

A note on the Dembowski-Prohaska conjecture for finite inversive planes

GÜNTER F. STEINKE

*School of Mathematics and Statistics
University of Canterbury
Private Bag 4800, Christchurch 8140
New Zealand
Gunter.Steinke@canterbury.ac.nz*

Abstract

Peter Dembowski, at the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications at the University of North Carolina in 1970, announced a result by his student Olaf Prohaska that a finite inversive plane of prime power order q is miquelian if and only if its automorphism group contains a subgroup isomorphic to $\text{PSL}(2, q)$ which leaves a circle invariant and acts faithfully on it. No proof was subsequently published by either Prohaska or Dembowski.

We prove the Dembowski-Prohaska conjecture in case of inversive planes of even order and take some steps towards the odd order case. In particular we show that the action on the point set is equivalent to the standard action of $\text{PSL}(2, q)$ in the corresponding miquelian inversive plane of order q and that circles that touch the fixed circle are as in the miquelian plane.

1 Introduction

Inversive planes, also known as Möbius planes, are incidence geometries with points and circles, see Section 2 for a definition. They have their origins in the geometry of circles on a 2-sphere. In case of finitely many points these planes can simply be described as $3 - (n^2 + 1, n + 1, 1)$ designs. Finite inversive planes have been investigated from many different perspectives: geometric, algebraic, combinatorial, and through their automorphism groups.

Peter Dembowski announced at the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications at the University of North Carolina in 1970 a result by his student Olaf Prohaska that a finite inversive plane of prime power order q is miquelian if and only if its automorphism group contains a subgroup isomorphic to $\text{PSL}(2, q)$ which leaves a circle invariant and acts faithfully on it. He

commented that such a “group can act in only one way on the plane, that the plane can be reconstructed within the group, and that this reconstruction is the same as that for the miquelian inversive plane of the same order q ”. Unfortunately, neither Prohaska nor Dembowski subsequently published a proof. We therefore refer to the claim as the *Dembowski-Prohaska conjecture*.

The strategy for a proof outlined by Dembowski has been employed successfully in other characterizations of classical geometries, for example, that an automorphism group isomorphic to $\text{PSL}(2, q^2)$ on an inversive plane of order q characterizes the miquelian plane or that the Suzuki group $\text{Sz}(q)$ characterizes the inversive planes over Suzuki-Tits ovoids; see [18, Satz 1 and 2]. It normally requires some kind of transitivity properties.

In Section 2 we recall the basic definitions of inversive planes and some results on finite inversive planes and central automorphisms of such planes. In the last section we investigate finite inversive planes that admit a group Σ of automorphisms isomorphic to $\text{PSL}(2, q)$ which leaves a circle invariant. We show that the assumption on the faithfulness of the action in the Dembowski-Prohaska conjecture can be removed, collect some results on Sylow subgroups in the general finite case, and then prove the Dembowski-Prohaska conjecture in case of even order. In the odd order case we take some steps towards a proof and show that the action of Σ on the point set is equivalent to the standard action of $\text{PSL}(2, q)$ in the corresponding miquelian inversive plane of the same order. This confirms Dembowski’s claim about the group action in the outline of his strategy to prove the conjecture, but reconstructing the geometry within the group proves difficult. As a partial result in this direction we further obtain that circles that touch the distinguished circle stabilized by $\text{PSL}(2, q)$ are as in the miquelian inversive plane of order q . However, a description of other circles remains elusive, and the Dembowski-Prohaska conjecture remains open so far in the odd order case.

2 Inversive planes and their automorphisms

An *inversive plane* or *Möbius plane* $\mathcal{I} = (P, \mathcal{C})$ is an incidence structure consisting of a point set P and a circle set \mathcal{C} , elements of which are non-empty subsets of P . Furthermore, the following three axioms are satisfied, compare [4] or [1, Abschnitt III.2.2]:

- Joining: three mutually distinct points can be joined by a unique circle.
- Touching: the circles which touch a fixed circle K at $p \in K$ partition $P \setminus \{p\}$ where a circle L touches K at p if and only if $L = K$ or $K \cap L = \{p\}$.
- Richness: there is a circle that contains at least three points and there are at least two circles.

It readily follows that for each point p of \mathcal{I} the incidence structure $\mathcal{A}_p = (A_p, \mathcal{L}_p)$ whose point set is $A_p = P \setminus \{p\}$ and whose line set \mathcal{L}_p consists of all circles of \mathcal{I}

passing through p but without p is an affine plane, called the *derived affine plane at p* . This affine plane extends to a projective plane \mathcal{P}_p , which we call the *derived projective plane at p* . The axioms of an inversive plane are equivalent to each internal incidence structure being an affine plane. Furthermore, a circle not passing through the distinguished point p induces an oval in \mathcal{A}_p (or in \mathcal{P}_p such that the ideal line is exterior). An inversive plane can thus be described in one derived affine plane \mathcal{A} by the lines of \mathcal{A} and a collection of ovals. This planar description of an inversive plane, which is the most commonly used, is then extended by one point which is adjoined to all the lines of the affine plane.

The *miquelian inversive plane* is obtained as the geometry of non-trivial plane sections of an elliptic quadric in 3-dimensional projective space over some field \mathbb{F} . The derived affine planes of the miquelian inversive planes are desarguesian and the ovals are conics that are obtained from a given conic via dilatations. Geometrically, the miquelian inversive planes can be characterized by Miquel's theorem, cf. [1].

Another description of this model is as follows. Let \mathbb{E} be a quadratic extension of \mathbb{F} . The point set is $\overline{\mathbb{E}}$ where $\overline{\mathbb{E}} = \mathbb{E} \cup \{\infty\}$ and ∞ is an element not contained in \mathbb{E} . ($\overline{\mathbb{E}}$ can be identified with the projective line over \mathbb{E} .) Each circle is the image of $\overline{\mathbb{F}} = \mathbb{F} \cup \{\infty\}$ under a fractional linear map $x \mapsto \frac{ax+b}{cx+d}$ in $\text{PGL}(2, \mathbb{E})$.

Generalizing the notion of an elliptic quadric, one defines an *ovoid* to be a subset of points of a 3-dimensional projective space such that no line has more than two points in common with it and such that the collection of all tangents at a point fills a plane, called the *tangent plane* at that point. Then the model for the miquelian inversive plane can be generalized to an *ovoidal* (or *egglike*) *inversive plane* where one takes an ovoid instead of an elliptic quadric as point set. These ovoidal inversive planes obviously comprise the miquelian planes.

The spatial description of an ovoidal inversive plane as the geometry of plane sections of an ovoid is related to the planar description in one derived affine plane by stereographic projection from one point of the ovoid onto a plane not passing through the point of projection. In this description all points of the inversive plane except the point of projection are covered.

A finite inversive plane \mathcal{I} is one which has only a finite number of points. In this case the order of \mathcal{I} is the order of any of its derived affine (or projective) planes. If \mathcal{I} has order n , then each circle has $n + 1$ points and \mathcal{I} has $n^2 + 1$ points altogether. Furthermore, the plane has $n(n^2 + 1)$ circles. In this case the axiom of touching follows from the axiom of joining. The finite inversive planes of order n are precisely the $3 - (n^2 + 1, n + 1, 1)$ designs (or Steiner systems $S(3, n + 1, n^2 + 1)$).

There are many models of inversive planes, see for example, [11] for planes with point set the 2-sphere $\mathbb{S}^2 = \overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, the projective line over the complex numbers \mathbb{C} . However, all known finite inversive planes are ovoidal. There is only one family of finite non-miquelian inversive planes known. These planes are over Tits ovoids $\mathcal{O}_T(q)$ where $q = 2^{2h+1}$, $h \geq 1$. The ovoid $\mathcal{O}_T(q)$ can be described in $\text{PG}(3, q)$ as the collection of the ideal point of the z -axis and all affine points $(x, y, xy + x^2\sigma(x) + \sigma(y))$ where $x, y \in \text{GF}(q)$, the Galois field of order q , and σ is the unique automorphism of $\text{GF}(q)$ such that $\sigma^2(x) = x^2$ for all $x \in \text{GF}(q)$. We denote

the corresponding inversive plane by $\mathcal{I}(\mathcal{O}_T(q))$.

The following result on finite inversive planes, due to Dembowski [4] for even order and Thas [25] for odd order, shows that many of the principles of construction of infinite inversive planes do not apply for finite planes, and thus that one can expect the number of models of finite inversive planes of a given order to be very limited.

Theorem 2.1 *A finite inversive plane of even order is ovoidal. A finite inversive plane of odd order is miquelian if at least one of its derived affine planes is desarguesian.*

Theorem 2.1 combined with the classification of ovoids in 3-dimensional projective spaces of small orders and of finite projective planes of small orders and their ovals can be used to obtain the following result; see [3], [8], [9], [24, Theorem C], [12], [22, Corollary 2.4], [23, Corollary 4.3].

Theorem 2.2 *A finite inversive plane of order at most 7 or order 9 or 16 is miquelian. There is no finite inversive plane of order 6 or 10. Up to isomorphism there are precisely two inversive planes of order 8 and precisely two inversive planes of order 32.*

An *automorphism* of an inversive plane is a permutation of the point set such that circles are mapped to circles. The collection of all automorphisms of an inversive plane $\mathcal{I} = (P, \mathcal{C})$ forms a group with respect to composition, the automorphism group $\text{Aut}(\mathcal{I})$ of \mathcal{I} . The automorphism group of the miquelian inversive plane of order q is isomorphic to $\text{P}\Gamma\text{L}_2(q^2)$, see [6, 6.4.1], and the automorphism group of the ovoidal inversive plane $\mathcal{I}(\mathcal{O}_T(q))$ over a Tits ovoid $\mathcal{O}_T(q)$ is isomorphic to the semidirect product of the Suzuki group $Sz(q)$ and the automorphism group of $\text{GF}(q)$, see [6, 6.4.4]. Clearly, every collineation of 3-dimensional projective space that leaves an ovoid \mathcal{O} invariant induces an automorphism of the ovoidal inversive plane $\mathcal{I}(\mathcal{O})$ obtained from \mathcal{O} . Conversely, one has the following.

Theorem 2.3 (H. Mäurer [21, Folgerung 4.3.2]) *Each automorphism of an ovoidal inversive plane $\mathcal{I}(\mathcal{O})$ is induced by a collineation of the ambient 3-dimensional projective space that leaves the ovoid \mathcal{O} invariant.*

A *central automorphism* of an inversive plane is an automorphism that fixes at least one point and induces a central collineation in the derived projective plane at each of its fixed points.

Hering [14] studied two types of central automorphisms in inversive planes. These are automorphisms that fix precisely one or two points (except the identity) and that induce a translation or homothety, respectively, in the derived affine plane at each of these fixed points. In fact, in his classification Hering considered groups of automorphisms and determined their types according to transitive subgroups of central automorphisms contained in them.

The first kind of central automorphisms investigated by Hering are translations of \mathcal{I} . They have exactly one fixed point except for the identity. More precisely, let C

be a circle passing through p and let $\mathcal{B}(p, C)$ denote the *touching pencil with carrier* p , that is, $\mathcal{B}(p, C)$ consists of all circles that touch the circle C at the point p . In the derived affine plane at p the touching pencil represents a parallel class of lines and one can consider translations in this direction. Then a $\mathcal{B}(p, C)$ -translation of \mathcal{I} is an automorphism of \mathcal{I} that is either the identity or fixes precisely the point p and each circle in $\mathcal{B}(p, C)$ globally. A group of $\mathcal{B}(p, C)$ -translations of \mathcal{I} is called $\mathcal{B}(p, C)$ -transitive if it acts transitively on $C \setminus \{p\}$.

The second kind of central automorphisms considered by Hering fix precisely two points except for the identity. Let p and p' be two distinct points of an inversive plane \mathcal{I} . A $\{p, p'\}$ -homothety of \mathcal{I} is an automorphism of \mathcal{I} that is either the identity or fixes precisely the points p and p' and induces a homothety with centre p' in the derived affine plane \mathcal{A}_p at p . (Then we also obtain a homothety with centre p in the derived affine plane $\mathcal{A}_{p'}$ at p' .) So a $\{p, p'\}$ -homothety fixes every circle in the bundle $\mathcal{B}(p, p')$ of circles through p and p' . A group of $\{p, p'\}$ -homotheties is called $\{p, p'\}$ -transitive if it acts transitively on each circle through p and p' minus the two points p and p' .

We say that a group Γ of automorphisms of \mathcal{I} is $\mathcal{B}(p, C)$ -transitive or $\{p, p'\}$ -transitive if Γ contains a $\mathcal{B}(p, C)$ -transitive subgroup of $\mathcal{B}(p, C)$ -translations or a $\{p, p'\}$ -transitive subgroup of $\{p, p'\}$ -homotheties, respectively. Let $\mathcal{H} = \mathcal{H}(\Gamma)$ be the collection of all touching pencils $\mathcal{B}(p, C)$, $p \in C$ for which Γ is $\mathcal{B}(p, C)$ -transitive and let $\mathcal{K} = \mathcal{K}(\Gamma)$ be the collection of all unordered pairs $\{p, p'\}$ of points for which Γ is $\{p, p'\}$ -transitive.

Hering determined the feasible configurations for \mathcal{H} and \mathcal{K} . Possible types with respect to transitive sets of $\mathcal{B}(p, C)$ -translations are denoted by Roman numerals I to VII. If the inversive plane under consideration is not the finite (miquelian) inversive plane of order 2 all possible configurations of \mathcal{K} given the type $X \in \{\text{I, II, } \dots, \text{VII}\}$ with respect to $\mathcal{B}(p, C)$ -translations were determined, and type X is further distinguished by Arabic numerals which indicate types with respect to $\{p, p'\}$ -homotheties. In type $X.1$ one always has $\mathcal{K} = \emptyset$. This leads to 18 different possible types $X.y$ of groups of automorphisms of inversive planes; see [14], [6, 6.1.14] or [13, Theorem 2.I] for a full list of all 18 types. We only mention three Hering types explicitly.

I.1 $\mathcal{H} = \emptyset$, $\mathcal{K} = \emptyset$;

VI.1 For every point p of \mathcal{I} there is exactly one touching pencil with carrier p that is in \mathcal{H} and $\mathcal{K} = \emptyset$.

VII.2 \mathcal{H} contains all touching pencils in \mathcal{I} and \mathcal{K} contains all unordered pairs of points in \mathcal{I} .

We say that an inversive plane \mathcal{I} is of Hering type $X.y$ if the full automorphism group of \mathcal{I} is of Hering type $X.y$. The miquelian inversive planes are precisely the planes of type VII.2; compare [6, 6.4.12] for finite planes. The only known Hering types of finite inversive planes are VI.1 and VII.2. Indeed, the ovoidal inversive planes over Tits ovoids have type VI.1; compare [6, 6.4.4]. In fact, these last two

types and possibly I.1 are the only Hering types that can occur for finite inversive planes of even order.

Theorem 2.4 (D. Glynn [13]) *A finite ovoidal inversive plane is miquelian, an ovoidal inversive plane $\mathcal{I}(\mathcal{O}_T)$ over a Tits ovoid \mathcal{O}_T or of Hering type I.1.*

Some of the types described by Hering are known to be empty or to occur only in finite inversive planes or of proper subgroups of the (full) automorphism groups of miquelian inversive planes, see [6, Table II on page 262 and 6.4.15, 17, 18] and the survey [17] by Krier.

We lastly mention very special central automorphisms of an inversive plane \mathcal{I} . An *inversion at a circle C* of \mathcal{I} is an automorphism of \mathcal{I} that fixes precisely the points of C . In the derived projective plane at a point p of C an inversion at C induces a central collineation with axis the line L_C induced by C . We therefore also call C the axis of the inversion. For example, in the miquelian inversive plane described via a separable quadratic extension \mathbb{E} of \mathbb{F} conjugation $\kappa : z \mapsto \bar{z}$ is an inversion. Dembowski [4, (5.3) and Zusatz 5] showed the following, see also [20, Lemmas 25.3 and 25.4].

Proposition 2.5 *Each inversion at a circle C in an inversive plane \mathcal{I} is an involution. Moreover, \mathcal{I} admits at most one inversion at C .*

A finite inversive plane is miquelian if and only if every circle is the axis of an inversion, see [6, 6.4.9] or [5, Satz 5.5]. In this case an inversion at a circle C comes from a reflection in ambient projective space $\text{PG}(3, q)$ about the plane that determines C such that the quadric that is the point set of the miquelian plane is left invariant. On the other hand the ovoidal inversive plane $\mathcal{I}(\mathcal{O}_T(q))$ over a Tits ovoid $\mathcal{O}_T(q)$ admits no inversion, see [6, 6.4.5]. (The Suzuki group $Sz(q)$ is transitive on the circles of $\mathcal{I}(\mathcal{O}_T(q))$; see [18, Corollary 1] or [20, Lemma 26.3].)

Conversely, one has a complete geometric description of involutions in finite inversive planes, see [6, 6.3.4] or [5, Satz 2.3].

Proposition 2.6 *An involution in a finite inversive plane \mathcal{I} of order n is an inversion, a homothety, a translation or fixed-point-free. Moreover, in case of a translation n must be even and in case of a homothety or fixed-point-free involution n must be odd.*

3 The Dembowski-Prohaska conjecture for finite inversive planes

In [7, 3.3] Dembowski made the following claim.

Conjecture 3.1 (Dembowski-Prohaska, [7]) *A finite inversive plane of prime power order q is miquelian if and only if its automorphism group contains a subgroup isomorphic to $\text{PSL}(2, q)$ which leaves a circle invariant and acts faithfully on it.*

Clearly, each miquelian inversive plane admits such a group of automorphisms. Throughout this section we use the following notation:

- \mathcal{I} denotes a finite inversive plane of prime power order $q = r^h$ where r is a prime.
- Σ is a subgroup of the automorphism group of \mathcal{I} such that Σ is isomorphic to $\text{PSL}(2, q)$ and leaves a circle C of \mathcal{I} invariant.

We prove the above conjecture in case of even order. We only partially follow the strategy outlined by Dembowski. As a first step we make a straightforward observation that shows that the assumption on the faithfulness of the action on the circle is unnecessary.

Lemma 3.2 *Σ acts faithfully and transitively on C . Moreover, the action of Σ on C is equivalent to the standard action of $\text{PSL}(2, q)$ on the projective line $\text{PG}(1, q)$.*

Proof. The group $\text{PSL}(2, q)$ is simple when $q \geq 4$, see for example [16, Hauptsatz II.6.15]. Hence Σ acts either trivially or faithfully on C . Assume the former. A Sylow 2-subgroup S of Σ is elementary abelian of order q when q is even or a Klein 4-group or a dihedral group when q is odd. In either case S contains at least three distinct involutions. Each involution fixes C pointwise and thus is an inversion with axis C . However, there can be only one inversion with axis C by Proposition 2.5. This shows that Σ acts faithfully on C .

When $q = 2$ or 3 , then \mathcal{I} is miquelian, and $\text{PSL}(2, q)$ is isomorphic to the symmetric group S_3 and the alternating group A_4 , respectively. The stabilizer of a circle in the miquelian plane in these cases is $\text{P}\Gamma\text{L}(2, q) = \text{PGL}(2, q)$, which is isomorphic to S_3 and S_4 , respectively. Hence the stabilizer of a circle contains a unique subgroup that is isomorphic to $\text{PSL}(2, q)$. Furthermore, this subgroup acts in the standard way on the circle. We conclude that Σ acts faithfully and transitively on C in these two cases.

Since $\text{PSL}(2, q)$ does not have a proper subgroup of index $\leq q$ if $q > 11$ (see [10, Theorem 262] or [16, Hauptsatz II.8.27]), we see that Σ must act transitively on C . Hence the action of Σ on C is equivalent to the action of Σ on the cosets of a stabilizer Σ_x . But Σ_x is conjugate to the affine group $\text{L}(2, q)$. Thus the action of Σ on C is equivalent to the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q)$.

In case $q < 11$ the inversive plane is miquelian. This follows from Theorem 2.2 when $q \neq 8$ without any further assumptions. When $q = 8$ there are two inversive planes of that order. The non-miquelian inversive plane of order 8 is ovoidal over a Tits-Suzuki ovoid. Its automorphism group is isomorphic to the semidirect product of the Suzuki group $Sz(8)$ and a cyclic group of order 3, and thus has order $87360 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ (see [6, 6.4.4]). Therefore the automorphism group cannot contain $\text{PSL}(2, 8)$ as a subgroup, which has order $504 = 2^3 \cdot 3^2 \cdot 7$.

The miquelian inversive plane of order q has automorphism group isomorphic to $\text{P}\Gamma\text{L}(2, q^2)$; see [6, 6.4.1]. The stabilizer of a circle is $\text{P}\Gamma\text{L}(2, q)$. When $q \in \{4, 5, 7\}$

the group Σ has index 2 in $\text{P}\Gamma\text{L}(2, q)$; when $q = 8, 9$ then Σ has index 3 and 4, respectively. By the second isomorphism theorem for groups $\Sigma \cap \text{PSL}(2, q)$ has index at most 4 in Σ . Hence Σ coincides with the standard $\text{PSL}(2, q)$ in $\text{P}\Gamma\text{L}(2, q)$ by the simplicity of Σ . In particular, Σ is transitive on C and the action of Σ on C is equivalent to the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q)$.

In the remaining case when $q = 11$ the group $\text{PSL}(2, 11)$ has a proper subgroup of index 11 and thus a transitive permutation representation on 11 points; compare [16, Satz II.8.28]. Such a subgroup of index 11 is isomorphic to A_5 . So assume that Σ fixes a point $x \in C$ and acts transitively on $C \setminus \{x\}$. Let $y \in C$, $y \neq x$. Then Σ_y can neither be transitive on nor fix a point in $C \setminus \{x, y\}$. Indeed, in each of these two cases the stabilizer of a point in $C \setminus \{x, y\}$ contains an involution which must be an inversion with axis C by Proposition 2.6, a contradiction to the faithful action of Σ on C . One concludes that Σ_y has two orbits of length 5 on $C \setminus \{x, y\}$. If S is a Sylow 2-subgroup of Σ_y , then S fixes a point in each orbit so that every $\sigma \in S$ fixes at least four points on C . However, $S \setminus \{\text{id}\}$ consists of three involutions, which then must all be inversions with axis C , a contradiction to Proposition 2.5. This shows that Σ acts transitively on C , and equivalence to the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q)$ follows as before. \square

Lemma 3.3 *Let Δ be a Sylow r -subgroup of Σ , and let $\delta \in \Delta \setminus \{\text{id}\}$. Then δ fixes a point p on C and p is the only fixed point of δ .*

Proof. By Lemma 3.2 we know that Σ acts faithfully on C and that the action of Σ on C is equivalent to the standard action of $\text{PSL}(2, q)$ on the projective line $\text{PG}(1, q)$. In particular, Δ fixes precisely one point p on C and acts regularly on $C \setminus \{p\}$.

Assume that δ fixes a second point $p' \neq p$. Then $p' \notin C$. Since the bundle of circles through p and p' contains $q + 1$ circles, we see that δ fixes a circle D through p and p' . Now $C \cap D$ is fixed by δ so that $C \cap D = \{p\}$, that is, C and D are tangent at p .

In case of q being odd we consider the derived projective plane $\mathcal{P}_{p'}$ at p' . The circle D induces a line L_D in $\mathcal{P}_{p'}$, and the circle C appears as an oval \mathcal{O}_C in $\mathcal{P}_{p'}$. As seen above, L_D is a tangent to \mathcal{O}_C at p . Since q is odd, there is a unique second tangent $\neq L_D$ to \mathcal{O}_C through the ideal point of L_D . But \mathcal{O}_C has no ideal points, so the second tangent touches \mathcal{O}_C in an affine point $x \neq p$. Hence $x \in C$ is also fixed by δ , a contradiction to the regularity of Δ on $C \setminus \{p\}$.

If $q > 2$ is even, then δ is an involution. The circle D has $q + 1$ points and two fixed points p and p' of δ on it. Hence δ fixes at least one other point $p'' \in D$, $p'' \neq p, p'$, and must be the unique inversion with axis D . In fact, because Δ is abelian, Δ leaves D invariant.

Let $x \in C \setminus \{p\}$ and $\Phi = \Sigma_{p,x}$ the stabilizer of p and x . Then Φ has order $q - 1$. Furthermore, in $\text{PSL}(2, q)$ we see that $\{\phi\delta\phi^{-1} \mid \phi \in \Phi\} = \Delta \setminus \{\text{id}\}$. But $\phi\delta\phi^{-1}$ is an inversion with axis $\phi(D)$. However, if $\delta_1, \delta_2 \in \Delta \setminus \{\text{id}\}$ are distinct, then $\delta_1\delta_2 \in \Delta \setminus \{\text{id}\}$ and $\delta_1\delta_2$ is a translation by [5, Satz 4.2.(a)], see also [6, 6.3.12.(a)], and we have a contradiction. (Alternately, Δ is a 2-group all whose elements of order 2

are inversions. By [6, 63.13] such a group is cyclic or a generalized quaternion group. However, Δ is elementary abelian of order $q > 2$, a contradiction.)

When $q = 2$, the plane \mathcal{I} is miquelian and the statement follows.

This shows that δ has a unique fixed point in any case. □

Lemma 3.4 *Each involution in Σ is a homothety in case q is odd and a translation in case q is even.*

Proof. We first assume that $r = 2$ so that \mathcal{I} has even order. Let $\delta \in \Delta \setminus \{\text{id}\}$ and let $x \neq p$ be a point where p is the unique fixed point of Δ , compare Lemma 3.3. Then $\delta(x) \neq x$ and there is a unique circle C_x through the three points $p, x, \delta(x)$. Clearly, C_x is fixed by δ . Furthermore, two distinct of these circles can only intersect in p . Hence these circles are exactly the circles in the touching pencil $\mathcal{B}(p, C)$. Thus δ is a $\mathcal{B}(p, C)$ -translation.

We now assume that q is odd. All involutions in $\text{PSL}(2, q)$ are conjugate to each other, and, in particular, conjugate to

$$\sigma : x \mapsto -\frac{1}{x}.$$

Let $a \in \text{GF}(q)$ such that $-a^2 - 1$ is a square in $\text{GF}(q)$. Such an a exists. When $q \equiv 1 \pmod{4}$, then -1 is a square in $\text{GF}(q)$, and we can choose $a = 0$. In case $q \equiv -1 \pmod{4}$ we know that -1 is a non-square in $\text{GF}(q)$, and there must be an $a \in \text{GF}(r)$ such that $a^2 + 1$ is a non-square in $\text{GF}(q)$. (Otherwise each of $1, 2, \dots, r - 1$ is a non-zero square — a contradiction as $r - 1 = -1$ in $\text{GF}(q)$.)

For such an a as above let

$$\sigma_a : a \mapsto \frac{ax + 1}{x - a}.$$

Then $\sigma_a \in \text{PSL}(2, q)$ is an involution that commutes with σ . Now consider the automorphisms $\tilde{\sigma}, \tilde{\sigma}_a \in \Sigma$ that induce σ and σ_a on C , respectively. By Proposition 2.6 each involution of \mathcal{I} is an inversion, a homothety or fixed-point-free (as q is odd).

Assume that there is an involution in $\text{PSL}(2, q)$ that extends to an inversion of \mathcal{I} . Then every involution in Σ is an inversion. In particular this is true for σ and σ_a from above. Since these two inversions commute, their composition $\tilde{\sigma}_a \circ \tilde{\sigma}$ is an involution and a homothety of \mathcal{I} by [6, 6.3.12] or [5, Satz 4.2], a contradiction to our assumption that all involutions are inversions.

Finally assume that there is a fixed-point-free involution in Σ . Then every involution in Σ is fixed-point-free. We now consider the Klein 4-group V generated by $\tilde{\sigma}$ and $\tilde{\sigma}_a$. This group has order 4 and acts on the point set P of \mathcal{I} . However, $|P| = q^2 + 1 \equiv 2 \pmod{4}$ is not divisible by 4. Thus there must be a point p that has an orbit of length 1 or 2. In either case there is an involution in V that fixes p , a contradiction to our assumption that all involutions are fixed-point-free. □

Corollary 3.5 *If q is even then Σ is $\mathcal{B}(p, C)$ -transitive for each point $p \in C$.*

Proof. Let $p \in C$ and let $\Delta \leq \Sigma_p$ be a Sylow 2-subgroup of Σ . By Lemma 3.4 we know that each $\delta \in \Delta$ is a $\mathcal{B}(p, C)$ -translation. Since $|\Delta| = |C \setminus \{p\}| = q$, we conclude that Δ (and thus Σ) is $\mathcal{B}(p, C)$ -transitive. \square

We are now ready to prove the Dembowski-Prohaska conjecture for finite inversive planes of even order.

Theorem 3.6 *Let \mathcal{I} be a finite inversive plane of order $q = 2^h$ and assume that the automorphism group of \mathcal{I} contains a subgroup isomorphic to $\text{PSL}(2, q)$ which leaves a circle invariant. Then \mathcal{I} is miquelian.*

Proof. Since finite inversive planes of order ≤ 7 are miquelian by Theorem 2.2, we may assume that $q \geq 8$. Let $\Sigma \cong \text{PSL}(2, q)$ be a group of automorphisms of \mathcal{I} that leaves the circle C invariant. By Lemma 3.2 we know that Σ acts faithfully on C .

By Corollary 3.5 the inversive plane \mathcal{I} is $\mathcal{B}(p, C)$ -transitive for each $p \in C$. Hence the Hering type of \mathcal{I} is not I.1. Thus, by Glynn's theorem, Theorem 2.4, the plane is miquelian or ovoidal over a Tits ovoid $\mathcal{O}_T(q)$. However, the automorphism group of an ovoidal inversive plane $\mathcal{I}(\mathcal{O}_T(q))$ is the semi-direct product of the Suzuki group $Sz(q)$ by the cyclic automorphism group of the field $\text{GF}(q)$ and thus has order $hq^2(q^2 + 1)(q - 1)$. This order is not divisible by $q(q + 1)(q - 1)$ and so the automorphism group of $\mathcal{I}(\mathcal{O}_T(q))$ does not contain $\text{PSL}(2, q)$ as a subgroup. This finally proves that \mathcal{I} must be miquelian. \square

Remark 3.7 An alternative route for a proof of Theorem 3.6 was suggested by the referee. It is based on a characterization of elliptic quadrics among ovoids in 3-dimensional projective space of even order by Matthew Brown [2]: An ovoid of $\text{PG}(3, q)$, $q = 2^h$, is an elliptic quadric if and only if some secant plane section is a conic.

Since the order q of \mathcal{I} is even, the inversive plane is ovoidal over some ovoid \mathcal{O} in 3-dimensional projective space $\text{PG}(3, q)$ over $\text{GF}(q)$. If, as before, $\Sigma \cong \text{PSL}(2, q) = \text{SL}(2, q)$ is a group of automorphisms of $\mathcal{I} = \mathcal{I}(\mathcal{O})$ that leaves the circle C invariant, then Σ is induced by a group Σ' of collineations of $\text{PG}(3, q)$ by Mäurer's result, Theorem 2.3. Now Σ' fixes C and thus the plane \mathcal{E}_C whose intersection with \mathcal{O} is C . By the determination of the possible actions of $\text{SL}(2, q)$ on a desarguesian projective plane of order q in [19, Korollar 1], see also [6, 1.4.51], one obtains that C is a conic in \mathcal{E}_C . Hence the above characterization by M. Brown yields that \mathcal{O} is an elliptic quadric. Thus $\mathcal{I}(\mathcal{O})$ is miquelian. \square

The Dembowski-Prohaska conjecture for finite inversive planes could be verified above in case of even order because one has so much more information about inversive planes of even order than inversive planes of odd order. If one wants to follow the strategy originally outlined by Dembowski to prove the conjecture in odd order, it seems the first steps are to verify that automorphisms in a Sylow r -subgroup

are translations of the inversive plane and that the action of Σ on the point set is equivalent to the corresponding action in the the miquelian plane of order q . We take these steps in the following.

Theorem 3.8 *Let Σ be a subgroup of the automorphism group of a finite inversive plane \mathcal{I} of order $q = r^h$ where r is an odd prime. Assume that Σ is isomorphic to $\text{PSL}(2, q)$ and fixes a circle C .*

Then Σ is transitive on $P \setminus C$. Moreover, the action of Σ on P is equivalent to the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q^2)$ (as a subgroup of $\text{PSL}(2, q^2)$).

Proof. Let $p \in P \setminus C$. By Lemma 3.3 no automorphism in Σ_p can have order divisible by r . Hence the order of Σ_p is a divisor of $\frac{1}{2}(q^2 - 1)$. On the other hand, the orbit $\Sigma(p)$ of p has length at most $|P \setminus C| = q(q - 1)$ so that $|\Sigma_p| \geq \frac{q+1}{2}$. From the list of subgroups of $\text{PSL}(2, q)$, see [10, 260] or [16, Hauptsatz II.8.27], we obtain that Σ_p is cyclic, a dihedral group or isomorphic to an alternating group A_4 or A_5 or a symmetric group S_4 .

We first show that Σ_p cannot contain a Klein 4-group V as a subgroup. Assume to the contrary that it does. In this case Σ_p contains three distinct commuting involutions $\sigma_1, \sigma_2, \sigma_3 \in V$. Each σ_i is a homothety by Lemma 3.4. Hence each σ_i fixes precisely a second point $p_i \neq p$ of the inversive plane. But the σ_i commute so that $p_1 = p_2 = p_3 = p'$. This shows that V fixes p and p' , and these two points are the only fixed points of V . Furthermore, V fixes every circle through p and p' .

Pick $x \in C$. The circle C_x through p, p' and x is fixed by V and must meet C in another point $x' \neq x$, otherwise x is fixed by V . But then $\{x, x'\}$ is invariant under V . Since V has order 4, there must be a $\sigma_i \in V$ that fixes x , a contradiction to σ_i being a non-trivial homothety with centres p and p' . This proves our claim that V cannot be contained in Σ_p . Thus Σ_p cannot be isomorphic to A_4, S_4 or A_5 , or be a dihedral group of order divisible by 4.

Assume that Σ_p is a dihedral group whose order is not divisible by 4. Then Σ_p is generated by involutions. Again by Lemma 3.4 these involutions are homotheties. So in the derived projective plane \mathcal{P}_p at p we have central collineations with axis the ideal line W (with respect to the derived affine plane \mathcal{A}_p at p). But then each collineation $\tilde{\sigma}$ of \mathcal{P}_p that is induced by $\sigma \in \Sigma_p$ also has W as an axis. The circle C induces an oval \mathcal{O} in \mathcal{P}_p . Let $x \in \mathcal{O}$ and let T_x be the tangent to \mathcal{O} at x . Since q is odd, there is a tangent $T'_x \neq T_x$ to \mathcal{O} that passes through the ideal point $w_x \in W$ on T_x . This second tangent touches \mathcal{O} in an affine point $x' \neq x$. A collineation $\tilde{\sigma}$ where $\sigma \in \Sigma_p$ fixes w_x and thus $\{x, x'\}$. By assumption there is a $\sigma \in \Sigma_p$ of odd order. Then $\tilde{\sigma}$ fixes x . Since $x \in C$ was arbitrary, this implies that σ acts trivially on C , a contradiction to the faithfulness of Σ on C .

This shows that Σ_p is cyclic. From the list of subgroups of $\text{PSL}(2, q)$ and because q is odd one sees that $\frac{q+1}{2}$ is the maximum order a cyclic subgroup can have. Hence Σ_p has order $\frac{q+1}{2}$ and Σ is transitive on $P \setminus C$.

Any two cyclic subgroups of order $\frac{q+1}{2}$ are conjugate in $\text{PSL}(2, q)$. In the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q^2)$ (as a subgroup of $\text{PSL}(2, q^2)$) one sees that one can

identify Σ_p with the stabilizer of a point in $\text{PG}(1, q^2) \setminus \text{PG}(1, q)$. Hence the statement of the action of Σ follows. \square

Theorem 3.9 *Let Σ be a subgroup of the automorphism group of finite inversive plane \mathcal{I} of prime power order $q = r^h$. Assume that Σ is isomorphic to $\text{PSL}(2, q)$ and fixes a circle C . Let Δ be a Sylow r -subgroup of Σ and let $p \in C$ be the unique fixed point of Δ .*

Then Δ consists of $\mathcal{B}(p, C)$ -translations. Hence Σ is $\mathcal{B}(p, C)$ -transitive for each $p \in C$.

Proof. In the case $r = 2$ the statement of the theorem has been established in Corollary 3.5.

We now assume that q is odd. Let $p' \in C \setminus \{p\}$ and let $\Phi = \Sigma_{p,p'}$ be the stabilizer of p and p' . Then Φ has order $n = \frac{q-1}{2}$.

We first show that Φ has precisely three orbits in $\mathcal{B}(p, C)$, namely $\{C\}$ and two orbits \mathcal{O}_1 and \mathcal{O}_2 , each of length n . Assume otherwise. Then there is a circle $C' \neq C$ in $\mathcal{B}(p, C)$ and a $\phi \in \Phi \setminus \{\text{id}\}$ that fixes C' . We consider the derived projective plane $\mathcal{P}_{p'}$ at p' . The line L_C in $\mathcal{P}_{p'}$ induced by C is a tangent to the oval \mathcal{O}' in $\mathcal{P}_{p'}$ induced by the circle C' (the point of tangency being p). Since q is odd, there is a unique second tangent $\neq L_C$ to \mathcal{O}' through the ideal point of L_C . This second tangent touches \mathcal{O}' in an affine point $x \neq p$. Hence $x \in C'$ is also fixed by ϕ , a contradiction to Theorem 3.8 because in the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q^2)$ no element other than the identity fixes more than two points.

Δ acts on $\mathcal{B}(p, C)$ and because it is an r -group and already fixes C must fix a second circle $C_1 \in \mathcal{B}(p, C) \setminus \{C\}$. Without loss of generality we may assume that $C_1 \in \mathcal{O}_1$. But Φ normalizes Δ so that Δ fixes each circle in \mathcal{O}_1 , the orbit of C_1 under Φ . It follows that Δ leaves \mathcal{O}_2 invariant. Again, because r does not divide n , we obtain that Δ fixes a circle $C_2 \in \mathcal{O}_2$. As before we see that Δ fixes each circle in \mathcal{O}_2 , the orbit of C_2 under Φ .

This shows that Δ acts trivially on $\mathcal{B}(p, C)$ and thus consists of $\mathcal{B}(p, C)$ -translations. But then Δ and thus Σ is $\mathcal{B}(p, C)$ -transitive. \square

Corollary 3.10 *Circles that touch C are as in the miquelian inversive plane of order q .*

Proof. From Theorem 3.8 we know that the action of Σ on P is equivalent to the standard action of $\text{PSL}(2, q)$ on $\text{PG}(1, q^2)$ as a subgroup of $\text{PSL}(2, q^2)$. Circles that touch C are apart from the point of tangency in C orbits of Sylow r -subgroups by Theorem 3.9. Hence, in suitable coordinates, they can be described as in the miquelian inversive plane of order q . \square

Remark 3.11 (a) There are a number of cases apart from Corollary 3.5 where one can directly show (that is, without the use of Theorem 3.8) that a Sylow

r -subgroup Δ of Σ that fixes $p \in C$ consists of $\mathcal{B}(p, C)$ -translations, namely when $r = 3$, $h = 1$, or $q \equiv 1 \pmod{4}$.

Indeed, when $r = 3$ one considers the circles C_x through $x, \delta(x), \delta^2(x)$ where $\delta \in \Delta \setminus \{\text{id}\}$. Such a circle is left invariant by δ because δ has order 3. Moreover, δ has a fixed point on C_x , which must be the point p by Lemma 3.3. Two distinct of these circles can only intersect in p . Hence these circles are exactly the circles in the touching pencil $\mathcal{B}(p, C)$ and δ is a $\mathcal{B}(p, C)$ -translation.

In case $h = 1$ the group Δ is cyclic of prime order r . This group fixes p and C and thus leaves the touching pencil $\mathcal{B}(p, C)$ invariant. Since $\mathcal{B}(p, C)$ contains exactly r circles with at least one of them fixed, one sees that $\mathcal{B}(p, C)$ is fixed elementwise by Δ .

Lastly, when $q \equiv 1 \pmod{4}$ then -1 is a square in $\text{GF}(q)$. All involutions in $\text{PSL}(2, q)$ are conjugate to each other, and each has precisely two fixed points on C . By Lemma 3.4 every automorphism $\tilde{\sigma}$ of \mathcal{I} that induces an involution $\sigma \in \text{PSL}(2, q)$ on C is a homothety with centres on C . Specifically, one considers the following involutions of $\text{PSL}(2, q)$:

$$\sigma_t : x \mapsto t - x$$

where $t \in \text{GF}(q)$. Then $\tilde{\sigma}_t$ is a homothety of \mathcal{I} that fixes the point $\infty \in C$. Clearly, $\tau_t = \sigma_t \circ \sigma_0$ is the map $x \mapsto x + t$ on $\text{GF}(q) \cup \{\infty\}$, and $\{\tau_t \mid t \in \text{GF}(q)\}$ is a Sylow r -subgroup of $\text{PSL}(2, q)$. In the derived projective plane \mathcal{P}_∞ we have three collineations σ'_0, σ'_t and τ'_t . Since σ'_0 and σ'_t are involutory homotheties with centres on the line L_C induced by C , their composition τ'_t is a translation with centre the ideal point of L_C , see [15, Lemma 4.21]. But then $\tilde{\tau}_t$ is a translation in \mathcal{I} .

- (b) The orders not covered in (a) are $q = r^h$ where $r \equiv 3 \pmod{4}$, $r \geq 7$ and $h \geq 3$ is odd. Involutions in these cases behave quite differently. They are homotheties that are fixed-point-free on C . Furthermore, the sets of centres of all involutions in Σ form a partition of $P \setminus C$. Therefore the method of proof from the case $q \equiv 1 \pmod{4}$ is not applicable.
- (c) In each of the cases from (a) the Sylow r -group Δ is $\mathcal{B}(p, C)$ -transitive. The transitivity of Σ on C then implies that Σ is $\mathcal{B}(x, C)$ -transitive for each $x \in C$. Thus Σ acts transitively on $P \setminus C$ by [6, 6.3.14] or [14, Hilfssatz 2.6].
- (d) Once transitivity on $P \setminus C$ is established as in (c), the stabilizer of a point $p \notin C$ has order $\frac{q+1}{2}$ and thus is cyclic, a dihedral group or isomorphic to A_4 when $q = 23$ or S_4 when $q = 47$. So only A_5 is directly eliminated this way.

Although the action of Σ on the point set is as in the miquelian plane of the same order q this does not give us enough information to determine the circles of \mathcal{I} , except for those circles that touch C . By Theorem 2.1 it will suffice in case of odd order q that every circle in the bundle $\mathcal{B}(p_1, p_2)$ of circles through p_1 and p_2 on C is as in the miquelian plane of order q , that is, in this case one does not have to determine

the circles that do not meet C . If $C' \neq C$ belongs to $\mathcal{B}(p_1, p_2)$, then the stabilizer $\Sigma_{C'}$ of C' is contained in the stabilizer $\Sigma_{\{p_1, p_2\}}$ of $C' \cap C = \{p_1, p_2\}$. The latter is a dihedral group of order $q - 1$ and any two such groups are conjugate in Σ .

The first problem then is to geometrically identify $\Sigma_{C'}$ within $\Sigma_{\{p_1, p_2\}}$. There may even be different stabilizers for different C' 's in $\mathcal{B}(p_1, p_2)$. The second problem one faces is that $\Sigma_{\{p_1, p_2\}}$ does not act trivially on $\mathcal{B}(p_1, p_2)$ (not in the miquelian plane anyway) and so there are circles $C' \neq C$ in $\mathcal{B}(p_1, p_2)$ such that $C' \setminus C$ is not an orbit under the stabilizer $\Sigma_{C'}$. So different orbits need to be glued together to obtain the circle C' .

In summary, there are several problems to overcome before the Dembowski-Prohaska conjecture can be proved in case of odd order and the conjecture in these cases remains open for now.

References

- [1] W. Benz, *Vorlesungen über Geometrie der Algebren*, Springer, Berlin, 1973.
- [2] M. R. Brown, Ovoids of $\text{PG}(3, q)$, q even, with a conic section, *J. London Math. Soc.* (2) **62** (2000), 569–582.
- [3] Y. Chen, The Steiner system $S(3, 6, 26)$, *J. Geom.* **2** (1972), 7–28.
- [4] P. Dembowski, Möbiusebenen gerader Ordnung, *Math. Ann.* **157** (1964), 179–205.
- [5] P. Dembowski, Automorphismen endlicher Möbius-Ebenen, *Math. Z.* **87** (1965), 115–136.
- [6] P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.
- [7] P. Dembowski, Finite planes with prescribed groups, Proc. Second Chapel Hill Conf. on Combinatorial Mathematics and its Applications, Univ. North Carolina, 1970, pp. 114–125, 1970.
- [8] R. H. F. Denniston, Uniqueness of the inversive plane of order 5, *Manuscr. Math.* **8** (1973), 11–19.
- [9] R. H. F. Denniston, Uniqueness of the inversive plane of order 7, *Manuscr. Math.* **8** (1973), 21–26.
- [10] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications, Inc., New York, 1958, xvi+312 pp.
- [11] G. Ewald, Aus konvexen Kurven bestehende Möbiusebenen, *Abh. Math. Sem. Univ. Hamburg* **30** (1967), 179–187.

- [12] G. Fellegara, Gli ovaloidi di uno spazio tridimensionale di Galois di ordine 8, *Atti Acad. Naz. Lincei Rend.* **32** (1962), 170–176.
- [13] D.G. Glynn, The Hering classification for inversive planes of even order, *Simon Stevin* **58** (1984), no. 4, 319–353.
- [14] C.H. Hering, Eine Klassifikation der Möbius-Ebenen, *Math. Z.* **87** (1965), 252–262.
- [15] D.R. Hughes and F.C. Piper, *Projective Planes*, Springer, New York, 1973.
- [16] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, vol. 134, Springer, Berlin, 1967.
- [17] N. Krier, The Hering classification of Möbius planes, Proc. Int. Conf. Projective Planes (Washington State Univ., Pullman, Wash., 1973), pp. 157–163, Washington State Univ. Press, Pullman, Wash., 1973.
- [18] H. Lüneburg, Finite Möbius planes admitting a Zassenhaus group as group of automorphisms, *Ill. J. Math.* **8** (1964), 586–592.
- [19] H. Lüneburg, Charakterisierungen der endlichen desarguesschen projektiven Ebenen, *Math. Z.* **85** (1964), 419–450.
- [20] H. Lüneburg, *Translation planes*, Springer-Verlag, Berlin-New York, 1980.
- [21] H. Mäurer, Möbius- und Laguerre-Geometrien über schwach konvexen Semi-flächen, *Math. Z.* **98** (1967), 355–386.
- [22] C.M. O’Keefe and T. Penttila, Ovoids of PG(3,16) are elliptic quadrics, *J. Geom.* **38** (1990), 95–106.
- [23] C.M. O’Keefe, T. Penttila and G.F. Royle, Classification of ovoids of PG(3,32), *J. Geom.* **50** (1994), 143–150.
- [24] G.F. Steinke, A remark on Benz planes of order 9, *Ars Comb.* **34** (1992), 257–267.
- [25] J.A. Thas, The affine plane AG(2, q), q odd, has a unique one point extension, *Invent. Math.* **118** (1994), 133–139.

(Received 29 Sep 2020; revised 26 Jan 2021)