract system of circles. We note:

**Lemma 7.2.** If $(\lambda, \eta)$ is an admissible pair, so too are $(\lambda^{-1} \eta, \lambda^{-1})$ and $(\eta^{-1}, \lambda \eta^{-1})$.

**Proof.** We use Lemma 6.2. If $D$ is a system of circles, so too is $\phi_{\lambda^{-1} \omega^{-1}}(D)$. To the latter systems of circles belongs the set

$$
\lambda^{-1} \omega^{-1} C = \{ \omega^{3i}, \lambda^{-1} \eta \omega^{3i+1}, \lambda^{-1} \omega^{3i+2} \}, \quad 0 \leq i < (q + 1)/3.
$$

This latter circle is fixed by the subgroup $W$ of Section 6 and contains the point 1. Thus, $(\lambda^{-1} \eta, \lambda^{-1})$ is admissible. A similar argument demonstrates the admissibility of $(\eta^{-1}, \lambda \eta^{-1})$.

It follows from Lemma 7.2 that if the admissibility of the pair $(\lambda, \eta)$ implies that the quantities $x$ and $y$ satisfy an equation $f(x, y) = 0$, then we also have $f(x^{-1} y, x^{-1}) = f(y^{-1} x y^{-1}) = 0$.

Henceforth $v$ will denote the quantity $\omega^{(q+1)/3}$ with $\omega$ a fixed primitive $(q + 1)$-st root of unity. Since $\omega^{q+1} = 1$, $\omega^3 = 1$. Since $\omega = \omega^{-1}$, $v = v^{-1} = v^2$. Clearly, $v \neq 1$. Since $v^3 - 1 = (v - 1)(v^2 + v + 1) = 0$, $v^2 + v + 1 = 0$. Also, $v + v + 1 = 1$.

**Lemma 7.3.** Let $x_1, x_2, \ldots, x_{q+1} \in E$. Suppose further that $x_i$ and $x_j$, $i \neq j$, are linearly independent in $E$ regarded as a vector space over $F$. Then, if $\zeta$ is an indeterminate,

$$
\prod_{i} (\zeta - \bar{x}_i/x_i) = \zeta^{q+1} - 1.
$$

**Proof.** By Lemma 3.9 of [6] the quantities $\bar{x}_i/x_i$ for $i = 1, 2, \ldots, q + 1$ are distinct. Each also is a $(q + 1)$-st root of unity. It follows therefore that the $q + 1$ quantities $\bar{x}_i/x_i$ exhaust the $(q + 1)$-st roots of unity and the result follows.
COROLLARY. If $x_1, x_2, \ldots, x_{q+1}$ are as in Lemma 7.3,

$$\sum \overline{x}_i/x_i = 0 \quad \text{and} \quad \pi(x_i/x_i) = -1.$$ 

By Lemma 6.6 if $D$ is a circle of $\mathcal{D}$ containing 0 and $x_1, x_2, \ldots, x_q$ are the nonzero points of $D$, the subspaces spanned by different $x$'s are distinct. In particular, $\{\omega^{3i} - 1, \lambda \omega^{3i+1} - 1, \eta \omega^{3i+2} - 1\}$, $0 \leq i < (q + 1)/3$ is such a circle. Its nonzero points are

$$\omega^{3i} - 1; \quad \lambda \omega^{3i+1} - 1; \quad \eta \omega^{3i+2} - 1$$

$$0 < i < (q + 1)/3 \quad 0 \leq i < (q + 1)/3 \quad 0 \leq i < (q + 1)/3.$$

Let $m$ be a nonzero point of the tangent line of this circle at 0. Recall that $m$ spans the unique subspace not spanned by one of the forgoing $q$ quantities. Thus, every one-dimensional subspace of $E$ is spanned by $m$ or one of the $q$ quantities.

**Lemma 7.4.**

$$(\frac{\bar{m}}{m})(1 - \bar{v}x)(1 - \bar{v}y) = -1.$$ 

*Proof.* We use the corollary to Lemma 7.3 with $x_1, x_2, \ldots, x_{q+1}$ replaced by $m$, $\omega^{3i} - 1$ ($0 < i < (q + 1)/3$), $\lambda \omega^{3i+1} - 1$ ($0 \leq i < (q + 1)/3$), and $\eta \omega^{3i+2} - 1$ ($0 \leq i < (q + 1)/3$). Henceforth, if the range of $i$ is unspecified it is assumed to run through the integers from 0 to $(q - 2)/3$. We find:

$$-1 = (\frac{\bar{m}}{m}) \prod_{i \neq 0} (\frac{\omega^{3i} - 1}{\omega^{3i} - 1}) \prod_{i} (\frac{\lambda \omega^{3i+1} - 1}{\lambda \omega^{3i+1} - 1}) \prod_{i} (\frac{\eta \omega^{3i+2} - 1}{\eta \omega^{3i+2} - 1}).$$

Now, for any $\zeta$,

$$\prod_{i} (\zeta \omega^{3i} - 1) = 1 - \zeta^{(q+1)/3},$$

$$\prod_{i \neq 0} (\zeta \omega^{3i} - 1) = -\sum_{i} \zeta^i.$$ 

Thus, $\prod_{i \neq 0} (\omega^{3i} - 1) = (q + 1)/3$.

Using these relations in the previous equations, together with $\omega^{(q+1)/3} = \nu$, $\lambda^{(q+1)/3} = x$, $\eta^{(q+1)/3} = y$, and $\bar{x} = x$, $\bar{y} = y$, we find

$$-1 = (\frac{\bar{m}}{m})(1 - \bar{v}x)(1 - \bar{v}y).$$

**Lemma 7.5.**

$$0 = \frac{\bar{m}}{m} + 1 + (\frac{q + 1}{3})(\frac{\lambda^3 - 1}{\lambda \nu - 1} + \frac{\gamma^3 - 1}{\gamma \nu - 1}).$$
Proof. We proceed as in Lemma 7.4 using the relation $\sum \frac{x_i}{x_i} = 0$. We have

(A) \[ 0 = \frac{m}{m} + \sum_{i \neq 0} \frac{\omega^{3i}}{\omega^{3i} - 1} + \sum_i \frac{(\lambda\omega)\omega^{-3i} - 1}{(\lambda\omega)\omega^{3i} - 1} + \sum_i \frac{((\eta\omega)\omega^{-3i} - 1)}{(\eta\omega)\omega^{3i} - 1}. \]

Now:

\[ \sum_i \frac{\xi\omega^{-3i} - 1}{\xi\omega^{3i} - 1} = \frac{1}{\prod_i (\xi\omega^{3i} - 1)} \sum_i \left( \prod_j (\xi\omega^{3j} - 1) \right) \left( \xi\omega^{-3i} - 1 \right). \]

Since

\[ \prod_i (\xi\omega^{3i} - 1) = -\sum_k \omega^{3ik} \xi^k \]

and since $\prod(\xi\omega^{3i} - 1) = 1 - \xi^{(q+1)/3}$,

\[ \sum_i \frac{\xi\omega^{-3i} - 1}{\xi\omega^{3i} - 1} = \frac{1}{\xi^{(q+1)/3} - 1} \sum_k \left( \sum_{k'} \omega^{3(k-k')} \xi^{k'} - \omega^{3ik} \xi^{k'} \right) \]

\[ = \frac{1}{\xi^{(q+1)/3} - 1} \left( \frac{q + 1}{3} \right) (\xi^{q} - 1), \]

where we have used

\[ \sum_{i=0}^{(q-2)/3} \omega^{3i} = \begin{cases} 0 & \text{if } s \neq 0(q + 1)/3 \\ (q + 1)/3 & \text{if } s = 0(q + 1)/3. \end{cases} \]

Thus, from (A),

\[ 0 = \frac{m}{m} + \sum_{i \neq 0} \frac{\omega^{-3i} - 1}{\omega^{3i} - 1} + \left( \frac{q + 1}{3} \right) \left( \frac{(\lambda\omega)(\lambda\omega) - 1}{(\lambda\omega)\xi^{(q+1)/3} - 1} + \frac{(\eta\omega^2)(\eta\omega^2) - 1}{(\eta\omega^2)\xi^{(q+1)/3} - 1}. \right) \]

Now,

\[ \frac{\omega^{-3i} - 1}{\omega^{3i} - 1} = -\omega^{-3i} \quad \text{and} \quad \sum_{i \neq 0} \omega^{-3i} = -1. \]

Using $\omega\bar{\omega} = 1$, $\bar{\lambda} = \lambda^{q+1}$, $\eta\bar{\eta} = \eta^{q+1}$, $\omega^{(q+1)/3} = \nu$, in the previous equation, we obtain the desired result.

**Lemma 7.6.**

\[
\begin{align*}
x^3y + 2xy^2 + x^2y - y^3 - 3xy + 2x^2 + y^2 + 4y - 5x - 2 &= 0 \\
x^3y + 2x^2y + xy^2 - x^3 - 3xy + 2y^2 + x^2 + 4x - 5y - 2 &= 0.
\end{align*}
\]
Proof. Using Lemmas 7.4 and 7.5 and eliminating \(\bar{m}/m\), we find

\[
\frac{1 - \nu x}{1 - \nu x} \frac{1 - \nu y}{1 - \nu y} = 1 + \frac{1}{3} \left( \frac{x^3 - 1}{\nu x - 1} + \frac{y^3 - 1}{\nu y - 1} \right).
\]

Using \(z^3 - 1 = (z - 1)(vz - 1)(\bar{v}z - 1)\), we find

\[
(1 - \nu x)(1 - \nu y) = (1 - \nu x)(1 - \nu y)
+ \frac{1}{3}(1 - \nu x)(1 - \nu y)((x - 1)(\nu x - 1) + (y - 1)(\nu y - 1)).
\]

Multiplying out, (using \((x - 1)(\nu x - 1) = \nu x^2 + \nu x + 1\) etc.)

\[
3(\nu(y - x) + \nu(x - y))
= \nu x^2 + \nu x + 1 + \nu y^2 + 1 + \nu x^2 y + \nu x^2 y
+ xy + \nu xy^2 + \nu xy^2 + xy - \nu x^3 - \nu y - \nu x
- \nu y + \nu x - x^2 y - \nu xy - \nu y - \nu y^2 - \nu y - \nu y.
\]

Now \(\nu + \nu = -1\) and \(\nu\) and \(\bar{\nu}\) are linearly independent over \(F\). Replacing 1 by \(-(\nu + \bar{\nu})\) and equating coefficients of \(\nu\) and \(\bar{\nu}\), we find the equations of Lemma 7.6.

Dr. A. Mann pointed out the simplified version of the author's original calculations used in the next three lemmas.

Lemma 7.7. Either \(x = 1, y = 1,\) or \(x = y\).

Proof. Subtracting the second from the first equation of Lemma 7.6, we obtain

\[
x^2 y - xy^3 + xy^2 - x^2 y - y^3 + x^3 + x^2 - y^2 + 9 y - 9 x = 0.
\]

Therefore,

\[
(x - y)(xy(x + y) - xy + x^2 + xy + y^2 + x + y - 9) = 0.
\]

Now, if \((x, y)\) is a solution, so too is \((x^{-1} y, x^{-1})\). Using this fact in the previous equation, we find either \(x = y, x^{-1} y - x^{-1} = 0,\) or

\[
x^2 y + xy^2 + x^2 + y^2 + x + y - 9 = 0
\]

and

\[
x^{-3} y^2 + x^{-3} y + x^{-2} y^2 + x^{-2} + x^{-1} y + x^{-1} - 9 = 0.
\]

Thus, either \(x = y, y = 1,\) or we obtain the equations

\[
x^2 y + xy^2 + x^2 + y^2 + x + y - 9 = 0
\]
A CHARACTERIZATION OF $U_d(q)$

and

$$y^3 + y + xy^2 + x + x^2y + x^2 - 9x^3 = 0.$$  

Subtracting we obtain,

$$9(x^3 - 1) = 0.$$  

Since $F$ is not of characteristic 3, $x^3 - 1 = 0$. Since no solution of $x^2 + x + 1 = 0$ belongs to $F$, $x = 1$.

**Lemma 7.8.** If $x = 1$ and the characteristic of $F$ is not 5, $y = 1$ also. If $x = 1$ and the characteristic of $F$ is 5, $y = 1$ or $y = 2$.

**Proof.** Setting $x = 1$ in the equations of Lemma 7.6,

$$y^3 | 3y^2 | 3y 5 = 0, \quad y^3 | 3y^2 | 6y + 2 = 0.$$  

Adding and using the fact that $F$ is not of characteristic 3, $2y^3 - y - 1 = 0$.

Thus, $(2y + 1)(y - 1) = 0$, and either $y = 1$ or $y = -1/2$.

If $y = -1/2$, using the equation $-y^3 + 3y^2 + 3y - 5 = 0$, we find $1/8 + 3/4 - 3/2 - 5 = 0$, or $-45 = 0$.

Thus, either $y = 1$, or $F$ is of characteristic 5 and $y = -1/2 = -3 = 2$.

**Lemma 7.9.** If $F$ is not of characteristic 5, $x = 1$ and $y = 1$.

**Proof.** By Lemma 7.7 one of the following must hold: $x = y$, $x = 1$, or $y = 1$. We use repeatedly the fact that if $(x, y)$ is a solution, so is $(x^{-1}y, x^{-1})$.

Thus, if $x = y = \alpha$, $\alpha \in F$, since $(\alpha, \alpha)$ is a solution; so too is $(1, \alpha^{-1})$.

By Lemma 7.8, $\alpha = 1$. Thus, $x = y = 1$.

If $x = 1$, by Lemma 7.8, also $y = 1$.

If $y = 1$, $(1, 1)$ is a solution for $\alpha \in F$. Then, $(\alpha^{-1}, \alpha^{-1})$ is also a solution.

By the above, $x = 1$.

**Lemma 7.10.** If $F$ is not of characteristic 5, $\mathcal{C} = \mathcal{D}$.

**Proof.** This is immediate from the facts that the group $M$ is transitive on both $\mathcal{C}$ and $\mathcal{D}$, and $\mathcal{C}$ and $\mathcal{D}$ have in common the circle $C$.

**Lemma 7.11.** If $F$ is of characteristic 5, the only solutions to the equations of Lemma 7.6 are $(1, 1)$, $(1, 2)$, $(2, 1)$, and $(3, 3)$.

**Proof.** By Lemma 7.8, if $x = 1$, either $y = 1$ or $y = 2$. By Lemma 7.7, either $x = 1, y = 1$, or $x = y$.

We also know that if $(x, y)$ is a solution, so are $(x^{-1}y, x^{-1})$ and $(y^{-1}, y^{-1}x)$.

Lemma 7.11 follows quickly from these facts.
We shall now show that if $F$ is of characteristic 5 and $|F| > 5$, then $c = \mathcal{D}$, as in Lemma 7.10. Since the admissibility of $(2, 1)$ or $(3, 3)$ implies that of $(1, 2)$, it suffices to show that $(1, 2)$ is not an admissible pair. We do this by assuming the admissibility of $(1, 2)$ and deriving a contradiction. Throughout the remainder of this section then we assume $x = 1$ and $y = 2$. Then $\lambda$ may be taken to be 1 and $\eta$ some root of the equation $\eta^{(q+1)/3} = 2$.

By Lemma 6.6 the quantities
\[
m; \quad \omega^{3i} - 1; \quad \omega^{3i+1} - 1; \quad \eta \omega^{3i+2} - 1
\]
\[
0 < i < (q + 1)/3 \quad 0 \leq i < (q + 1)/3 \quad 0 \leq i < (q + 1)/3
\]
span distinct subspaces of $E$ regarded as a vector space over $F$.

**Lemma 7.12.** $\overline{m}/m = 1 + \nu = -\bar{\nu}$.

**Proof.** Since $x = 1$ and $y = 2$, we have using Lemma 7.5
\[
0 = \frac{\overline{m}}{m} + 1 - \frac{1}{2\bar{\nu} - 1}.
\]
Then, $\frac{\overline{m}}{m} = -\bar{\nu}$.

For convenience we let $\sigma = \omega^2 \eta$.

**Lemma 7.13.** Let $\zeta$ be an indeterminate. Then
\[
(\zeta + 1)(\zeta^{(q+1)/3} - \nu) = (\zeta - (1 + \nu)) \prod_{i=0}^{(q-2)/3} \left( \zeta - \omega^{-3i} \frac{\bar{\sigma} - \omega^{3i}}{(\sigma \omega^{3i} - 1)} \right).
\]

**Proof.** By Lemma 7.3 and the remarks preceding Lemma 7.12 as well as Lemma 7.12 itself,
\[
\zeta^{q+1} - 1 = (\zeta - (1 + \nu)) \prod_{i \neq 0} \left( \zeta - \frac{\omega^{-3i} - 1}{\omega^{3i} - 1} \right)
\]
\[
\cdot \prod_{i} \left( \zeta - \frac{\omega^{-3i-1} - 1}{\omega^{3i+1} - 1} \right) \prod_{i} \left( \zeta - \frac{\bar{\sigma} \omega^{3i} - 1}{\sigma \omega^{3i} - 1} \right).
\]

Now if $\zeta \bar{\zeta} = 1$, $(\bar{\zeta} - 1)/(\zeta - 1) = -\zeta^{-1}$. Thus,
\[
\prod_{i \neq 0} \left( \zeta - \frac{\omega^{-3i} - 1}{\omega^{3i} - 1} \right) - \prod_{i \neq 0} \left( \zeta + \omega^{3i} \right) - (\zeta^{(q+1)/3} - 1)/(\zeta + 1),
\]
\[
\prod_{i} \left( \zeta - \frac{\omega^{-3i-1} - 1}{\omega^{3i+1} - 1} \right) = \prod_{i} \left( \zeta + \omega^{(3i+1)} \right) = \zeta^{(q+1)/3} - \bar{\nu},
\]
since $\omega^{(q+1)/3} = \nu$. 
Since $\zeta^{q+1} - 1 = (\zeta^{(q+1)/3} - 1)(\zeta^{(q+1)/3} - v)(\zeta^{(q+1)/3} - \bar{\sigma})$, the result follows.

Now let

$$r(\zeta) = \prod_i \left( \zeta - \omega^{-3i} \frac{\bar{\sigma} - \omega^{3i}}{\sigma \omega^{3i} - 1} \right).$$

**Lemma 7.14.** If $\zeta = \frac{\bar{\sigma} - z}{z(z - 1)}$ with $z$ an indeterminate,

$$r(\zeta) = \frac{\sigma^{(q+1)/3}}{(z(z - 1))(q+1)/3} \frac{(z^{(q+1)/3} - 1)}{(\sigma^{(q+1)/3} - 1)} \cdot \left( \frac{\bar{\sigma}}{\sigma} \right)^{(q+1)/3} \left( 1 - \sigma z \right)^{(q+1)/3} \left( \sigma z - 1 \right)^{(q+1)/3} \left( \sigma z - 1 \right).$$

**Proof.**

$$r(\zeta) = r \left( \frac{1}{z} \frac{\bar{\sigma} - z}{\sigma z - 1} \right)$$

$$= \frac{1}{(z(z - 1))(q+1)/3} \prod_i \left( \bar{\sigma} - z - \omega^{-3i} \frac{\bar{\sigma} - \omega^{3i}}{\sigma \omega^{3i} - 1} \right).$$

Let

$$\delta = \omega^{-3i} \frac{\bar{\sigma} - \omega^{3i}}{\sigma \omega^{3i} - 1}.$$

Then, $\bar{\sigma} - z - \delta \sigma (z - 1) = -((\delta \sigma) z^2 + (1 - \delta) z - \bar{\sigma})$. Now one root of this polynomial is $\omega^{3i}$. If $a$ is the other root, then, from $a \omega^{3i} = -\bar{\sigma} / \delta \sigma$, we find that

$$a = -\frac{\bar{\sigma} \sigma \omega^{3i} - 1}{\sigma \bar{\sigma} - \omega^{3i}}.$$

Thus,

$$r(\zeta) = \prod_i -\frac{\sigma \omega^{3i} - 1}{\sigma \omega^{3i} - 1} \prod \left( z - \omega^{3i} \right) \prod \left( z + \frac{\bar{\sigma} \sigma \omega^{3i} - 1}{\sigma \bar{\sigma} - \omega^{3i}} \right)$$

$$\cdot \frac{1}{(z(z - 1))(q+1)/3}$$

$$= \frac{\sigma^{(q+1)/3}}{(z(z - 1))(q+1)/3} \frac{(z^{(q+1)/3} - 1)(\sigma^{(q+1)/3} - 1)}{(\sigma^{(q+1)/3} - 1)} \cdot \prod_i \left( z + \frac{\bar{\sigma} \sigma \omega^{3i} - 1}{\sigma \bar{\sigma} - \omega^{3i}} \right).$$

We consider the last term in the above expression for $r(\zeta)$. Replacing $z$ by $-(\bar{\sigma} / \sigma) t$, it becomes

$$\left( \frac{\bar{\sigma}}{\sigma} \right)^{(q+1)/3} \prod_i \left( t - \frac{\sigma \omega^{3i} - 1}{\sigma \bar{\sigma} - \omega^{3i}} \right).$$
Now,
\[ \prod_i \left( \tau - \frac{\sigma \omega^{3i} - 1}{\sigma} \right) = \frac{(\tau \bar{\sigma} + 1)^{(q+1)/3} - (\tau + \sigma)^{(q+1)/3}}{\bar{\sigma}^{(q+1)/3} - 1}. \]

To see this note that both expressions are polynomials with leading coefficient 1 and having the same roots.

Replacing \( \tau \) by \( -(\sigma/\bar{\sigma})x \), the last term in the expression for \( r(\zeta) \) becomes

\[ \left( \frac{\sigma (q+1)/3}{\bar{\sigma}} \right)^{(q+1)/3} \frac{(1 - \sigma x)^{(q+1)/3} - \left( -\frac{x}{\bar{\sigma}} + 1 \right)^{(q+1)/3}}{\bar{\sigma}^{(q+1)/3} - 1}. \]

Substituting into the expression for \( r(\zeta) \), the result follows.

**COROLLARY.**

\[ (\sigma z^2 - 2z + \bar{\sigma})(\bar{\sigma} - z)^{(q+1)/3} - \nu(z(\sigma z - 1))^{(q+1)/3} \]

\[ = (2 - \nu)(-\nu \sigma^2 + \nu z + \bar{\sigma}) \times (\overline{z^{(q+1)/3}} - 1), \]

with \( z \) an indeterminate.

**Proof.** Now \( (\zeta + 1)(\overline{z^{(q+1)/3}} - \nu) = (\zeta - (1 + \nu)) r(\zeta) \), with \( \zeta = (\bar{\sigma} - z)/z(\sigma z - 1) \). Substituting into the expression for \( r(\zeta) \) and clearing fractions,

\[ (\bar{\sigma} - z + \sigma z - z)(\bar{\sigma} - z)^{(q+1)/3} - \nu(z(\sigma z - 1))^{(q+1)/3} \]

\[ = \frac{\sigma}{\sigma^{(q+1)/3} - 1} \left( -(1 + \nu) \sigma z^2 + \nu z + \bar{\sigma} \right) \times \left( \overline{z^{(q+1)/3}} - 1 \right). \]

Now \( \sigma = \omega^{2} \). Thus, \( \sigma^{(q+1)/3} = 2\nu \), and \( 2\nu/(2\nu - 1) = 2 - \nu \).

**LEMMA 7.15.** If \( F \) is of characteristic 5 and \( |F| > 5 \), \( x = y = 1 \) and \( \mathcal{C} = \mathcal{D} \).

**Proof.** We obtain a contradiction using the corollary to Lemma 7.14. In the equality of this corollary we calculate the coefficient of \( z^{(q+1)/3} \) on both sides of the equation.

Assuming \( q > 5 \), \( 2(q + 1)/3 > 2 + (q + 1)/3 \). Thus, the term
\((az^2 - 2z + \bar{\sigma})(\bar{\sigma} - z)^{(q+1)/3}\) on the left contributes nothing to the term of degree \(2(q + 1)/3\). We consider the second term on the left:

\[
(az^2 - 2z + \bar{\sigma})(-\nu) z^{(q+1)/3}(\sigma z - 1)^{(q+1)/3}
\]

\[
= (\sigma z^2 - 2z + \bar{\sigma})(-\nu) z^{(q+1)/3}
\]

\[
\times \left(\sigma^{(q+1)/3} z^{(q+1)/3} - \left(\frac{q + 1}{3}\right) \sigma^{(q-2)/3} z^{(q-2)/3}
\right.
\]

\[
+ \frac{1}{2} \left(\frac{q + 1}{3}\right) \left(\frac{q - 2}{3}\right) \sigma^{(q-5)/3} z^{(q-5)/3}
\left. + \ldots\right).
\]

The coefficient of \(z^{2(q+1)/3}\) is then:

\[
-\nu \left(\bar{\sigma}(q+1) - 2(q + 1)/3 \sigma^{(q+1)/3-1} + \frac{1}{2} \left(\frac{q + 1}{3}\right) \left(\frac{q - 2}{3}\right) \sigma^{(q+1)/3-1}\right).
\]

Since in \(n\), \(q = 0\) and \(1/3 = 2\), this is:

\[-\gamma \bar{\sigma}(q+1)/3.\]

Next we calculate the coefficient of \(z^{2(q+1)/3}\) on the right-hand side of the equation. Since \(q > 5\), \(2(q + 1)/3 > 2 + (q + 1)/3\) and the term

\[
(2 - \nu)(-(1 + \nu) \sigma z^2 + z + \bar{\sigma})(-1)(\bar{\nu}(1 - \sigma z)^{(q+1)/3} - (\bar{\sigma} - z)^{(q+1)/3})
\]

contributes nothing. Then,

\[
(2 - \nu)(-(1 + \nu) \sigma z^2 + z + \bar{\sigma}) z^{(q+1)/3}(\bar{\nu}(1 - \sigma z)^{(q+1)/3} - (\bar{\sigma} - z)^{(q+1)/3})
\]

\[
= (2 - \nu)(-(1 + \nu) \sigma z^2 + z + \bar{\sigma}) z^{(q+1)/3}
\]

\[
\times \left(\bar{\nu}(\sigma^{(q+1)/3} z^{(q+1)/3} - \left(\frac{q + 1}{3}\right) \sigma^{(q+1)/3} - 1 - 2z^{(q+1)/3-1} + \ldots\right)
\]

\[
+ \frac{1}{2} \left(\frac{q + 1}{3}\right) \left(\frac{q - 2}{3}\right) \sigma^{(q+1)/3-2} z^{(q+1)/3-2} + \ldots\right).
\]

The coefficient of \(z^{2(q+1)/3}\) is:

\[
(2 - \nu)(\bar{\nu}\sigma^{(q+1)/3} - \bar{\sigma} + 3\sigma^{(q+1)/3-1} + 2\nu\bar{\sigma} - (1 + \nu) \bar{\nu}\sigma^{(q+1)/3-1} + (1 + \nu)\bar{\sigma}^2).\]
Equating coefficients of $x^{2(q+1)/3}$, multiplying both sides by $\sigma$, and noting $\sigma = \omega^2 \eta$, $\sigma \overline{\eta} = \eta \overline{\eta} = 3$, and $\sigma^{(q+1)/3} = 2 \overline{\nu}$,

$$(-\nu)(3)(2\overline{\nu}) = (2 - \overline{\nu})(3\overline{\nu} - 3 + \overline{\nu} + \nu - (1 + \overline{\nu})(2\overline{\nu}) + 4(1 + \nu)).$$

It follows that

$$-1 = (2 - \overline{\nu})(\nu - 3 + \overline{\nu} + \nu - 2\overline{\nu} - 2\nu + 4 + 4\nu),$$

$$-1 = (2 - \overline{\nu})(-\overline{\nu} - \nu + 1),$$

$$-1 = (2 - \overline{\nu})(2).$$

So $2 = 2 - \overline{\nu}$, or $\overline{\nu} = 0$, a contradiction, implying the desired result.

8. Calculation of $u$ and $v$

In this section we complete the proof of our theorem by showing that in the block $A$ of Section 4, $u = 0$ and $v = 0$. It follows from Lemmas 7.10 and 7.15 that $A$ is of the form

$$\{(\omega^i, -1/2), (\omega^{3i+1}, -1/2 + u), (\omega^{3i+2}, -1/2 + v)\} \quad 0 \leq i < (q + 1)/3,$$

so long as $q \neq 5$. If $u$ and $v$ are such that the blocks containing $\infty$ (of the form $\infty \cup hP$ by Lemma 4.2) together with the translates of $A$ under $H$ form a block design on $X$, we say that $(u, v)$ gives rise to a block design. By Lemma 2.8 of [6] $(0, 0)$ gives rise to the block design $A$. We wish to show that if $(u, v)$ gives rise to a block design, $u = 0$ and $v = 0$.

We note that since $(\omega^{3i+1}, -1/2 + u)$ and $(\omega^{3i+2}, -1/2 + v)$ belong to $Q$, $(\omega^{3i+1})(\omega^{3i+2}) | (1/2 | u) | (-1/2 | v) = 0$. Therefore, $u + \overline{u} = 0$. Likewise $v + \overline{v} = 0$.

The following will save some labor.

**Lemma 8.1.** If $(u, v)$ gives rise to a block design, so too do $(-v, u - v)$, $(v - u, -u)$, and $(-v, -u)$.

**Proof.** If $\phi$ is an automorphism of $H$ and if the blocks containing $\infty$ together with the translates of $A$ form a block design, then so too do the blocks containing $\infty$ together with the translates of $\phi(A)$.

In particular, if $\phi((\alpha, \beta)) = (\omega \alpha, \beta)$, $(\alpha, \beta) \in Q$, $\phi$ is an automorphism of $H$. Then $\phi(A) = \{(\omega^{3i+1}, -1/2), (\omega^{3i+2}, -1/2 + u), (\omega^i, -1/2 + v)\}_{0 \leq i < (q+1)/3}$. Translating by $(0, -\nu)$, we find the block

$$\{(\omega^i, -1/2), (\omega^{3i+1}, -1/2 + \nu), (\omega^{3i+2}, -1/2 + u - \nu)\}_{0 \leq i < (q+1)/3}.$$
Thus, \((-v, u - v)\) gives rise to a block design.

If, however, \(\phi((\alpha, \beta)) = (\tilde{\alpha}, \tilde{\beta}), (\alpha, \beta) \in Q\),

\[
\phi(A) = \{(\omega^{-3i}, -1/2), (\omega^{-3i-1}, -1/2 + \tilde{u}), (\omega^{-3i-2}, -1/2 + \tilde{v})\}_{0 \leq i < (\sigma + 1)/3}
\]

\[
= \{(\omega^{3i}, -1/2), (\omega^{3i+1}, -1/2 - v), (\omega^{3i+2}, -1/2 - u)\}_{0 \leq i < (\sigma + 1)/3}.
\]

Then, \((-v, -u)\) gives rise to a block design.

Shortly, we shall derive algebraic equations which \((u, v)\) must satisfy if \((-v, -u)\) gives rise to a block design. By Lemma 8.1, \((-v, u - v), (v - u, -u),\) and \((-v, -u)\) must also satisfy these equations.

As usual the block containing 0 and \(\infty\) is denoted by \(\Delta\). Of course, \(\Delta = \infty \cup P\).

**Lemma 8.2.** There are \(q^2 - 1\) blocks containing \((0, 0)\) but not \(\infty\). Denoting these blocks by \(B_1, B_2, ..., B_{q^2-1}\), we have

\[
(B_i - (0, 0)) \cap (B_j - (0, 0)) = \phi \quad \text{if} \quad i \neq j,
\]

and

\[
\bigcup_{i=1}^{q^2-1} (B_i - (0, 0)) = X - \Delta.
\]

**Proof.** This follows immediately from the definition of a block design.

**Corollary.** If \(\tau, \delta \in E, \tau \neq 0\), and \(\tau \tau + \delta + \delta = 0\), (of course, then \((\tau, \delta)\) belongs to \(Q\), there is a block \(B_i\) in the above collection containing \((\tau, \delta)\).

**Proof.** Since \(\tau \neq 0\) and \(\Delta = \infty \cup P = \infty \cup \{(0, \delta) : \delta + \delta = 0\}, (\tau, \delta) \notin \Delta,\) so \((\tau, \delta) \in X - \Delta.\)

**Lemma 8.3.** Let \(a_1, a_2, ..., a_{q+1}\) be the elements of the block \(A\) and assume \(\infty \notin A\). The blocks \(k_\lambda(a_i^{-1}A)\), for all \(k_\lambda \in K\) and \(i = 1, ..., q + 1\), are all the blocks which contain \((0, 0)\) but not \(\infty\).

**Proof.** Since \((0, 0)\) is the identity of \(Q\), \((0, 0) \in a_i^{-1}A\). Since \(k_\lambda\) fixes \((0, 0)\), \((0, 0) \in k_\lambda(a_i^{-1}A)\). Since \(\infty \notin A\) and \(k_\lambda a^{-1}\) fixes \(\infty\), \(\infty \notin k_\lambda(a_i^{-1}A)\). Thus, each block of the above form contains \((0, 0)\) but not \(\infty\).

If \(B\) is a block not containing \(\infty\), \(B = k_\lambda(bA), k_\lambda \in K\) and \(b \in Q\). If \((0, 0) \in B, \) since \(k_\lambda\) fixes \((0, 0), (0, 0) \in bA\). Then, \(b^{-1} \in A, \) so \(b = a_i^{-1}\), for some \(i\), and the converse follows.

We now calculate explicitly the blocks containing \((0, 0)\) but not \(\infty\).
Lemma 8.4. Let $j$ be an integer, $0 \leq j < (q + 1)/3$. The sets

\[ B_j = \{(\omega^{3i} - \omega^{3j}, -1 + \omega^{3j-3i}), (\omega^{3i+1} - \omega^{3j}, -1 + u + \omega^{3j-3i-1}), \] \[ (\omega^{3i+2} - \omega^{3j}, -1 + v + \omega^{3j-3i-2})\} \text{ with } 0 \leq i < (q + 1)/3, \]

\[ C_j = \{(\omega^{3i} - \omega^{3j+1}, -1 - u + \omega^{3j+1-3i}), (\omega^{3i+1} - \omega^{3j+1}, -1 + \omega^{3j-3i}), \] \[ (\omega^{3i+2} - \omega^{3j+1}, -1 + v - u + \omega^{3j-3i-1})\} \text{ with } 0 \leq i < (q + 1)/3, \]

\[ D_j = \{(\omega^{3i} - \omega^{3j+2}, -1 - v + \omega^{3j+2-3i}), (\omega^{3i+1} - \omega^{3j+2}, -1 + u - v + \omega^{3j+2-3i}), \] \[ (\omega^{3i+2} - \omega^{3j+2}, -1 + \omega^{3j-3i})\} \text{ with } 0 \leq i < (q + 1)/3, \]

are blocks containing $(0, 0)$. All other blocks containing $(0, 0)$ but not $\infty$ can be obtained from these blocks by applying the transformations $k, k, k, k \in K$, $\mu \neq 0$.

Proof. We use Lemma 8.3 and calculate the sets $a_i^{-1}A$, for $a_i \in A$.

The block $A$ is

\[ \{(\omega^{3i}, -1/2), (\omega^{3i+1}, -1/2 + u), (\omega^{3i+2}, -1/2 + v)\}_{0 \leq i < (q + 1)/3}. \]

The multiplication law is

\[ (\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2 - \alpha_3 \beta_2). \]

It follows from this that $(\alpha, \beta)^{-1} = (-\alpha, -\beta - \alpha \bar{\alpha})$.

Thus, $(\omega^{3j}, -1/2)^{-1} = (-\omega^{3j}, -1/2)$.

Then, $R_j = (\omega^{3j}, -1/2)^{-1} \cdot A$.

Likewise,

\[ (\omega^{3j+1}, -1/2 + u)^{-1} = (-\omega^{3j+1}, -1/2 - u) \]

and

\[ (\omega^{3j+2}, -1/2 + v)^{-1} = (-\omega^{3j+2}, -1/2 - v). \]

Moreover, $C_j = (\omega^{3j+1}, -1/2 + u)^{-1} \cdot A$ and $D_j = (\omega^{3j+2}, -1/2 + v)^{-1} \cdot A$.

The following is somewhat surprising and will be useful in subsequent calculations.

Lemma 8.5. The multiplicative group of $E$ has a cyclic subgroup of order $(q^2 - 1)/3$. Let $\mu$ be its generator. Then, $1, \omega, \omega^2$ represent the cosets of $\langle \mu \rangle$ in $E$. Let $k$ and $\ell$ be integers. Then,

\[ \omega^k - \omega^\ell \in \langle \mu \rangle \text{ if and only if } k + \ell = 0 \pmod{3}, \]

\[ \omega^k - \omega^\ell \in \omega \langle \mu \rangle \text{ if and only if } k + \ell \equiv 2 \pmod{3}, \]

\[ \omega^k - \omega^\ell \in \omega^2 \langle \mu \rangle \text{ if and only if } k + \ell \equiv 1 \pmod{3}. \]
Proof. As usual $\omega^{(q+1)/3} = \nu$. $(\omega^3)^{(q+1)/3} = \nu^2 = \tilde{\nu}$.

Let $x \neq 0$ belong to $E$.
If $x \in \langle \mu \rangle$, $x^{(q^2-1)/3} = 1$, and conversely.
If $x \in \omega \langle \mu \rangle$, $x^{(q^2-1)/3} = (\omega^{-1})^{(q+1)/3}$
$= (\omega/\nu)^{(q+1)/3}$
$= \tilde{\nu}/\nu = \nu$, and conversely.
If $x \in \omega^2 \langle \mu \rangle$, $x^{(q^2-1)/3} = \tilde{\nu}$, and conversely.

Next:

$$(\omega^k - \omega^\ell)^{(q^2-1)/3} = \left(\frac{\omega^{-k} - \omega^{-\ell}}{\omega^k - \omega^\ell}\right)^{(q+1)/3}$$

$$= \left(-\omega^{-(\ell+k)}\right)^{(q+1)/3}$$

Now:

$$(\omega^{-(\ell+k)})^{(q+1)/3} = 1 \quad \text{if and only if } \ell + k \equiv 0 \pmod{3}.$$  
$$(\omega^{-(\ell+k)})^{(q+1)/3} = \nu \quad \text{if and only if } \ell + k \equiv 2 \pmod{3}.$$  
$$(\omega^{-(\ell+k)})^{(q+1)/3} = \tilde{\nu} \quad \text{if and only if } \ell + k \equiv 1 \pmod{3}.$$  

The result follows.

We now use the foregoing results to derive the principal facts used in the calculation of $u$ and $v$.

Lemma 8.6. $(\omega^2, \tau)$ belongs to a block containing $(0,0)$ if and only if $\tau$ belongs to one of the sets

$$\begin{array}{ll}
1 & | u | \omega^{3k-1} \\
(1 - \omega^{3k-1})(1 - \omega^{-3k+1}) & 0 \leq k < (q+1)/3 \\
-1 - u + \omega^{3k+1} & (1 - \omega^{3k+1})(1 - \omega^{-3k-1}) \quad 0 \leq k < (q+1)/3 \\
-1 + \omega^{3k} & (1 - \omega^{3k})(1 - \omega^{-3k}) \quad 0 < k < (q+1)/3.
\end{array}$$

Proof. Using explicitly the forms of the blocks given in Lemma 8.4, we determine explicitly the possible values of $\tau$, where $\tau + \bar{\tau} + 1 = 0$ and $\tau \in E$, such that $(\omega^2, \tau)$ belongs to one of the blocks containing $(0,0)$.

We fix an integer $j$ and determine $\lambda \in E$, such that for some $\tau \in E$, $(\omega^k, \tau) \in k_j(B_j)$, with $B_j$ given by Lemma 8.4. Now, $k_3((\alpha, \beta)) = ((\lambda^3/\bar{\lambda})x, \lambda \bar{\lambda} \beta)$ and the quantities $\lambda^3/\bar{\lambda}$ for $\lambda \neq 0$ in $E$ are precisely the subgroup of the multiplicative group of $E$ of order $(q^2 - 1)/3$. 

If then \((\omega^2, \tau) \in k_\lambda(B_j)\), we must have for some integer \(i,\)

\[
\omega^2 = (\lambda^2/\lambda)(\omega^{3i} - \omega^{3j}), \quad \text{or}
\]

\[
\omega^2 = (\lambda^2/\lambda)(\omega^{3i+1} - \omega^{3j}), \quad \text{or}
\]

\[
\omega^2 = (\lambda^2/\lambda)(\omega^{3i+2} - \omega^{3j}).
\]

By Lemma 8.5, the first of the above right-hand quantities belong to \(\langle \mu \rangle\), the second to \(\omega^2\langle \mu \rangle\), and the third to \(\omega\langle \mu \rangle\). Thus, the only possibility is the second.

Conversely, Lemma 8.5 guarantees that given any integers \(i\) and \(j\), we can choose a suitable \(\lambda\), so that

\[
\omega^2 = (\lambda^2/\lambda)(\omega^{3i+1} - \omega^{3j}).
\]

This yields

\[
\frac{\omega^2}{\omega^{3i+1} - \omega^{3j}} = \frac{\omega^2}{\omega^{3i+1} - \omega^{3j}}.
\]

Consequently

\[
\lambda^2/\lambda = \frac{\omega^2}{\omega^{3i+1} - \omega^{3j}}.
\]

Since \((\omega^2, \tau) = k_\lambda((\omega^{3i+1} - \omega^{3j}, -1 + u + \omega^{3j-3i-1}))\), we obtain

\[
\tau = \frac{-1 + u + \omega^{3j-3i-1}}{(\omega^{3i+1} - \omega^{3j})(\omega^{3i+1} - \omega^{3j-1})}.
\]

\[
= \frac{-1 + u + \omega^{3j-3i-1}}{(1 - \omega^{3j-3i-1})(1 - \omega^{3j-3i})}.
\]

Therefore, \((\omega^2, \tau) \in k_\lambda(B_j)\) if and only if \(\tau\) is of the first form expressed in Lemma 8.6.

Next we consider under what circumstances \((\omega^2, \tau)\) belongs to \(k_\lambda(C_j)\) for some \(\lambda\) and \(j\). Using Lemma 8.5 as before,

\[
\omega^2 = (\lambda^2/\lambda)(\omega^{3i} - \omega^{3j+1}).
\]

Lemma 8.5 guarantees the solvability of this equation for \(\lambda\) and we find

\[
\lambda^2 = \frac{1}{(\omega^{3i} - \omega^{3j+1})(\omega^{3i+1} - \omega^{3j})}.
\]
This yields
\[ \tau = \frac{-1 - u + \omega^{3j+1-3i}}{(\omega^{3i} - \omega^{3j+1})(\omega^{-3i} - \omega^{-3j-1})} = \frac{-1 - u + \omega^{3k+1}}{(1 - \omega^{3k+1})(1 - \omega^{-3k-1})}, \quad \text{with} \quad k = j - i. \]

Thus, \((\omega^2, \tau)\) belongs to some \(k_\lambda(C_j)\) if and only if \(\tau\) belongs to the second set expressed in Lemma 8.6.

Lastly, we consider under what circumstances \((\omega^2, \tau) \in k_\lambda(D_j)\). We find we must have
\[ \omega^2 = \left(\frac{\lambda^2/\lambda}{\lambda^2/\lambda} - \omega^{3j+2}\right). \]

Of course, since \(\omega \neq 0\), \(i \neq j\). Proceeding as before we find
\[ \tau = \frac{-1 - \omega^{3k}}{(1 - \omega^{3k})(1 - \omega^{-3k})} \]
for some integer \(k, k \neq 0\). This yields the result.

**Lemma 8.7.** If \((u, v)\) gives rise to a block design, the \(q\) quantities
\[ u + \frac{1}{2}(\omega^{2k-1} - \omega^{-2k+1}) \quad u + \frac{1}{2}(\omega^{2k+1} - \omega^{-1-2k}) \quad \frac{1}{2}(\omega^{3k} + 1) \quad \frac{1}{2}(\omega^{3k} - 1) \]
\[ 0 \leq k < (q + 1)/3 \quad 0 \leq k < (q + 1)/3 \quad 0 < k < (q + 1)/3 \]
are precisely the \(q\) solutions to the equation
\[ z + \bar{z} = 0 \quad z \in E. \]

**Proof.** By the corollary to Lemma 8.2, given any \(\tau\) such that \(\tau + \bar{\tau} + 1 = 0\), \((\omega^2, \tau)\) belongs to some block containing \((0, 0)\) but not \(\infty\). Since the equation \(\tau + \bar{\tau} + 1 = 0\) has exactly \(q\) solutions, it follows that the \(q\) quantities listed in Lemma 8.6 are precisely the \(q\) solutions to the equation \(\tau + \bar{\tau} + 1 = 0\). Since \(\tau + \bar{\tau} + 1 = 0\) implies \((\tau + \frac{1}{2}) + (\bar{\tau} + \frac{1}{2}) = 0\), adding \(\frac{1}{2}\) to each of the \(q\) quantities listed in Lemma 8.6 gives the \(q\) solutions to the equation \(z + \bar{z} = 0\).

**Lemma 8.8.** Let \(b_1, b_2, \ldots, b_q\) in \(E\) be the \(q\) solutions to the equation \(z + \bar{z} = 0\). Then \(\prod_{i=1}^{q} (z - b_i) = z^q + z\), with \(z\) an indeterminate.

**Proof.** Since \(\bar{z} = z^q\), each \(b_i\) is a root of the polynomial \(z^q + z\). From this the result follows.
COROLLARY. Let \( \sigma_q(x_1, x_2, \ldots, x_q) = \sum_{1 \leq i < j \leq q} x_i x_j \) be the elementary symmetric function. With \( b_1, b_2, \ldots, b_q \) as in Lemma 8.8 \( \sigma_q(b_1, b_2, \ldots, b_q) = 0 \).

**Lemma 8.9.** \( Mu^2 + Nu = 0 \), where

\[
M = \sum_{k=0}^{(q-2)/3} \frac{1}{((1 - \omega^{3k-1})(1 - \omega^{-3k+1}))^2} \\
N = \sum_{k=0}^{(q-2)/3} \frac{\omega^{3k-1} - \omega^{-3k+1}}{((1 - \omega^{3k-1})(1 - \omega^{-3k+1}))^2}
\]

**Proof.** Let

\[
A_k = \frac{1}{(1 - \omega^{3k-1})(1 - \omega^{-3k+1})}, \quad B_k = \frac{\frac{1}{2}(\omega^{3k-1} - \omega^{-3k+1})}{(1 - \omega^{3k-1})(1 - \omega^{-3k+1})}, \\
C_k = \frac{-1}{(1 - \omega^{3k+1})(1 - \omega^{-3k+1})}, \quad D_k = \frac{\frac{1}{2}(\omega^{3k+1} - \omega^{-3k+1})}{(1 - \omega^{3k+1})(1 - \omega^{-3k-1})}, \\
E_k = \frac{1}{2} \frac{\omega^{3k} + 1}{(\omega^{3k} - 1)}, \quad k \neq 0.
\]

By Lemma 8.7 the quantities \( A_k u + B_k, C_k u + D_k \), and \( E_k \) are precisely the solutions to the equation \( z + \bar{z} = 0 \).

By the corollary to Lemma 8.8,

\[
\sigma_2(\cdots A_k u + B_k, \ldots, C_k u + D_k, \ldots, E_k \cdots) = 0.
\]

Therefore,

\[
0 = \sum_{0 \leq \ell < m < (q+1)/3} (A_\ell u + B_\ell)(A_m u + B_m) + (C_\ell u + D_\ell)(C_m u + D_m) \\
+ \sum_{0 < \ell < m < (q+1)/3} E_\ell E_m + \sum_{0 < \ell < m < (q+1)/3} \frac{2}{0 < m < (q+1)/3} (A_\ell u + B_\ell)(C_m u + D_m) \\
+ \frac{2}{0 < \ell < m < (q+1)/3} E_\ell (A_m u + B_m) + E_\ell (C_m u + D_m)
\]

Note that \( A_{-k} = -C_k, B_{-k} = -D_k \). Therefore,

\[
0 = 2 \sum_{0 \leq \ell < m < (q+1)/3} (A_\ell u + B_\ell)(A_m u + B_m) \\
- \sum_{0 \leq \ell < (q+1)/3} \frac{2}{0 < m < (q+1)/3} (A_\ell u + B_\ell)(A_m u + B_m) \\
+ \sum_{0 < \ell < m < (q+1)/3} E_\ell E_m.
\]
A CHARACTERIZATION OF $U_d(q)$

From this it follows that

$$- \sum_{0 < \ell < (q+1)/3} (A \ell B + B \ell)^2 + \sum_{0 < \ell < (q+1)/3} E \ell E m = 0.$$ 

As noted earlier $(0, 0)$ is an admissible pair and so $u = 0$ is a solution to this equation.

Consequently,

$$\left( \sum_{0 < \ell < (q+1)/3} A \ell^2 \right) u^2 + \left( \sum_{0 < \ell < (q+1)/3} 2A \ell B \ell \right) u = 0.$$ 

Interpretation of this equation yields Lemma 8.9.

**Lemma 8.10.** $N = (\tilde{v} - v)/3^5$, with $v = \omega^{(q+1)/3}$.

$(N$ is defined in Lemma 8.9$).$

**Proof.** We consider the contour integral

$$I = \frac{1}{2\pi i} \int_R \frac{m(z \omega^{-1} - \omega z^{-1})}{z(z^m - 1)} \frac{(z \omega^{-1} - \omega z^{-1})}{(2 - \omega^{-1}z - \omega z^{-1})^2} dz,$$

where $I$ is a circle of radius $R$ in the complex plane, centered at $0$, $R > 1$.

$\omega$ is a primitive $3m$-th root of unity.

Now,

$$\frac{m(z \omega^{-1} - \omega z^{-1})}{z(z^m - 1)(2 - \omega^{-1}z - \omega z^{-1})^2} = \frac{m\omega(z + \omega)}{(z^m - 1)(z - \omega)^3}.$$

This function therefore has simple poles at the points $z = \omega^{3k}$, where $k$ is some integer. The only other pole is at the point $z = \omega$.

The residue of the function at $\omega^{3k}$ is

$$\lim_{z \to \omega^{3k}} \frac{m(z \omega^{-1} - \omega z^{-1})(z - \omega^{3k})}{z(z^m - 1)(2 - \omega^{-1}z - \omega z^{-1})^2}$$

$$= (\omega^{3k-1} - \omega^{1-3k}) \lim_{z \to \omega^{3k}} \frac{m(z - \omega^{3k})}{z(z^m - 1)(2 - \omega^{-1}z - \omega z^{-1})^2}$$

$$= (\omega^{3k-1} - \omega^{1-3k}) \lim_{z \to \omega^{3k}} \frac{m}{z(z^m - 1)(2 - \omega^{-1}z - \omega z^{-1})^2}$$

$$= \frac{\omega^{3k-1} - \omega^{1-3k}}{(1 - \omega^{3k-1})(1 - \omega^{1-3k})^3}.$$
Next, we calculate the residue of this function at \( z = \omega \). We determine the Taylor series expansion of
\[
\frac{z + \omega}{z^m - 1} = a_0 + a_1(z - \omega) + a_2(z - \omega)^2 + \ldots
\]
at \( z = \omega \). The residue of the function is then \( m\omega a_2 \).

Now,
\[
\frac{1}{z^m - 1} = \frac{1}{((z - \omega) + \omega)m - 1} = \frac{1}{\omega^m - 1 + \sum_{k=0}^{m-1} \left( \frac{m}{k} \right) \omega^k(z - \omega)^{m-k}}
\]
\[
= \frac{1}{\omega^m - 1} \left( 1 + \frac{m\omega^{m-1}}{1 - \omega^m} (z - \omega) \right)
\]
\[
+ \left( \frac{\omega^{m-2}}{1 - \omega^m} \frac{m(m - 1)}{2} + \frac{1}{(1 - \omega^m)^2} m^2\omega^{2m-2} \right) (z - \omega)^2
\]
\[
+ O((z - \omega)^3).
\]

Then,
\[
\frac{z + \omega}{z^m - 1} = ((z - \omega) + 2\omega) \frac{1}{z^m - 1}.
\]

Therefore,
\[
a_2 = \frac{1}{\omega^m - 1} \left( \frac{2\omega^{m-1}}{1 - \omega^m} \cdot \frac{m(m - 1)}{2} + \frac{2m^2\omega^{2m-1}}{(1 - \omega^m)^2} + \frac{m\omega^{m-1}}{1 - \omega^m} \right).
\]

The residue at \( z = \omega \) is therefore
\[
m\omega a_2 = \frac{-m}{(1 - \omega^m)^2} ((1 - \omega^m)(m(m - 1)\omega^m + m\omega^m) + 2m^2\omega^{2m})
\]
\[
= \frac{-m^3}{(1 - \omega^m)^2} (\omega^m + \omega^{2m}).
\]

Letting \( \omega^m = \nu \), since \( \omega \) is a primitive \((3m)\)-th root of unity, \( \nu \) is a cube root of unity and \( \nu \neq 1 \). The residue is therefore \(-m^3/(1 - \nu^3)(\nu + \nu^2)\). Since \((1 - \nu)^3 = 1 - 3\nu + 3\nu^2 - \nu^3 = 3\nu^2 - 3\nu\) and since \( \nu + \nu^2 = -1 \), the
A CHARACTERIZATION OF \( U_3(q) \)

residue is \( m^3/3(v^2 - v) \). Now \( (v^2 - v)(v^2 - v) = v + v^2 - 2 = -3 \). Thus, the residue is \( m^3(v - v^3)/9 \).

It follows that

\[
I = \sum_{0 \leq k < m} \frac{\omega^{3k-1} - \omega^{1-3k}}{(1 - \omega^{3k})(1 - \omega^{1-3k})^2} + \frac{m^3(v - v^2)}{9}.
\]

Examination of the integrand shows that as \( R \to \infty, I \to 0 \). Since \( I \) is independent of \( R \), \( I = 0 \). Thus,

\[
T = \sum_{0 \leq k < m} \frac{\omega^{3k-1} - \omega^{1-3k}}{(1 - \omega^{3k})(1 - \omega^{1-3k})^2} = \frac{m^3(v^2 - v)}{9}.
\]

Letting \( m = (1 + q)/3 \), we find \( T = (q + 1)^3(v^2 - v)/3^5 \). Multiplying both sides of the foregoing identity by \( 3^5 \prod_{0 \leq k < m} ((1 - \omega^{3k})(1 - \omega^{1-3k}))^2 \), we obtain an identity (A) valid in the ring \( \mathbb{Z}[\omega] \). Quotienting by a suitable prime ideal in \( \mathbb{Z}[\omega] \), we find a similar identity in the field \( E \). From this the desired result follows.

**Lemma 8.11.** \( u = 0 \) and \( v = 0 \).

**Proof.** By Lemma 8.9 \( M u^2 + N u = 0 \). By Lemma 8.10, \( N \neq 0 \). By Lemma 8.1 \( (-v, u - v), (v - u, -u), \) and \( (-v, -u) \) are also solutions to this equation. In particular, \( M v^2 - N v = 0 \).

If \( M = 0 \), then \( u = v = 0 \).

If \( M \neq 0 \), let \( a = -N/M \). Then, we must have \( u = 0 \) or \( u = a \) and \( v = 0 \) or \( v = -a \). Thus, the only possible solutions giving rise to block designs are \( (0, 0), (a, 0), (0, -a), \) and \( (a, -a) \).

If \((a, 0)\) is a solution, applying \((u, v) \rightarrow (-v, u - v)\), we find \((0, a)\) is a solution, a contradiction by looking at our list of possible solutions.

If \((0, -a)\) is a solution, applying \((u, v) \rightarrow (-v, -u)\), we find that \((a, 0)\) is a solution, which is impossible by the previous paragraph.

If \((a, -a)\) is a solution, applying \((u, v) \rightarrow (-v, u - v)\), we find that \((a, 2a)\) is a solution. Since \((a, 2a) \neq (a, -a)\), as \( 3 \neq 0 \) in \( F \), this is again impossible.

It follows that \( u = 0 \) and \( v = 0 \).

We immediately obtain:

**Lemma 8.12.** \( \mathcal{A} = \mathcal{B} \).

**Proof.** This is immediate from Lemma 4.5 and the previous lemma.

By the corollary to the main theorem of [6], the proof of the theorem is complete.
ACKNOWLEDGMENT

The author wishes to extend his thanks to his advisor Professor Daniel Gorenstein.

REFERENCES