TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 232, 1977

DISJOINT CIRCLES: A CLASSIFICATION

BY

GARY L. EBERT([1])

ABSTRACT. For q a prime-power, let IP(q) denote the miquelian inversive plane of order q. The classification of certain translation planes of order q^2, called subregular, has been reduced to the classification of sets of disjoint circles in IP(q). While R. H. Bruck has extensively studied triples of disjoint circles, this paper is concerned with sets of four or more circles in IP(q). In a previous paper, the author has shown (for odd q) that the number of quadruples of disjoint circles in IP(q) is asymptotic to $q^{12}/1536$. Hence a judicious approach to the classification problem is to study "interesting" quadruples. In general, let $C_1, \ldots, C_n$ be a nonlinear set of n disjoint circles in IP(q). Let H be the subgroup of the collineation group of IP(q) composed of collineations that permute the C_i's among themselves, and let K be that subgroup composed of collineations fixing each of the C_i's. An interesting set of n disjoint circles would be one for which $K = 1$. It is shown that $K = 1$ if and only if

(*) $\begin{cases} \text{(i) there does not exist a circle } D \text{ orthogonal to} \\ \qquad \text{each of the given } n \text{ circles, and} \\ \text{(ii) we do not have one circle in our set orthogonal} \\ \qquad \text{to each of the other } n-1 \text{ circles.} \end{cases}$

When $n = 4$ and under mild restrictions on q, an algorithm is developed that finds all nonlinear quadruples of disjoint circles satisfying the orthogonality conditions (*) and having nontrivial group H. Given such a quadruple, the algorithm determines exactly what group H is acting. It is also shown that most quadruples in IP(q), for large q, do indeed satisfy the conditions (*). In addition, the cases when $n = 5$, 6, or 7 are explored to a lesser degree.

0. **Introduction.** Let q be a prime-power such that $q > 3$. Let IP(q) denote the miquelian inversive plane of order q. In [2, §7] it was pointed out that a one-to-one correspondence exists between the isomorphism classes of translation planes of order q^2 which are subregular of index k and the equivalence

Presented to the Society, January 23, 1975 under the title *Disjoint circles in finite miquelian inversive planes*; received by the editors September 8, 1975.

AMS (MOS) subject classifications (1970). Primary 50D45, 20B25; Secondary 05B25, 15A63, 12C15, 10A10.

Key words and phrases. Finite miquelian inversive plane, disjoint circles, linear sets of circles, collineation group, orthogonality, inversion, conjugate pairs of points, linear fractional transformations, triple transitivity, cycle structure in symmetric groups, matrix representation of circles, nonzero squares in finite fields, Sylow theorems.

([1]) This work was part of the author's Ph. D. thesis presented at the University of Wisconsin under the direction of R. H. Bruck.

© American Mathematical Society 1977

classes of sets of k disjoint circles in IP(q) under the group of all collineations of IP(q). Hence the classification of sets of disjoint circles in IP(q) is equivalent to the classification of subregular translation planes of order q^2. In this paper, we take the former approach and study sets of four or more disjoint circles in IP(q). It should be noted that triples of disjoint circles were extensively studied by R. H. Bruck in [1].

1. **Preliminary results.** An *inversive plane* is a set I of objects, called points, and a collection of subsets of I, called circles, such that (i) every three distinct points of I lie on exactly one circle; (ii) given a circle C of I, a point P on C, and a point Q which is not on C, there exists exactly one circle C' of I such that C' contains P, Q and has only P in common with C; (iii) every circle of I is nonempty, and there exist four points of I not lying on any circle.

Let I be an inversive plane. Any two distinct circles of I must be *disjoint*, *tangent*, or *secant* accordingly as they have zero, one, or two points in common. I is called *finite* if it contains only a finite number of points. For a finite inversive plane I, it is easy to show (see [3]) that there exists a positive integer n, called the *order* of I, such that:

(1) I has exactly $n^2 + 1$ points.

(2) I has exactly $n(n^2 + 1)$ circles.

(3) There are exactly $n + 1$ points on every circle.

(4) There are exactly $n(n + 1)$ circles through each point of I.

We will be concerned with finite inversive planes of a special type, called *miquelian*. It can be shown (see [8]) that a finite miquelian inversive plane must have prime-power order, and there exists a unique (up to isomorphism) miquelian inversive plane of order q, denoted by IP(q), for every prime-power q. A well-known representation for IP(q) is the following (see [1, §7]). Let $L = \mathrm{PG}(1, q^2)$ denote the projective line of order q^2. Then the $q^2 + 1$ points of L can be thought of as the points of IP(q), with the projective sublines of L of order q regarded as the circles of IP(q). In affine terms, the points of IP(q) can be represented by the elements of $\mathrm{GF}(q^2) \cup \infty$. In this notation, the elements of $\mathrm{GF}(q) \cup \infty$ represent a circle C_0. We will use this affine treatment for the remainder of the paper.

A *collineation* of an inversive plane I is a bijection of the points of I onto itself which sends concircular sets onto concircular sets and preserves incidence. A nonidentity collineation of I that fixes some circle C pointwise is called an *inversion with respect to* C. If an inversion with respect to C exists, it is unique, has order two, and fixes no points other than those of C (see [6]). For finite miquelian inversive planes, a unique inversion exists with respect to every circle in the plane.

Two distinct points P and Q of I are called *conjugate* with respect to some circle C if inversion with respect to C interchanges P and Q. A collection of

circles $C_1, \ldots, C_d$ (where $d \geqslant 3$) is called *linear* if there exists a conjugate pair P, Q or points common to all the circles $C_1, \ldots, C_d$. As shown in [1, Lemma 7.4], two distinct circles of IP(q) are disjoint if and only if they have a common pair P, Q of conjugate points. This common pair is unique if it exists. Therefore distinct circles in a linear set are necessarily disjoint. A *complete* linear set (i.e. *linear flock*) in IP(q) is a linear set consisting of $q - 1$ circles. The two points of IP(q) not covered by the linear flock are called the *carriers* of the flock. Any two distinct points in IP(q) determine a unique linear flock with the given two points as carriers.

Two distinct circles C and D of I are called *orthogonal* if inversion with respect to one of the circles fixes the other as a circle. This is written $C \perp D$. Let C, D be two distinct circles in IP(q), and let θ, φ be their respective inversions. It can be shown (see [1, Lemma 7.12]) that the following are equivalent:

(i) $\theta\varphi = \varphi\theta$.
(ii) $D\theta = D$.
(iii) $C\varphi = C$.
(iv) D contains a pair of conjugate points with respect to C.
(v) C contains a pair of conjugate points with respect to D.

If the above conditions hold (i.e. $C \perp D$), then C and D are tangent if q is even, and C and D are secant or disjoint if q is odd. In [4] it is shown that, for q even, two distinct circles of IP(q) are orthogonal if and only if they are tangent.

Let G be the group of collineations of IP(q) generated by the inversions and the collineations induced by the projective linear group of the line $L = \mathrm{PG}(1, q^2)$. This latter set of collineations is strictly transitive on the ordered triples of three distinct points P, Q, R of L. When q is a prime, G is the group of all collineations of IP(q). It can be shown (see [1, Lemma 7.3]) that G consists of all mappings of the form

$$f: z \to \frac{\alpha z^n + \beta}{\gamma z^n + \delta} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $n = 1$ or q, and $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q^2)$ such that $\alpha\delta - \beta\gamma \neq 0$. When $n = 1$, we obtain the linear fractional collineations; and when $n = q$, we obtain the semilinear fractional collineations in G. Every inversion must have the form

$$h: z \to \frac{\lambda z^q + a}{bz^q - \lambda^q} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $\lambda \in \mathrm{GF}(q^2)$; $a, b \in \mathrm{GF}(q)$; and $\lambda^{q+1} + ab \neq 0$.

The following collection of lemmas will provide useful tools later on.

LEMMA (1.1). *Let C, D, E be distinct circles of* IP(q). *Let P, Q be a conjugate*

pair of points for C, and let φ denote inversion with respect to C. Let θ be any element of G. Then

(1) *$\theta^{-1}\varphi\theta$ is inversion with respect to the circle $C\theta$.*

(2) *$P\theta$, $Q\theta$ is a conjugate pair of points for $C\theta$.*

(3) *If C, D, E is a linear set, then $C\theta$, $D\theta$, $E\theta$ is a linear set.*

(4) *If $C \perp D$, then $C\theta \perp D\theta$.*

PROOF. (1) Let $R\theta$ be an arbitrary point of the circle $C\theta$, where R is a point of C. Then $(R\theta)\theta^{-1}\varphi\theta = R\varphi\theta = R\theta$, and $\theta^{-1}\varphi\theta$ fixes every point of $C\theta$. By definition, $\theta^{-1}\varphi\theta$ is inversion with respect to $C\theta$.

(2) $(P\theta)\theta^{-1}\varphi\theta = P\varphi\theta = Q\theta$, where $\theta^{-1}\varphi\theta$ is inversion with respect to $C\theta$. Hence, by definition, $P\theta$ and $Q\theta$ are conjugate with respect to $C\theta$.

(3) Assume that C, D, E is a linear set with carriers R and S. By part (2), $R\theta$ and $S\theta$ are conjugate with respect to $C\theta$, $D\theta$, and $E\theta$. Therefore $C\theta$, $D\theta$, $E\theta$ is a linear set.

(4) Assume that $C \perp D$. Then $(D\theta)\theta^{-1}\varphi\theta = D\varphi\theta = D\theta$, where $\theta^{-1}\varphi\theta$ is inversion with respect to $C\theta$. Thus, by definition, $C\theta \perp D\theta$. This completes the proof of the lemma.

LEMMA (1.2). *Let θ be any element of G.*

(1) *If θ fixes the points 0 and ∞, then θ must have the form*

$$\theta\colon z \to vz^n \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $n = 1$ or q, and $0 \neq v \in \mathrm{GF}(q^2)$.

(2) *If θ interchanges the points 0 and ∞, then θ must have the form*

$$\theta\colon z \to v/z^n \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $n = 1$ or q, and $0 \neq v \in \mathrm{GF}(q^2)$.

PROOF. As stated previously, any element of G must have the form

$$\theta\colon z \to \frac{\alpha z^n + \beta}{\gamma z^n + \delta} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $n = 1$ or q, and $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q^2)$ such that $\alpha\delta - \beta\gamma \neq 0$. To prove (1), assume that θ fixes 0 and ∞. Then $\beta = 0 = \gamma$ above, and hence $\alpha\delta \neq 0$. Thus $\theta\colon z \to \alpha z^n/\delta = vz^n$, where $v = \alpha/\delta$ is a nonzero element of $\mathrm{GF}(q^2)$. The proof of (2) is similar.

LEMMA (1.3). *The composition of two semilinear fractional collineations in G is a linear fractional collineation.*

PROOF. Follows immediately.

LEMMA (1.4). *Let $\theta\colon z \to vz^q$ for all z in $\mathrm{GF}(q^2) \cup \infty$, where $v \in \mathrm{GF}(q^2)$ such that $v^{q+1} = 1$. Then θ is an inversion.*

PROOF. Since $v^{q+1} = 1$, $|v|$ divides $q + 1$ and $|v| \cdot (q - 1)$ divides $q^2 - 1$. Hence there exists an element λ in GF(q^2) such that $|\lambda| = |v| \cdot (q - 1)$. Thus $|\lambda^{q-1}| = |v| = |v^{-1}|$, and $v^{-1} = (\lambda^{q-1})^s = (\lambda^s)^{q-1}$ for some integer s. Let ε be an element of GF(q^2) such that $\varepsilon^{q-1} = -1$. Set $x = \varepsilon\lambda^s$, which is a nonzero element of GF(q^2). Then $x^{q-1} = -v^{-1}$ and $v = -x/x^q$. Hence θ: $z \to xz^q/-x^q$ for all z in GF(q^2) $\cup \infty$, and θ has the previously given form of an inversion. This proves the lemma.

LEMMA (1.5). *Let θ be a nonidentity element of G, and assume that θ fixes at least three distinct points of* IP(q). *Then θ is an inversion.*

PROOF. Suppose that θ fixes the distinct points P, Q, R of IP(q). Since G is triply transitive on the points of IP(q), there exists an element ψ in G (linear fractional, in fact) that maps P into 0, Q into 1, and R into ∞. Then $\psi^{-1}\theta\psi$ is a nonidentity element of G fixing the points 0, 1 and ∞. If $\psi^{-1}\theta\psi$ is an inversion, so is θ by Lemma (1.1)(1). Hence, without loss of generality, we may assume θ fixes the points 0, 1 and ∞. By Lemma (1.2)(1), θ must have the form θ: $z \to vz^n$ where $n = 1$ or q and $0 \neq v \in$ GF(q^2). Since $1\theta = 1$, $v = 1$ and θ: $z \to z^n$. But $\theta \neq 1$, and therefore $n = q$. Hence θ: $z \to z^q$, and θ is an inversion by Lemma (1.4). This completes the proof.

The next two results are due to Bruck (see [1, Theorem 7.14 and his ensuing discussion]), and will be stated here without proof.

THEOREM (1.6). *Assume that $q > 4$. Then* IP(q) *has at least one nonlinear triple C_1, C_2, C_3 of disjoint circles. Given any such triple, let P_{ij}, Q_{ij} denote the common conjugate pair for C_i, C_j ($1 \leqslant i < j \leqslant 3$). Then*

(1) *the six points P_{ij}, Q_{ij} are distinct points of a (unique) circle D in* IP(q), *and*

(2) *no circle of* IP(q) *has all three pairs P_{ij}, Q_{ij} as pairs of conjugate points.*

If q is even, then D is tangent to C_1, C_2 and C_3. If q is odd, then D and C_i are secant or disjoint for each i. In any case, each C_i is orthogonal to D.

COROLLARY (1.7). *Let C_1, C_2, C_3 be a nonlinear triple of disjoint circles in* IP(q), *where $q > 4$. Let P_{ij}, Q_{ij} be defined as above. Then no element of G can induce the permutation $(P_{12}Q_{12})(P_{13}Q_{13})(P_{23}Q_{23})$.*

The model we will use for IP(q) in the remainder of this paper is a slight variation of that given above, and was first discussed by W. F. Orr in [7]. The elements of GF(q^2) $\cup \infty$ will still be regarded as the points of IP(q). However, a circle will be represented as a one-dimensional vector space over GF(q) with basis element a 2×2 matrix of the form

$$\begin{pmatrix} x & a \\ b & -x^q \end{pmatrix},$$

where $x \in$ GF(q^2); $a, b \in$ GF(q), and $x^{q+1} + ab \neq 0$. Such a circle will have

as its inversion

$$z \to \frac{xz^q + a}{bz^q - x^q} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty.$$

As stated previously, every circle of IP(q) has a unique inversion associated with it, and every inversion does indeed have the form listed above. The points of IP(q) lying on a given circle C are simply those points that are fixed under inversion with respect to C.

In the work that follows, we will write

$$C = \begin{pmatrix} x & a \\ b & -x^q \end{pmatrix}$$

to denote a circle, rather than writing

$$C = \left\langle \begin{pmatrix} x & a \\ b & -x^q \end{pmatrix} \right\rangle,$$

where $\langle\ \rangle$ designates the one-dimensional vector space over GF(q). Although only a basis element is given, it is to be understood that the circle is really a one-dimensional vector space over GF(q). We will use C to represent both the circle of IP(q) and the corresponding inversion matrix, so long as the context makes it clear what we are saying. When we write

$$\begin{pmatrix} x & a \\ b & -x^q \end{pmatrix} \cong \begin{pmatrix} y & c \\ d & -y^q \end{pmatrix},$$

we mean that the two matrices represent the same circle. That is, there exists a nonzero element λ of GF(q) such that one matrix is a scalar multiple of the other by means of the element λ.

If R is any 2×2 matrix, R' will denote the matrix obtained from R by raising each entry to the qth power, and R^* will denote the adjoint of the matrix R. Let

$$R = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\alpha, \beta, \gamma, \delta \in \mathrm{GF}(q^2)$ such that $\alpha\delta - \beta\gamma \neq 0$. Define the following two collineations of IP(q):

$$\varphi_R: z \to \frac{\alpha z + \beta}{\gamma z + \delta} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

$$\varphi'_R: z \to \frac{\alpha z^q + \beta}{\gamma z^q + \delta} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty.$$

As pointed out in [7, §1], the mappings φ_R and φ'_R have the following effect on a circle C:

$$\varphi_R: C \to RCR'^*, \qquad \varphi'_R: C \to RC'R'^*.$$

If $R = D$ represents a circle, then φ'_D is inversion with respect to D.

Let C, D be matrices representing circles of IP(q). We define $\|C\|$ to be the determinant of C, and define

$$h(C, D) = \|C + D\| - \|C\| - \|D\|.$$

Orr has shown (see [7, Lemma 1.3]) that

$$D\varphi'_C \cong D \quad \text{if and only if } C \cong D \text{ or } h(C, D) = 0.$$

Thus it makes sense to say that two distinct circles C, D of IP(q) are orthogonal if and only if $h(C, D) = 0$. We say that a circle C is self-orthogonal if and only if $h(C, C) = 0$. It should be noted that

$$h(C, C) = \|2C\| - 2\|C\| = 2\|C\|.$$

Hence, if q is odd, $h(C, C) \neq 0$ and a circle of IP(q) is never orthogonal to itself. On the other hand, if q is even, every circle of IP(q) is self-orthogonal.

We now restrict ourselves to odd prime-powers q. For two distinct circles C, D of IP(q), we define the following products:

$$C \cdot D = h(C, D)/2, \qquad C \times D = (C \cdot D)^2 - \|C\| \, \|D\|.$$

Orr has shown (see [7, Lemma 2.1]) that C and D are disjoint, tangent, or secant accordingly as $C \times D$ is a nonzero square, zero, or a nonsquare in GF(q). These tools will help us greatly in our later studies.

2. **A general result.** The purpose of this paper is to study sets of n disjoint circles in IP(q), where $n \geq 4$. In [5, Theorem 2] it was pointed out that, for q an odd prime-power, the number of quadruples of disjoint circles in IP(q) is asymptotic to $q^{12}/1536$. Since there are so many quadruples, a judicious approach to the classification problem is simply to study "interesting" quadruples. In general, let $C_1, \ldots, C_n$ be n pairwise disjoint circles in IP(q). Since linear sets of disjoint circles have been extensively studied, we will assume this set is nonlinear. Let G be defined as in §1. Let

$$H = \{\theta \in G/\theta \text{ permutes the } C_i\text{'s among themselves}\},$$

$$K = \{\theta \in G/\theta \text{ fixes each of the } C_i\text{'s}\}.$$

Clearly, H/K is isomorphic to a subgroup of S_n, the symmetric group on n letters. An interesting set of n disjoint circles would be one for which $K = 1$. The following two results tell us precisely when that situation occurs.

LEMMA (2.1). *Let q be any prime-power. Let $C_1, \ldots, C_n$ be a nonlinear set of pairwise disjoint circles in* IP(q), *where $n \geq 4$. Assume that $C_1, C_2, \ldots, C_{n-1}$ is a linear subset with carriers P and Q, and assume that C_n does not contain both points P and Q. Then any collineation in G that fixes each of the n circles is either the identity mapping or an inversion.*

PROOF. Let θ be an element of G that fixes each of the circles $C_1, \ldots, C_n$.

Since G is doubly transitive on the points of IP(q), there exists an element ψ in G that maps P into 0 and Q into ∞. By Lemma (1.1), $C_1\psi, \ldots, C_n\psi$ is a set of n circles satisfying all the hypotheses of the lemma. The carriers of the linear subset $C_1\psi, \ldots, C_{n-1}\psi$ are 0 and ∞. Also $\psi^{-1}\theta\psi$ is a collineation of G fixing each of the circles $C_1\psi, \ldots, C_n\psi$. If the lemma is true in this case, then $\psi^{-1}\theta\psi$ is either the identity mapping or an inversion. This implies, by Lemma (1.1)(1), that θ is either the identity mapping or an inversion. Thus, without loss of generality, we may assume that $P = 0$ and $Q = \infty$.

Let φ_1 denote inversion with respect to C_1. Since φ_1 interchanges 0 and ∞, Lemma (1.2)(2) implies that φ_1 must have the form $\varphi_1\colon z \to v/z^t$ where $t = 1$ or q, and $0 \neq v \in \mathrm{GF}(q^2)$. Since φ_1 is an inversion, $t = q$ and $v \in \mathrm{GF}(q)$. We now apply the same argument to $C_2, C_3, \ldots, C_{n-1}$. Thus, without loss of generality, we may write

$$C_i = \begin{pmatrix} 0 & a_i \\ 1 & 0 \end{pmatrix} \quad \text{for } i = 1, 2, \ldots, n-1,$$

where $a_1, a_2, \ldots, a_{n-1}$ are distinct nonzero elements of GF(q). As always, we may write

$$C_n = \begin{pmatrix} x & b \\ c & -x^q \end{pmatrix} \quad \begin{array}{l} \text{where } x \in \mathrm{GF}(q^2);\ b, c \in \mathrm{GF}(q); \\ \text{and } x^{q+1} + bc \neq 0. \end{array}$$

Note that $x \neq 0$ since $C_1, \ldots, C_n$ is a nonlinear set. Since θ fixes $C_1, \ldots, C_{n-1}$, Lemma (1.1)(2) implies that θ fixes the pair of points $\{0, \infty\}$. Hence, by Lemma (1.2), θ must have the form $\theta\colon z \to vz^t$ for all z in $\mathrm{GF}(q^2) \cup \infty$, where $t = \pm 1$ or $\pm q$, and $0 \neq v \in \mathrm{GF}(q^2)$.

Suppose first that $t = 1$. In the notation of §1, $\theta = \varphi_R$ where $R = \left(\begin{smallmatrix} v & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Thus

$$C_1\theta = \begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & a_1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & v^q \end{pmatrix} = \begin{pmatrix} 0 & a_1 v^{q+1} \\ 1 & 0 \end{pmatrix}.$$

Since $C_1\theta = C_1$, we must have $v^{q+1} = 1$. Now

$$\begin{pmatrix} x & b \\ c & -x^q \end{pmatrix} = C_n \cong C_n\theta = \begin{pmatrix} vx & b \\ c & -v^q x^q \end{pmatrix}.$$

If $b \neq 0$ or $c \neq 0$, then $vx = x$ and hence $v = 1$ since $x \neq 0$. Thus $\theta\colon z \to z$ is the identity mapping, and we are done. If $b = 0 = c$, then

$$C_n = \begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix}.$$

In this case, it is easy to see that inversion with respect to C_n fixes both points 0 and ∞, which contradicts the hypotheses.

Next assume that $t = q$, and therefore $\theta = \varphi_R'$ where $R = \left(\begin{smallmatrix} v & 0 \\ 0 & 1 \end{smallmatrix}\right)$. $C_1\theta = C_1$ again implies that $v^{q+1} = 1$. This time,

$$\begin{pmatrix} x & b \\ c & -x^q \end{pmatrix} = C_n \cong C_n\theta = \begin{pmatrix} vx^q & b \\ c & -v^q x \end{pmatrix}.$$

If $c \neq 0$ or $b \neq 0$, then $vx^q = x$. This implies that x is fixed by θ, and therefore θ fixes the three distinct points 0, x, and ∞. By Lemma (1.5), θ is an inversion and we are done. If $b = 0 = c$, we again obtain the contradiction that C_n contains both 0 and ∞.

Next assume that $t = -1$, and therefore $\theta = \varphi_R$ where $R = \left(\begin{smallmatrix} 0 & v \\ 1 & 0 \end{smallmatrix}\right)$. Then

$$C_1\theta = \begin{pmatrix} 0 & -v^{q+1} \\ -a_1 & 0 \end{pmatrix} \cong \begin{pmatrix} 0 & v^{q+1}/a_1 \\ 1 & 0 \end{pmatrix}.$$

Since $C_1\theta = C_1$, we must have $v^{q+1} = a_1^2$. Similarly, $C_2\theta = C_2$ and $C_3\theta = C_3$ imply that $a_2^2 = v^{q+1} = a_3^2$. Now $a_1^2 = a_2^2$ implies that $a_1 = -a_2$ since the a_i's are distinct. Similarly, $a_3 = -a_2$ and therefore $a_1 = a_3$, which is a contradiction.

Finally, when $t = -q$, we arrive at the same contradiction as when $t = -1$. This completes the proof of the lemma.

THEOREM (2.2). *Let $C_1, \ldots, C_n$ be a nonlinear set of pairwise disjoint circles in* IP(q), *where $q > 4$ is a prime-power and $n \geqslant 4$. Let G, H, K be defined as above. Then $K = 1$ (and thus H is isomorphic to a subgroup of S_n) if and only if the following two conditions hold*:

(*)
- (i) *There does not exist a circle D orthogonal to each of the given n circles.*
- (ii) *We do not have one circle in our set orthogonal to each of the other $n - 1$ circles.*

PROOF. If condition (i) does not hold, then there exists a circle D orthogonal to $C_1, \ldots, C_n$. Let φ denote inversion with respect to D. Clearly $\varphi \in K$ and thus $K \neq 1$. If condition (ii) does not hold, we can say, without loss of generality, that C_1 is orthogonal to $C_2, C_3, \ldots, C_n$. Let φ_1 denote inversion with respect to C_1. Clearly $\varphi_1 \in K$ and again $K \neq 1$. Therefore, if $K = 1$, the conditions (*) must hold.

Now suppose that the conditions (*) do hold. We want to show that $K = 1$. Suppose not, and let θ be a nonidentity element in K. Assume first that θ fixes at most two distinct points of IP(q), and hence is not an inversion. Since $C_1, \ldots, C_n$ is a nonlinear set, some of the subtriples must be nonlinear. Without loss of generality, say that C_1, C_2, C_3 is a nonlinear subtriple. Let P_{ij}, Q_{ij} denote the unique common conjugate pair of points for the two disjoint circles C_i and C_j whenever $i < j$. Since $C_i\theta = C_i$ for $1 \leqslant i \leqslant n$, Lemma (1.1)(2) implies that θ fixes the pair $\{P_{ij}, Q_{ij}\}$ for $i < j$. Thus θ either fixes or interchanges the two points P_{ij}, Q_{ij}.

Since C_1, C_2, C_3 is a nonlinear triple, Theorem (1.6) implies that the six points $P_{12}, Q_{12}, P_{13}, Q_{13}, P_{23}, Q_{23}$ are all distinct. By Corollary (1.7), θ cannot induce the permutation $(P_{12}Q_{12})(P_{13}Q_{13})(P_{23}Q_{23})$. Since θ fixes at most two distinct points, θ induces, without loss of generality, the permutation $(P_{12})(Q_{12})(P_{13}Q_{13})(P_{23}Q_{23})$.

Suppose that all the subtriples

$$C_1, C_2, C_4; \quad C_1, C_2, C_5; \quad \cdots; \quad C_1, C_2, C_n$$

are linear. Then $C_1, C_2, C_4, C_5, \ldots, C_n$ is a linear set. By Lemma (2.1), C_3 must be orthogonal to $C_1, C_2, C_4, C_5, \ldots, C_n$. But this contradicts condition (ii). Hence, without loss of generality, we may assume C_1, C_2, C_4 is a nonlinear triple. Again, by Theorem (1.6), the six points $P_{12}, Q_{12}, P_{14}, Q_{14}, P_{24}, Q_{24}$ are all distinct. Since θ fixes at most two distinct points, θ must induce the permutation $(P_{12})(Q_{12})(P_{14}Q_{14})(P_{24}Q_{24})$.

Now consider the subtriple C_1, C_3, C_4. If the triple C_1, C_3, C_4 is nonlinear, look at the six distinct points $P_{13}, Q_{13}, P_{14}, Q_{14}, P_{34}, Q_{34}$. Since θ induces $(P_{13}Q_{13})(P_{14}Q_{14})$, Corollary (1.7) implies that θ fixes the points P_{34} and Q_{34}. But θ fixes at most two distinct points, and therefore, without loss of generality, $P_{12} = P_{34}$ and $Q_{12} = Q_{34}$. This implies that C_1, C_2, C_3, C_4 is a linear set, which contradicts the fact that C_1, C_2, C_3 is a nonlinear triple. Hence we must assume that C_1, C_3, C_4 is a linear subtriple. Similarly, the subtriple C_2, C_3, C_4 must be linear. But this again implies that C_1, C_2, C_3, C_4 is a linear set, yielding the same contradiction as above.

Therefore we must assume that θ fixes more than two points of IP(q), and hence, by Lemma (1.5), θ is an inversion with respect to some circle D. Since $C_i\theta = C_i$ for all i, either $D \perp C_i$ or $D = C_i$ for each i. If $D = C_i$ for some i, then $D \perp C_j$ for all j distinct from i, which contradicts condition (ii). If $D \neq C_i$ for every i, then $D \perp C_i$ for all i, which contradicts condition (i). Hence our original supposition is false, and $K = 1$. This proves the theorem.

We will assume that the orthogonality conditions (*) are satisfied for the remainder of this paper. In considering the possibilities for the group H, it will be useful to assume that $q \not\equiv 0\ (p)$ for all primes $p < n$. The following notation will be helpful:

S_n = the symmetric group on n letters,

A_n = the alternating group on n letters,

D_n = the dihedral group of order $2n$,

Z_n = the cyclic group of order n.

Returning to the case $n = 4$, in Appendix A we show that, for q an odd prime-power, the conditions (*) do indeed hold for most quadruples in IP(q) as q gets large. Hence we are not only studying interesting quadruples, but we

are studying the most common quadruples as well.

3. **Nonlinear quadruples.** We now investigate in detail nonlinear quadruples of disjoint circles in IP(q), where q is an odd prime-power such that $q \not\equiv 0$ (3). We assume that the orthogonality conditions (*) of the previous section hold. We say that two quadruples are in the same equivalence class under G if there exists an element in G that takes one quadruple into the other. As pointed out in the introduction, we are only interested in classifying quadruples up to their equivalence classes. Let C_1, C_2, C_3, C_4 be a quadruple as described above, and let H be the corresponding permutation subgroup as defined in the previous section. Since H is isomorphic to a subgroup of S_4, we will study the collineations in H in terms of their cycle structure on the four elements C_1, C_2, C_3, C_4. The purpose of this section is to develop an algorithm that will find all quadruples of disjoint circles with the above-mentioned characteristics and having nontrivial group H. Given such a quadruple, the algorithm should determine exactly what group H is acting on it.

Suppose there exists a 2-cycle ψ in H. Without loss of generality, say that ψ induces the permutation $(C_1C_2)(C_3)(C_4)$. Since H is embedded in S_4, ψ has order 2 as a collineation of IP(q). There are $q^2 + 1$ points in IP(q), and $q^2 + 1 \equiv 0$ (2) since q is odd. Hence ψ must fix an even number of points in IP(q).

Assume first that ψ is fixed-point-free. As before, let P_{ij}, Q_{ij} denote the unique common conjugate pair of points for C_i and C_j when $i < j$. Since G is doubly transitive on the points of IP(q), there exists a collineation θ in G that maps P_{34} into 0 and Q_{34} into ∞. Then $\theta^{-1}\psi\theta$ is a fixed-point-free collineation of order 2 that induces the permutation $(C_1\theta C_2\theta)(C_3\theta)(C_4\theta)$. By Lemma (1.1), the quadruple $C_1\theta$, $C_2\theta$, $C_3\theta$, $C_4\theta$ satisfies the conditions (*), and the common conjugate pair for $C_3\theta$ and $C_4\theta$ is 0, ∞. Hence, by replacing C_1, C_2, C_3, C_4 with $C_1\theta$, $C_2\theta$, $C_3\theta$, $C_4\theta$ and replacing ψ with $\theta^{-1}\psi\theta$, we can assume that $P_{34} = 0$ and $Q_{34} = \infty$ in our original situation. This is all made possible since C_1, C_2, C_3, C_4 and $C_1\theta$, $C_2\theta$, $C_3\theta$, $C_4\theta$ are in the same equivalence class under G.

Since $C_3\psi = C_3$ and $C_4\psi = C_4$, Lemma (1.1)(2) implies that ψ fixes the pair of points $\{0, \infty\}$. Since Ψ is fixed-point-free, ψ interchanges 0 and ∞. By Lemma (1.2)(2), ψ must have the form ψ: $z \to v/z^n$ where $n = 1$ or q, and $0 \neq v \in \mathrm{GF}(q^2)$. It should be noted that $z^{n^2} = z$ for $n = 1$ or q whenever z is in $\mathrm{GF}(q^2) \cup \infty$. Hence ψ^2: $z \to z/v^{n-1}$. Since ψ has order 2, $v^{n-1} = 1$. If $n = q$, then $v \in \mathrm{GF}(q)$ and ψ has the form of an inversion, contradicting the fact that ψ is fixed-point-free. Thus $n = 1$ and ψ: $z \to v/z$ where $0 \neq v \in \mathrm{GF}(q^2)$. Since ψ is fixed-point-free, v must be a nonsquare in $\mathrm{GF}(q^2)$.

As in the proof of Lemma (2.1), since 0, ∞ is a conjugate pair for C_3, we may write $C_3 = \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)$ where $0 \neq a \in \mathrm{GF}(q)$. Using computations similar to

those in Lemma (2.1), we see that $C_3\psi = C_3$ implies that $v^{q+1} = a^2$. Then

$$(v^{q+1})^{(q-1)/2} = (a^2)^{(q-1)/2} = a^{q-1} = 1.$$

Thus $|v|$ divides $(q^2 - 1)/2$, which implies that v is a nonzero square in $GF(q^2)$. This contradiction eliminates this case.

Next assume that ψ fixes exactly two points of $IP(q)$. Since G is doubly transitive on the points of $IP(q)$, an argument similar to that used above shows that we may assume ψ fixes the two points 0 and ∞. By Lemma (1.2)(1), ψ must have the form $\psi\colon z \to vz^n$ where $n = 1$ or q, and $0 \neq v \in GF(q^2)$. Since ψ has order 2, $v^{n+1} = 1$. If $n = q$, then ψ is an inversion by Lemma (1.4) and therefore fixes more than two points. This contradicts our assumption.

Hence $n = 1$ and $\psi\colon z \to -z$. Write

$$C_3 = \begin{pmatrix} x & a \\ b & -x^q \end{pmatrix} \quad \text{where } x \in GF(q^2);\ a, b \in GF(q); \text{ and } x^{q+1} + ab \neq 0.$$

Then

$$\begin{pmatrix} x & a \\ b & -x^q \end{pmatrix} = C_3 \cong C_3\psi = \begin{pmatrix} -x & a \\ b & x^q \end{pmatrix}.$$

If $x = 0$, then $ab \neq 0$ and, without loss of generality, $C_3 \cong \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)$ where $0 \neq a \in GF(q)$. If $x \neq 0$, then $C_3 \cong C_3\psi$ implies that $a = 0 = b$ and

$$C_3 = \begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix}.$$

Since $C_4\psi = C_4$, C_4 must also have one of the above two forms. It is easy to see that any circle of the form

$$\begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix}$$

contains both points 0 and ∞. Since C_3 and C_4 are disjoint, they cannot both have this second form.

Write

$$C_1 = \begin{pmatrix} y & d \\ c & -y^q \end{pmatrix} \quad \text{where } y \in GF(q^2);\ c, d \in GF(q); \text{ and } y^{q+1} + cd \neq 0.$$

Now ψ fixes the points 0 and ∞, and takes the circle C_1 into the disjoint circle C_2. Hence C_1 contains neither 0 nor ∞. Thus $d \neq 0$ and $c \neq 0$ above. If $y = 0$, then $C_1\psi = C_1$, a contradiction. Hence $y \neq 0$ and y/c, 0, ∞ are three distinct points of $IP(q)$. Since G is triply transitive on the points of $IP(q)$, we may assume, without loss of generality, that $y/c = 1$. Hence $y = c \in GF(q)$ and $C_1 \cong \left(\begin{smallmatrix} 1 & d \\ 1 & -1 \end{smallmatrix}\right)$ where $0, -1 \neq d \in GF(q)$. Then $C_2 = C_1\psi = \left(\begin{smallmatrix} -1 & d \\ 1 & 1 \end{smallmatrix}\right)$.

Suppose that C_3 and C_4 have the same form, as given above. If we set

$D = \left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right)$, where $\varepsilon \in \mathrm{GF}(q^2)$ such that $\varepsilon^{q-1} = -1$, it is easy to check that D is a circle orthogonal to C_1, C_2, C_3, C_4. This contradicts the conditions (*).

Hence we may assume, without loss of generality, that

$$C_3 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad C_4 = \begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix},$$

where a, x are nonzero elements of $\mathrm{GF}(q)$, $\mathrm{GF}(q^2)$ respectively. The following cross products are easily computed:

$$C_1 \times C_2 = -4d,$$
$$C_1 \times C_3 = \tfrac{1}{4}(a^2 + d^2) - \tfrac{1}{2}ad - a,$$
$$C_1 \times C_4 = \tfrac{1}{4}(x^{2q} + x^2) - \left(\tfrac{1}{2} + d\right)x^{q+1},$$
$$C_3 \times C_4 = -ax^{q+1}.$$

Since C_1, C_2, C_3, C_4 are pairwise disjoint circles, all the above cross products must be nonzero squares in $\mathrm{GF}(q)$. Using the fact that ψ induces the permutation $(C_1C_2)(C_3)(C_4)$, we only need check the above cross products to insure that our four circles are pairwise disjoint.

Now we must check that the conditions (*) hold for this quadruple of disjoint circles. Recall that circle A is orthogonal to circle B if and only if $h(A, B) = 0$. Suppose there exists a circle D orthogonal to C_1, C_2, C_3, C_4. Write

$$D = \begin{pmatrix} y & b \\ c & -y^q \end{pmatrix} \quad \begin{array}{l} \text{where } y \in \mathrm{GF}(q^2);\ b, c \in \mathrm{GF}(q); \\ \text{and } y^{q+1} + bc \neq 0. \end{array}$$

Then it is easy to check that

$$h(C_1, D) = -y^q - y - b - cd,$$
$$h(C_2, D) = y^q + y - b - cd,$$
$$h(C_3, D) = -ac - b,$$
$$h(C_4, D) = -xy^q - yx^q.$$

If $a \neq d$, then $h(C_i, D) = 0$ for $i = 1, 2, 3, 4$ implies that $b = 0 = c$, $y^{q-1} = -1$, and hence $x^{q-1} = 1$. In this case, $D = \left(\begin{smallmatrix} y & 0 \\ 0 & y \end{smallmatrix}\right)$ will be orthogonal to C_1, C_2, C_3, C_4. If $a = d$, then $D \cong \left(\begin{smallmatrix} 0 & -d \\ 1 & 0 \end{smallmatrix}\right)$ is orthogonal to C_1, C_2, C_3, C_4. Hence condition (i) of (*) holds for C_1, C_2, C_3, C_4 if and only if $a \neq d$ and $x \notin \mathrm{GF}(q)$.

Similar computations show that condition (ii) of (*) holds for C_1, C_2, C_3, C_4 if and only if $x^{q-1} \neq -1$ and $d \neq -a$. It only remains to be checked that our quadruple is nonlinear. Suppose that C_1, C_2, C_3 is linear. Then there exists an element α of $\mathrm{GF}(q^2)$ such that

$$\frac{\alpha^q + d}{\alpha^q - 1} = \frac{-\alpha^q + d}{\alpha^q + 1} = \frac{a}{\alpha^q}.$$

Solving the above equations simultaneously, we obtain $a = d$, which contradicts condition (i) of (*). Thus our quadruple is nonlinear, completing the case when our 2-cycle ψ has exactly two fixed points.

Finally assume that ψ has more than two fixed points, and therefore ψ is an inversion by Lemma (1.5). By transitivity we can assume that 0, ∞ is the unique common conjugate pair of points for C_3 and C_4. Since ψ fixes C_3 and C_4, Lemma (1.1)(2) implies that ψ either fixes or interchanges the two points 0 and ∞. If ψ interchanges 0 and ∞, arguments similar to those given above show that either C_1, C_2, C_3, C_4 is linear or there exists a circle D orthogonal to C_1, C_2, C_3, C_4. These are both contradictions to assumption. If ψ fixes 0 and ∞, specific requirements on C_1, C_2, C_3, C_4 can be obtained as above. All these results are stated in the following proposition.

PROPOSITION (3.1). *Let $q \not\equiv 0$ (3) be an odd prime-power. Suppose that C_1, C_2, C_3, C_4 is a nonlinear quadruple of pairwise disjoint circles in* IP(q), *and let G, H, K be defined as always. Assume that the conditions* (*) *hold for this quadruple, and assume H contains a 2-cycle. Then the equivalence class of this quadruple under G contains a quadruple of one of the following types*:

(I)
$$C_1 = \begin{pmatrix} 1 & d \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} -1 & d \\ 1 & 1 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix},$$

where $0, -1 \neq d \in \mathrm{GF}(q)$; $0 \neq a \in \mathrm{GF}(q)$; $0 \neq x \in \mathrm{GF}(q^2)$; $a \neq \pm d$; $x^q \neq \pm x$; *and the expressions* $-4d$, $\frac{1}{4}(a^2 + d^2) - \frac{1}{2}ad - a$, $\frac{1}{4}(x^{2q} + x^2) - (\frac{1}{2} + d)x^{q+1}$, $-ax^{q+1}$ *all are nonzero squares in* GF(q). *In this situation, the linear fractional collineation* ψ: $z \to -z$ *induces the permutation* $(C_1C_2)(C_3)(C_4)$.

(II)
$$C_1 = \begin{pmatrix} 1 & d \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} v & d \\ 1 & -v^q \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix},$$

where $0, -1 \neq d \in \mathrm{GF}(q)$; $v \in \mathrm{GF}(q^2)$ *such that* $v^{q+1} = 1$; $a, b \in \mathrm{GF}(q) \setminus \{0\}$; $a \neq b$; $v \neq \pm 1$; *we do not have* $a = -b = \pm d$; *and the expressions* $\frac{1}{4}(v^2 + v^{q-1}) + d(v + v^q) - 2d - \frac{1}{2}$, $\frac{1}{4}(a^2 + d^2) - \frac{1}{2}ad - a$, $\frac{1}{4}(b^2 + d^2) - \frac{1}{2}bd - b$ *are all nonzero squares in* GF(q). *In this situation, the inversion* ψ: $z \to vz^q$ *induces the permutation* $(C_1C_2)(C_3)(C_4)$.

On the other hand, any quadruple of type (I) *or type* (II) *is a nonlinear*

quadruple of pairwise disjoint circles satisfying the conditions (*) *and having a 2-cycle in its permutation group H.*

The next lemma tells us that, if H contains a 3-cycle or a 4-cycle, then H also contains a 2-cycle, and hence the equivalence class of our quadruple contains a quadruple of type (I) or (II) above.

LEMMA (3.2). *Let* $q \not\equiv 0\ (3)$ *be an odd prime-power. Suppose that* C_1, C_2, C_3, C_4 *is a nonlinear quadruple of pairwise disjoint circles in* IP(q) *satisfying the conditions* (*). *Let G, H, K be defined as always.*

(1) *If H contains a 3-cycle, then H contains a subgroup isomorphic to* S_3.

(2) *If H contains a 4-cycle, then H contains a subgroup isomorphic to* D_4.

PROOF. (1) Suppose that H contains a 3-cycle ψ. Without loss of generality, ψ induces the permutation $(C_1C_2C_3)(C_4)$. Since H is embedded in S_4, ψ has order 3 as a collineation of IP(q). Now IP(q) has $q^2 + 1$ points, where $q^2 + 1 \equiv 2\ (3)$ since $q \not\equiv 0\ (3)$. Thus ψ has at least two fixed points of IP(q). Since ψ has order 3, ψ cannot be an inversion. Therefore, by Lemma (1.5), ψ fixes exactly two points. Using the fact that G is doubly transitive on the points of IP(q), we may assume that ψ fixes 0 and ∞. Hence, by Lemma (1.2)(1), ψ must have the form $\psi\colon z \to vz^n$ where $n = 1$ or q, and $0 \neq v \in \mathrm{GF}(q^2)$. Thus $\psi^3\colon z \to v^{n+2}z^n$ for all z in $\mathrm{GF}(q^2) \cup \infty$. Since ψ has order 3, $n = 1$ and $v^3 = 1$. Hence we may assume $\psi\colon z \to wz$ where $w \in \mathrm{GF}(q^2)$ such that $|w| = 3$. It should be noted that w always exists since $q \not\equiv 0\ (3)$ and therefore 3 divides $q^2 - 1$.

Write

$$C_4 = \begin{pmatrix} x & a \\ b & -x^q \end{pmatrix} \quad \text{where } x \in \mathrm{GF}(q^2);\ a, b \in \mathrm{GF}(q);\ \text{and } x^{q+1} + ab \neq 0.$$

Since $C_4\psi = C_4$, either $C_4 \cong \left(\begin{smallmatrix} 0 & a \\ 1 & 0 \end{smallmatrix}\right)$ where $0 \neq a \in \mathrm{GF}(q)$ and $q \equiv 2\ (3)$, or else

$$C_4 \cong \begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix}$$

where $0 \neq x \in \mathrm{GF}(q^2)$ and $q \equiv 1\ (3)$.

Assume first that $q \equiv 2\ (3)$. C_1 does not contain either the point 0 or ∞ since ψ fixes both 0 and ∞ but takes the circle C_1 into the disjoint circle C_2. Using the triple transitivity of G as before, we may write

$$C_1 = \begin{pmatrix} 1 & d \\ 1 & -1 \end{pmatrix} \quad \text{where } 0, -1 \neq d \in \mathrm{GF}(q).$$

Thus

$$C_2 = C_1\psi = \begin{pmatrix} w & d \\ 1 & -w^2 \end{pmatrix} \quad \text{and} \quad C_3 = C_2\psi = \begin{pmatrix} w^2 & d \\ 1 & -w \end{pmatrix}.$$

Set $D = \left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right)$, where $\varepsilon \in \mathrm{GF}(q^2)$ such that $\varepsilon^{q-1} = -1$, and let $\varphi = \varphi'_D$ denote inversion with respect to the circle D. It is easy to check that φ induces the permutation $(C_1)(C_4)(C_2C_3)$. Hence $\varphi \in H$ and H contains a copy of S_3. Note that Lemma (1.4) implies that all three 2-cycles in our copy of S_3 are inversions.

If $q \equiv 1\ (3)$, a similar argument shows that H contains a subgroup isomorphic to S_3, and all three 2-cycles in our copy of S_3 are again inversions. This completes the proof of part (1). The proof of part (2) is much like that above, and will be left to the reader.

The only remaining possibility for a nonidentity element in H is a double transposition. Arguments similar to those above lead to the following proposition. The proof will be omitted.

PROPOSITION (3.3). *Let $q \not\equiv 0\ (3)$ be an odd prime-power. Suppose that C_1, C_2, C_3, C_4 is a nonlinear quadruple of pairwise disjoint circles in* IP(q), *and let G, H, K be defined as always. Assume that the conditions* (*) *hold for this quadruple, and assume H contains a double transposition. Then the equivalence class of this quadruple under G contains a quadruple of the following type*:

(III)
$$C_1 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} 0 & v^{q+1}/a \\ 1 & 0 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 1 & d \\ 1 & -1 \end{pmatrix}, \qquad C_4 = \begin{pmatrix} v & -v^{q+1} \\ -d & -v^q \end{pmatrix},$$

where $0 \neq a \in \mathrm{GF}(q)$; $0 \neq v \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$; $-1 \neq d \in \mathrm{GF}(q)$; $v^{q+1} \neq a^2$; *and the expressions* $\frac{1}{4}(a^2 + d^2) - \frac{1}{2}ad - a$, $\frac{1}{4}(v^{2q+2} + a^2d^2) - av^{q+1}(\frac{1}{2}d + 1)$, $v^{q+1}(-\frac{1}{2}d^2 - 2d - \frac{1}{2}) + \frac{1}{4}(d^4 + v^{2q+2})$, $-\frac{1}{2}(d^2 + v^{q+1})(v + v^q) + \frac{1}{4}(v^2 + v^{2q})$ *are all nonzero squares in* GF(q). *In this situation, the linear fractional collineation $\Psi: z \to v/z$ induces the permutation $(C_1C_2)(C_3C_4)$.*

On the other hand, any quadruple of the above type is a nonlinear quadruple of pairwise disjoint circles satisfying the conditions (*) *and having a double transposition in its permutation group H.*

REMARK. It should be noted that Proposition (3.1) implies that all 2-cycles in H are either inversions or linear fractional collineations, and Proposition (3.3) implies that all double transpositions in H are linear fractional.

At this stage, we have shown that any nonlinear quadruple of pairwise disjoint circles satisfying the conditions (*) and having nontrivial permutation group H must be in the same equivalence class under G as a quadruple of type (I), (II), or (III) above. Next, given a quadruple of type (I), (II), or (III), we would like to determine its permutation group H. The following lemmas will prove useful in that respect.

LEMMA (3.4). *Let q be an odd prime-power. Suppose that θ is a linear fractional collineation of* IP(q), *and suppose θ has order 2. Then θ must have the form*

$$\theta: z \to \frac{\alpha z + \beta}{\gamma z - \alpha} \quad \text{for all } z \text{ in } \mathrm{GF}(q^2) \cup \infty,$$

where $\alpha, \beta, \gamma \in \mathrm{GF}(q^2)$ such that $\alpha^2 + \beta\gamma \neq 0$.

PROOF. Follows immediately.

LEMMA (3.5). *Suppose C_1, C_2, C_3, C_4 is a quadruple of type* (I) *given in the notation of Proposition* (3.1). *Let ψ be the collineation inducing the permutation $(C_1C_2)(C_3)(C_4)$. Then $H = \{1, \psi\}$.*

PROOF. Recall that H is isomorphic to a subgroup of S_4, and H contains the element ψ. To simplify the notation, we will think of H as permuting the four letters 1, 2, 3, 4. For example, ψ will simply be denoted by (1 2) whenever it is convenient. It should be noted that the only subgroup of S_4 with order 12 is A_4. A_4 contains all the 3-cycles but no 2-cycles. Lemma (3.2) implies that, if H contains a 3-cycle, then H also contains a 2-cycle. Hence, H can never be equal to A_4. This is true for type (I), (II), or (III) quadruples.

The only subgroups of S_4 containing the element (1 2) are:

(i) {(1 2), (1)}, which is isomorphic to Z_2,

(ii) {(1, 2), (3 4), (1 2)(3 4), (1)}, which is isomorphic to D_2,

(iii) {(1 2), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 3 2 4), (1 4 2 3), (1)}, which is isomorphic to D_4,

(iv) {(1 2), (1 3), (2 3), (1 2 3), (1 3 2), (1)} or {(1 2), (1 4), (2 4), (1 2 4), (1 4 2), (1)}, both of which are isomorphic to S_3,

(v) S_4.

As shown in the proof of Lemma (3.2), if H contains a copy of S_3, then all three 2-cycles in that copy of S_3 are inversions. Since $\psi: z \to -z$ is not an inversion, H is not isomorphic to S_3 or S_4. Hence the only possibilities for H are (i), (ii), and (iii) above. If $H \neq \{(1\ 2), (1)\}$, then H must contain the element (3 4).

Assume, first of all, that there exists an inversion θ inducing the permutation $(C_3C_4)(C_1)(C_2)$. Then $\theta = \varphi'_C$ for some circle C. If $C = C_1$, then $C_1 \perp C_2$ since θ fixes C_2. Thus $0 = h(C_1, C_2) = 2(1 - d)$ implies that $d = 1$. Hence $C_1 = \left(\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right)$ and

$$\begin{pmatrix} x & 0 \\ 0 & -x^q \end{pmatrix} = C_4 \cong C_3\theta = \begin{pmatrix} -1-a & -1+a \\ 1-a & 1+a \end{pmatrix}.$$

This implies that $a = 1$ and therefore $a = d$, which is a contradiction to type (I). If $C = C_2$, we arrive at a similar contradiction. Therefore we may assume

C is a circle distinct from both C_1 and C_2. Hence C is orthogonal to both C_1 and C_2.

Write

$$C = \begin{pmatrix} y & b \\ c & -y^q \end{pmatrix} \quad \begin{array}{l} \text{where } y \in \mathrm{GF}(q^2);\ b, c \in \mathrm{GF}(q); \\ \text{and } y^{q+1} + bc \neq 0. \end{array}$$

Then $h(C, C_1) = 0 = h(C, C_2)$ implies that $b = -dc$ and $y(y^{q-1} + 1) = 0$. If $b = 0$, then $c = 0$ and $y^{q-1} = -1$. Thus $C_3\theta \cong C_3$, a contradiction. Hence we may assume $b \neq 0$ and therefore $c \neq 0$. If $y = 0$, then $C_4 \ncong C_3\theta$ and we arrive at another contradiction. Thus $y \neq 0$ and, in fact, $y^{q-1} = -1$. This means we may write $C \cong \left(\begin{smallmatrix} y & -d \\ 1 & y \end{smallmatrix}\right)$, and the fact that $C_4 \cong C_3\theta$ implies that $x^{q-1} = (d - a)^{q-1}y^{q-1} = y^{q-1} = -1$. But this is a contradiction to type (I). Thus, all cases being considered, there does not exist an inversion which induces the permutation $(C_3C_4)(C_1)(C_2)$.

As previously remarked, all 2-cycles in H are either inversions or linear fractional collineations. Hence suppose that θ is a linear fractional collineation inducing the permutation $(C_3C_4)(C_1)(C_2)$. By Lemma (3.4), θ: $z \to (\alpha z + \beta)/(\gamma z - \alpha)$ where $\alpha, \beta, \gamma \in \mathrm{GF}(q^2)$ such that $\alpha^2 + \beta\gamma \neq 0$. Also ψ: $z \to -z$ induces the permutation $(C_1C_2)(C_3)(C_4)$. Thus $\psi\theta$: $z \to (\alpha z - \beta)/(\gamma z + \alpha)$ induces the permutation $(C_1C_2)(C_3C_4)$. Lemma (3.4) now implies that $\alpha = 0$ and, without loss of generality, θ: $z \to \beta/z$ where $0 \neq \beta \in \mathrm{GF}(q^2)$. But $C_4 \cong C_3\theta$ now implies that $a = 0$, which is a contradiction to type (I). Therefore H does not contain the element (3 4) and $H = \{(1\ 2), (1)\}$. This completes the proof of the lemma.

The following corollary is immediate.

COROLLARY (3.6). *If H is not isomorphic to Z_2, then all 2-cycles in H must be inversions.*

Now assume that we have a quadruple of type (II), again given in the notation of Proposition (3.1). Thus H contains the element (1 2), and the only possibilities for H are (i), (ii), (iii), (iv), and (v) given in the proof of Lemma (3.5). Suppose, first of all, that (3 4) $\in H$. Corollary (3.6) now implies that $\theta = (3\ 4)$ is an inversion. Hence $\theta = \varphi'_C$ for some circle C. Arguments similar to those used in Lemma (3.5) show that C must be orthogonal to both C_1 and C_2.

Write

$$C = \begin{pmatrix} x & e \\ f & -x^q \end{pmatrix} \quad \begin{array}{l} \text{where } x \in \mathrm{GF}(q^2);\ e, f \in \mathrm{GF}(q); \\ \text{and } x^{q+1} + ef \neq 0. \end{array}$$

Then $h(C, C_1) = 0 = h(C, C_2)$ implies that $vx^q = x$ and $x(1 + v^q) = -(e + df)$. To show the above we used the facts that $v^{q+1} = 1$ and $v \neq 1$. Also $C_4 \cong C_3\theta$ implies that $x(e + af) = 0$ and $b(x^{q+1} - af^2) = ax^{q+1} - e^2$. If

$e + af = 0$, then $e = -af$ and $bx^{q+1} - abf^2 = ax^{q+1} - a^2f^2$. This implies that $\det(C) = 0$, a contradiction. Hence $e + af \neq 0$ and thus $x = 0$, $ef \neq 0$. This forces $d^2 = ab$. On the other hnd, if $d^2 = ab$, then setting $C = \left(\begin{smallmatrix} 0 & -d \\ 1 & 0 \end{smallmatrix}\right)$ and $\theta = \varphi_C'$ will yield a collineation which induces the permutation $(C_1)(C_2)(C_3C_4)$. Therefore $(3\ 4) \in H$ if and only if $d^2 = ab$.

Similar computations show that $(1\ 3) \in H$ if and only if

$$\left\{\begin{array}{c} (a+b)^2 = (d-a)(ad-b^2) \\ (a+b)(v+v^q) = (b-d)(a-d) \end{array}\right\}.$$

To interchange the roles of C_3 and C_4, we only need interchange the letters a and b. Hence $(1\ 4) \in H$ if and only if

$$\left\{\begin{array}{c} (a+b)^2 = (d-b)(bd-a^2) \\ (a+b)(v+v^q) = (a-d)(b-d) \end{array}\right\}.$$

Finally, suppose that $\theta = (1\ 3)(2\ 4) \in H$. Then the only possibilities for H are (iii) and (v). In either case, H contains the element $(3\ 4)$, and therefore $d^2 = ab$ as above. As remarked earlier, all double tranpositions in H are linear fractional collineations. By Lemma (3.4), we may write $\theta = \varphi_R$ where $R = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right)$ with $\alpha, \beta, \gamma \in \mathrm{GF}(q^2)$ such that $\alpha^2 + \beta\gamma \neq 0$.

If $\gamma = 0$, then $C_3 \cong C_1\theta$ and $C_2 \cong C_4\theta$ together imply that $v = 1$, a contradiction. Hence we may assume $\gamma \neq 0$. Recall that $\psi\colon z \to vz^q$ induces the permutation $(C_1C_2)(C_3)(C_4)$. Since $d^2 = ab$, $\eta\colon z \to -d/z^q$ induces the permutation $(C_1)(C_2)(C_3C_4)$. Thus, using the fact that $v^{q+1} = 1$, we see that $\psi\eta\colon z \to -dv/z$ induces the permutation $(C_1C_2)(C_3C_4)$. Hence

$$\psi\eta\theta\colon z \to (\beta z - dv\alpha)/(-\alpha z - dv\gamma)$$

induces the permutation $(C_1C_4)(C_2C_3)$. Lemma (3.4) now implies that $\beta = dv\gamma$ and, without loss of generality, we may write $\theta = \varphi_R$ where

$$R = \begin{pmatrix} \alpha & dv \\ 1 & -\alpha \end{pmatrix} \quad \text{with } \alpha \in \mathrm{GF}(q^2) \text{ and } \alpha^2 + dv \neq 0.$$

Using $C_1 \cong C_3\theta$ and $C_2 \cong C_4\theta$ simultaneously, some straightforward but messy algebra now shows that $(1\ 3)(2\ 4) \in H$ if and only if

$$\left\{\begin{array}{l} d^2 = ab \\ \left[v(b+d) - (a+d)\right]^2 \neq -dv(b-a)^2 \\ (b+d)^2 - (a+d)(b+d)(v+v^q) + (a+d)^2 = -d(b-a)^2 \\ a(b+d)^2(v+v^q) = (a+d)(b+d)(a+b) + d^2(b-a)^2 \end{array}\right\}.$$

We now have enough information to determine the permutation group H for

our quadruple of type (II). Rather than formally stating this result here, we will incorporate it into a later theorem.

Now assume that we have a quadruple of type (III), given in the notation of Proposition (3.3). Thus we may think of H as being a subgroup of S_4 containing the element (1 2)(3 4). As in a previous argument, $H \neq A_4$ and therefore $|H| \neq 12$. By Lemma (3.2), H is not isomorphic to Z_4. Since the only subgroups of S_4 with order 6 are copies of S_3, $|H| \neq 6$. If H contains a 2-cycle, then the equivalence class of our quadruple under G contains a quadruple of type (II), and the previous calculations will determine H (up to conjugation). Therefore we are now interested in determining H when H does not contain a 2-cycle. That is, we want to determine when the following possibilities occur:

(i)′ $\{(1\ 2)(3\ 4), (1)\}$, which is isomorphic to Z_2,

(ii)′ $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1)\}$, which is isomorphic to D_2.

Arguments similar to those given above show that:

$(1\ 2) \in H$ if and only if $d^2 = v^{q+1}$.

$(1\ 3) \in H$ if and only if

$$\left\{\begin{array}{l} (a^2 + v^{q+1})^2 = (d - a)(a^3 d - v^{2q+2}) \\ (a^2 + v^{q+1})(v + v^q) = (a - d)^2 v^{q+1} \\ d \neq a \\ a^2 + v^{q+1} \neq a(v + v^q) \end{array}\right\}.$$

$(2\ 3) \in H$ if and only if

$$\left\{\begin{array}{l} (a^2 + v^{q+1})^2 = (ad - v^{q+1})(v^{q+1} d - a^3) \\ (a^2 + v^{q+1})(v + v^q) = (v^{q+1} - ad)^2 \\ ad \neq v^{q+1} \\ a^2 + v^{q+1} \neq a(v + v^q) \end{array}\right\}.$$

$(1\ 3)(2\ 4) \in H$ if and only if

$$\left\{\begin{array}{l} (d - a)(ad - v^{q+1}) = a^2 + a(v + v^q) + v^{q+1} \\ a \neq d \\ (d - a)^2 v \neq (a + v)^2 \end{array}\right\}.$$

We now have enough information to determine the group H for our gradruple of type (III).

Suppose that we have any nonlinear quadruple of disjoint circles satisfying the conditons (*). We define the following classes, depending on the group H:

(1) H is isomorphic to Z_2, being generated by a linear fractional 2-cycle.

(2) H is isomorphic to Z_2, being generated by a 2-cycle which is an inversion.

(3) H is isomorphic to Z_2, being generated by a double transposition.

(4) H is isomorphic to D_2, containing two 2-cycles and one double transposition.

(5) H is isomorphic to D_2, containing three double transpositions.

(6) H is isomorphic to D_4, being a Sylow 2-subgroup of S_4.

(7) H is isomorphic to S_3, acting on 3 letters.

(8) H is isomorphic to S_4, acting on 4 letters.

It should be noted that two quadruples of the same equivalence class under G must have the same class as defined above. Hence it makes sense to say that the equivalence class of a quadruple under G is of class (1), etc. The following theorem has now been proved.

THEOREM (3.7). *Let $q \not\equiv 0$ (3) be an odd prime-power. Let C_1, C_2, C_3, C_4 be a nonlinear quadruple of pairwise disjoint circles in* IP(q), *and let G, H, K be defined as always. Assume that the conditions* (*) *hold for this quadruple, and assume that H is nontrivial. Then the equivalence class χ of this quadruple under G must be of class* (1), (2), (3), (4), (5), (6), (7), *or* (8) *as defined above. These classes are mutually disjoint. Moreover,*

χ is of class (1) *if and only if it contains a quadruple of type* (I) *given in the notation of Proposition* (3.1).

χ is of class (2) *if and only if it contains a quadruple of type* (II) *given in the notation of Proposition* (3.1) *and satisfying the additional conditions*:

(i) $d^2 \neq ab$,

(ii) *either* $(a + b)(v + v^q) \neq (a - d)(b - d)$ *or else both* $(a + b)^2 \neq (d - a)(ad - b^2)$ *and* $(a + b)^2 \neq (d - b)(bd - a^2)$.

χ is of class (3) *if and only if it contains a quadruple of type* (III) *given in the notation of Proposition* (3.3) *and satisfying the additional conditions*:

(i) $d^2 \neq v^{q+1}$,

(ii) *either* $(d - a)(ad - v^{q+1}) \neq a^2 + a(v + v^q) + v^{q+1}$ *or* $a = d$ *or* $(d - a)^2 v = (a + v)^2$.

χ is of class (4) *if and only if it contains a quadruple of type* (II) *given in the notation of Proposition* (3.1) *and satisfying the additional conditions*:

(i) $d^2 = ab$,

(ii) *either* $(b + d)^2 - (a + d)(b + d)(v + v^q) + (a + d)^2 \neq -d(b - a)^2$ *or* $a(b + d)^2(v + v^q) \neq (a + d)(b + d)(a + b) + d^2(b - a)^2$ *or* $[v(b + d) - (a + d)]^2 = -dv(b - a)^2$.

χ is of class (5) *if and only if it contains a quadruple of type* (III) *given in the notation of Proposition* (3.3) *and satisfying the additional conditions*:

(i) $d^2 \neq v^{q+1}$,

(ii) $a \neq d$,

(iii) $(d-a)^2v \neq (a+v)^2$,

(iv) $(d-a)(ad-v^{q+1}) = a^2 + a(v+v^q) + v^{q+1}$,

(v) *either* $(a^2+v^{q+1})^2 \neq (d-a)(a^3d - v^{2q+1})$ *or* $(a^2+v^{q+1})(v+v^q) \neq (a-d)^2v^{q+1}$ *or* $a^2+v^{q+1} = a(v+v^q)$,

(vi) *either* $(a^2+v^{q+1})^2 \neq (ad-v^{q+1})(v^{q+1}d-a^3)$ *or* $(a^2+v^{q+1})(v+v^q) \neq (v^{q+1}-ad)^2$ *or* $ad = v^{q+1}$ *or* $a^2+v^{q+1} = a(v+v^q)$.

χ *is of class* (6) *if and only if it contains a quadruple of type* (II) *given in the notation of Proposition* (3.1) *and satisfying the additional conditions*:

(i) $d^2 = ab$,

(ii) $[v(b+d) - (a+d)]^2 \neq -dv(b-a)^2$,

(iii) $(b+d)^2 - (a+d)(b+d)(v+v^q) + (a+d)^2 = -d(b-a)^2$,

(iv) $a(b+d)^2(v+v^q) = (a+d)(b+d)(a+b) + d^2(b-a)^2$,

(v) *either* $(a+b)^2 \neq (d-a)(ad-b^2)$ *or* $(a+b)(v+v^q) \neq (b-d)(a-d)$.

χ *is of class* (7) *if and only if it contains a quadruple of type* (II) *given in the notation of Proposition* (3.1) *and satisfying the additional conditions*:

(i) $d^2 \neq ab$,

(ii) $(a+b)(v+v^q) = (b-d)(a-d)$,

(iii) *either* $(a+b)^2 = (d-a)(ad-b^2)$ *or* $(a+b)^2 = (d-b)(bd-a^2)$.

χ *is of class* (8) *if and only if it contains a quadruple of type* (II) *given in the notation of Proposition* (3.1) *and satisfying the additional conditions*:

(i) $d^2 = ab$,

(ii) $(a+b)(v+v^q) = (b-d)(a-d)$,

(iii) *either* $(a+b)^2 = (d-a)(ad-b^2)$ *or* $(a+b)^2 = (d-b)(bd-a^2)$.

REMARK. It should be noted that all the above classes are nonempty already when $q = 11$, as shown in Appendix B.

4. **Nonlinear sets of 5, 6, and 7 disjoint circles.** As with four circles, we could now develop an algorithm to find all nonlinear sets of five disjoint circles satisfying the orthogonality conditions (*) and having nontrivial permutation group H. Given such a set of circles, we could explicitly determine the group H. However, in view of §3, one can imagine how messy the details would be, and we will be satisfied with listing the possibilities for H (up to isomorphism). The following lemma is proved by using the techniques of §3, and will be stated here without proof. It is very similar to Lemma (3.2).

LEMMA (4.1). *Let q be an odd prime-power such that $q \not\equiv 0$ (3) and $q \not\equiv 0$ (5). Let $C_1, \ldots, C_5$ be a nonlinear set of pairwise disjoint circles in* IP(q) *satisfying the conditions* (*). *Let H be defined as always.*

(1) *If H contains a 4-cycle, then H contains a subgroup isomorphic to D_4. In particular, H contains a 2-cycle.*

(2) *If H contains a 3-cycle, then H contains a subgroup isomorphic to S_3, and*

$q \equiv 2$ (3). *In particular, H contains a 2-cycle.*

(3) *If H contains a 5-cycle, then $q \equiv \pm 2$ (5).*

The following theorem gives the possibilities for H, up to isomorphism. Its proof is based on the above lemma, some simple counting arguments, and the Sylow theorems. This will again be left to the reader.

THEOREM (4.2). *Let q be an odd prime-power such that $q \not\equiv 0$ (3) and $q \not\equiv 0$ (5). Let $C_1, \ldots, C_5$ be a nonlinear set of pairwise disjoint circles in* IP(q) *satisfying the conditions* (*). *Let H be defined as always, and assume that H is nontrivial.*

(1) *Suppose that $q \equiv \pm 1$ (5). Then H is isomorphic to S_4, S_3, D_6, D_4, D_2, or Z_2. If $q \equiv 1$ (3) as well, then H must be isomorphic to D_4, D_2, or Z_2.*

(2) *Suppose that $q \equiv \pm 2$ (5). Then H is isomorphic to S_5, S_4, S_3, D_6, D_5, D_4, D_2, Z_5, or Z_2. If $q \equiv 1$ (3) as well, then H must be isomorphic to D_5, D_4, D_2, Z_5, or Z_2.*

Finally we consider nonlinear sets of 6 or 7 pairwise disjoint circles satisfying the conditions (*). Limiting ourselves to determining the possible orders of the permutation group H, we merely state the following two theorems. Preliminary lemmas similar to Lemma (4.1) will not be given. All the proofs consist of elementary group theoretical arguments and techniques like those used in §3.

THEOREM (4.3). *Let q be an odd prime-power such that $q \not\equiv 0$ (3) and $q \not\equiv 0$ (5). Let $C_1, \ldots, C_6$ be a nonlinear set of pairwise disjoint circles in* IP(q) *satisfying the conditions* (*). *Let H be defined as always.*

(1) *Suppose that $q \equiv \pm 2$ (5). Then $|H|$ is a divisor of 48. If $q \equiv 1$ (4) as well, then $|H|$ is a divisor of 24.*

(2) *Suppose that $q \equiv \pm 1$ (5). Then $|H| = 10, 60, 120$, or a divisor of 48. If $q \equiv 1$ (3), then $|H| \neq 120$. Once again, the divisors of 48 may be replaced by the divisors of 24 if $q \equiv 1$ (4).*

THEOREM (4.4). *Let q be an odd prime-power such that $q \not\equiv 0$ (3), $q \not\equiv 0$ (5), and $q \not\equiv 0$ (7). Let $C_1, \ldots, C_7$ be a nonlinear set of pairwise disjoint circles in* IP(q) *satisfying the conditions* (*). *Let H be defined as always.*

(1) *Suppose that $q \not\equiv -1$ (5). Then $|H|$ is a divisor of 48. If $q \equiv 1$ (4) as well, then $|H|$ is a divisor of 24.*

(2) *Suppose $q \equiv -1$ (5). Then $|H| = 10, 20, 60, 120, 240$, or a divisor of 48. If $q \equiv 1$ (4) as well, then $|H| = 10, 20, 60, 120$, or a divisor of 24.*

We could continue in an analogous manner and attempt to find the possibilities for our permutation group H when we have a nonlinear set of $n = 8, 9, 10, \ldots$ disjoint circles satisfying the conditions (*). Although this

approach seems fruitless, it should be pointed out that the possibilities for H appear to remain quite limited as the number of circles increases.

APPENDIX A. ASYMPTOTIC ESTIMATES OF QUADRUPLES NOT SATISFYING (*). Throughout this appendix, q denotes an odd prime-power. We want to approximate for large q the number of quadruples of pairwise disjoint circles in IP(q) which do not satisfy the orthogonality conditions (*) given in Theorem (2.2). In particular, we want to find upper bounds for these asymptotic estimates.

The following theorem (see [5, Theorem 2]) will be used throughout Appendix A, and will be stated here without proof.

THEOREM (A.1). *Let q be an odd prime-power. Then*

(i) *the number of triples of disjoint circles in* IP(q) *is asymptotic to* $q^9/48$, *and*

(ii) *the number of quadruples of disjoint circles in* IP(q) *is asymptotic to* $q^{12}/1536$.

We now show practically all quadruples (for large q) have no linear subtriples. It was pointed out in [5] that almost all quadruples are nonlinear. A nonlinear quadruple can have one linear subtriple or no linear subtriples. As in [1, Theorem 7.5 and §8], the number of linear triples in IP(q) is asymptotic to $q^7/12$. In [5, Corollary to Theorem 1] it was pointed out that the number of circles disjoint from each member of a given triple of disjoint circles in IP(q) is asymptotic to $q^3/8$. Hence, once a linear triple has been chosen, the number of choices for the fourth circle of our quadruple is asymptotic to $q^3/8$. Thus the number of nonlinear quadruples with one linear subtriple is asymptotic to $q^{10}/96$. Since the number of nonlinear quadruples is asymptotic to $q^{12}/1536$ by Theorem (A.1)(ii), practically all (nonlinear) quadruples have no linear subtriples. Therefore we will assume throughout this appendix that all subtriples are nonlinear.

Now suppose that we have a quadruple which does not satisfy condition (ii) of (*). That is, one circle in our quadruple is orthogonal to the other three circles. According to Theorem (A.1)(i), the number of (nonlinear) triples of disjoint circles in IP(q) is asymptotic to $q^9/48$. Once a nonlinear triple has been chosen, the common orthogonal circle is uniquely determined by Theorem (1.6). This common orthogonal circle may or may not be disjoint from the given three circles.

Since we are seeking an upper bound for the number of quadruples not satisfying (ii), we assume the worst possible situation and suppose that this common orthogonal circle is disjoint from the given three circles most of the time. Then the number of quadruples of disjoint circles in IP(q) not satisfying (ii) is asymptotic to at most $q^9/48$. Since the number of quadruples of disjoint

circles in IP(q) is asymptotic to $q^{12}/1536$, we see that for large q practically all quadruples satisfy condition (ii).

Finally, suppose that we have a quadruple which does not satisfy condition (i) of (*). That is, there exists a common orthogonal circle D to our quadruple. Once three of the circles have been chosen, D is uniquely determined by Theorem (1.6) and the fourth circle must be orthogonal to D. As shown in [4], there are q^2 circles orthogonal to any given circle in IP(q). Thus there are q^2 distinct circles orthogonal to D, and these circles may or may not be disjoint from the chosen three. Assume the worst possible situation once again, and suppose that most of these circles are disjoint from the three chosen circles. Since the number of nonlinear triples is asymptotic to $q^9/48$, we obtain approximately $q^{11}/48$ (not necessarily distinct) quadruples with a common orthogonal circle. Since each of these quadruples is counted $\binom{4}{3} = 4$ times, the number of distinct quadruples of disjoint circles in IP(q) not satisfying condition (i) is asymptotic to at most $q^{11}/192$. Since the number of quadruples in IP(q) is asymptotic to $q^{12}/1536$, we see that for large q most quadruples satisfy condition (i).

Therefore, for large q, most quadruples of pairwise disjoint circles in IP(q) do indeed satisfy the orthogonality conditions (*).

APPENDIX B. EXAMPLES OF QUADRUPLES FOR $q = 11$. As stated in §3, there exist examples of nonlinear quadruples of pairwise disjoint circles in IP(11) satisfying the conditions (*) and having class (1), (2), (3), (4), (5), (6), (7), (8) as given in Theorem (3.7). We will give eight examples in this appendix, one for each class. Note that $q = 11$ throughout this appendix. Recall the definitions of type (I), (II), and (III) quadruples given in §3. Also let i designate an element of GF(121) with $|i| = 4$.

EXAMPLE (B.1). Let

$$C_1 = \begin{pmatrix} 1 & -3 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} -1 & -3 \\ 1 & 1 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} i+1 & 0 \\ 0 & 1 \end{pmatrix}.$$

It is easy to check that this is a quadruple of type (I), and hence is of class (1).

EXAMPLE (B.2). Let

$$C_1 = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} -3+5i & 2 \\ 1 & 3+5i \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & -3 \\ 1 & 0 \end{pmatrix}.$$

It is easy to check that this is a quadruple of type (II) and, according to Theorem (3.7), is of class (2).

EXAMPLE (B.3). Let

$$C_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad C_4 = \begin{pmatrix} i+1 & -2 \\ 0 & i-1 \end{pmatrix}.$$

This quadruple is of type (III) and, according to Theorem (3.7), is of class (3).

EXAMPLE (B.4). Let

$$C_1 = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} -3+5i & 2 \\ 1 & 3+5i \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & -3 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}.$$

This quadruple is of type (II) and, according to Theorem (3.7), is of class (4).

EXAMPLE (B.5). Let

$$C_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 4i & -5 \\ 0 & 4i \end{pmatrix}.$$

This quadruple is of type (III) and, according to Theorem (3.7), is of class (5).

EXAMPLE (B.6). Let

$$C_1 = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 3+5i & 2 \\ 1 & -3+5i \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & -3 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}.$$

This quadruple is of type (II) and, according to Theorem (3.7), is of class (6).

EXAMPLE (B.7). Let

$$C_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 3+5i & 1 \\ 1 & -3+5i \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}.$$

This quadruple is of type (II) and, according to Theorem (3.7), is of class (7).

EXAMPLE (B.8). Let

$$C_1 = \begin{pmatrix} 1 & 4 \\ 1 & -1 \end{pmatrix}, \quad C_2 = \begin{pmatrix} -3+5i & 4 \\ 1 & 3+5i \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix}.$$

This quadruple is of type (II) and, according to Theorem (3.7), is of class (8).

BIBLIOGRAPHY

1. R. H. Bruck, *Construction problems of finite projective planes*, Combinatorial Mathematics and Its Applications, Univ. North Carolina Press, Chapel Hill, N. C., 1969, pp. 426–514. MR **40** #3422.

2. _____, *Construction problems in finite projective spaces*, Finite Geometric Structures and Their Applications, Edizioni Cremonese, Rome, 1973, pp. 107–188. MR **49** #7159.

3. P. Dembowski, *Möbiusebenen gerader Ordnung*, Math. Ann. **157** (1964), 179–205. MR **31** #1607.

4. P. Dembowski and D. R. Hughes, *On finite inversive planes*, J. London Math. Soc. **40** (1965), 171–182. MR **30** #2382.

5. G. L. Ebert, *Translation planes of order q^2: asymptotic estimates*, Trans. Amer. Math. Soc. (submitted).

6. H. Lüneburg, *Die Suzukigruppen und ihre Geometrien*, Lecture Notes in Math., no. 10, Springer-Verlag, Berlin and New York, 1965. MR **34** #7634.

7. W. F. Orr, *The miquelian inversive plane* IP(q) *and the associated projective planes*, Dissertation, Univ. of Wisconsin, Madison, Wis., 1973.

8. B. L. Van der Waerden and L. J. Smid, *Eine Axiomatik der Kreisgeometrie und der Laguerre-geometrie*, Math. Ann. **110** (1935), 753–776.

DEPARTMENT OF MATHEMATICS, TEXAS TECH UNIVERSITY, LUBBOCK, TEXAS 79409

Current address: Department of Mathematics, University of Delaware, Newark, Delaware 19711