Subgroups of linear groups over $\mathbb{F}_2$

generated by elements

of order 3 with 2-dimensional commutator

Hans Cuypers

August 15, 2007

Abstract

Let $V$ be a vector space over the field $\mathbb{F}_2$. We investigate subgroups of the linear group $\text{GL}(V)$ which are generated by a conjugacy class $D$ of elements of order 3 such that all $d \in D$ have 2-dimensional commutator space $[V,d]$.

1 Introduction

In his revision of Quadratic Pairs [2, 3], Chermak [2] classifies various subgroups of the symplectic groups $\text{Sp}(2n, 2)$ generated by elements $d$ of order 3 with $[V,d]$ being 2-dimensional. Here $V$ is the natural module of $\text{Sp}(2n, 2)$. Besides the full symplectic group he encounters orthogonal and unitary groups over the field with 2 or 4 elements respectively, as well as alternating groups. Chermak’s proof of his classification theorem is inductive and relies mainly on methods from geometric algebra.

By using discrete geometric methods we are able to classify subgroups of $\text{GL}(V)$, where $V$ is an $\mathbb{F}_2$ vector space of possibly infinite dimension, generated by elements $d$ of order 3 with $[V,d]$ being 2-dimensional.

In particular, we prove the following.

1.1 Theorem. Let $V$ be a vector space of dimension at least 3 over the field $\mathbb{F}_2$. Suppose $G \leq \text{GL}(V)$ is a group generated by a conjugacy class $D$ of elements of order 3 such that

(a) $[V,d]$ is 2-dimensional for all $d \in D$;

(b) $[V,G] = V$ and $C_V(G) = 0$. 

1
Then we have one of the following.

(a) There exists a subspace $\Phi$ of $V^*$ annihilating $V$ such that $G = T(V, \Phi)$; the class $D$ is the unique class of elements of order 3 with 2-dimensional commutator on $V$.

(b) $\dim(V) = 3$ and $G = 7 : 3$; $D$ is one of the two classes of elements of order 3 in $G$.

(c) $\dim(V) = 4$ and $G \simeq \text{Alt}_7$ (inside $\text{Alt}_8 \simeq \text{GL}(4, 2)$); the class $D$ corresponds to the class of elements of order 3 which are products of two disjoint 3-cycles inside $\text{Alt}_7$.

(d) $\dim(V) \geq 6$, and $G = \text{Sp}(V, f)$ with respect to some nondegenerate symplectic form on $V$; the class $D$ is the unique class of elements of order 3 with 2-dimensional commutator on $V$.

(e) $\dim(V) \geq 6$ and $G$ is isomorphic to $\Omega(V, q)$ for some nondegenerate quadratic form $q$ on $V$. The class $D$ is the unique class of elements of order 3 with 2-dimensional commutator on $V$.

(f) $G$ is isomorphic to $\text{Alt}(\Omega)$ for some set $\Omega$ of size at least 5; the class $D$ corresponds to the class of 3-cycles, or in case $|\Omega| = 6$, the class of elements which are a products of two disjoint 3-cycles. The space $V$ is the subspace of the space $F_2\Omega$ generated by all vectors of even weight, or, in case $|\Omega|$ is even, the quotient of this subspace by the all one vector.

(g) $V$ carries a $G$-invariant structure of an $F_4$-space $V_4$ such that $G$ is isomorphic to $R(V_4, \Phi)$, where $\Phi$ is a subspace of $V_4^*$ annihilating $V_4$. The class $D$ is the class of reflections in $G$.

(h) $V$ carries a $G$-invariant structure $(V_4, h)$ of an $F_4$-space $V_4$ equipped with a nondegenerate hermitian form $h$ such that $G$ is isomorphic to $\text{RU}(V_4, h)$, the subgroup of $\text{GU}(V_4, h)$ generated by all reflections. The class $D$ is the class of reflections in $G$.

As indicated above, our proof of this theorem is of geometric nature. By using methods similar to those developed in Cameron and Hall [1] and Cohen, Cuypers and Sterk [4] we are able to show that the subspaces $[V, d]$ with $d \in D$, are either all the lines of $\mathbb{P}(V)$ (leading to the cases (a)-(c) of the theorem) or of a cotriangular space embedded in $\mathbb{P}(V)$ (cases (d)-(f)) or these spaces are (part of) the one dimensional subspaces of an $F_4$ space.
induced on $V$ (leading to the case (g) and (h)). Although not entirely self contained (we rely on Jonathan Hall’s classification of cotriangular spaces [8]), our methods are completely elementary.

In the following section we describe the examples occurring in the conclusion of Theorem 1.1 somewhat closer. The Sections 3 and 4 are devoted to the proof of Theorem 1.1. In particular, in Section 3 we consider the case where there are $d, e \in D$ with $[V, d] \cap [V, e]$ being one dimensional leading to the groups defined over $F_2$, while the final section covers the remaining cases of groups defined over $F_4$.

2 The examples and their geometries

Suppose $V$ is a vector space over the field $F_2$. If $\dim(V) < \infty$, then the generic example of a group $G$ generated by a class $D$ of elements $d$ with $[V, d]$ of dimension 2 is the group $\text{SL}(V)$. The elements in $D$ then correspond to conjugates of the element

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \ddots & \vdots & & & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

In small dimension we encounter two exceptional examples of groups satisfying the hypothesis of Theorem 1.1. If $V$ has dimension 4, then $\text{SL}(4, 2) \simeq \text{Alt}_8$. Under this isomorphism the elements in $D$ correspond to those elements in $\text{Alt}_8$ that are products of two disjoint 3-cycles. The subgroup $\text{Alt}_7$ of $\text{Alt}_8$ also acts irreducibly on $V$ is of course generated by such elements. If $\dim(V) = 3$, then $\text{SL}(3, 2)$ contains a subgroup $7:3$, which is irreducible on $V$. This subgroup is of course also generated by its elements of order 3.

Also if $\dim(V)$ is infinite we encounter more examples. Let $v \in V$ and $\varphi \in V^*$ with $\varphi(v) = 0$. Then $\tau_{v, \varphi}$ denotes the transvection

$$\tau_{v, \varphi} : V \to V, w \in V \mapsto w + \varphi(w)v.$$ 

The group $G = T(V, \Phi)$ where $\Phi$ is a subspace of $V^*$ is defined to be the subgroup of $\text{GL}(V)$ generated by all transvections $\tau_{v, \varphi}$ with $v \in V, \varphi \in \Phi$ where $\varphi(v) = 0$. Suppose $\Phi$ annihilates $V$, then $C_V(G) = 0$. If $v, w \in V$ and $\varphi, \psi \in \Psi$ such that $\varphi(v) = \psi(w) = 0$ but $\psi(v) = \varphi(w) = 1$, then the
product \( d = \tau_v \tau_w \) is an element of order 3 with commutator \([V, d] = \langle v, w \rangle\) of dimension 2. Let \( D \) denote the set of all such elements. Then \( D \) is a conjugacy class of \( G \) generating \( G \). Clearly \([V, d]\) with \( d \) running through \( D \) is the set of all 2-spaces of \( V \). So, \([V, G] = V\).

Next suppose \((V, f)\) be a nondegenerate symplectic space over \( \mathbb{F}_2 \). For any nonzero vector \( v \in V \) the transvection

\[
t_v : V \to V, w \in V \mapsto w + f(v, w)v
\]

is an element of \( \text{Sp}(V, f) \). It is well known that the set of such transvections forms a conjugacy class of 3-transpositions in \( \text{Sp}(V, f) \). If we set \( D \) to be the set of all products \( t_v t_w \) where \( v, w \in V \) with \( f(v, w) = 1 \), then \( D \) is a conjugacy class of elements of order 3 in \( G \) with \([V, d]\) of dimension 2.

By \( \text{Sp}(V, f) \) denotes the partial linear space \((P, L)\) where \( P \) consists of all the nonzero vectors of \( V \). A line in \( L \) is the set of three nonzero vectors in a 2-dimensional subspace \( W \) of \( V \) on which \( f \) does not vanish.

Notice that for each \( d \in D \), the commutator \([V, d]\) determines a unique line of \( \text{Sp}(V, f) \). The class \( D \) generates \( G \) provided \( \dim(V) \geq 6 \). If \( \dim(V) = 4 \) or 2, then \( D \) generates the derived groups \( \text{Alt}_6 \leq \text{Sp}(4, 2) \) and \( \text{Alt}_3 \leq \text{Sp}(2, 2) \), respectively.

Next consider a quadratic form \( Q \) on \( V \) whose associated symplectic form is \( f \). Then any transvection \( \tau_v \), where \( v \in V \) with \( Q(v) = 1 \), is in the orthogonal group \( \text{O}(V, Q) \). Suppose \( \dim(V) \geq 6 \). Then the subset \( D_Q \) of \( D \) of all elements obtained as products \( \tau_v \tau_w \) with \( Q(v) = Q(w) = 1 \) and \( f(v, w) = 1 \) is a conjugacy class of \( \Omega(V, Q) \) generating this group.

The corresponding geometry \( \mathcal{N}(V, Q) \) consists of has as points the vectors \( v \in V \) with \( Q(v) = 1 \). A typical line is the set of three nonzero vectors in an elliptic 2-space, i.e., a 2-space in which \( Q(v) = 1 \) for any nonzero vector \( v \) contained in it. Clearly, \( \mathcal{N}(V, Q) \) is contained in \( \text{Sp}(V, f) \).

There is yet another class of subgroups of \( \text{Sp}(V, f) \) generated by a subset of \( D \). Indeed, a symplectic space \((V, f)\) can be obtained as follows. Suppose \( \Omega \) is a set. Let \( \mathbb{F}_2 \Omega \) be the \( \mathbb{F}_2 \)-vector space with basis \( \Omega \). By \( E\mathbb{F}_2 \Omega \) we denote the subspace of \( \mathbb{F}_2 \Omega \) generated by the vectors \( \omega_1 + \omega_2 \), where \( \omega_1, \omega_2 \in \Omega \). Notice that the standard dot product on \( \mathbb{F}_2 \Omega \) induces a symplectic form on \( E\mathbb{F}_2 \Omega \). So, we can identify \((V, f)\) with this symplectic space. The transpositions in \( \text{Sym}(\Omega) \) induce transvections on \( V \). So, the 3-cycles in \( \text{Sym}(\Omega) \) induce a subset \( D_3 \) of \( D \) generating a subgroup of \( \text{GL}(V) \) isomorphic to the alternating group \( \text{Alt}(3) \). The corresponding geometry \( \mathcal{T}(\Omega) \) has as points the set of vectors \( \omega_1 + \omega_2 \), where \( \omega_1 \neq \omega_2 \in \Omega \), a line being the triples of points of the form \( \omega + \omega' \), where \( \omega \neq \omega' \) are from some subset of size 3 of \( \Omega \).
The above geometries are all examples of cotriangular spaces. These are partial linear spaces with lines of size three and the property that any point \( p \) not on a line \( l \) is collinear with no point or with two points on \( l \). A cotriangular space is called irreducible if it is connected and for any pair of points \( p, q \) we have that \( p^\perp = q^\perp \) implies \( p = q \). Here \( p^\perp \) denotes the set consisting of \( p \) and all points not collinear with \( p \). The spaces described above are characterized by the following result of Jonathan Hall.

2.1 (J.I. Hall [8]) Let \( V \) be a vector space over the field \( \mathbb{F}_2 \). Let \( \Pi = (P, L) \) be an irreducible cotriangular space, where \( P \) is a subset of \( V \setminus \{0\} \), and each line in \( L \) is a triple of points inside a 2-dimension subspace of \( V \). If \( P \) generates \( V \) and \( \bigcap_{p \in P} \langle p^\perp \rangle = 0 \) we have one of the following.

(a) \( \Pi = Sp(V, f) \) for some nondegenerate symplectic form \( f \) on \( V \).

(b) \( \Pi = N(V, Q) \) for some nondegenerate quadratic form \( Q \) on \( V \).

(c) There is a set \( \Omega \) such that \( V = E_{\mathbb{F}_2}(\Omega) \) and \( \Pi = T(\Omega) \).

Finally we shall discuss the examples coming from groups defined over \( \mathbb{F}_4 \). Let \( V_4 \) be a vector space over \( \mathbb{F}_4 \). For every \( v \in V_4 \) and \( \varphi \in V_4^* \), with \( \varphi(v) \neq 0,1 \) we define the map

\[
 r_{v,\varphi} : V \to V_4, w \in V_4 \mapsto w - \varphi(w)v.
\]

The map \( r_{v,\varphi} \) is a reflection with center \( \langle v \rangle \) and axis \( \ker \varphi \). A reflection has order 3. If \( \Phi \) is a subspace of \( V_4^* \), then denote by \( R(V_4, \Phi) \) the subgroup of \( GL(V_4) \) generated by all reflections \( r_{v,\varphi} \) with \( v \in V_4, \varphi \in \Phi \) and \( \varphi(v) \neq 0,1 \). If \( \dim(V_4) \) is finite dimensional, then \( R(V_4, V_4^*) = GL(V_4) \). Let \( V \) denote the space \( V_4 \) considered as an \( \mathbb{F}_2 \)-space. The reflections provide examples of elements of order 3 having a 2-dimensional commutator on \( V \).

If \( h \) is a nondegenerate Hermitian form on \( V_4 \), then for each vector \( v \in V \) with \( h(v,v) = 1 \) and \( \alpha \in k, \alpha \neq 0,1 \), the map

\[
 r_v : w \in V_4 \mapsto w + \alpha h(w,v)v
\]

is a reflection in the finitary unitary group

\[
 FU(V_4, h) = \{ g \in FGL(V) \mid \forall x, y \in V \quad h(xg, yg) = h(x, y) \}.
\]

In fact all these reflections generate the group \( FU(V_4, h) \).

Notice that in these examples over \( \mathbb{F}_4 \), the commutators \([V, r_1]\) and \([V, r_2]\), where \( r_1 \) and \( r_2 \) are reflections on \( V_4 \) either are equal or meet trivially.
3 Geometries with points and groups over $\mathbb{F}_2$

Let $V$ be vector space over $\mathbb{F}_2$, and suppose $G \leq \text{GL}(V)$ is generated by a normal set $D$ of elements $d \in G$ of order 3 such that $[V, d]$ is 2-dimensional. (Here normal means closed under conjugation.)

3.1 Suppose $d \in D$. Then $V = [V, d] \oplus C_V(d)$

Proof. Suppose $v \in V$ with $[v, d] \in [V, d] \cap C_V(d)$. Then $0 = [vd + v, d] = vd^2 + vd + vd + v = vd^2 + v$. But then $[v, d] = (vd^2 + v)d = 0$. We have found that $[V, d] \cap C_V(d) = 0$. As each $v \in V$ equals $v = v + [vd, d] + [vd, d] = v + vd + vd^2 + [vd, d] \in C_V(d) + [V, d]$ we have proven that $V = [V, d] + C_V(d)$.

3.2 Let $W$ be a subspace invariant under $d \in D$. Then $W \subseteq C_V(d)$ or $[V, d] \subseteq W$.

Proof. Suppose $w \in W$ is not centralized by $d$. Then $0 \neq [w, d] \in W \cap [V, d]$. But then $[V, d] = ([w, d], [w, d]d)$ is contained in $W$.

A $D$-line, or just line is a subspace of $V$ of the form $[V, d]$ with $d \in D$. A $D$-point is a 1-space of $V$ which is the intersection of two distinct $D$-lines. Both points and lines are also considered to be points and lines in the projective space $\mathbb{P}(V)$.

Let $\mathcal{P}$ be the set of $D$-points and $\mathcal{L}$ the set of $D$-lines. The geometry $\Pi(D)$ is the pair $(\mathcal{P}, \mathcal{L})$, where incidence is symmetrized containment.

If $W$ is a subspace of $V$, then by $\Pi(D)_W$ we denote the pair $(\mathcal{P}_W, \mathcal{L}_W)$ where $\mathcal{L}_W$ is the set of $D$-lines contained in $W$, and $\mathcal{P}_W$ the set of intersection points of two distinct lines in $\mathcal{L}_W$.

Let $U$ be a subspace of $V$. Then by $D_U$ we denote the set of all $d \in D$ with $[V, d] \subseteq U$. The subspace $A_U$ of $V$ is equal to $\bigcap_{d \in D_U} C_V(d)$.

3.3 If $l$ is a $D$-line, then it contains no or three $D$-point.

Proof. Since $[V, d] \cap C_V(d) = 0$ by (3.1), we find that $d$ is transitive on the three nonzero vectors in $[V, d]$.

3.4 Suppose $l$ and $m$ are distinct $D$-lines intersecting at a point. Let $W$ be the subspace $l + m$ of $V$. Then $\Pi(D)_W$ is either a dual affine plane or a projective plane in $\mathbb{P}(W)$.

The group $\langle D_W \rangle$ is transitive on the lines in $\mathcal{L}_W$. 

6
Proof. Straightforward computation in $GL(3, 2)$. \hfill\Box

3.5 If $D$ is a conjugacy class in $G$, then $G$ is transitive on $\mathcal{L}$ and $\mathcal{P}$.

Proof. Transitivity of $G$ on $D$ implies transitivity on lines. As each $d \in D$ is transitive on the three 1-spaces of the line $[V, d]$, transitivity on points follows immediately. \hfill\Box

3.6 If $l, m \in \mathcal{L}$ are in the same connected component $\Pi_0$ and $l = l_0, \ldots, l_k = m$ is a path from $l$ to $m$ inside $\Pi_0$, then there is a $g \in \langle D_{l_1}, \ldots, D_{l_k} \rangle$ with $lg = m$.

Proof. By (3.4), there is for $i = 1, \ldots, k - 1$ a $g_i \in \langle D_{l_1}, \ldots, D_{l_k} \rangle$ with $l_i g_i = l_{i+1}$. But then $g = g_1 \cdots g_{k-1}$ maps $l$ to $m$. \hfill\Box

3.7 Suppose $l \neq m \in \mathcal{L}$ are in the same $G$-orbit on $\mathcal{L}$. Then $l \subseteq A_m$ if and only if $m \subseteq A_l$.

Proof. Suppose $l \subseteq A_m$, then $l$ and therefore also $\text{Alt}_l$ is invariant under each element $d \in D_m$. So, by (3.2) we either have $m \subseteq A_l$ or $A_l \subseteq A_m$. In the latter case the inclusion is proper since $l \in A_m$ but not in $A_l$.

Now suppose $m \not\subseteq A_l$. Then $A_l \subset A_m$. Let $g$ be an element in $G$ with $mg = l$. Then $A_l = A_m g \subset A_m$. However, as $g \in G$ is the product of a finite number of elements from $D$, the subspace $C_V(g)$ has finite codimension in $V$. As $g$ induces a bijective map $A_m/(A_m \cap C_V(g)) \to A_m g/(A_m g \cap C_V(g))$ between finite dimensional spaces, these spaces are equal. This implies $A_l = A_m g = A_m$ contradicting the above. \hfill\Box

3.8 Suppose $\mathcal{L}$ is a single $G$-orbit. Let $d, e \in D$. If $\dim(C_V(d) \cap [V, e]) = 1$, then $[V, d]$ to $[V, e]$ are in the same connected component of $\Pi(D)_{[V, d] + [V, e]}$.

Proof. Notice that $[V, e] \not\subseteq A_{[V, e]}$. So, by (3.7) we can assume, eventually after replacing $e$ by some appropriate element in $A_{[V, e]}$, that $[V, d] \not\subseteq C_V(e)$.

The line $[V, e]d$ and $[V, e]$ intersect in the point $C_V(d) \cap [V, e]$ and are contained in the 4-dimensional subspace $[V, d] + [V, e]$. The subspace $W = [V, e] + [V, e]d$ is 3-dimensional and $\Pi(D)_{|W}$ is a dual affine of projective plane inside $\mathbb{P}(W)$.

The line $[V, d]$ intersects $\mathbb{P}(W)$ in a point $p$ of $\mathbb{P}(W)$. If this point $p$ is in $\mathcal{P}_W$ we are done. Thus assume that this point is not in $\mathcal{P}$. In this case $\Pi(D)_{|W}$ is a dual affine plane and $p$ is the unique point of $\mathbb{P}(W)$ not in this dual affine plane. Moreover, $p$ equals $C_W(e)$. 7
By the same arguments we can assume that \([V,d]\) meets \(W' = [V,e] + [V,e]d^2\) in the point \(q = C_{W'}(e)\) which is the unique point of \(\mathbb{P}(W')\) not in \(\Pi(D)_{W'}\). As \(p \neq q\), we find that \([V,d] = \langle p, q \rangle \subseteq C_V(e)\), which contradicts our assumption. □

3.9 Suppose \(\mathcal{L}\) is a single \(G\)-orbit, \(C_V(G) = 0\) and \(\mathcal{P} \neq \emptyset\). Then \(\Pi(D)\) is connected.

Proof. Assume that \([V,d]\) and \([V,e]\) are in distinct connected components of \(\Pi\). Since \(G\) is generated by \(D\), we can assume that \(d\) and \(e\) do not commute.

By (3.8) we can assume that \(C_{V}(e) \cap [V,d] = 0\). Let \(f \in D\) such that \([V,f]\) meets \([V,d]\) in a point and let \(W\) be the subspace \([V,d] + [V,f]\). If \(\Pi(D)_{W}\) contains a line \([V,g]\) with \(g \in D\) such that \(C_{V}(e) \cap [V,g]\) is 1-dimensional, then (3.8) gives a contradiction with \([V,e]\) being in a connected component of \(\Pi(D)\) different from the one containing \([V,d]\). Hence \(\Pi(D)_{W}\) is a dual affine plane, moreover, \(C_{V}(e)\) meets \(W\) in the unique point \(p\) not in that dual affine plane.

As \(C_{V}(G) = 0\), there is an element \(h \in D\) not centralizing \(p\). But then \(C_{V}(h)\) meets at least one of the lines of the dual affine plane \(\Pi(D)_{W}\) in a point. Without loss of generality we may assume this line to be \([V,d]\). Let \(U = [V,d] + [V,h]\). If \([V,d]\) and \([V,h]\) meet nontrivially, then \(\Pi(D)_{U}\) is a projective plane containing a line \(l \in \mathcal{L}\) which meets \(C_{V}(e)\) in a point. As above, this leads by (3.8) to a contradiction. Thus \(\dim(U) = 4\). But then \(U_1 = [V,d] + [V,d]h\) and \(U_2 = [V,d] + [V,d]h^2\) are two distinct 3-dimensional spaces on \([V,d]\). As above, for both \(i = 1\) or \(2\), we can assume that \(C_{V}(e)\) meets \(U_i\) in a point, which is the unique point of \(U_i\) which is not in \(\mathcal{P}_{U_i}\). But that implies that \(C_{U_i}(e) = C_{U_i}(d)\).

By (3.6) the above reasoning also applies to \([V,h]\) and \(h\), so that \(C_{V}(e) = C_{V}(h)\). But \(C_{V}(h) \neq C_{V}(d)\), which is a final contradiction. □

Let \(p, q \in \mathcal{P}\) be points. We write \(p \sim q\) if \(p\) and \(q\) are distinct collinear points of \(\Pi\). By \(p \perp q\) we mean that \(p\) and \(q\) are equal or noncollinear. By \(p^\perp\) we denote the set of all points collinear to \(p\) (excluding \(p\)). The complement of \(p^\perp\) is the set \(p^\perp\).

If for \(p\) and \(q\) we have \(p^\perp = q^\perp\), then we write \(p \equiv q\). The relation \(\equiv\) is obviously an equivalence relation.

3.10 Suppose \(\Pi\) is connected. If \(p \neq q \in \mathcal{P}\) with \(p \equiv q\), then \(C_V(G) \cap p + q \neq 0\).
Proof. Suppose $p \neq q \in \mathcal{P}$ with $p \equiv q$. Notice that $p \perp q$. Let $r$ be the third point on the projective line through $p$ and $q$. If $l \in \mathcal{L}$ is a line on $p$, then $\Pi_W$ is a dual affine plane, where $W$ is the subspace spanned by $l$ and $q$. So, each $d \in D_l$ centralizes $r$.

If $p_1$ and $q_1$ are two noncollinear points in $\Pi_W$, then the projective line on $p_1$ and $q_1$ contains $r$. Moreover, if $s \in p_1^\perp$ but not in $q_1^\perp$, then either $s$ is collinear to $p$ but not to $q$, or vice versa. As this contradicts $p \equiv q$, we find that $p_1 \equiv q_1$.

But that implies that by connectivity of $\Pi$ we find that $r$ is in $C_V(d)$ for each $d \in D$. In particular, $C_V(G) \cap p + q \neq 0$. \hfill \Box

3.11 Theorem. Suppose $D$ is a conjugacy class in $G$, $C_V(G) = 0$, $[V,G] = V$ and $\mathcal{P} \neq \emptyset$. Then $\Pi$ is one of the following spaces:

(a) $\Pi = \mathbb{P}(V)$.

(b) $\Pi = \mathcal{Sp}(V,f)$ for some nondegenerate symplectic form $f$ on $V$.

(c) $\Pi = \mathcal{N}(V,Q)$ for some nondegenerate quadratic form $Q$ on $V$.

(d) There is a set $\Omega$ such that $V = E\mathbb{F}_2(\Omega)$ and $\Pi = T(\Omega)$.

Proof. Suppose $\Pi$ contains two lines $l$ and $m$ such that for $W = l + m$ we have $\Pi(D)_W = \mathbb{P}(W)$. Denote the latter plane by $\pi$. We claim that $\Pi(D) = \mathbb{P}(V)$. To prove this claim it suffices to show that all planes of $\Pi(D)$ are projective. Suppose not, then by transitivity of $G$ on $\mathcal{L}$, there is a line $n \in \mathcal{L}$ meeting $l$ such that $\Pi(D)_U$ is a dual affine plane, where $U = l + n$. Let $p$ be the unique point of $\mathbb{P}(U)$ not in $\Pi(D)_U$. Now consider $U + W$. The geometry $\Pi(D)_{U+W}$ consists of all the lines of $\mathbb{P}(U + W)$ not on $p$. As a consequence we see that all elements in $D_{U+W}$ have to centralize $p$.

Since $C_V(G) = 0$, there is a $d \in D$ not centralizing $p$. But then the element $d$ centralizes a line $k$ in $U + W$ not on $p$ and thus in $\mathcal{L}$. \hfill \Box

3.12 Theorem. Suppose $\Pi = \mathbb{P}(V)$. Then $G = T(V,\Phi)$ for some subspace $\Phi$ of $V^*$ annihilating $V$, or $\dim(V) = 4$ and $G \simeq \text{Alt}_7$, or $\dim(V) = 3$ and $G = 7 : 3$.

Proof. First assume that the group $G$ contains a transvection $\tau$. As $G$ is transitive on the points in $\mathbb{P}(V)$, see (3.5), each point in $\mathbb{P}(V)$ serves as center of some transvection in $G$. Suppose $H$ is a hyperplane of $V$ serving as the axis of some transvection $\tau \in G$. Let $p$ be the center of this transvection. If $q$
is now a second point in $H$, then let $e$ be an element of $D$ with $p, q \leq [V, e]$. Then $q = pe$ or $q = pe^{-1}$ and the transvection with center $q$ and axis $H$ is a conjugate of $\tau$ in $G$.

Now let $K$ be a second hyperplane of $\mathbb{P}(V)$ serving as transvection axis for some transvection in $G$. Then by the above we can find transvections $\tau$ and $\sigma$ in $G$ with the same center and with axis $H$ and $K$ respectively. But then $\sigma \tau$ is a transvection with axis the unique hyperplane $L$ distinct from $H$ and $K$ containing $H \cap K$. So the elements of $V^*$ serving as transvection axis for some transvection in $G$ form the nonzero vectors of a subspace $\Phi$ of $V^*$. This implies that the transvections in $G$ generate the subgroup $T(V, \Phi)$ of $G$.

If $\dim(V) = 3$ or 4, and $G$ contains a transvection, then by the above $G = \text{GL}(V)$. So, assume that $G$ does not contain any transvection. If $\dim(V) = 3$, then any involution in $\text{GL}(V)$ is a transvection. So, $|G| \mid 21$. On the other hand, $G$ is transitive on the 7 lines, while an element $d \in D$ fixes a line. Hence $G$ has order 21 and is isomorphic to $7 : 3$.

If $\dim(V) = 4$, then $G$ has order divisible by $3 \cdot 15 \ast 7$ as the stabilizer of a point-line flag has order at least 3. Indeed, an element $d \in D$, fixes a point-line-flag. An easy computation within $\text{Alt}_8 \simeq \text{GL}(4, 2)$ reveals that $G \simeq \text{Alt}_7$.

Now assume that $\dim(V) \geq 5$. Fix an element $d \in D$ and the consider the line $[V, d]$. This line is contained in 5-dimensional subspace $U$ of $V$. The intersection of $U$ with $C_V(d)$ is 3-dimensional. Pick two lines $l$ and $m$ in $\mathcal{L}$ spanning $C_V(d) \cap \Delta$. The above shows that inside the subgroups generated by $D_{[V, d] + l}$ and $D_{[V, d] + m}$, respectively, we can find the elements $e \in D_l$ and $f \in D_m$ not centralizing $[V, d]$. But then it is straightforward to check that among the conjugates of $d$ under $\langle e, f \rangle$ we find two elements $d_1$ and $d_2$ say with $[V, d_1]$ and $[V, d_2]$ meeting at a point. Moreover, as both $e$ and $f$ leave $C_V(d)$ invariant, we have $C_V(d_1) = C_V(d_2) = C_V(d)$. But then either $d_1 d_2$ or $d_1 d_2^{-1}$ induces a transvection on $[V, d_1] + [V, d_2]$ with center $[V, d_1] \cap [V, d_2]$. But as $C_V(d)$ is centralized by $d_1 d_2$ or $d_1 d_2^{-1}$, we have found a transvection on $V$ in $G$. So, the above applies. Denote this transvection with $\tau$. Now notice that $d_1 \in \langle \tau, \tau d_1 \rangle$. Hence $G = T(V, \Phi)$ for some subspace $\Phi$ of $V^*$. Since $\bigcap_{\varphi \in \Phi} \ker \varphi$ is centralized by $G$, we can conclude that $\bigcap_{\varphi \in \Phi} \ker \varphi = 0$ and $\Phi$ annihilates $V$.

3.13 Theorem. Suppose $\Pi$ is a non degenerate cotriangular space. Then we have one of the following.

(a) $G = \text{Sp}(V, f)$ for some non degenerate symplectic form $f$. 


(b) \(G = \Omega(V, Q)\) for some quadratic form \(Q\) with trivial radical.

c) \(G = \text{Alt}(\Omega)\) for some set \(\Omega\), where \(V = E\mathbb{F}_2\Omega\).

In all cases \(D\) is uniquely determined.

Proof. For each line \(l\) of \(\Pi\), there is (upto taking inverses) at most element \(d \in \text{GL}(V)\) with \([V, d] = l\) and centralizing the codimension 2 subspace \(\bigcap_{p \in l} (p^\perp)\) of \(V\). So, this element is in \(D\). But now it is straightforward to check that the theorem holds.

The above results classify all the groups satisfying the hypothesis of Theorem 1.1 for which the set \(\mathcal{P}\) is nonempty.

4 Pointless Geometries and groups over \(\mathbb{F}_4\)

Suppose \(V\) is an \(\mathbb{F}_2\)-vector space and \(G \leq \text{GL}(V)\) a subgroup generated by a conjugacy class \(D\) as in the hypothesis of Theorem 1.1. We keep the notation of the previous section.

In this final section we consider the case where \(\mathcal{P}\) is the empty set. Although the set \(\mathcal{P}\) is empty, we will still be able to construct a useful geometry. However, now the elements of \(\mathcal{L}\) will play the role of ‘points’ and certain 4-dimensional subspaces of \(V\) will play the role of ‘lines’. We make this precise in the sequel of this section.

Let \(d, e\) be elements in \(D\) with \([V, d] \neq [V, e]\). Then, as by assumption \([V, d] \cap [V, e] = 0\), the space \([V, d] + [V, e]\) is 4-dimensional. If \(d\) does not centralize \([V, e]\) (or vice versa) then \([V, d] + [V, e]\) contains 4 or 5 lines from \(\mathcal{L}\). These lines form (part of) a spread of \([V, d] + [V, e]\). Such a 4-dimensional subspace containing at least 4 lines from \(\mathcal{L}\) will be called a spread. A spread is called full if it contains 5 lines from \(\mathcal{L}\) and tangent otherwise. The set of all full spreads is denoted by \(\mathcal{F}\), the set of all tangent spreads by \(\mathcal{T}\). If \(S\) is a tangent spread, then there is a unique projective line in \(S\) not meeting one of the 4 lines of \(\mathcal{L}\) in \(S\). This line is called the singular line of \(S\). The set of all singular lines is denoted by \(\mathcal{L}_S\).

If we identify spreads with the set of lines from \(\mathcal{L}\) contained in it, then \((\mathcal{L}, \mathcal{F} \cup \mathcal{T})\) is a partial linear space, which we denote by \(\Delta\).

If \(W\) is a subspace of \(V\), then \(\Delta_W\) is the geometry with as ‘lines’ the spreads from \(\mathcal{F} \cup \mathcal{T}\) contained in \(W\) and as ‘points’ those elements from \(\mathcal{L}\) which are contained in some spread \(S \in \mathcal{F} \cup \mathcal{T}\) contained in \(W\).
4.1 If $S$ is a tangent spread, then $\langle D_S \rangle$ induces $\text{Alt}_4$ on the lines of $\mathcal{L}$ in $S$. If $S$ is full, then $\langle D_S \rangle$ induces $\text{Alt}_5$ on the lines of $\mathcal{L}$ in $S$.

Proof. Let $l$ be a line of $S$. An element $d \in D_l$ induces a 3-cycle on the lines in $S$ and fixes $l$. So, if $S$ is a tangent spread, then the stabilizer in $G$ of $S$ induces the 2-transitive group $\text{Alt}_4$ on the 4 lines in $S$.

If $S$ is full, then let $m$ be the unique line of $S$ different from $l$ fixed by $d$. If there is an element $e \in D_m$ not fixing $l$, then $\langle d, e \rangle$ induces the 2-transitive group $\text{Alt}_5$ on $S$.

So, assume that $l \subseteq A_m$, then any line $k \neq l, m$ in $S$ is not in $A_k$, see (3.7). Let $k$ be such a line and $f \in D_k$ an element not fixing $m$. Then $\langle d, e, f \rangle$ induces the the 2-transitive group $\text{Alt}_5$ on $S$.

4.2 If $S$ is a spread and $d \in D$ then $C_V(d)$ either contains $S$ or $C_V(d) \cap S$ is a line in $\mathcal{L} \cup \mathcal{L}_S$.

Proof. This follows from (3.8).

4.3 If $d, e \in D$ such that $[V, d] + [V, e]$ is a tangent spread. Then there exists an involution $t \in \langle d, e \rangle$ with $h = [V, t]$ the singular line of the spread.

Moreover, if $f \in D$ does not centralize $h$, then $t$ does not centralize $[V, f]$.

Proof. Let $S$ be the tangent spread $[V, d] + [V, e]$ and $h$ its singular line. The group $\langle d, e \rangle$ induces $\text{Alt}_4$ on $S$. Now suppose $g = de$ is the preimage of the element $(1, 2)(3, 4) \in \text{Alt}_4$ and set $t = g^2$.

Let $f \in D$ be an element not centralizing $h$. Then, without loss of generality we can assume that $f$ centralizes $[V, d]$. If $d$ does not centralize $[V, f]$, then $[V, d] + [V, f]$ is a full spread. So, after replacing $d$ by a suitable element in $D_{[V, d]}$, we can assume that $d$ centralizes $[V, f]$, see (3.7). Then for $v \in [V, f]$, we have $vdede = vde = v(ede) \neq v$. So $t = g^2 \neq 1$ and does not centralize $[V, f]$.

As $[V, t] \subseteq S \subseteq C_V(t)$ we deduce that $t$ has order 2. Indeed, for all $v \in V$ we have $vt^2 + vt = [v, t]t = [v, t] = vt + v$, and thus $vt^2 = v$. Moreover, $C_V(t)$ contains $C_V(d) \cap C_V(e)$ and $S$ and therefore is of codimension at most 2. Since $t$ commutes with $g$, we find that $[V, t]$ is contained in $h$. Indeed, for all $v \in V$ we have $[[v, t], g] = (vt+v)g + (vt+v) = vgt + vg + vt + v = [vg + v, t] = [v, g] + t = 0$. So $[V, t] \subseteq C_V(g) \cap S = h$. Hence, either $t$ is a transvection, or $[V, t] = h$. If $t$ is a transvection, then there is a line $k$ in $\mathcal{L}$ meeting the axis of $t$ in a point. But then $k$ and $k^t$ meet nontrivially, contradicting $\mathcal{P}$ to be empty.
4.4 Let $h \in \mathcal{L}_S$. Let $t_1, t_2$ be two involutions to $h$ as above, then $t_1 = t_2$.

Proof. Suppose $f \in D$ is an element not centralizing $h$, then $t_1 t_2$ acts trivially on $[V, f]$ as follows from the above. If $f$ does centralize $h$, then both $t_1$ and $t_2$ centralize $[V, f]$. As $V = [V, G]$, the product $t_1 t_2$ equals $1$. \square

If $h \notin \mathcal{H}$, then by $t_h$ we denote the unique involution described above.

4.5 If $l \in \mathcal{L}$ and $h \in \mathcal{L}_S$ then $h \cap l = 0$.

Proof. Suppose $h \cap l$ is a 1-dimensional subspace of $V$. Let $S$ be a tangent spread containing $h$ and $d \in D$ with $l = [V, d]$. Then $C_V(d) \cap S$ is a line $m \in \mathcal{L}$ of $S$. Now let $e \in D$ with $[V, e]$ a line of $S$ distinct from $m$. Then $[V, e] + [V, d]$ is a spread meeting $S$ in $[V, e] + (l \cap h)$. A point in $[V, e] + (l \cap h)$ not on $[V, e]$ or $h$ is on a line of $L$ inside $S$ and on some line in $L \cup L_S$ of $T$. Since there is at most one line of $L_S$ in $T$, there is a point in $[V, e] + (l \cap h)$ on two distinct lines of $\mathcal{L}$, which contradicts $\mathcal{P}$ being empty. \square

4.6 Suppose $h \in L_S$ and $d \in D$ not centralizing $h$. Then $[V, d] + h$ is a 4 dimensional space containing two lines from $\mathcal{L}$ and three from $L_S$, pairwise nonintersecting.

Proof. Fix a tangent spread $S$ containing $h$ and an element $d \in D$ not centralizing $h$. Let $t$ be the involution from (4.3). Then $[V, d]$ and $[V, dt]$ are two lines from $L$ in $[V, d] + h$, and $h, hd$ and $hd^2$ are three lines from $\mathcal{H}$ in $S$. By construction the three lines in $L_S$ do not intersect. So, the result follows by (4.5). \square

The five lines from $L \cup L_S$ in a subspace $[V, d] + h$ where $h \in L_S$ and $d \in D$ not centralizing $h$ form a spread of $[V, d] + h$. The subspaces of this form are called hyperbolic spreads. The set of all hyperbolic spreads is denoted by $\mathcal{H}$.

4.7 If $l, h \in L_S$ are distinct, then $h \cap l = 0$.

Proof. Suppose $h$ and $l$ meet in a point $p$. Let $S$ be a tangent spread containing $l$ and suppose $d \in D$ is an element not centralizing $l$. By (4.3) there are involutions $t_l$ and $t_h$ in $G$ with $[V, t_l] = l$ and $[V, t_h] = h$ not centralizing $[V, f]$. The space $[V, f] + h$ is a hyperbolic spread meeting $L$ in the lines $[V, f]$ and $[V, f] t_h$, see (4.3), where $[V, f] t = C_V(f) \cap S$. Similarly $[V, f] + l$ is a hyperbolic spread $T$ meeting $L$ in the two lines $[V, f]$ and $[V, f] t_l$, where $[V, f] t_l = C_V(f) \cap T$. But since $([V, f] + l) \cap ([V, f] + h)$ is 3-dimensional, there is a point in $C_V(f) \cap S \cap T$, which has to be on two lines from $L$. This contradicts our assumption that $\mathcal{P}$ is empty. \square
4.8 If $S$ and $T$ are two spreads, then $S \cap T = 0$ or a line in $\mathcal{L} \cup S$.

Proof. This follows immediately from the assumption that $\mathcal{P}$ is empty and (4.7) and (4.5).

4.9 $\Delta$ is connected; the diameter of its collinearity graph is at most 2.

Proof. Suppose $d, e$ are elements from $D$ with $[V, d]$ and $[V, e]$ lines not in a spread. Then $d$ centralizes $[V, e]$ and $e$ centralizes $[V, d]$. Since $D$ is a conjugacy class of $(D)$, the space $\Delta$ has to be connected.

Now suppose $[V, d], [V, f], [V, g], [V, e]$ is a path of length 3 in the collinearity graph of $\Delta$. Let $S$ be the spread $[V, f] + [V, g]$. As both $[V, d]$ and $[V, e]$ are in a spread with at least 3 lines inside $S$, there is at least one line in $S$ at distance 1 from both $[V, d]$ and $[V, e]$. So the distance between $[V, d]$ and $[V, e]$ is at most 2. This implies that the diameter of the collinearity graph of $\Delta$ is at most 2.

4.10 If there exists a full spread, then there are non singular lines.

Proof. Fix $d \in D$ and let $S$ be a full spread on $[V, d]$. Suppose $\mathcal{L}_S$ is nonempty. Then there exists a hyperbolic spread $T$ on $[V, d]$ containing a second line $[V, e]$ with $e \in D$ from $\mathcal{L}$ and three lines from $\mathcal{L}_S$. Let $h$ be a singular line in $T$. The involution $t_h$ centralizes a line $l$ in $S$ distinct from $[V, d]$, but it maps $[V, d]$ to $[V, e]$. So, $l + [V, e]$ is also a full spread.

As the group $D_{[V, d]}$ is transitive on the 4 lines in the full spread $l + [V, e]$, see (4.1), but fixes $[V, d]$ distinct from $l$, we find at least 4 full spreads on $[V, d]$ inside $S + T$. In particular, there are at least $2 + 16$ lines from $\mathcal{L}$ in $S + T$.

Now fix an element $f \in D_l$ not centralizing $[V, d]$. By (4.3) we find that $f$ centralizes $h$ but not the two other singular lines on $T$. So, we find at least $1 + 3 \cdot 2 = 7$ singular lines in $S + T$. As no two lines from $\mathcal{L} \cup \mathcal{H}$ intersect, there are at least $3(18 + 7) = 75$ projective points in $S + T$, which contradicts that $S + T$ has dimension 6, and thus only 63 points.

4.11 Theorem. Suppose that there is a full spread. Then $\Delta$ is isomorphic to a projective space of order 4. In particular, $G$ preserves an $\mathbb{F}_4$-structure $V_4$ on $V$. Moreover, the group $G$ is isomorphic to $R(V_4, \Phi)$ for some subspace $\Phi$ of $V_4^*$ annihilating $V_4$.

Proof. Let $l, m \in \mathcal{L}$ be distinct lines not in a full spread. Then $l \subseteq A_m$ and $m \subseteq A_l$. 

14
By (4.9) there are two full spreads \( S \) on \( l \) and \( T \) on \( m \) meeting at a line \( n \). Let \( k \) be a line in \( S \) distinct from \( l \) and \( n \). Then \( m \) and \( k \) are in a full spread \( R \). Inside \( R \) we can find a line \( h \) which spans a full spread with \( n \) distinct from \( S \) and \( T \). But then none of the lines in \( R \) is inside \( A_l \) and each of them spans a full spread together with \( l \). So, \( l \) is on 5 full spreads each meeting \( T \) in a line. Hence, at least one of these spreads contains \( m \). A contradiction. Thus any two lines from \( L \) are in a full spread.

Now \((L,F)\) is a linear space of order 4. Moreover, it satisfies the Veblen and Young axiom. Indeed, suppose \( S_1, S_2 \) are two spreads on a line \( l \in L \), and \( T_1 \) and \( T_2 \) are two spreads meeting both \( S_1 \) and \( S_2 \) at lines distinct from \( l \), then as subspaces of \( V \), the intersection \( T_1 \cap T_2 \) is 2-dimensional and thus, by (4.8), a line of \( L \).

Thus \( V \) carries an \( G \)-invariant \( F_4 \) structure \( V_4 \) and we can consider \( G \) as subgroup of \( GL(V_4) \). The elements in \( D \) induce reflections on \( V_4 \). Each 1-dimensional subspace of \( V_4 \) is in \( L \) and thus serves as center of a reflection. Let \( l \in L \). By (4.1), no element from \( L \) is in \( A_l \). As in [4, 6.2], we can conclude that there is a subspace \( \Phi \) of \( V_4^* \) annihilating \( V \) with \( G \simeq R(V, \Phi) \).

From now one we can assume that \( F \) is empty.

**4.12** Suppose \( S \) is a tangent spread and \( h \) its singular line. If \( d \in D \) does not centralize \( h \), then \( \Delta_W \) is a dual affine plane, where \( W = [V,d] + S \).

**Proof.** Let \( S \) be a tangent spread and \( h \) its singular line. Let \( d \in D \) not centralizing \( h \). Then there is a unique line \( m \) in \( S \) centralized by \( d \). The space \( [V,d] + m \) meets \( L \) in just \( [V,d] \) and \( m \), for otherwise it would be a full spread. So, on \( [V,d] \) there are 3 tangent and one hyperbolic spread inside \( W \). We now easily deduce that there are \( 1 + 9 + 2 = 12 \) lines of \( L \) in \( W \), each on three tangent spreads. Together they form a dual affine plane \( \Delta_W \).

A 2-dimensional subspace \( W \) is called a singular spread if it contains 5 singular line.

**4.13** Let \( S \) be a tangent spread with the singular line \( h \) of \( S \). If \( d \in D \) with \( [V,d] \) not in \( S \) and \( C_V(f) \cap S \) equal to \( h \), then \( S + [V,f] \) contains 5 singular lines contained in a singular spread and 16 lines, together forming a projective plane of order 4.

**Proof.** Every line \( l \) of \( S \) determines a unique tangent spread with \( [V,d] \). So, \( [V,d] \) is on at least 4 distinct spreads inside \( W := S + [V,d] \). Thus there are at least 13 lines from \( L \) and 5 singular lines from \( H \), which are all in the
4-dimensional space $C_W(d)$. Thus the latter 5 lines form a singular spread $T$. By similar argument we find that all lines form $\mathcal{L}$ inside $W$ are on 4 tangent spreads. But that implies that there are 16 lines from $\mathcal{L}$ in $W$ forming an affine plane $\Delta_W$. The rest follows immediately. 

4.14 If $d \in D$ centralizes $h \in \mathcal{L}_S$, then there is a tangent spread $S$ containing $[V,d]$ and $h$.

Proof. Let $S$ be a tangent spread on $h$. If $d$ does not centralize the spread (i.e. is collinear in $\Delta$ with some point of $S$), then we are done by (4.13). Since the graph $\Delta$ is connected, the result follows.

4.15 If $h,l \in \mathcal{L}_S$ are two singular lines, then $h+l$ a hyperbolic or singular spread.

Proof. Let $S$ be a tangent spread on $h$ and $d \in D$ with $[V,d] \in S$. Let $t_h$ be an involution in $G$ with $[V,t_h] = h$ as in (4.3). If $d$ does not centralize $l$, then inside the subspace $[V,d]t_h + S$ we find that $h+l$ is a hyperbolic spread, see (4.12).

If $d$ centralizes $h$, then $[V,d] + h$ is a tangent spread and we can apply (4.13) to find that $h+l$ is a singular spread.

4.16 Theorem. Suppose there are no full spreads. Then the geometry $(\mathcal{L} \cup \mathcal{L}_S, T \cup \mathcal{H} \cup S)$ is a projective space of order 4. The set $\mathcal{L}_S$ is the set of absolute points of this projective space with respect to some hermitian polarity.

In particular, $G$ preserves a nondegenerate Hermitian $\mathbb{F}_4$ structure $(V_4,h)$. Moreover, $G$ is isomorphic to $FU(V_4,h)$, with $D$ corresponding to the class of reflections in $G$.

Proof. By the above we find that the geometry $(\mathcal{L} \cup \mathcal{L}_S, T \cup \mathcal{H} \cup S)$ is a linear space. As in the proof of (4.11) we can prove this space to be a projective space of order 4. The map $l \in \mathcal{L} \mapsto A_l$ and $h \in \mathcal{L}_S \mapsto C_V(t_h)$ is a nondegenerate hermitian polarity on this projective space. As each $d$ induces a unitary reflection with center $[V,d]$ the theorem follows.

Now Theorem 1.1 follows from the Theorems 3.12, 3.13, 4.11 and 4.16.

References


Hans Cuypers
Department of Mathematics
Eindhoven University of Technology
P.O. BOX 513
5600 MB Eindhoven
The Netherlands