ELSEVIER

Linear Algebra and its Applications 304 (2000) 1–31

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

# The correlations with identity companion automorphism, of finite Desarguesian planes ☆

Barbu C. Kestenband

*Depatment of Mathematics, New York Institute of Technology, Old Westbury, NY 11568, USA*

Received 8 September 1998; accepted 16 June 1999

Submitted by R.A. Brualdi

**Abstract**

As a first step towards the general classification of correlations of finite Desarguesian planes, we present, up to isomorphism, all the correlations with identity companion automorphism which are not polarities, of such planes. © 2000 Elsevier Science Inc. All rights reserved.

*Keywords:* Desarguesian plane; Correlation; Absolute set; Companion automorphism

## 1. Introduction

We shall denote the points of a plane by boldface lowercase Latin letters. They will be viewed as column vectors:

$$\mathbf{a} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

If the point $\mathbf{c}$ is incident with the line $L$, we write $\mathbf{c} \in L$.

A correlation $\beta$ of a projective plane is a one-to-one mapping of its points onto its lines and its lines onto its points, such that $\mathbf{c} \in L$ if and only if $L^\beta \in \mathbf{c}^\beta$. It can be represented as follows [5, p. 47]:

$$\mathbf{a}^\beta = \{\mathbf{x}\colon\ \mathbf{x}^{\mathrm{T}} A \mathbf{a}^\phi = 0\}\,, \quad \{\mathbf{x}\colon\ \mathbf{x}^{\mathrm{T}}\mathbf{d} = 0\}^\beta = A^{-\mathrm{T}}\mathbf{d}^\phi. \tag{1}$$

☆ This research was supported in part by the New York Institute of Technology.


PII: S 0 0 2 4 - 3 7 9 5 ( 9 9 ) 0 0 1 4 0 - 8

Here, $A$ is a nonsingular $3 \times 3$ matrix over the underlying field, $A^{-\mathrm{T}} = (A^{-1})^{\mathrm{T}}$, and $\phi$, an automorphism of the field.

In agreement with [2], we call $\phi$ the companion automorphism of $\beta$.

The simplest correlations are polarities and they have long been classified.

The present article should be viewed as the first step towards the general classification of correlations of finite Desarguesian planes. This author has undertaken to classify these correlations, and as of this writing, the correlations of planes of odd nonsquare order have been almost completely determined, up to isomorphism (in the sense of Definition 1 below). It is not a simple problem, and the results will be presented, not surprisingly, in a long article: classification papers are notoriously lengthy.

As one begins to classify correlations, it soon becomes apparent that a great deal hinges upon the order of the plane being odd or even, and also a square or a nonsquare. Thus, there are actually four different classifications, and, as mentioned above, one of them is nearing completion at this time.

Besides, and this brings us to the article at hand, one also notices that the methods employed in classifying the correlations with companion automorphism $\phi = (q^m)$, of planes of order $q^n$, do not work if $m = 0$. Therefore the problem must be approached differently if $\phi = (1)$.

Not only is the approach different (and considerably easier), but so are the results. For example, if the automorphism is the identity, and three absolute points of the given correlation are collinear, then *all* the points on that line are absolute. This never happens with other companion automorphisms.

It is also evident that if $\phi = (1)$, it does not matter whether the order of the plane is a square or not, and not much whether it is odd or even. This is by no means the case for other automorphisms. One thus naturally arrives at the decision to discuss these correlations in a separate, introductory paper.

For ease of reference, definitions, propositions, etc., will be numbered sequentially.

We will denote the correlation defined by the matrix $A$, with companion automorphism $\phi = (1)$, by $(A)$. Thus (1) becomes

$$\mathbf{a}^{(A)} = \{\mathbf{x} : \mathbf{x}^{\mathrm{T}} A\mathbf{a} = 0\}\,, \quad \{\mathbf{x} : \mathbf{x}^{\mathrm{T}}\mathbf{d} = 0\}^{(A)} = A^{-\mathrm{T}}\mathbf{d}. \tag{2}$$

The collineation $(A)^2$ shall be referred to as the collineation induced by the correlation $(A)$. The image of the point $\mathbf{a}$ under the collineation $(A)^2$ is

$$\mathbf{a}^{(A)^2} = \{\mathbf{x} : \mathbf{x}^{\mathrm{T}} A\mathbf{a} = 0\}^{(A)} = A^{-\mathrm{T}} A\mathbf{a}. \tag{3}$$

A point $\mathbf{a}$ is an absolute point of the correlation $(A)$ if $\mathbf{a} \in \mathbf{a}^{(A)}$, i.e. if $\mathbf{a}^{\mathrm{T}} A\mathbf{a} = 0$. As in [6], by the absolute set of a correlation we shall mean the set of its absolute points. The equation of the absolute set of the correlation $(A)$ is $\mathbf{x}^{\mathrm{T}} A\mathbf{x} = 0$.

As we are not interested in polarities, our correlations will never be defined by symmetric matrices.

**Definition 1.** Two correlations $(A)$, $(B)$ are equivalent (or isomorphic) if there exists a collineation $\gamma$ such that $\mathbf{x} \in \mathbf{a}^{(A)} \iff \mathbf{x}^\gamma \in \mathbf{a}^{\gamma(B)}$, or, equivalently, such that $\mathbf{a}^{(A)\gamma} = \mathbf{a}^{\gamma(B)}$ for all the points $\mathbf{a}$.

If the correlations $(A)$, $(B)$ are equivalent, we will write $(A) \sim (B)$.

If $A = (a_{ij})$ is a matrix over a field, and $\alpha$, an automorphism of the field, we denote $A^\alpha = (a_{ij}^\alpha)$.

Following [1], we introduce:

**Definition 2.** Two nonsingular $3 \times 3$ matrices $A$, $B$, over a finite field are congruent (written $A \sim B$) if there exist a matrix $C$, an automorphism $\alpha$ of the field, and a $\lambda$ such that $A^\alpha = \lambda C^{\mathrm{T}} B C$.

**Proposition 3.** $(A) \sim (B) \iff A \sim B$.

**Proof.** Assume $(A) \sim (B)$, where $\mathbf{x}^\gamma = C\mathbf{x}^\alpha$ for some matrix $C$ and automorphism $\alpha$. By assumption, $\mathbf{x} \in \mathbf{a}^{(A)} \iff \mathbf{x}^\gamma \in \mathbf{a}^{\gamma(B)}$ for all points $\mathbf{a}$.

Hence $\mathbf{x}^{\mathrm{T}} A \mathbf{a} = 0 \iff (C\mathbf{x}^\alpha)^{\mathrm{T}} B C \mathbf{a}^\alpha = 0$, or $\mathbf{x}^{\mathrm{T}} R \mathbf{a} = 0$, where $R = (C^{\mathrm{T}} B C)^{\alpha^{-1}}$. Thus:

$$\mathbf{x}^{\mathrm{T}} A \mathbf{a} = 0 \iff \mathbf{x}^{\mathrm{T}} R \mathbf{a} = 0 \text{ for all points } \mathbf{a}.$$

Upon letting

$$\mathbf{a} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

it follows that $A$ and $R$ must be scalar multiples of each other, so that $A^\alpha = \lambda C^{\mathrm{T}} B C$.

Conversely, let $A^\alpha = \lambda C^{\mathrm{T}} B C$. Define $\gamma$ as before: $\mathbf{x}^\gamma = C\mathbf{x}^\alpha$.

By (2) we have $\mathbf{a}^{\gamma(B)} = \{\mathbf{x} : \mathbf{x}^{\mathrm{T}} B \mathbf{a}^\gamma = 0\}$. Hence $\mathbf{x}^\gamma \in \mathbf{a}^{\gamma(B)}$ means $\mathbf{x}^{\gamma\mathrm{T}} B \mathbf{a}^\gamma = 0$. But the last equation is equivalent to $\mathbf{x}^{\mathrm{T}} A \mathbf{a} = 0$:

$$\mathbf{x}^{\gamma\mathrm{T}} B \mathbf{a}^\gamma = (C\mathbf{x}^\alpha)^{\mathrm{T}} B (C\mathbf{a}^\alpha) = \mathbf{x}^{\alpha\mathrm{T}} C^{\mathrm{T}} B C \mathbf{a}^\alpha = \frac{1}{\lambda} (\mathbf{x}^{\mathrm{T}} A \mathbf{a})^\alpha. \qquad \square$$

At this point we shall state the main classification results, in the form of two theorems, although the complete proofs will only emerge gradually in the sections that follow.

**Theorem 4.** *Let $q$ be an odd prime power, and $w$, a primitive root of $GF(q)$. Then, up to isomorphism, the correlations defined by the following matrices are all the correlations of $PG(2, q)$ with identity companion automorphism which are not polarities*:

$$L = \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$N = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & w \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$Q_\rho = \begin{pmatrix} 1 & \rho & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho \neq 0, \pm 2, \quad R_\rho = \begin{pmatrix} 1 & \rho & 0 \\ 0 & w & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho \neq 0.$$

*No two matrices on this list are congruent, with the following exceptions*:

*Two matrices $Q_\rho$, $Q_{\rho'}$ are congruent if and only if $\rho' = \pm\rho^\alpha$ for some automorphism $\alpha$ of the field.*

*Two matrices $R_\rho$, $R_{\rho'}$ are congruent if and only if $\rho' = \pm\rho^\alpha w^{-\frac{1}{2}(\alpha-1)}$ for some automorphism $\alpha$ of the field.*

**Theorem 5.** *Let $q$ be a power of 2, and $w$, a primitive root of $GF(q)$. Then, up to isomorphism, the correlations defined by the following matrices are all the correlations of $PG(2, q)$ with identity companion automorphism which are not polarities*:

$$S_\rho = \begin{pmatrix} 1 & \rho & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho \neq 0; \quad V = \begin{pmatrix} 1 & v & 0 \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix},$$

*where $v$ is a fixed element of $GF(q)$ for which the trinomial $x^2 + vx + 1$ is not factorable*;

$$W = \begin{pmatrix} 1 & w + \frac{1}{w} & 0 \\ 0 & 1 & w + \frac{1}{w} \\ 0 & 0 & 1 \end{pmatrix}.$$

*No two matrices on this list are congruent, with the following exception*:

*Two matrices $S_\rho$, $S_{\rho'}$, are congruent if and only if $\rho' = \rho^\alpha$ for some automorphism $\alpha$ of the field.*

The remainder of the article is devoted to proving these two theorems.

## 2. Preliminary results

The first proposition follows readily from Proposition 3.

**Proposition 6.** *If $(A) \sim (B)$, the collineation $\gamma$ in Definition 1 maps the absolute set of the correlation $(A)$ onto the absolute set of the correlation $(B)$.*

**Proposition 7.** *The absolute set of the correlation $(A)$ is invariant under the induced collineation $(A)^2$.*

**Proof.** Let $\mathbf{a}$ be an absolute point of $(A)$ : $\mathbf{a}^{\mathrm{T}}A\mathbf{a} = 0$.

Then $\mathbf{a}^{(A)^2}$, as given by (3), is an absolute point of $(A)$:

$$(A^{-\mathrm{T}}A\mathbf{a})^{\mathrm{T}}A(A^{-\mathrm{T}}A\mathbf{a}) = \mathbf{a}^{\mathrm{T}}A^{\mathrm{T}}A^{-1}AA^{-\mathrm{T}}A\mathbf{a} = \mathbf{a}^{\mathrm{T}}A\mathbf{a} = 0. \qquad \square$$

**Proposition 8.** *Let $(A) \sim (B)$ and denote the corresponding collineation by $\gamma$. If $\mathbf{a}$, $\mathbf{b}$ are two points such that $\mathbf{a}^{\gamma} = \mathbf{b}$, then $\mathbf{a}^{(A)^2\gamma} = \mathbf{b}^{(B)^2}$.*

**Proof.** We have $\mathbf{b} = \mathbf{a}^{\gamma} = C\mathbf{a}^{\alpha}$, and by Proposition 3, $A^{\alpha} = \lambda C^{\mathrm{T}}BC$. By virtue of (3), we get

$$\mathbf{a}^{(A)^2\gamma} = C(A^{-\mathrm{T}}A\mathbf{a})^{\alpha}. \tag{4}$$

On the other hand, $B = \lambda^{-1}C^{-\mathrm{T}}A^{\alpha}C^{-1}$, whence $B^{-\mathrm{T}} = \lambda CA^{-\mathrm{T}\alpha}C^{\mathrm{T}}$.

Now, by (3) again

$$\mathbf{b}^{(B)^2} = B^{-\mathrm{T}}B\mathbf{b} = (\lambda CA^{-\mathrm{T}\alpha}C^{T})(\lambda^{-1}C^{-\mathrm{T}}A^{\alpha}C^{-1})C\mathbf{a}^{\alpha} = CA^{-\mathrm{T}\alpha}A^{\alpha}\mathbf{a}^{\alpha}.$$

Comparing this expression for $\mathbf{b}^{(B)^2}$ with (4) establishes the claim. $\square$

**Corollary 9.** *The collineation $\gamma$ maps the fixed points of the collineation $(A)^2$ onto those of $(B)^2$.*

**Proof.** If $\mathbf{a}^{(A)^2} = \mathbf{a}$ and $\mathbf{b} = \mathbf{a}^{\gamma}$, we have $\mathbf{b}^{(B)^2} = \mathbf{a}^{(A)^2\gamma} = \mathbf{a}^{\gamma} = \mathbf{b}$. $\square$

A few algebraic results are also needed. The next lemma is a simple consequence of [3, Theorem 67].

**Lemma 10.** *For $q$ odd, the field $GF(q)$ contains, according as $q \equiv 3$ or $1 \bmod 4$:*

*$\frac{1}{4}(q-3)$ or $\frac{1}{4}(q-5)$ nonzero squares $S$ for which $S+1$ is a nonzero square;*
*$\frac{1}{4}(q+1)$ or $\frac{1}{4}(q-1)$ squares $S$ for which $S+1$ is a nonsquare;*
*$\frac{1}{4}(q-3)$ or $\frac{1}{4}(q-1)$ nonsquares $N$ for which $N+1$ is a nonzero square;*
*$\frac{1}{4}(q-3)$ or $\frac{1}{4}(q-1)$ nonsquares $N$ for which $N+1$ is a nonsquare.*

We will let $SQ$, $NS$, stand for the set of squares and nonsquares, respectively, in $GF(q)$, $q$ odd.

**Proposition 11.** *Let $q$ be an odd prime power, and $u \neq \pm 2$, a fixed element of $GF(q)$. Then, as $x$ ranges through $GF(q)$, the trinomial $x^2 + ux + 1$ takes on $\frac{1}{2}(q+1)$ distinct values, of which:*

*$\frac{1}{4}(q+1)$ are squares and $\frac{1}{4}(q+1)$ are nonsquares, if $q \equiv 3 \bmod 4$;*
*$\frac{1}{4}(q+3)$ are squares and $\frac{1}{4}(q-1)$ are nonsquares,*
*if $q \equiv 1 \bmod 4$ and $u^2 - 4 \in SQ$;*
*$\frac{1}{4}(q-1)$ are squares and $\frac{1}{4}(q+3)$ are nonsquares,*
*if $q \equiv 1 \bmod 4$ and $u^2 - 4 \in NS$.*

**Proof.** Let $a \in GF(q)$. The trinomial $x^2 + ux + 1$ will take on the value $a$ if and only if the equation $x^2 + ux + 1 - a = 0$ has roots, i.e. if and only if $v + 4a = s \in SQ$, where $v = u^2 - 4 \neq 0$. In other words, we have the condition

$$-\frac{s}{v} + 1 = -\frac{4a}{v}. \tag{5}$$

Let first $q \equiv 3 \bmod 4$ and $v \in SQ$. Then, if $s \neq 0$, we have $-s/v \in NS$. Also, $-4/v \in NS$.

If $s = 0$, $a = -v/4 \in NS$.

As $s$ ranges through $SQ \setminus \{0, v\}$, $-s/v$ ranges through $NS \setminus \{-1\}$. Hence, by Lemma 10, we get $\frac{1}{4}(q-3)$ nonvanishing square values and the same number of nonsquare values for $-4a/v$, which produces $\frac{1}{4}(q-3)$ nonsquare values and $\frac{1}{4}(q-3)$ nonzero square values for $a$. Lemma 10 does not consider the nonsquare $N = -1$, as it assumes $N + 1 \neq 0$. That is why we have not allowed $s = v$, which would imply $a = 0 \in SQ$. So there is one more square value for $a$.

Therefore $a$ takes on $\frac{1}{4}(q+1)$ square values and the same number of nonsquare values, as claimed in the statement of the proposition.

Let now $q \equiv 3 \bmod 4$, and $v \in NS$. Then $-s/v \in SQ$. Also, $-4/v \in SQ$.

If $s = 0$, $a = -v/4 \in SQ$.

As $s$ ranges through $SQ \setminus \{0\}$, so does $-s/v$. By Lemma 10 again, there are $\frac{1}{4}(q-3)$ nonzero values of $s$ for which $-4a/v \in SQ$ (i.e. a $\in SQ$), and $\frac{1}{4}(q+1)$ values of $s$ for which $-4a/v \in NS$ (i.e. $a \in NS$).

We have thus obtained the same numbers as in the case $v \in SQ$.

Assume next $q \equiv 1 \bmod 4$ and $v \in SQ$. Then $-s/v \in SQ$. Also, $-4/v \in SQ$.

If $s = 0$, $a = -v/4 \in SQ$.

As $s$ ranges through $SQ \setminus \{0, v\}$, $-s/v$ ranges through $SQ \setminus \{0, -1\}$. Hence there are $\frac{1}{4}(q-5)$ nonvanishing square values and $\frac{1}{4}(q-1)$ nonsquare values for $-4a/v$, and for $a$ as well.

We have not allowed $s = v$, because then $-s/v + 1 = 0$ and Lemma 10 assumes $S + 1 \neq 0$.

If $s = v$, we get $a = 0 \in SQ$ from (5), as earlier. Thus we have gotten $\frac{1}{4}(q-5) + 2 = \frac{1}{4}(q+3)$ square values, and $\frac{1}{4}(q-1)$ nonsquare values for $a$.

Finally, let $q \equiv 1 \bmod 4$ and $v \in NS$. Then $-s/v \in NS$. Also, $-4/v \in NS$.

If $s = 0$, $a = -v/4 \in NS$.

As $s$ ranges through $SQ \setminus \{0\}$, $-s/v$ ranges through $NS$. There are $\frac{1}{4}(q-1)$ values of $s$ for which $-4a/v \in SQ$ (i.e. $a \in NS$) and the same number of values of $s$ for which $a \in SQ$.

Hence we end up with $\frac{1}{4}(q-1)$ square values and $\frac{1}{4}(q+3)$ nonsquare values of $a$. □

**Proposition 12.** *Consider the distinct trinomials* $x^2 + sx + 1, x^2 + vx + 1, x^2 + (sv/(s+v))x + 1, sv \neq 0$, *over* $GF(q)$, $q$ *even.*

*If the first two trinomials have zeros, or if neither of them does, then the third trinomial has zeros. Otherwise, the third trinomial possesses no zeros.*

**Proof.** If the zeros of the first two trinomials are $a$, $1/a$, and $b$, $1/b$, then $(ab+1)/(a+b)$ and its reciprocal are zeros of the third: we have $a+1/a=s$ and $b+1/b=v$ by assumption, and then one readily verifies that $(ab+1)/(a+b)+(a+b)/(ab+1)=sv/(s+v)$.

Assume now that the first trinomial, say, and the third, have zeros, but the second one does not, contrary to the assertion in the last sentence of this proposition.

Let $u=sv/(s+v)$. Then, by what has been shown above, the trinomial $x^2+(su/(s+u))x+1$ possesses zeros. But $su/(s+u)=v$, and this contradiction settles the matter.

Finally, assume that the first two trinomials have no zeros. We need to show that in this case the last one does have zeros.

Letting $s'=1/s$ and $v'=1/v$, we can reword this claim as follows:

If the trinomials $s'x^2+x+s'$ and $v'x^2+x+v'$ do not have zeros, then $(s'+v')x^2+x+s'+v'$ has zeros.

Partition the given field (with zero removed) into two subsets T, U, such that $a\in T \iff ax^2+x+a$ has zeros, and $b\in U \iff bx^2+x+b$ does not have zeros.

We have to demonstrate that $s', v'\in U \Rightarrow s'+v'\in T$.

Since the zeros come in pairs, and 0,1 cannot be zeros, it follows that $|T|=\frac{1}{2}q-1$, therefore $|U|=\frac{1}{2}q$. We have seen earlier in the proof that $a\in T, s'\in U \Rightarrow a+s'\in U$. Hence, if $s'\in U$ is fixed, the $\frac{1}{2}q$ elements $s', s'+a,\ a$ ranging through $T$, make up the $U$ subset. In other words, to each $v'\in U$, $v'\neq s'$, there corresponds an $a\in T$ such that $v'=s'+a$, whence $s'+v'=a\in T$. □

We are now prepared to prove the main results that have been set forth in the Introduction. The plan of the work is as follows: in the next section we shall examine the configurations of the absolute sets of the correlations defined by the matrices in Theorem 4, and we will also determine the points left invariant by the induced collineations. This discussion will establish that the respective matrices are not congruent, with the possible exception that some of the matrices of type $Q_\rho$ or $R_\rho$ might be congruent.

Then, in Section 4 we show that the list in Theorem 4 is exhaustive, in the sense that every correlation of a Desarguesian plane of odd order, with identity companion automorphism (polarities excluded) is equivalent to a correlation defined by a matrix listed there. Thus Theorem 4 represents the complete classification for planes of odd order.

Sections 5, 6 are devoted to the same task for the situation in which $q$ is a power of 2, thereby supplying the proof of Theorem 5.

## 3. Inequivalent correlations of planes of odd order

The next proposition is valid regardless of the parity of $q$.

**Proposition 13.** *Let*

$$A = \begin{pmatrix} 1 & t & 0 \\ 0 & u & 0 \\ 0 & 0 & v \end{pmatrix}, \quad tuv \neq 0,$$

*define the correlation* $(A)$ *of* $PG(2, q)$, *with identity companion automorphism.*

*Then the induced collineation* $(A)^2$ *leaves invariant the nonabsolute point* $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ *of* $(A)$, *and also the absolute points of* $(A)$ *on the line* $z = 0$, *if any*, *and none other.*

**Proof.** We have

$$A^{-\mathrm{T}}A = \begin{pmatrix} 1 & t & 0 \\ -\frac{t}{u} & 1 - \frac{t^2}{u} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

whence, by (3)

$$\begin{pmatrix} c \\ d \\ 1 \end{pmatrix}^{(A)^2} = A^{-\mathrm{T}}A \begin{pmatrix} c \\ d \\ 1 \end{pmatrix} = \begin{pmatrix} c + td \\ -\frac{tc}{u} + d - \frac{t^2 d}{u} \\ 1 \end{pmatrix}.$$

If the point $\begin{pmatrix} c \\ d \\ 1 \end{pmatrix}$ is to be fixed, we must have

$$\begin{pmatrix} c \\ d \\ 1 \end{pmatrix}^{(A)^2} = \begin{pmatrix} \lambda c \\ \lambda d \\ \lambda \end{pmatrix},$$

whence $\lambda = 1$ and then $d = c = 0$. Thus $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ is the only fixed point with $z \neq 0$.

The points $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ are not left invariant by $(A)^2$, obviously, because $t \neq 0$ by assumption.

Assume now that the point $\begin{pmatrix} c \\ 1 \\ 0 \end{pmatrix}$, $c \neq 0$, is fixed:

$$A^{-\mathrm{T}}A \begin{pmatrix} c \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} c + t \\ \frac{-tc}{u} + 1 - \frac{t^2}{u} \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda c \\ \lambda \\ 0 \end{pmatrix}.$$

This is readily seen to lead to $c^2 + tc + u = 0$, which shows that $\begin{pmatrix} c \\ 1 \\ 0 \end{pmatrix}$ must be an absolute point of the correlation $(A)$.

Conversely, it is a simple check that an absolute point $\begin{pmatrix} c \\ 1 \\ 0 \end{pmatrix}$ of $(A)$ is fixed by the induced collineation. □

**Proposition 14.** *The absolute set of the correlation* $(L)$ *consists of the points on the line* $x + y + z = 0$.

*The induced collineation is a homology with axis* $x + y + z = 0$ *and center* $\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, *the latter being a nonabsolute point of* $(L)$.

**Proof.** The absolute set of the correlation $(L)$ is the set of points $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ satisfying the equation

$$(x\ y\ z)\begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

This reduces to $x + y + z = 0$. Then

$$L^{-\mathrm{T}}L = \begin{pmatrix} 1 & 2 & 2 \\ -2 & -3 & -2 \\ 2 & 2 & 1 \end{pmatrix}.$$

The eigenvalues of this matrix are $\pm 1$, and the eigenvectors are

$$\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -a-b \\ a \\ b \end{pmatrix}. \qquad \square$$

**Proposition 15.** *The absolute set of the correlation* $(M)$ *is the conic* $y^2 + 2xz + yz = 0$. *The induced collineation leaves invariant the absolute point* $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ *of* $(M)$, *and no other point.*

**Proof.** Since $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, we have $M^{-T}M = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

The only eigenvector of this matrix is $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. $\square$

**Proposition 16.** *If* $q \equiv 1 \bmod 4$, *the absolute set of the correlation* $(N)$ *consists of the single point* $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$.

*If* $q \equiv 3 \bmod 4$, *the absolute set comprises the points on the two lines* $x + y = \pm\sqrt{-w}z$. *In both cases, the induced collineation fixes the nonabsolute point* $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, *the absolute point* $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, *and no other point.*

**Proof.** Since

$$N = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & w \end{pmatrix},$$

the absolute set has equation $(x + y)^2 + wz^2 = 0$.

If $q \equiv 1 \bmod 4$, $-w \in NS$, hence this equation has the unique solution $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$.

If $q \equiv 3 \bmod 4$, we obtain $x + y = \pm\sqrt{-w}z$.

The last sentence of the proposition is a straightforward consequence of Proposition 13, concluding the proof. □

If $q \equiv 1 \bmod 4$, we shall let J stand for $\sqrt{-1}$.

The next proposition is similar to the preceding one and we omit the proof.

**Proposition 17.** *If $q \equiv 1 \bmod 4$, the absolute set of the correlation $(P)$ comprises the points on the two lines $x + y = \pm Jz$.*

*If $q \equiv 3 \bmod 4$, the absolute set consists of the unique point $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$.*

*In both cases, the induced collineation fixes the nonabsolute point $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, the absolute point $\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$, and no other point.*

It is apparent now, in virtue of Proposition 6, that the correlations $(L)$, $(M)$, $(N)$, $(P)$ are mutually inequivalent.

**Proposition 18.** *The absolute sets of the correlations $(Q_\rho)$, $(R_\rho)$, are nondegenerate conics.*

*The induced collineations fix the nonabsolute point $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, and either two, or none, of the absolute points of the respective correlations.*

**Proof.** The two absolute sets have equations $x^2 + \rho xy + y^2 + z^2 = 0$ and $x^2 + \rho xy + wy^2 + z^2 = 0$, i.e. $(x + \frac{1}{2}\rho y)^2 + (1 - \frac{1}{4}\rho^2)y^2 + z^2 = 0$ and $(x + \frac{1}{2}\rho y)^2 + (w - \frac{1}{4}\rho^2)y^2 + z^2 = 0$.

Since $\rho \neq \pm 2$ (for $Q_\rho$) and also $w \in NS$ (which implies $w \neq \frac{1}{4}\rho^2$), these two conics are nondegenerate.

By Proposition 13, the induced collineations fix the point $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ and the absolute points on the line $z = 0$.

Letting $z = 0$ and $y = 1$ in the equations of the two conics produces two quadratic equations in $x$, neither of whose discriminant vanishes. Thus we obtain either two points with $z = 0$, or none. □

Of the first four matrices in Theorem 4, only $M$ gives rise to a correlation with a conic as its absolute set (Proposition 15). But the induced collineation $(M)^2$ does not fix any nonabsolute point, unlike $(Q_\rho)^2$ or $(R_\rho)^2$.

Therefore we have established that no two matrices listed in Theorem 4 are congruent, except that, perhaps, some of the matrices of type $Q_\rho$ or $R_\rho$ might be congruent among themselves. The next two propositions serve to elucidate this point.

We introduced further notation:
$*$ shall stand for an element that is not necessarily zero.
$\circledast$ shall stand for an element that is necessarily nonzero.
The next proposition is valid regardless of the parity of $q$.

**Proposition 19.** *For a fixed* $\mu \neq 0$,

$$\begin{pmatrix} 1 & \rho & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & \rho' & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

*if and only if* $\rho' = \pm\rho^\alpha \mu^{-\frac{1}{2}(\alpha-1)}$ *for some automorphism* $\alpha$ *of the field.*

**Proof.** Denote the two matrices by $K_\rho$, $K_{\rho'}$. To prove necessity, assume $K_\rho \sim K_{\rho'}$. Then, by Definition 2, we can write

$$K_\rho^\alpha = \lambda C^{\mathrm{T}} K_{\rho'} C. \tag{6}$$

The point $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ is not an absolute point of the correlations $(K_\rho)$, $(K_{\rho'})$, but it is fixed by the induced collineations, obviously.

By Proposition 13, no other nonabsolute point is left invariant by these collineations. As a consequence (see Proposition 6 and Corollary 9), we must have

$$C \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \circledast \end{pmatrix}, \quad \text{so that} \quad C = \begin{pmatrix} x & z & 0 \\ y & t & 0 \\ u & v & s \end{pmatrix}.$$

Therefore Eq. (6) is

$$\begin{pmatrix} 1 & \rho^\alpha & 0 \\ 0 & \mu^\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} = \lambda \begin{pmatrix} x & y & u \\ z & t & v \\ 0 & 0 & s \end{pmatrix} \begin{pmatrix} 1 & \rho' & 0 \\ 0 & \mu & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x & z & 0 \\ y & t & 0 \\ u & v & s \end{pmatrix}. \tag{7}$$

This matrix equation shows that $\lambda s^2 = 1$ and $u = v = 0$, and also that

$$xz + \rho' tx + \mu ty = s^2 \rho^\alpha \quad \text{and} \quad xz + \rho' yz + \mu ty = 0.$$

The last two equations imply that

$$\rho'(tx - yz) = s^2 \rho^\alpha. \tag{8}$$

On the other hand, by taking determinants in Eq. (7), we get

$$\mu^\alpha = \lambda^3 \mu s^2 (tx - yz)^2.$$

But $\lambda s^2 = 1$, so this equation reduces to

$$\lambda = \pm \frac{\mu^{\frac{1}{2}(\alpha-1)}}{tx - yz}, \quad \text{i.e.} \quad s^2 = \pm \mu^{-\frac{1}{2}(\alpha-1)} (tx - yz).$$

Substituting this expression for $s^2$ into (8) reduces it to the equation in the statement of the proposition, proving necessity.

Sufficiency follows from the equations

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \mu^{\frac{1}{2}(\alpha-1)} \end{pmatrix} \begin{pmatrix} 1 & \pm\rho^{\alpha}\mu^{-\frac{1}{2}(\alpha-1)} \\ 0 & \mu \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & \mu^{\frac{1}{2}(\alpha-1)} \end{pmatrix} = \begin{pmatrix} 1 & \rho^{\alpha} \\ 0 & \mu^{\alpha} \end{pmatrix},$$

where the $+$'s and $-$'s (if $q$ is odd) are to be matched in the usual manner. □

**Proposition 20.** *If $q$ is odd,*

$$\begin{pmatrix} 1 & \rho' & 0 \\ 0 & w & 0 \\ 0 & 0 & 1 \end{pmatrix} \not\sim \begin{pmatrix} 1 & \rho & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

*for any nonvanishing $\rho$, $\rho'$, where $w$ represents a primitive root of $GF(q)$.*

**Proof.** Reasoning as in the proof of the preceding proposition, if the two matrices were congruent, we would have:

$$\begin{pmatrix} 1 & \rho^{\alpha} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \lambda \begin{pmatrix} x & y & u \\ z & t & v \\ 0 & 0 & s \end{pmatrix} \begin{pmatrix} 1 & \rho' & 0 \\ 0 & w & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x & z & 0 \\ y & t & 0 \\ u & v & s \end{pmatrix}.$$

This matrix equation implies $\lambda s^2 = 1$ and also $\lambda^3 w s^2 (tx - yz)^2 = 1$. But $\lambda$ being a square, the last equation is an impossibility. □

The last two propositions have demonstrated the last three paragraphs of Theorem 4. What remains to be done to complete the proof of the theorem is to show that every nonsingular, nonsymmetric $3 \times 3$ matrix over $GF(q)$, $q$ odd, is congruent to one of the matrices in that theorem. The next section is devoted to this task.

## 4. Equivalent correlations of planes of odd order

Some of the results in this section hold true for $q$ odd or even. Whether or not this is the case will be made apparent in the statement of each claim.

**Proposition 21.** *A nonsingular matrix over a finite field is congruent to*

$$\begin{pmatrix} 1 & * & * \\ * & * & * \\ * & * & * \end{pmatrix}.$$

**Proof.** Let

$$V = \begin{pmatrix} 0 & a & c \\ b & 0 & e \\ d & f & 0 \end{pmatrix},$$

where $a + b$, $c + d$, $e + f$ are not all zero (because $|V| \neq 0$).

Let

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

depending upon which of the above sums, in the given order, does not vanish.

In each case, the matrix $C^{\mathrm{T}}VC$ has the respective expression as its first entry. □

The main result in this section is in Proposition 23. But first we need the following.

**Proposition 22.** *Let*

$$V = \begin{pmatrix} 1 & b & c \\ b & b^2 & bg \\ g & bc & cg \end{pmatrix}, \quad b \neq 0,\ c \neq g, \text{ over } GF(q), q \text{ odd}.$$

*If* $q \equiv 1 \bmod 4$, $V \sim P$. *If* $q \equiv 3 \bmod 4$, $V \sim N$.

**Proof.** For $q \equiv 1 \bmod 4$, let

$$C = \begin{pmatrix} -(3c+g)b & -2(c+g)b & \mathrm{J}(c-g)b \\ c-g & 0 & \mathrm{J}(c-g) \\ 4b & 4b & 0 \end{pmatrix}.$$

Then $C^{\mathrm{T}}VC = -4b^2(c-g)^2P$.

For $q \equiv 3 \bmod 4$, let $C$ be as above, but with $\sqrt{-w}$ instead of J. Then $C^{\mathrm{T}}VC = -4b^2(c-g)^2N$. □

**Proposition 23.** *A nonsingular* $3 \times 3$ *matrix over* $GF(q)$, $q$ *odd, is congruent to an upper triangular matrix.*

**Proof.** The first part of the proof is valid for even prime powers, too.

Let

$$A = \begin{pmatrix} 1 & b & c \\ d & e & f \\ g & h & i \end{pmatrix}.$$

If $e \neq bd$, let

$$C = \begin{pmatrix} 1 & -d & dh-eg \\ 0 & 1 & bg-h \\ 0 & 0 & e-bd \end{pmatrix}.$$

If $i \neq cg$, let

$$C = \begin{pmatrix} 1 & -g & fg-di \\ 0 & 0 & i-cg \\ 0 & 1 & cd-f \end{pmatrix}.$$

In both cases, $C^{\mathrm{T}}AC$ is an upper triangular matrix.

If $e = bd$ and $i = cg$, but $h - bg \neq cd - f$, let

$$C = \begin{pmatrix} 1 & df - cd^2 - g & bdg - dh - g \\ 0 & cd - f & h - bg \\ 0 & 1 & 1 \end{pmatrix}.$$

Note that in this case neither $h - bg$ nor $cd - f$ can vanish, as that would entail $|A| = 0$. Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & b & c \\ d & bd & f \\ g & h & cg \end{pmatrix} C$$

is upper triangular again.

The remainder of the proof is devoted to the more complicated situation in which $e = bd$, $i = cg$ and $h - bg = cd - f$.

What follows is no longer valid for $q$ even, except in Case V (if $f \neq 0$) and VI.

There are six cases to be considered.

*Case* I. $b = d = 0$, which entails $e = 0$ and $f = -h$, so that

$$A = \begin{pmatrix} 1 & 0 & c \\ 0 & 0 & -h \\ g & h & cg \end{pmatrix}.$$

There are three possibilities:

(1) $c \neq g$. In this case, for $q \equiv 1 \bmod 4$, let

$$C = \begin{pmatrix} -2(c+g)h & -2(c+g)h & 2\mathrm{J}(c-g)h \\ 0 & -(c-g)^2 & \mathrm{J}(c-g)^2 \\ 4h & 4h & 0 \end{pmatrix}.$$

Then $C^{\mathrm{T}}AC = -4h^2(c-g)^2P$ (see Theorem 4).

If $q \equiv 3 \bmod 4$, let $C$ be as above, but with $\sqrt{-w}$ replacing J, where $w$, as always, is a primitive root of the field. Then $C^{\mathrm{T}}AC = -4h^2(c-g)^2N$.

(2) $c = g \neq 0$, i.e.

$$A = \begin{pmatrix} 1 & 0 & c \\ 0 & 0 & -h \\ c & h & c^2 \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} 0 & -ch & 0 \\ -c^2 & -c^2 & 0 \\ h & 2h & h \end{pmatrix}.$$

Then $C^T AC = c^2h^2L$.

(3) $c = g = 0$, i.e.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -h \\ 0 & h & 0 \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} h & h & h \\ -1 & -1 & 0 \\ h & 2h & h \end{pmatrix}.$$

Then $C^{\mathrm{T}}AC = h^2L$.

*Case* II. $b = 0$, $d \neq 0$. Then $e = 0$ and $h = cd - f$, so

$$A = \begin{pmatrix} 1 & 0 & c \\ d & 0 & f \\ g & cd - f & cg \end{pmatrix}.$$

If $q \equiv 1 \bmod 4$, let

$$C = \begin{pmatrix} d(cd - 2f) & 2d(cd - f) & \mathrm{J}d(2f - cd) \\ 4f - 3cd - dg & -4(cd - f) & \mathrm{J}d(g - c) \\ d^2 & 0 & -\mathrm{J}d^2 \end{pmatrix}.$$

Then $C^{\mathrm{T}}AC = -4d^2(cd - f)^2P$.

For $q \equiv 3 \bmod 4$, let $C$ be as above, but with $\sqrt{-w}$ in lieu of J. Then $C^{\mathrm{T}}AC = -4d^2(cd - f)^2N$.

*Case* III. $b \neq 0$, $d = 0$. Then $e = 0$ again, and $f = bg - h$, so that

$$A = \begin{pmatrix} 1 & b & c \\ 0 & 0 & bg - h \\ g & h & cg \end{pmatrix}.$$

For $q \equiv 1 \bmod 4$, let

$$C = \begin{pmatrix} 2b(bg - h) & b(bg - 2h) & \mathrm{J}b(2h - bg) \\ -4(bg - h) & 4h - 3bg - bc & \mathrm{J}b(c - g) \\ 0 & b^2 & -\mathrm{J}b^2 \end{pmatrix}.$$

Then $C^{\mathrm{T}}AC = -4b^2(bg - h)^2P$.

For $q \equiv 3 \bmod 4$, proceed as in the other cases, to arrive at $C^{\mathrm{T}}AC = -4b^2(bg - h)^2N$.

*Case* IV. $b = d \neq 0$ and $fh = b^2cg$.

In this case, the equation $h - bg = cd - f$ become $f + h = b(c + g)$, whence $f^2 + 2fh + h^2 = b^2c^2 + 2b^2cg + b^2g^2$. But $fh = b^2cg$, so the last equation reduces to

$$f^2 + h^2 = b^2c^2 + b^2g^2 \tag{9}$$

Since $h - bg = bc - f \neq 0$, Eq. (9) further reduces to $h + bg = bc + f$, whence by adding the last two equations, we obtain $h = bc$ and $f = bg$.

Therefore

$$A = \begin{pmatrix} 1 & b & c \\ b & b^2 & bg \\ g & bc & cg \end{pmatrix}.$$

But this is the $V$ matrix of Proposition 22 and it has been shown there that $V \sim P$ or $N$.

*Case* V. $0 \neq b \neq d \neq 0$ and $fh = bcdg$. There are two possibilities.

(1) If $f = 0$, then $bcdg = 0$. But $bd \neq 0$ by assumption, while $c = 0$ would cause the last column of $A$ to have only zeros. Hence

$$f = 0 \quad \Rightarrow \quad g = 0 \quad \Rightarrow \quad h = cd \quad \text{and} \quad A = \begin{pmatrix} 1 & b & c \\ d & bd & 0 \\ 0 & cd & 0 \end{pmatrix}.$$

If $q \equiv 1 \bmod 4$, let

$$C = \begin{pmatrix} 2\mathrm{J}cd & \mathrm{J}cd & cd \\ 0 & \mathrm{J}c & c \\ -4\mathrm{J}d & -3\mathrm{J}d - \mathrm{J}b & d - b \end{pmatrix}.$$

Then $C^{\mathrm{T}}AC = 4c^2d^2P$.

If $q \equiv 3 \bmod 4$, let C be as above, but with $\sqrt{-w}$ instead of J. Then

$$C^{\mathrm{T}}AC = 4wc^2d^2 \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{w} \end{pmatrix}$$

and

$$\operatorname{diag}(1, 1, w) \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{w} \end{pmatrix} \operatorname{diag}(1, 1, w) = N,$$

so that $A \sim N$.

(2) If $f \neq 0$, the parity of $q$ is not relevant.

Let

$$C = \begin{pmatrix} -bf & 0 & -bdg \\ 0 & bd & bg - h \\ bd & 0 & bd \end{pmatrix}.$$

We first need to make sure that $C$ is nonsingular.

We have $|C| = b^3d^2(dg - f)$. If $|C| = 0$, then $f = dg$. If so, the equation $fh = bcdg$ reduces to $h = bc$ (because $f \neq 0$). As a consequence, the equation $h - bg = cd - f$ becomes $b(c - g) = d(c - g)$. As $b \neq d$ by assumption, we must have $c = g$. But then $h = bg$, which entails $|A| = 0$. Therefore $C$ is nondegenerate.

Now one verifies that

$$C^{\mathrm{T}} \begin{pmatrix} 1 & b & c \\ d & bd & f \\ g & h & cg \end{pmatrix} C$$

is upper triangular indeed.

*Case* VI. $bd \neq 0$ and $fh \neq bcdg$. Here again it does not matter whether $q$ is odd or even.

Let

$$C = \begin{pmatrix} 0 & 0 & \frac{bcdg - fh}{b(f - cd)} \\ -\frac{f}{bd} & 1 & -\frac{c}{b} \\ 1 & 0 & 1 \end{pmatrix}.$$

One verifies, using the equation $h - bg = cd - f$, that

$$C^{\mathrm{T}} \begin{pmatrix} 1 & b & c \\ d & bd & f \\ g & h & cg \end{pmatrix} C$$

is an upper triangular matrix.

The proof is now complete. □

In the light of the last proposition, it suffices to prove that every upper triangular matrix is congruent to one of the matrices listed in the statement of Theorem 4. First we have the following.

**Proposition 24.** *Let*

$$A = \begin{pmatrix} 1 & t & v \\ 0 & n & u \\ 0 & 0 & r \end{pmatrix}, \quad nrv \neq 0, \text{ over } GF(q).$$

*If $q$ is an odd prime power, then*

$$\text{either} \quad A \sim L \quad \text{or} \quad A \sim \begin{pmatrix} 1 & * & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}.$$

*If $q$ is a power of 2, then*

$$A \sim \begin{pmatrix} 1 & * & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

**Proof.** There are four possibilities which need to be analyzed separately. In the first three cases, the proof is valid for all prime powers. In each of these cases we will construct a matrix $C$ such that

$$C^{\mathrm{T}} A C = \begin{pmatrix} 1 & * & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}.$$

If $q$ is even, every element is a square, so there was no loss of generality in replacing the two $*$ entries with 1's in the statement of the proposition.

*Case* I. $uv = rt$. This case includes the possibility $u = t = 0$.

Then

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & v \\ 0 & 1 & -t \end{pmatrix}.$$

*Case* II. $uv \neq rt$ and $nv^2 - tuv + rt^2 \neq 0$. The possibility $u \neq 0$, $t = 0$, is part of this case.

Then

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -v \\ 0 & \frac{nv}{rt-uv} & t \end{pmatrix}.$$

*Case* III. $uv \neq rt$ and $nv^2 - tuv + u^2 \neq 0$. This includes the possibility $u = 0$, $t \neq 0$.

Then

$$C = \begin{pmatrix} u & -1 & 0 \\ -v & \frac{tv-u}{nv} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

*Case* IV. $uv \neq rt$ and $nv^2 - tuv + rt^2 = nv^2 - tuv + u^2 = 0$. Then we have $r = u^2/t^2$, clearly.

The approach in this case depends upon the parity of $q$.

Let first $q$ be odd.

As we have just seen, $r$, the last entry of $A$, must be a square. If $n \in NS$, let

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & \frac{t}{u} & \frac{t^2}{u} \end{pmatrix}.$$

We get

$$C^{\mathrm{T}}AC = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & n \end{pmatrix}.$$

As $n \in NS$, this last matrix cannot fulfill the requirements of Case IV, hence (at least) one of the other cases applies.

If $n \in \mathrm{SQ}$, we have

$$\mathrm{diag}\left(1, \frac{1}{\sqrt{n}}, \frac{t}{u}\right) \begin{pmatrix} 1 & t & v \\ 0 & n & u \\ 0 & 0 & \frac{u^2}{t^2} \end{pmatrix} \mathrm{diag}\left(1, \frac{1}{\sqrt{n}}, \frac{t}{u}\right) = \begin{pmatrix} 1 & \frac{t}{\sqrt{n}} & \frac{tv}{u} \\ 0 & 1 & \frac{t}{\sqrt{n}} \\ 0 & 0 & 1 \end{pmatrix},$$

i.e.

$$A \sim \begin{pmatrix} 1 & \frac{t}{\sqrt{n}} & \frac{tv}{u} \\ 0 & 1 & \frac{t}{\sqrt{n}} \\ 0 & 0 & 1 \end{pmatrix}.$$

In $t = 2\sqrt{n}$, the equation $nv^2 - tuv + u^2 = 0$ in the statement of the case under consideration becomes $(v\sqrt{n} - u)^2 = 0$, whence $u = v\sqrt{n}$ and then $tv/u = 2\sqrt{n}v/v\sqrt{n} = 2$. Therefore $A \sim L$ in this case.

If $t = -2\sqrt{n}$, we obtain likewise

$$A \sim \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}.$$

But the last matrix is obviously congruent to $L$, so $A \sim L$ again.

If $t \neq \pm 2\sqrt{n}$, choose $b$ such that $b^2 + (t/\sqrt{n})b + 1 \in NS$, which is always possible, by virtue of Proposition 11.

Let

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\frac{t}{\sqrt{n}} - \frac{1}{b} & b \\ 0 & 1 & 1 \end{pmatrix}.$$

Since $b$ is not a zero of the trinomial $x^2 + (t/\sqrt{n})x + 1$, $C$ is nonsingular.

Then one calculates

$$C^{\mathrm{T}} \begin{pmatrix} 1 & \frac{t}{\sqrt{n}} & \frac{tv}{u} \\ 0 & 1 & \frac{t}{\sqrt{n}} \\ 0 & 0 & 1 \end{pmatrix} C,$$

and it turns out to be an upper triangular matrix whose last entry is $b^2 + (t/\sqrt{n})b + 1 \in NS$, and thus the other cases apply.

Now assume $q$ is power of 2. Let

$$C = \begin{pmatrix} 1 + \frac{tv}{u} & 1 + \frac{t^3 v}{nu} & \frac{t}{\sqrt{n}} \\ 0 & \frac{t^2 v}{nu} & \frac{1}{\sqrt{n}} \\ \frac{t}{u} & \frac{t}{u} & 0 \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & t & v \\ 0 & n & u \\ 0 & 0 & \frac{u^2}{t^2} \end{pmatrix} C = \begin{pmatrix} \frac{tv}{u} & \frac{t^2 v^2}{u^2} & 0 \\ 0 & \frac{tv}{u} & \frac{t^2 v}{u\sqrt{n}} \\ 0 & 0 & 1 \end{pmatrix}.$$

As every element of $GF(q)$, $q$ even, is a square, the conclusion is immediate. □

We will now demonstrate that for odd prime powers, matrices of form

$$\begin{pmatrix} 1 & * & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$$

are congruent to one of the matrices in the statement of Theorem 4.

First note that every matrix of that form is congruent to one of the following matrices:

$$\begin{pmatrix} 1 & * & 0 \\ 0 & w & * \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 \\ 0 & w & * \\ 0 & 0 & w \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 \\ 0 & 1 & * \\ 0 & 0 & w \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix},$$

where $w$ is a primitive root of the field.

**Proposition 25.** *Let $q$ be an odd prime power, and, in addition, if $q \equiv 1 \bmod 4$, assume $s \neq \pm \mathrm{J}t$. Then*:

*If* $s^2 + t^2 = \rho^2$, *we have*

$$\begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix} \sim R_\rho.$$

*If* $s^2 + t^2 \in NS$, *let* $\rho^2 = \frac{1}{w}(s^2 + t^2)$. *Then*

$$\begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix} \sim Q_\rho.$$

**Proof.** In the first case, let

$$C = \begin{pmatrix} -\frac{ws}{\rho} & 0 & \frac{wt}{\rho} \\ 0 & -w & 0 \\ \frac{wt}{\rho} & wt & \frac{ws}{\rho} \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix} C = w^2 R_\rho.$$

The condition $s \neq \pm \mathrm{J}t$ is necessary to ensure the nonsingularity of $C$; the next proposition will show what happens if $s = \pm \mathrm{J}t$.

In the second case, let

$$C = \begin{pmatrix} -s & -\frac{s}{\rho} & \frac{t}{\rho} \\ 1 & 0 & 0 \\ 0 & \frac{t}{\rho} & \frac{s}{\rho} \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix} C = w Q_\rho. \qquad \square$$

**Proposition 26.** *Let* $q \equiv 1 \bmod 4$. *Then*

$$\begin{pmatrix} 1 & \pm \mathrm{J}t & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix} \sim M.$$

**Proof.** Let

$$D = \begin{pmatrix} 1 & \mathrm{J}t & 0 \\ 0 & w & t \\ 0 & 0 & 1 \end{pmatrix}.$$

The proof is quite similar if the minus sign is used.

The absolute set of the correlation $(D)$ has equation $x^2 + \mathrm{J}txy + wy^2 + tyz + z^2 = 0$, i.e. it is the conic $(x + \frac{1}{2}\mathrm{J}ty)^2 + wy^2 + (\frac{1}{2}ty + z)^2 = 0$.

We have

$$D^{-T}D = \begin{pmatrix} 1 & \mathrm{J}t & 0 \\ -\frac{\mathrm{J}t}{w} & 1+\frac{t^2}{w} & \frac{t}{w} \\ \frac{\mathrm{J}t^2}{w} & -\frac{t^3}{w}-t & 1-\frac{t^2}{w} \end{pmatrix}$$

and it is easy to see that $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}$ is an eigenvector of this matrix (as a matter of fact it is the only eigenvector), hence the collineation $(D)^2$ fixes the point $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}$.

The image of this point under the correlation $(D)$ is the line: $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}^{(D)}$, with equation $(xyz)D\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix} = 0$, i.e. $-Jx + ty + z = 0$.

If this line contained another absolute point $\mathbf{b}$, we would have $\mathbf{b} \in \mathbf{b}^{(D)}$, $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}^{(D)}$, which entails $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}, \mathbf{b} \in \mathbf{b}^{(D)}$, in other words the line $\mathbf{b}^{(D)}$ would be the same as $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}^{(D)}$, and this is not possible.

Since the absolute set of $(D)$ is a $(q+1)$-arc, and there are $q+1$ lines through every point, it follows that every line through $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}$, except $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}^{(D)}$, contains one other absolute point of $(D)$.

Let then $\begin{pmatrix} u \\ v \\ r \end{pmatrix}$ be the absolute point of $(D)$ distinct from $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}$, on the line $\mathrm{J}tx + (w - t^2)y - tz = 0$; this line is not $\begin{pmatrix} -\mathrm{J} \\ 0 \\ 1 \end{pmatrix}^{(D)}$, as $w \neq 0$. We have

$$\begin{pmatrix} -\mathrm{J} & 0 & 1 \\ 0 & 1 & -t \\ u & v & r \end{pmatrix} D \begin{pmatrix} -\mathrm{J} & 0 & u \\ 0 & 1 & v \\ 1 & -t & r \end{pmatrix} = \begin{pmatrix} 0 & 0 & -\mathrm{J}u + tv + r \\ 0 & w & wv \\ -\mathrm{J}u + tv + r & 0 & 0 \end{pmatrix} = F.$$

Then

$$\operatorname{diag}\left(\frac{w^2v^2}{-\mathrm{J}u + tv + r}, wv, w\right) \cdot F \cdot \operatorname{diag}\left(\frac{w^2v^2}{-\mathrm{J}u + tv + r}, wv, w\right)$$
$$= w^3v^2 \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \qquad \square$$

The last two propositions have disposed of the matrices of the form

$$\begin{pmatrix} 1 & * & 0 \\ 0 & w & * \\ 0 & 0 & 1 \end{pmatrix}.$$

The next three propositions serve to reduce the matrices of the remaining three types to either $M$ or

$$\begin{pmatrix} 1 & * & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}.$$

**Proposition 27.**

$$\begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & w \end{pmatrix} \sim \begin{pmatrix} 1 & \frac{t}{w} & 0 \\ 0 & 1 & s \\ 0 & 0 & w \end{pmatrix} \quad \textit{over a finite field}.$$

**Proof.** Let

$$C = \begin{pmatrix} 0 & s & w \\ 0 & -1 & 0 \\ 1 & \frac{t}{w} & 0 \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & s & 0 \\ 0 & w & t \\ 0 & 0 & w \end{pmatrix} C = w \begin{pmatrix} 1 & \frac{t}{w} & 0 \\ 0 & 1 & s \\ 0 & 0 & w \end{pmatrix}. \qquad \square$$

**Proposition 28.** *Let*

$$A = \begin{pmatrix} 1 & s & 0 \\ 0 & 1 & t \\ 0 & 0 & r \end{pmatrix}, \quad r \neq 0, \textit{ over a finite field}.$$

*Then*

$$A \sim \begin{pmatrix} 1 & * & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \quad \textit{if and only if} \quad rs^2 + t^2 \neq 0.$$

**Proof.** We have in this case

$$A^{-\mathrm{T}}A = \begin{pmatrix} 1 & s & 0 \\ -s & 1 - s^2 & t \\ \frac{st}{r} & (s^2 - 1)\frac{t}{r} & 1 - \frac{t^2}{r} \end{pmatrix}.$$

The characteristic polynomial of $A^{-\mathrm{T}}A$ is $(1 - \lambda)[\lambda^2 + (s^2 + \frac{t^2}{r} - 2)\lambda + 1]$.

If $rs^2 + t^2 = 0$, the only eigenvalue is 1 and the only eigenvector is $\begin{pmatrix} \frac{t}{s} \\ 0 \\ 1 \end{pmatrix}$.

But this point is readily seen to be an absolute point of the correlation $(A)$. It follows that the collineation $(A)^2$ does not leave invariant any nonabsolute point of $(A)$. Therefore, by Proposition 6, Corollary 9 and Proposition 13,

$$A \not\sim \begin{pmatrix} 1 & * & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}.$$

If $rs^2 + t^2 \neq 0$, let

$$C = \begin{pmatrix} -s & -\frac{rs}{t} & \frac{t}{s} \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Then

$$C^{\mathrm{T}}AC = \begin{pmatrix} 1 & t + \frac{rs^2}{t} & 0 \\ 0 & r + \frac{r^2s^2}{t^2} & 0 \\ 0 & 0 & r + \frac{t^2}{s^2} \end{pmatrix}. \qquad \square$$

The next proposition deals with the situation in which $rs^2 + t^2 = 0$, but only if $q$ is odd.

**Proposition 29.**

$$\begin{pmatrix} 1 & s & 0 \\ 0 & 1 & t \\ 0 & 0 & -\frac{t^2}{s^2} \end{pmatrix} \sim M \quad over\ GF(q),\ q\ odd.$$

**Proof.** Denoting the first matrix by $A$, the absolute set of the correlation $(A)$ is the conic $(x + \frac{1}{2}sy)^2 + y^2 - (\frac{tz}{s} - \frac{1}{2}sy)^2 = 0$.

As in the preceding proposition, the absolute point $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)$ is the unique point fixed by the induced collineation. Since the absolute set is a $(q+1)$-arc, every line through $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)$, except $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)^{(A)}$, contains one, and only one, absolute point of $(A)$ distinct from $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)$.

Let

$$\begin{pmatrix} d \\ e \\ 1 \end{pmatrix} \neq \begin{pmatrix} t/s \\ 0 \\ 1 \end{pmatrix}$$

be a point on the line $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)^{(A)}$. Then let $\left(\begin{smallmatrix} u \\ v \\ r \end{smallmatrix}\right)$ be the unique absolute point distinct from $\left(\begin{smallmatrix} t/s \\ 0 \\ 1 \end{smallmatrix}\right)$ on the line $\left(\begin{smallmatrix} d \\ e \\ 1 \end{smallmatrix}\right)^{(A)}$. The equations of the two lines are:

$$\begin{pmatrix} t/s \\ 0 \\ 1 \end{pmatrix}^{(A)} : \quad \frac{t}{s}x + ty - \frac{t^2}{s^2}z = 0,$$

$$\begin{pmatrix} d \\ e \\ 1 \end{pmatrix}^{(A)} : \quad (d + se)x + (e + t)y - \frac{t^2}{s^2}z = 0.$$

One now verifies that

$$C^{\mathrm{T}}\begin{pmatrix}1 & s & 0\\ 0 & 1 & t\\ 0 & 0 & -\frac{t^2}{s^2}\end{pmatrix}C=\begin{pmatrix}0 & 0 & m\\ 0 & a & b\\ m & 0 & 0\end{pmatrix},\quad mab\neq 0,$$

where

$$C=\begin{pmatrix}\frac{t}{s} & d & u\\ 0 & e & v\\ 1 & 1 & r\end{pmatrix}.$$

The actual expressions for $a, b, m$ are not relevant. Finally:

$$\operatorname{diag}\left(\frac{b^2}{m},b,a\right)\begin{pmatrix}0 & 0 & m\\ 0 & a & b\\ m & 0 & 0\end{pmatrix}\operatorname{diag}\left(\frac{b^2}{m},b,a\right)=ab^2\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 1\\ 1 & 0 & 0\end{pmatrix}.\qquad\square$$

The next proposition constitutes the last link in the proof of Theorem 4.

**Proposition 30.** *Every matrix of the form*

$$\begin{pmatrix}1 & * & 0\\ 0 & * & 0\\ 0 & 0 & *\end{pmatrix}\quad \textit{over } GF(q),\ q \textit{ odd},$$

*is congruent to a matrix in the statement of Theorem* 4.

**Proof.** Let

$$C=\begin{pmatrix}0 & -w & 0\\ 1 & \rho & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}\begin{pmatrix}1 & \rho & 0\\ 0 & w & 0\\ 0 & 0 & w\end{pmatrix}C=wR_\rho.$$

Let next $\rho\neq 0$ or $\pm 2$. We will show that

$$\begin{pmatrix}1 & \rho & 0\\ 0 & 1 & 0\\ 0 & 0 & w\end{pmatrix}\sim Q_{\rho'}\quad \text{for some } \rho'\neq 0.$$

Choose $a$ such that $\gamma=a^2+\rho a+1\in NS$. Hence $a+\rho\neq 0$, evidently. Let

$$C=\begin{pmatrix}a & -\frac{1}{a+\rho} & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}\begin{pmatrix}1 & \rho & 0\\ 0 & 1 & 0\\ 0 & 0 & w\end{pmatrix}C=\begin{pmatrix}\gamma & \frac{\rho\gamma}{a+\rho} & 0\\ 0 & \frac{\gamma}{(a+\rho)^2} & 0\\ 0 & 0 & w\end{pmatrix}.$$

As the main diagonal is made up of nonsquares, the conclusion is obvious. □

## 5. Inequivalent correlations of planes of even order

The last paragraph of Theorem 5 follows from Proposition 19.

**Proposition 31.** *The absolute set of the correlation $(S_\rho)$ is a nondegenerate conic, whose nucleus (a.k.a. knot) is the nonabsolute point $\begin{pmatrix}0\\0\\1\end{pmatrix}$.*

*The induced collineation leaves invariant the point $\begin{pmatrix}0\\0\\1\end{pmatrix}$ and either two, or none, of the absolute points of the respective correlation.*

**Proof.** Let

$$C=\begin{pmatrix}1 & \frac{1}{\rho^2} & 0\\ 0 & \frac{1}{\rho} & 0\\ 1 & \frac{1}{\rho^2} & 1\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}S_\rho C=\begin{pmatrix}0 & 1 & 1\\ 0 & 0 & \frac{1}{\rho^2}\\ 1 & \frac{1}{\rho^2} & 1\end{pmatrix}.$$

The absolute set of the correlation defined by the last matrix has equation $xy=z^2$, which is the canonical form of a nonsingular conic [4, Theorem 5.1.7]. Its nucleus is $\begin{pmatrix}0\\0\\1\end{pmatrix}$. But $C\begin{pmatrix}0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}$, so the nucleus of the conic $x^2+\rho xy+y^2+z^2=0$ is also $\begin{pmatrix}0\\0\\1\end{pmatrix}$.

By Proposition 13, the induced collineation leaves invariant the point $\begin{pmatrix}0\\0\\1\end{pmatrix}$ and the absolute points with $z=0$, if any.

As in the case $q$ odd, the equation $x^2+\rho x+1=0$ has two roots, or none. □

**Proposition 32.** *Let*

$$V=\begin{pmatrix}1 & v & 0\\ 0 & 1 & v\\ 0 & 0 & 1\end{pmatrix},\quad v\neq 0,\ \textit{over } GF(q)\ \textit{even}.$$

*If the trinomial $x^2+vx+1$ has the zeros $e$, $1/e$, the absolute set of the correlation $(V)$ consists of the two lines $x+ey+z=0$ and $x+y/e+z=0$.*

*If the above trinomial has no zeros, the absolute set of the correlation* $(V)$ *comprises one point, namely* $\begin{pmatrix}1\\0\\1\end{pmatrix}$.

*In both cases, the induced collineation leaves invariant the absolute point* $\begin{pmatrix}1\\0\\1\end{pmatrix}$, *and no other point.*

**Proof.** The absolute set of $(V)$ has equation $x^2 + vxy + y^2 + vyz + z^2 = 0$. The point $\begin{pmatrix}1\\0\\1\end{pmatrix}$ is clearly absolute.

If $y \neq 0$, the above equation can be written as

$$\left(\frac{x+y+z}{y\sqrt{v}}\right)^2 + \sqrt{v}\left(\frac{x+y+z}{y\sqrt{v}}\right) + 1 = 0. \tag{10}$$

If the trinomial $x^2 + vx + 1$ has the zeros $e$, $1/e$, Eq. (10) produces two lines: $x + y + z = y\sqrt{ev}$ and $x + y + z = y\sqrt{v/e}$.

But $v = e + 1/e$, so $\sqrt{ev} = e + 1$ and $\sqrt{v/e} = 1 + 1/e$.

As a consequence, the two lines become $x + ey + z = 0$ and $x + y/e + z = 0$, as claimed.

If said trinomial has no zeros, Eq. (10) has no solution. About the induced collineation:

With $V$ as in the statement of the proposition, we have

$$V^{-\mathrm{T}}V = \begin{pmatrix} 1 & v & 0 \\ v & v^2+1 & v \\ v^2 & v^3+v & v^2+1 \end{pmatrix}.$$

This matrix has 1 as its unique eigenvalue, and $\begin{pmatrix}1\\0\\1\end{pmatrix}$ as its unique eigenvector. □

An immediate consequence of the last proposition is that if the trinomial $x^2 + vx + 1$ has no zeros,

$$\begin{pmatrix} 1 & v & 0 \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} \nsim \begin{pmatrix} 1 & w+\frac{1}{w} & 0 \\ 0 & 1 & w+\frac{1}{w} \\ 0 & 0 & 1 \end{pmatrix},$$

because the trinomial $x^2 + (w + 1/w)x + 1$ has the zeros $w, 1/w$.

It now follows from Proposition 13 that the next to last paragraph of Theorem 5 holds true.

## 6. Equivalent correlations of planes of even order

**Proposition 33.** *Let*

$$S = \begin{pmatrix} 1 & s & 0 \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & v & 0 \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix}, \quad \textit{over } GF(q),\ q \textit{ even.}$$

*If both trinomials $x^2+sx+1$, $x^2+vx+1$ are factorable, or if both are not factorable, then $S\sim V$. Otherwise, $S\nsim V$.*

**Proof.** The last sentence is a trivial consequence of Proposition 32.

Assume both trinomials do, or both do not, have zeros. Consider the following variable $\tau$ in the equation:

$$s^2\tau^2+v^2\tau^2+sv^2\tau+v^2=0. \tag{11}$$

It can be rewritten as

$$\left[\left(1+\frac{s}{v}\right)\tau\right]^2+\frac{sv}{s+v}\left[\left(1+\frac{s}{v}\right)\tau\right]+1=0.$$

According to Proposition 12, this equation has solutions for $\tau$. Choose one of the values of $\tau$ thus obtained and let

$$C=\begin{pmatrix}(s+\tau)v^2\tau & v^3+sv\tau & v^2\\ v^2\tau & v^3\tau+sv\tau^2 & v^2\tau\\ 0 & sv\tau & s^2\tau^2\end{pmatrix}.$$

Now one verifies, making repeated use of Eq. (11), that $C^TSC=s^2v^2\tau^4V$. □

The preceding proposition justifies the use of the matrix $W$ in Theorem 5: as mentioned already, the trinomial $x^2+(w+1/w)x+1$ is factorable.

By Proposition 21, a nonsingular matrix is congruent to

$$\begin{pmatrix}1 & * & *\\ * & * & *\\ * & * & *\end{pmatrix}.$$

**Proposition 34.** *Let*

$$D=\begin{pmatrix}1 & b & c\\ b & b^2 & bg\\ g & bc & cg\end{pmatrix},\quad b\neq 0,\ c\neq g,\ \text{over } GF(q),\ q \text{ even}.$$

*Then $D\sim W$.*

**Proof.** If $c\neq 0$, let

$$C=\begin{pmatrix}\frac{w^2c+g}{wc(w^2+1)} & \frac{w^4c+g}{w^2c(w^2+1)} & \frac{g}{wc}\\ \frac{w(w^2c+g)}{bc(w^2+1)} & \frac{w^4c+g}{bc(w^2+1)} & \frac{w}{b}\\ \frac{w^2+1}{wc} & \frac{w^4+1}{w^2c} & \frac{w^2+1}{wc}\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}DC=\frac{c^2+g^2}{c^2}W.$$

If $C = 0$, then

$$D = \begin{pmatrix} 1 & b & 0 \\ b & b^2 & bg \\ g & 0 & 0 \end{pmatrix},$$

hence

$$\operatorname{diag}\left(1, \frac{1}{b}, 1\right) \cdot D \cdot \operatorname{diag}\left(1, \frac{1}{b}, 1\right) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & g \\ g & 0 & 0 \end{pmatrix} = D'.$$

Let

$$C = \begin{pmatrix} 0 & gw^4 & gw^3 \\ gw^5 + gw^3 & gw^6 & gw^5 \\ w^5 + w & (w+1)^6 & w^5 + w \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} D' C = g^2(w^8 + w^4)W. \qquad \square$$

**Proposition 35.** *A nonsingular* $3 \times 3$ *matrix over* $GF(q)$, $q$ *even, is congruent to an upper triangular matrix.*

**Proof.** Let

$$A = \begin{pmatrix} 1 & b & c \\ d & e & f \\ g & h & i \end{pmatrix}.$$

The following three possibilities have been examined in the proof of Proposition 23: $e \neq bd$; $i \neq cg$; $e = bd$ and $i = cg$, but $h + bg \neq cd + f$.

We need to discuss the situation in which $e = bd$, $i = cg$ and $h + bg = cd + f$. The same six cases as in Proposition 23 have to be dealt with.

*Case* I. $b = d = 0$, i.e. $e = 0$ as well, and also $h = f$. Then

$$A = \begin{pmatrix} 1 & 0 & c \\ 0 & 0 & h \\ g & h & cg \end{pmatrix},$$

with $c \neq g$ (because $A$ is not supposed to be symmetric). Let

$$C = \begin{pmatrix} (cw + gw^3)(w^2+1)h & (c + w^4 g)(w^2+1)h & (cw + gw^3)(w^2+1)h \\ 0 & w^2(c+g)^2 & w^3(c+g)^2 \\ (w^5 + w)h & (w+1)^6 h & (w^5 + w)h \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & 0 & c \\ 0 & 0 & h \\ g & h & cg \end{pmatrix} C = (w^8 + w^4)(c^2 + g^2)h^2 W.$$

*Case* II. $b = 0$, $d \neq 0$. Then $e = 0$ and $h = cd + f$, so

$$A = \begin{pmatrix} 1 & 0 & c \\ d & 0 & f \\ g & cd+f & cg \end{pmatrix}.$$

We have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & g/d & 1 \end{pmatrix} A \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & g/d \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & c \\ d & 0 & f \\ 0 & cd+f & 0 \end{pmatrix}.$$

Assume first that $c \neq 0$. Then let

$$C = \begin{pmatrix} \frac{1}{w^2}cd + \frac{w^2+1}{w^2}f & \frac{w^4+w^2+1}{w^3}cd + \frac{w^2+1}{w^3}f & \frac{w^2+1}{w^2}(cd+f) \\ c & wc & 0 \\ \frac{w^4+w^2+1}{w^2}d + \frac{(w^4+1)f}{w^2c} & \frac{(w+1)^6 f}{w^3 c} + \frac{w^6+w^2+1}{w^3}d & \frac{(w^4+1)(cd+f)}{w^2 c} \end{pmatrix}.$$

It follows that

$$C^{\mathrm{T}} \begin{pmatrix} 1 & 0 & c \\ d & 0 & f \\ 0 & cd+f & 0 \end{pmatrix} C = \frac{w^4+1}{w^2}(cd+f)^2 W.$$

Assume next that $c = 0$. Then $i = 0$ and $f = h$, so that

$$A = \begin{pmatrix} 1 & 0 & 0 \\ d & 0 & h \\ g & h & 0 \end{pmatrix}.$$

Let

$$C = \begin{pmatrix} 1 & \frac{1}{w} & 1 \\ \frac{w^2+1}{d} + \frac{w^4 g}{(w^4+1)h} & \frac{w^4+1}{wd} & \frac{w^2+1}{d} + \frac{w^2 g}{(w^4+1)h} \\ \frac{w^4 d}{(w^4+1)h} & 0 & \frac{w^2 d}{(w^4+1)h} \end{pmatrix}.$$

Then

$$C^{\mathrm{T}} \begin{pmatrix} 1 & 0 & 0 \\ d & 0 & h \\ g & h & 0 \end{pmatrix} C = w^2 W.$$

*Case* III. $b \neq 0, d = 0$. Then $e = 0$ again, and $f = bg + h$, so

$$A = \begin{pmatrix} 1 & b & c \\ 0 & 0 & bg+h \\ g & h & cg \end{pmatrix}.$$

Then

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & c/b & 1 \end{pmatrix} A \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c/b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b & 0 \\ 0 & 0 & bg+h \\ g & h & 0 \end{pmatrix}.$$

Assume first that $g \neq 0$ and let

$$C = \begin{pmatrix} \frac{w^2+1}{w^2}(bg+h) & \frac{w^4+w^2+1}{w^3}bg + \frac{w^2+1}{w^3}h & \frac{1}{w^2}bg + \frac{w^2+1}{w^2}h \\ 0 & wg & g \\ \frac{w^4+1}{w^2}\left(b + \frac{h}{g}\right) & \frac{(w+1)^6 h}{w^3 g} + \frac{w^6+w^2+1}{w^3}b & \frac{w^4+w^2+1}{w^2}b + \frac{(w^4+1)h}{w^2 g} \end{pmatrix}.$$

One obtains

$$C^{\mathrm{T}}\begin{pmatrix}1 & b & 0\\ 0 & 0 & bg+h\\ g & h & 0\end{pmatrix}C=\frac{w^4+1}{w^2}(bg+h)^2W.$$

If $g=0$, then

$$A=\begin{pmatrix}1 & b & c\\ 0 & 0 & h\\ 0 & h & 0\end{pmatrix}.$$

Let

$$C=\begin{pmatrix}1 & \frac{1}{w} & 1\\ \frac{w^2+1}{b}+\frac{w^2c}{(w^4+1)h} & \frac{w^4+1}{wb} & \frac{w^2+1}{b}+\frac{w^4c}{(w^4+1)h}\\ \frac{w^2b}{(w^4+1)h} & 0 & \frac{w^4b}{(w^4+1)h}\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}\begin{pmatrix}1 & b & c\\ 0 & 0 & h\\ 0 & h & 0\end{pmatrix}C=w^2W.$$

*Case* IV. $b=d\neq 0$ and $fh=b^2cg$.

The relation $h+bg=cd+f$ becomes $f+h=bc+bg$. As a consequence, $f$ and $h$ are the roots of the equation $x^2+(bc+bg)x+b^2cg=0$, i.e. $bc$ and $bg$.

We cannot have $h=bg$ (or $f=bc$), because then $A$ would be singular. Hence $h=bc$ and $f=bg$ and we have obtained the matrix $D$ in Proposition 34, which was shown there to be congruent to $W$.

*Case* V. $0\neq b\neq d\neq 0$ and $fh=bcdg$.

As in the case in which $q$ is odd, there are two possibilities.

(1) $f=0$, which entails

$$A=\begin{pmatrix}1 & b & c\\ d & bd & 0\\ 0 & cd & 0\end{pmatrix},$$

exactly as there. Let

$$C=\begin{pmatrix}\frac{bcd(w^3+\frac{1}{w})}{b+d} & \frac{cd(w^2+1)(\frac{d}{w^2}+bw^2)}{b+d} & \frac{cd(w^2+1)(wb+\frac{d}{w})}{b+d}\\ \frac{cd(w^3+\frac{1}{w})}{b+d} & \frac{(w^2+1)bc+(w^4+\frac{1}{w^2})cd}{b+d} & \frac{(w+\frac{1}{w})bc+(w^3+w)cd}{b+d}\\ (w+\frac{1}{w^3})d & (1+\frac{1}{w^2})(\frac{d}{w^2}+bw^2) & (1+\frac{1}{w^2})(bw+\frac{d}{w})\end{pmatrix}.$$

Then

$$C^{\mathrm{T}}\begin{pmatrix}1 & b & c\\ d & bd & 0\\ 0 & cd & 0\end{pmatrix}C=\frac{(w+1)^8}{w^4}c^2d^2\begin{pmatrix}1 & w+\frac{1}{w} & 0\\ 0 & 1 & w+\frac{1}{w}\\ 0 & 0 & 1\end{pmatrix}.$$

(2) $f\neq 0$: proceed as in Proposition 23.

*Case* VI. $bd \neq 0$ and $fh \neq bcdg$: proceed as in Proposition 23. □

From Propositions 35 and 24 we infer that every nonsingular $3 \times 3$ matrix over GF($q$), $q$ even, is congruent to a matrix of form

$$\begin{pmatrix} 1 & s & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}.$$

If $s = t$, we get one of the matrices $V$, $W$ that appear in Theorem 5.

If $s \neq t$, then

$$\begin{pmatrix} 1 & s & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix} \sim S_\rho$$

for some $\rho \neq 0$, by Proposition 28.

This concludes the proof of Theorem 5.

## References

[1] G. Birkhoff, S. MacLane, A Survey of Modern Algebra, third ed., MacMillan, New York, 1966.
[2] P. Dembowski, Finite Geometries, Springer, New York, 1968.
[3] L. Dickson, Linear Groups, Dover Publications, New York, 1958.
[4] J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, Clarendon Press, Oxford, 1979.
[5] D.R. Hughes, F.C. Piper, Projective Planes, Springer, Berlin, 1973.
[6] B.C. Kestenband, Generalizing a non-existence theorem in finite projective planes, Geometriae Dedicata 44 (1992) 123–126.