Inherited conics in Hall planes

Aart Blokhuis[a], István Kovács[b,c,1], Gábor P. Nagy[d,e,2,3], Tamás Szőnyi[f,g,c,3]

[a]*Department of Mathematics and Computer Science, Eindhoven University of Technology, Den Dolech 2, Eindhoven, The Netherlands*
[b]*UP IAM, University of Primorska, Muzejski trg 2, 6000, Koper, Slovenia*
[c]*UP FAMNIT, University of Primorska, Glagoljaška 8, 6000, Koper, Slovenia*
[d]*Department of Algebra, Budapest University of Technology, H-1111, Budapest, Egri József utca 1, Hungary*
[e]*Bolyai Institute, University of Szeged, H-6720 Szeged, Aradi vértanúk tere 1, Hungary*
[f]*Department of Computer Science, Eötvös Loránd University, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary*
[g]*MTA-ELTE Geometric and Algebraic Combinatorics Research Group, H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary*

Abstract

The existence of ovals and hyperovals is an old question in the theory of non-Desarguesian planes. The aim of this paper is to describe when a conic of $\mathrm{PG}(2,q)$ remains an arc in the Hall plane obtained by derivation. Some combinatorial properties of the inherited conics are obtained also in those cases when it is not an arc. The key ingredient of the proof is an old lemma by Segre-Korchmáros on Desargues configurations with perspective triangles inscribed in a conic.

1. Introduction

An *arc* in a projective plane is a set of points no three of which are collinear. An old theorem of Bose says that an arc can have at most $q+2$ points if q is even, and at most $q+1$ points if q is odd. An arc having k points is also called a k-arc. A k-arc is said to be *complete* if it is not contained in a $(k+1)$-arc. $(q+1)$-arcs are called *ovals*, $(q+2)$-arcs are called *hyperovals*. It is also known that ovals in planes of even order are contained in a (unique) hyperoval. Arcs and ovals are among the most studied objects in finite geometry. A motivating question was the existence of ovals in any (not necessarily Desarguesian) plane. Several results are known for arcs in the Desarguesian plane $\mathrm{PG}(2,q)$, here we just mention some of them.

Email addresses: a.blokhuis@tue.nl (Aart Blokhuis), istvan.kovacs@upr.si (István Kovács), nagyg@math.u-szeged.hu (Gábor P. Nagy), szonyi@cs.elte.hu (Tamás Szőnyi)

[1]Partially supported by the Slovenian Research Agency (research program P1-0285 and research projects N1-0038, N1-0062, J1-6720 and J1-7051).

[2]Partially supported by OTKA grant 119687.

[3]Partially supported by the OTKA-ARRS Slovenian-Hungarian Joint Research Project, grant no. NN 114614 (in Hungary) and N1-0032 (in Slovenia).

Theorem 1.1 (Segre, [14]). *If K is a complete k-arc in* $\mathrm{PG}(2,q)$*, then* $k = q+2$ *or* $k \leq q - \sqrt{q} + 1$ *if q is even, and* $k = q+1$*, in which case K is a conic, or* $k \leq q - \frac{1}{4}\sqrt{q} + \frac{7}{4}$ *if q is odd.*

For a survey of results on arcs and blocking sets we refer to the book by Hirschfeld [4]. Relatively few results are known for (complete) arcs in non-Desarguesian planes. In particular, no embeddability results similar to Segre's theorems are known. Instead of giving a full list of the results we just refer to an old survey paper by the fourth author [16] and pick some characteristic results about arcs. Of course, the focus was on non-Desarguesian planes which are close to Galois planes. This means that most results are about arcs of Hall planes, André planes and their duals (Moulton planes). In the early years, researchers wanted to find ovals and hyperovals in non-Desarguesian planes. There are such examples by Rosati, Bartocci, Korchmáros [16, Theorem 3.1]. An early important result about complete arcs is due to Menichetti: there are complete q-arcs in Hall planes of even order (≥ 16) [10]. A similar but easier result is due to Szőnyi: there are complete $(q-1)$-arcs in Hall planes of odd order [16, Theorem 4.6]. A natural idea is to start with an oval (or a conic) of the Desarguesian plane and study the combinatorial properties of these sets in the non-Desarguesian plane (obtained from the Desarguesian one by replacing some of the lines).

In this paper, we shall systematically study inherited conics in Hall planes. In the next section some fundamental results used in the proofs are collected. Then we discuss old and new results about different types of conics: parabolas, hyperbolas, and ellipses and decide whether they yield inherited arcs or not. Some cases were completely known before, some were not. The precise results are stated in the corresponding sections.

We should remark that Barwick and Marshall [1] found a necessary and sufficient condition in terms of the equation of the conic guaranteeing that it remains an arc in the Hall plane. The disadvantage of the result is that the condition is not easy to check explicitly.

Throughout the paper *conic* will stand for *irreducible conic.*

2. The Hall plane

In this section, the Hall planes are described briefly by using derivation and also by giving the lines explicitly.

Consider the Desarguesian projective plane $\mathrm{PG}(2,q^2)$, let ℓ be a line and let D be a Baer subline of ℓ. So $D \cong \mathrm{PG}(1,q) \subset \mathrm{PG}(1,q^2) = \ell$. We call $\ell = \ell_\infty$ the line at infinity. The points of the affine Hall plane $\mathrm{Hall}(q^2)$ are the points of $\mathrm{PG}(2,q^2) \setminus \ell_\infty$. Lines whose infinite point does not belong to D remain the same ('old lines'). Instead of lines intersecting ℓ_∞ in a point of D we consider all Baer subplanes containing D. The affine part of these Baer subplanes are the 'new lines'. It is not difficult to show that this incidence structure is an affine plane (and the translations of the Desarguesian affine plane are translations in the Hall plane). The projective Hall plane is the projective closure of this affine plane.

For the sake of completeness, we describe the affine Hall plane $\mathrm{Hall}(q^2)$ explicitly. Points are the pairs (x, y), where $x, y \in \mathrm{GF}(q^2)$. Old lines have equation $Y = mX + b$, where $m \notin \mathrm{GF}(q)$. New lines are $\{(a + \lambda u, b + \lambda v) : u, v \in \mathrm{GF}(q)\}$, where a, b, λ are fixed elements of $\mathrm{GF}(q^2)$. Note that the same Baer subplane is obtained for several a, b, λ. In this case we have the *standard derivation set*, 'the usual $\mathrm{PG}(1, q)$':

$$D = \{(m) \mid m \in \mathrm{GF}(q) \cup \{\infty\}\} = \{(x : y : 0) \mid x, y \in \mathrm{GF}(q)\}.$$

3. Useful facts about conics

Let us begin with the following result by Segre and Korchmáros [15, page 617] which plays a crucial role in our proof.

Theorem 3.1 (Segre-Korchmáros). *(a) Let K be a conic of $\mathrm{PG}(2, q)$, q even, and r be a line which is not a tangent of K. For every triple $\{P_1, P_2, P_3\} \subset r \setminus K$ there exists one and only one triangle $\{A_1, A_2, A_3\}$ inscribed in $K \setminus r$ such that $A_iA_j \cap r = P_k$, where i, j, k is a permutation of $1, 2, 3$.*

(b) Let K be a conic of $\mathrm{PG}(2, q)$, q odd, and r be a line which is not a tangent of K. For every triple $\{P_1, P_2, P_3\} \subset r \setminus K$ there exist at most two triangles $\{A_1, A_2, A_3\}$ inscribed in $K \setminus r$ such that $A_iA_j \cap r = P_k$, where i, j, k is a permutation of $1, 2, 3$. Moreover, if r is a tangent to K then there is one and only one such triangle inscribed in $K \setminus r$.

Actually, one can say even more for q odd, by using an observation of Korchmáros [7, Teorema 1]. Sometimes this observation is called the axiom of Pasch for external/internal points.

Proposition 3.2. *Let K be a conic and r be a line of $\mathrm{PG}(2, q)$, q odd. If r is not a tangent and $\{P_1, P_2, P_3\}$ contains either three or exactly one external point then there are exactly two triangles $\{A_1, A_2, A_3\}$ inscribed in $K \setminus r$ such that $A_iA_j \cap r = P_k$, where i, j, k is a permutation of $1, 2, 3$. In the other cases, for example, when the three points are internal, there is no $\{A_1, A_2, A_3\}$ with this property.*

The next result is useful when we wish to determine the intersection of a conic and a Baer subplane.

Proposition 3.3. *Let K be a conic in $B = \mathrm{PG}(2, q)$, a Baer subplane of $\mathrm{PG}(2, q^2)$. Let r be line in B. Extend K and r to K' and r' in the larger plane by using the same equation. Then if r is a tangent, then so is r', otherwise r' is a secant of K'. In other words K' is a parabola if the original conic K was a parabola, where r and r' are the line at infinity, and it is a hyperbola if it is not.*

The difference in extending a hyperbola and an ellipse is that the infinite points in $\mathrm{PG}(2, q^2)$ belong to the Baer subplane or not. This observation can be used to determine the intersection of a Baer subplane and a conic. The only thing one needs is that five points determine a conic uniquely.

Corollary 3.4. *Let B be a Baer subplane and K a conic in $\mathrm{PG}(2, q^2)$. Then either $|B \cap K| \leq 4$ or $B \cap K$ is a conic of B.*

4. Consequences for the number of collinear points

Let $D = \{(m) \mid m \in \mathrm{GF}(q) \cup \{\infty\}\} = \{(x : y : 0) \mid x, y \in \mathrm{GF}(q)\}$ be the standard derivation set we used to define the Hall plane in Section 2. In this section we look at the case that the line at infinity, ℓ_∞ is not a tangent.

We first consider the case that q is even (and at least 4).

Proposition 4.1. *If K is a hyperbola either having two points in D, or two conjugate points outside D, then K is defined over a subplane (containing D), hence in the Hall plane it has $q-1$ or $q+1$ collinear points, and the remaining lines of the Hall plane intersect K in at most two points.*

Proof. Let P_1, P_2, and P_3 be any three points on ℓ_∞, and A_1, A_2 and A_3 be the affine points on K described in Theorem 3.1. Notice that, $\{P_1, P_2, P_3\} \subseteq D$ iff all points A_i belong to a subplane containing D. In particular, we can fix three affine points of K contained in a subplane containing D, and they together with the two points at infinity determine a conic (and this is of course K), whose homogeneous part of degree 2, which is determined by the infinite points, can be given coefficients from $\mathrm{GF}(q)$ and therefore, K intersects this subplane in a subconic. If the two infinite points belong to D, then we find $q-1$ collinear points, if they are conjugate, we find $q+1$ collinear points in the Hall plane. □

Theorem 4.2. *For q even the following hold.*

(a) If K is a hyperbola having two non-conjugate points on $\ell_\infty \setminus D$, or if K is an ellipse, then every line of the Hall plane intersects the affine part of K in at most 4 points and the number of collinear triples is $\binom{q+1}{3}$.

(b) If K is a hyperbola having one point in D, then every line of the Hall plane intersects the affine part of K in at most 3 points and the number of collinear triples is $\binom{q}{3}$.

Proof. By Corollary 3.4 the lines intersect K in at most 4 points, and if K has a point in D then at most 3, since in this case K does not intersect a Baer subplane containing D in a conic. If K has one point in D, then from the remaining q points we get $\binom{q}{3}$ triples, and by Theorem 3.1 the same number of triples in the intersection of K with a subplane containing D, otherwise K has no points in D and we find $\binom{q+1}{3}$ such triples. □

Next we consider the case that q is odd. In this case we have the following possibilities:

(1) All points of $D \setminus K$ are internal. Now we get from Proposition 3.2 that there are no collinear triples, so we get an inherited arc.

(2) D contains $s > 0$ external points. In this case we have roughly, but definitely at least $\binom{s}{3} + s\binom{q-1-s}{2}$ collinear triples, so certainly K does not give rise to an arc.

In the next section we will investigate the possible values of s.

5. External points in the derivation set

We consider the case that q is odd and want to determine the number of external/internal points of the conic in the derivation set.

The line at infinity is the line with equation $Z = 0$. D is the standard derivation set defined above. The conic K is given by $Q(X, Y, Z) = X^2 + aXY + bY^2 + ZL(X, Y, Z) = 0$, or just by $X^2 + aXY + bY^2 + L(X, Y)$, where of course $L(X, Y) = L(X, Y, 1)$. Note that K is an ellipse if $f = X^2 + aXY + bY^2$ is irreducible over $\mathrm{GF}(q^2)$, a parabola if f is a square, and a hyperbola if f factors into different linear factors. For convenience we take L so that the point $(1 : 0 : 0)$ is external, and now the infinite point $(u) := (1 : u : 0)$ is external/internal when $1 + au + bu^2 = \square$ or $\not\square$.

Remark: it is an exercise to show that if P_1 and P_2 are two (external) points on the same tangent, then either $Q(P_i)$ is a square for both points, or a non-square. As a consequence $Q(P)$ either is a square for all external points P, or a non-square. This is essentially Theorem 8.17 in [4].

To count the number of external/internal points in D, we therefore have to find the number of (affine) rational points (so $u, w \in \mathrm{GF}(q)$) on the curve $\mathcal{C}$ with equation

$$(1 + au + bu^2)(1 + \bar{a}u + \bar{b}u^2) - w^2 = p(u) - w^2 = 0.$$

This curve is absolutely irreducible unless the polynomial p is a square. One possibility for this is that $1 + au + bu^2$ is a square, in which case the conic is a parabola. The line at infinity is a tangent in this case, so we have:

Proposition 5.1. *If K is a parabola then all points in D different from the infinite point of K are external.*

The other possibility if p is a square, is that $1 + au + bu^2 = 1 + \bar{a}u + \bar{b}u^2$ and now $a, b \in \mathrm{GF}(q)$, so $1 + au + bu^2$ factors over $\mathrm{GF}(q^2)$. In this case the conic has two points at infinity so we have a hyperbola, and we have:

Proposition 5.2. *If K is a hyperbola and either both infinite points belong to D, or they are conjugates, (m) and $(\bar{m})$, both outside D, then either all (other) points of D are external, or all are internal.*

If p is not a square, then we first take care of the case that p has a repeated factor. If $1 + au + bu^2 = (1 - \alpha u)(1 - \beta u)$, then $1 + \bar{a}u + \bar{b}u^2 = (1 - \bar{\alpha}u)(1 - \bar{\beta}u)$

and if now $\alpha = \bar{\beta}$ then $\beta = \bar{\alpha}$, so p is a square, and we are back in the case of a hyperbola with conjugate infinite points, while if $\alpha = \bar{\alpha}$ but $\beta \neq \bar{\beta}$ then, K has one point in D, namely $(\alpha : 1 : 0)$ and one outside D namely $(\beta : 1 : 0)$, and we now look for the number of points on the curve

$$(1 + \alpha u)^2 (1 + \beta u)(1 + \bar{\beta} u) - w^2,$$

and this is essentially a conic, possibly with some points at infinity.

Proposition 5.3. *If K is a hyperbola with exactly one infinite point in D, then D contains $(q+1)/2$ external and $(q-1)/2$ internal points, or the other way around, depending on the quadratic character of $\beta\bar{\beta}$ in* GF(q).

So in the case of an ellipse, or a hyperbola with two non-conjugate points outside D we have no repeated factor, and now by [5, Example 5.59], $\mathcal{C}$ has genus $g = 1$. Let R_q denote the number of points $P \in \mathcal{C}$ that lie in PG$(2, q)$. On the one hand, [5, Theorem 9.57(i)] implies

$$|R_q - (q + 1)| \leq 2\sqrt{q} + 2.$$

On the other hand, $\mathcal{C}$ has a unique point at infinity and all GF(q)-rational affine points $\mathcal{C}$ have the form $(u, \pm w)$ with $w \neq 0$. That is, for $(R_q - 1)/2$ values $u \in$ GF(q), $p(u)$ is a square. We get:

Proposition 5.4. *If K is an ellipse, or a hyperbola with two non-conjugate infinite points outside D, then the number of internal (external) points on D is at least $q/2 - 1 - \sqrt{q}$ (at most $q/2 + 1 + \sqrt{q}$).*

6. Inherited parabolas

The complete solution to the problem of inherited parabolas was given in a sequence of papers. The story began with the results of Korchmáros [8, Theorem 1 and 2].

Theorem 6.1. *Let K be a parabola in* PG$(2, q)$ *where q is odd. If K is an arc in a translation plane having the same translation group as the Desarguesian plane, then the plane must be the Desarguesian one. For q even, there is a parabola which remains an arc in the Hall plane obtained by derivation.*

In the case q odd more information is given about parabolas as subsets of the Hall plane in the paper [17]. Namely, it is shown that they are sets having an internal nucleus set that is much larger than a subset of the Desarguesian plane can have ($P \in S$ is an *internal nucleus* if every line through P contains at most one other point of S [19]). This happens in the case when the infinite point of the parabola belongs to the derivation set.

If the infinite point of K is not in D, then we can use Theorem 3.1, which gives that for any $\{P_1, P_2, P_3\} \subseteq D$ there are $A_1, A_2, A_3 \in K$ that are collinear in Hall(q^2). By Proposition 3.3 and Corollary 3.4 it also follows that every new line intersects K in at most 4 points.

Lemma 6.2. *Let q be odd, and let K be a parabola whose infinite point does not belong to D. Then every line of* $\mathrm{Hall}(q^2)$ *meets K in at most four points.*

Proof. Consider a new line of the affine Hall plane $\mathrm{Hall}(q^2)$. This Baer subplane cannot meet K in a subconic, because the infinite point of K does not belong to D. Five points in a Baer subplane determine a subconic, hence the Baer subplane can meet K in at most four points. □

Moreover the number of collinear triples is $\binom{q+1}{3}$. Counting collinear triples in the Hall plane we get $a_3 + 4a_4 = \binom{q+1}{3}$, where a_i denotes the number of lines meeting K in i points. We prove below that the number of lines in the Hall plane interesecting K in exactly 3 points does not depend on the choice of K.

Let K' be another parabola with $D \cap K' \neq \emptyset$. There is a projectivity φ that maps K' to K and the infinite point of K' to the infinite point of K. Then φ maps ℓ_∞ to itself and D to another Baer subline, say r. The Baer subplanes containing D are mapped to the Baer subplanes containing r. It is enough to show that there is a projectivity ψ which fixes K and maps r to D because then the product $\psi\varphi$ will map the 3-secant new lines to K' to the 3-secant new lines to K. Denote by I the infinite point of K. Let G be the group of projectivities fixing K, and H be the stabilizer of I in G. The group $G \cong \mathrm{PGL}(2, q^2)$, which is sharply 3-transitive on the points of K. Thus H is sharply 2-transitive on $K \setminus \{I\}$, implying that it acts doubly transitively on the tangents of K distinct from ℓ_∞, and hence also on the points in $\ell_\infty \setminus \{I\}$. When we identify $\ell_\infty \setminus \{I\}$ with $\mathrm{GF}(q^2)$, then H acts as the set of maps $z \mapsto az + b$, $a \in GF(q^2)^*$, $b \in \mathrm{GF}(q^2)$ and Baer subplanes not containing I are circles $(z - c)(\bar{z} - \bar{c}) = r$ so we see that H contains a projectivity ψ that maps the first pair to the second. Clearly, ψ will map r to D, and by this we showed that the number of lines in the Hall plane interesecting K in exactly 3 points does not depend on the choice of K.

Lemma 6.3. *Let q be odd, and P_1, P_2 and P_3 be three affine points on a new line ℓ of the Hall plane. Then there are exactly* $3(q-1)$ *parabolas whose infinite points are not in D and which intersect ℓ in exactly P_1, P_2 and P_3.*

Proof. Let us write $P_i = (a_i, b_i)$ for $i = 1, 2, 3$. The translation $(x, y) \mapsto (x, y) - (a_1, b_1)$ maps ℓ to a new line through the point $(0, 0)$, and therefore, the affine points of the latter new line form the set $\{(\lambda x, \lambda y) \mid x, y \in \mathrm{GF}(q)\}$ for some $\lambda \in \mathrm{GF}(q^2)^*$. There exists a non-singular matrix A with entries in $\mathrm{GF}(q)$ such that $(a_2 - a_1, b_2 - b_1)A = \lambda(-1, 0)$ and $(a_3 - a_1, b_3 - b_1)A = \lambda(0, -1)$. Let φ be the automorphism of $\mathrm{AG}(q^2)$ defined by $\varphi : (x, y) \mapsto \lambda^{-1}(x - a_1, y - b_1)A$. This extends naturally to a projectivity of $\mathrm{PG}(2, q)$, which fixes ℓ_∞ setwise, and maps D to itself. The image $\varphi(\ell)$ is the new line for which

$$\varphi(\ell) \setminus \ell_\infty = \{(x, y) \mid x, y \in \mathrm{GF}(q)\}.$$

We are done if we show that there are exactly $3(q-1)$ parabolas whose infinite points are not in D and which intersect $\varphi(\ell)$ in exactly the points $(0, 0)$, $(-1, 0)$ and $(0, -1)$.

For $u \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, denote by K_u be the unique parabola that contains the points $(0,0)$, $(-1,0)$ and $(0,-1)$ and the infinite point $(-u : 1 : 0)$. Then K_u has affine equation

$$f(X,Y) = (X + uY)^2 + X + u^2 Y = 0.$$

We find next all $\mathrm{GF}(q)$-rational points of K_u. If $P = (a,b)$ is such a point, then we compute

$$\begin{aligned} f(a,b) - \overline{f(a,b)} &= (u - \bar{u})b(2a + (u + \bar{u})(b+1)) = 0, \\ -\bar{u}^2 f(a,b) + u^2\overline{f(a,b)} &= (u - \bar{u})a((u + \bar{u})(a+1) + 2u\bar{u}b) = 0. \end{aligned}$$

Since $u - \bar{u} \neq 0$, these show that $a = 0$ or $b = 0$ (and in this case $(a,b) \in \{(0,0),(-1,0),(0,-1)\}$), or (a,b) can be obtained as the unique solution of a system of linear equations, which then yields

$$P = \Big(\frac{(u+\bar{u})(2u\bar{u} - u - \bar{u})}{(u - \bar{u})^2}, \frac{(u + \bar{u})(2 - u - \bar{u})}{(u - \bar{u})^2} \Big).$$

It is clear that P is $\mathrm{GF}(q)$-rational, and we leave for the reader to check that it lies on K_u.

We conclude that $|\varphi(\ell) \cap K_u| \in \{3,4\}$, and $|\varphi(\ell) \cap K_u| = 3$ iff P is equal to one of the points $(0,0)$, $(-1,0)$ and $(0,-1)$. A quick computation gives that this occurs iff $u + \bar{u} \in \{0,2\}$ or $1/u + 1/\bar{u} = 2$. It can be easily checked that u satisfies one of the latter conditions iff $u \in \mathrm{GF}(q)^*\omega$ or $u \in \mathrm{GF}(q)^*\omega + 1$ or $u \in (\mathrm{GF}(q)^*\omega + 1)^{-1}$, where $\omega \in \mathrm{GF}(q^2)$ is any element such that ω^2 is a non-square in $\mathrm{GF}(q)$. This implies that there are $3(q-1)$ parabolas K_u intersecting $\varphi(\ell)$ in exactly the points $(0,0)$, $(-1,0)$ and $(0,-1)$, and this completes the proof of the lemma. □

Theorem 6.4. *Let D be a derivation set on ℓ_∞ of $\mathrm{AG}(2,q^2)$ with q odd. Let K be a parabola whose infinite point does not belong to D. Then there are $a_3 = (q^2-1)/2$ and $a_4 = (q-3)(q^2-1)/24$ lines of $\mathrm{Hall}(q^2)$ meeting K in 3 or 4 points, respectively.*

Proof. Let U be the set of parabolas whose infinite point does not belong to D. Any element of U has a uniquely defined equation of the form

$$Y = \alpha(X - uY)^2 + \beta(X - uY) + \gamma,$$

with $u \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$, $\alpha \in \mathrm{GF}(q^2)^*$, $\beta, \gamma \in \mathrm{GF}(q^2)$. Hence,

$$|U| = (q-1)(q^2-1)q^5.$$

We showed above that for any $K \in U$, the number of 3-secant new lines is a constant a_3.

Let V be the set of new lines; $|V| = (q+1)q^2$. For the set

$$W = \{(K, B, P_1, P_2, P_3) \mid K \in U, B \in V, K \cap B = \{P_1, P_2, P_3\}\},$$

one has

$$|W| = 6|U|a_3 = |V|q^2(q^2-1)(q^2-q)\cdot 3(q-1)$$

by Lemma 6.3. The value for a_4 follows from $a_3 + 4a_4 = \binom{q+1}{3}$. □

The case when q is even is more interesting. The four cases are treated by O'Keefe, Pascasio [12], O'Keefe, Pascasio, and Penttila [13] and Glynn, Steinke [3].

Theorem 6.5 ([12], [13], [3])**.** *Let D be a derivation set on ℓ_∞ of* $\mathrm{AG}(2, q^2)$*, with $q \geq 4$ even, and K a parabola with infinite point I and nucleus N.*

(i) If $I \in D$ and $N \in D$, then K is not an arc in the Hall plane.

(ii) If $I \notin D$ and $N \in D$, then K is a translation q^2-arc in the derived plane and it can be extended to a hyperoval. Any two hyperovals of the Hall plane arising from this construction are equivalent under the automorphism group of the Hall plane.

(iii) If $I \in D$ and $N \notin D$, then K is a translation q^2-arc in the derived plane and it can be extended to a hyperoval. Any two hyperovals of the Hall plane arising from this construction are equivalent under the automorphism group of the Hall plane. The two cases give inequivalent hyperovals in the Hall plane.

(iv) If $I \notin D$ and $N \notin D$, then $K \cup \{I\}$ is a translation oval if and only if q is a square, and I and N are conjugate with respect to D.

Also in the case q even, we know something about the combinatorial structure of K in $\mathrm{Hall}(q^2)$ if $I, N \in D$. In this case we may assume that the parabola has equation $K : Y = X^2$ and D is the standard derivation set. Points of K whose coordinates are in $\mathrm{GF}(q)$ are collinear in $\mathrm{Hall}(q^2)$ and the same is true for points whose first coordinate is in an additive coset of $\mathrm{GF}(q)$. So the points of K are on q parallel lines. Other triples are not collinear.

In the general Glynn–Steinke case $I, N \notin D$, we can show that each line meets K in 0, 1, 2 or 4 points.

Lemma 6.6. *Let q be a power of* 2 *and $\beta \in \mathrm{GF}(q^2)^*$. Let N_β be the number of* $\mathrm{GF}(q)$*-rational roots of*

$$f(T) = T^3 + \beta\bar{\beta}T + \beta\bar{\beta}(\beta + \bar{\beta}).$$

(a) If q is a square then

$$N_\beta = \begin{cases} 3 & \textit{for } \beta \in \mathrm{GF}(q), \\ 1 & \textit{for } \beta \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q). \end{cases}$$

(b) If q is not a square then

$$N_\beta = \begin{cases} 3 & \textit{if } \beta \textit{ is a cube in } \mathrm{GF}(q^2)^*, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $\beta = \bar{\beta}$ then the roots of $f(T)$ are $0, \beta, \beta$, in accordance with (a) and (b). For the remaining part, we assume $\beta \neq \bar{\beta}$. Let ε, d be elements of $\overline{\mathrm{GF}(q)}$ such that $\varepsilon^2 + \varepsilon + 1 = 0$ and $d^3 = \beta$. Then, the three different roots of $f(T)$ are

$$\begin{aligned} t_1 &= d^{q+1}(d + d^q), \\ t_2 &= d^{q+1}(\varepsilon^2 d + \varepsilon d^q), \\ t_3 &= d^{q+1}(\varepsilon d + \varepsilon^2 d^q). \end{aligned}$$

($\beta \neq \bar{\beta}$ implies $t_i \neq t_j$ for $i \neq j$.)

Assume that q is not a square. Then $\varepsilon^q = \varepsilon^2$, and thus if β is a cube in $\mathrm{GF}(q^2)$, then $d \in \mathrm{GF}(q^2)$, and $t_1, t_2, t_3 \in \mathrm{GF}(q)$. If $d \notin \mathrm{GF}(q^2)$ then the three cubic roots of β are d, d^{q^2}, d^{q^4}, and we have $d^{q^2} = \varepsilon d$. This implies $t_1^q = t_2$, $t_2^q = t_3$ and $t_3^q = t_1$, showing that no root of $f(T)$ lies in $\mathrm{GF}(q)$. This proves (b).

Now, let q be a square. Then $\varepsilon^q = \varepsilon$, and we obtain that $t_1^q = t_1$, $t_2^q = t_3$ and $t_3^q = t_2$ when β is a cube in $\mathrm{GF}(q^2)$, and $t_3^q = t_3$, $t_1^q = t_2$ and $t_2^q = t_1$ when β is not a cube. In either case $f(T)$ has one root in $\mathrm{GF}(q)$, as claimed in (a). □

Theorem 6.7. *Let D be a derivation set on ℓ_∞ of $\mathrm{AG}(2, q^2)$, with $q \geq 4$ even, and K a parabola with infinite point I and nucleus N. Assume that $I \notin D$ and $N \notin D$. Then the following holds:*

(i) Each line of the Hall plane intersects K in $0, 1, 2$ or 4 points.

(ii) If I and N are conjugate with respect to D, and q is not a square, then each point $P \in K$ is contained in $(q+1)/3$ 4-secant new lines and $2(q+1)/3$ 1-secant new lines. In particular, the Hall plane has no 2-secant new lines.

Proof. Let I and N be the points $(u : 1 : 0)$ and $(v : 1 : 0)$ of the line at infinity; $u, v \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$. Then, the homogeneous equation of K has the form

$$X^2 + u^2 Y^2 + \beta_0 Z(X + vY) + \beta_1 Z^2 = 0,$$

where $\beta_0 \in \mathrm{GF}(q^2)^*$ and $\beta_1 \in \mathrm{GF}(q^2)$. Let ℓ be a new line of the Hall plane and assume $K \cap \ell \neq \emptyset$. W.l.o.g. we can assume that $(0, 0) \in K \cap \ell$. Then $\beta_1 = 0$ and

$$\ell \setminus \ell_\infty = \{(\lambda x, \lambda y, 1) \mid x, y \in \mathrm{GF}(q)\}$$

for some $\lambda \in \mathrm{GF}(q^2)^*$. In order to compute $K \cap \ell$, we substitute $X = \lambda x$, $Y = \lambda y$, $Z = 1$ in the equation of K. We obtain

$$C : x^2 + u^2 y^2 + \beta(x + vy) = 0,$$

where $\beta = \beta_0/\lambda \in \mathrm{GF}(q^2)^*$. The $\mathrm{GF}(q)$-rational points of C are contained in $C \cap \bar{C}$.

Assume $\beta = \bar{\beta} \in \mathrm{GF}(q)^*$. Then $C + \bar{C} : (u^2 + \bar{u}^2)y^2 + \beta(v + \bar{v})y = 0$, giving two $\mathrm{GF}(q)$-rational roots $y_1 = 0$ and $y_2 = \frac{\beta(v+\bar{v})}{u^2+\bar{u}^2} = \gamma \in \mathrm{GF}(q)^*$. For $y_1 = 0$, we get $x_1 = 0$ or $x_2 = \beta$, two rational points. For $y_2 = \gamma$, we get two different roots x_3, x_4 of $x^2 + \beta x + u^2\gamma^2 + \beta v\gamma$. This means 2 or 4 GF($q$)-rational points on C.

Assume now $\beta \neq \bar{\beta}$ and compute the resultant

$$R_{C,\bar{C}}(y) = (u+\bar{u})^4 y^4 + [(u+\bar{u})^2\beta\bar{\beta} + (u+\bar{v})^2\bar{\beta}^2 + (v+\bar{u})^2\beta^2]y^2 + \beta\bar{\beta}(\beta+\bar{\beta})(v+\bar{v})y.$$

As the derivative is a nonzero constant, this resultant has four different roots. Clearly, if three of them sit in GF(q) then so does the fourth. If $y = \gamma$ is a rational root of the resultant, then

$$x^2 + \beta x + u^2\gamma^2 + \beta v\gamma, \quad x^2 + \bar{\beta}x + \bar{u}^2\gamma^2 + \bar{\beta}\bar{v}\gamma$$

have a unique rational common root, giving rise to a unique GF(q)-rational point of C. In particular, ℓ intersects K in $0, 1, 2$ or 4 points, and this together with the previous paragraph shows that (i) holds.

We turn now to the statement in (ii), and assume that q is not a square and I and N are conjugate w.r.t. D. This means $u = \bar{v}$ and the resultant $R_{C,\bar{C}}(y)$ becomes

$$r(T) = T^4 + \beta\bar{\beta}T^2 + \beta\bar{\beta}(\beta + \bar{\beta})T,$$

where $T = (u + \bar{u})y$. By Lemma 6.6, $r(T)$ has 1 or 4 GF(q)-rational roots, depending whether β is a cube or not in GF$(q^2)^*$. Moreover, these roots are different for $\beta \neq \bar{\beta}$, and hence ℓ is a 1- or a 4-secant of K depending whether β is a cube or not. If $\beta = \bar{\beta}$, then a straightforward calculation shows, that in this case, the four points of $C \cap \bar{C}$ are

$$(0,0), \quad (0,\beta), \quad \left(\frac{u\beta}{u+\bar{u}} + \varepsilon\beta, \frac{\beta}{u+\bar{u}}\right), \quad \left(\frac{u\beta}{u+\bar{u}} + \varepsilon^2\beta, \frac{\beta}{u+\bar{u}}\right),$$

where $\varepsilon^2 + \varepsilon + 1 = 0$. The last two points are GF(q)-rational iff $\varepsilon + \varepsilon^q = 1$, which holds iff q is not a square. The multiplicative group GF$(q^2)^*$ is a cyclic group of order $q^2 - 1$, let $\mathcal{K}$ and $\mathcal{L}$ be its unique subgroups of order $q - 1$ and $(q^2-1)/3$, resp. As q is not a square, $(q-1)$ divides $(q^2-1)/3$, and thus $\mathcal{K} < \mathcal{L}$. Our above discussion shows that the new line ℓ is a 1- or a 4-secant of K, and that it is a 4-secant is equivalent to say that $\beta \in \mathcal{L}$.

Recall that, $\beta = \beta_0/\lambda$, where β_0 is some fixed element in GF$(q^2)^*$, and $\lambda \in$ GF$(q^2)^*$ defines the new line ℓ. The $q+1$ new lines through the affine point $(0,0)$ can be listed by letting λ run over any complete set of coset representatives of $\mathcal{K}$ in GF$(q^2)^*$. Now, denoting by Λ such a set of coset representatives, the number of 4-secants through $(0,0)$ is equal to

$$|\{\lambda \in \Lambda : \beta_0/\lambda \in \mathcal{L}\}| = |\Lambda \cap \mathcal{L}\beta_0|.$$

Consider the canonical projection $\eta :$ GF$(q^2)^* \to$ GF$(q^2)^*/\mathcal{K}$. It follows that $\eta(\Lambda) = GF(q^2)^*/\mathcal{K}$, and η induces a bijection from $\Lambda \cap \mathcal{L}\beta_0$ to $\eta(\Lambda \cap \mathcal{L}\beta_0) = GF(q^2)^*/\mathcal{K} \cap \mathcal{L}/\mathcal{K}\,(\mathcal{K}\beta_0) = \mathcal{L}/\mathcal{K}\,(\mathcal{K}\beta_0)$ (here $\mathcal{K}\beta_0$ is regarded as an element in GF$(q^2)^*/\mathcal{K}$). This gives $|\Lambda \cap \mathcal{L}\beta_0| = |\mathcal{L}/\mathcal{K}| = (q+1)/3$, and (ii) follows. □

Part (i) of the last proposition also follows from the proof of Glynn–Steinke, see [3, Section 4].

Part (ii) implies that if I, N are conjugate w.r.t. D and q is not a square, then the number of i-secant new lines of the Hall plane is $a_0 = \frac{1}{4}q^2(q+1)$, $a_1 = \frac{2}{3}q^2(q+1)$ and $a_4 = \frac{1}{12}q^2(q+1)$ for $i = 0, 1, 4$.

7. Inherited hyperbolas

A surprising phenomenon occurs in this case. When the infinite points of a hyperbola belong to the derivation set, then it is possible that although the affine points of the hyperbola form an inherited arc, this arc is complete. This was pointed out in [17] and the possible configurations were fully described by O'Keefe and Pascasio. Note that in Galois planes there are no complete $(q-1)$-arcs by the theorems of Segre mentioned in the introduction.

Theorem 7.1 (O'Keefe-Pascasio, [12])**.** *Suppose that the line at infinity is a secant of a hyperbola K whose infinite points belong to the derivation set D. Assume that $q > 3$ is odd and D is the standard derivation set. Then either we have K equivalent to the hyperbola $XY = 1$ which does not give an inherited arc, or to the hyperbola $XY = -d$ with d a non-square in* $\mathrm{GF}(q^2)$ *and we get a complete (q^2-1)-arc in* $\mathrm{Hall}(q^2)$*. For $q > 2$ even, and D standard, K is equivalent to the hyperbola $XY = 1$ and does not give an inherited arc.*

Note that the odd case of the above theorem essentially is (one part of) Proposition 5.2.

O'Keefe and Pascasio [12] give a complete description of the resulting configurations in the Hall plane for $q = 3$.

The next case we consider is that the line at infinity is a secant of the hyperbola K with two conjugate infinite points outside the derivation set.

Theorem 7.2. *Suppose that the line at infinity is a secant of a hyperbola K whose infinite points are conjugate, so outside of the (standard) derivation set D. Assume that $q > 3$ is odd. Then either all points of D are internal, and K (together with the two infinite points) is an inherited oval in the Hall plane, or all points of D are external and now we find (two) lines containing $q+1$ points of K.*

The first case is just Proposition 5.2 together with Proposition 3.2. If all points are external, then again by Proposition 3.2, for every triple of points in D, there are two corresponding triangles in K, and these together form two ellipses in two Baer subplanes on D.

Remark: if q is even, and the two infinite points of K are conjugate, then we find exactly one line in the Hall plane with $q+1$ points of K as a consequence of Proposition 4.1.

The third case to consider is that the line at infinity is a secant of the hyperbola K with one point in the derivation set, and one outside.

The following proposition makes more precise what we already mentioned in the section about consequences of the theorem by Segre and Korchmáros, together with Proposition 5.3.

Theorem 7.3. *If $q > 5$ is odd and K is a hyperbola with one point in the derivation set, and one point outside of it, then the affine part of K does not give an arc in the Hall plane, moreover, lines of the Hall plane intersect it in at most three points. If $s = \frac{1}{2}(q \pm 1)$ denotes the number of external points on our derivation set D, then the total number of collinear triples in the Hall plane is $2s\binom{q-s}{2} + 2\binom{s}{3}$, which for q large enough is roughly $7q^3/48$, so small.*

The final case to consider is where both infinite points of the hyperbola K are outside the derivation set D and are not conjugate. From Proposition 5.4 we know that the number of internal/external points in D is at most $q/2 - 1 - \sqrt{q}$.

If s denotes the number of external points in our derivation set D, then the total number of collinear triples in the Hall plane is $2s\binom{q+1-s}{2} + 2\binom{s}{3}$, roughly $7q^3/48$, using the above bound on s. Note also that we do not have collinear sets of size 5 or more, since 5 points of our Baer subplanes extend to a conic with points at infinity. We will return to this case in section 9 where the case q even is studied in more detail.

8. Inherited ellipses for q odd

The last case to consider is an ellipse K in the affine plane $\mathrm{AG}(2, q^2)$, so a conic without points on the line at infinity. Let q be odd. Then, on the line at infinity ℓ_∞ we have $(q^2 + 1)/2$ external and $(q^2 + 1)/2$ internal points. If D is a Baer subline of ℓ_∞ then K is again an oval in the derived plane if and only if the derivation set D is disjoint from the set of external points (on ℓ_∞), as a consequence of Proposition 3.2. In Proposition 5.4 we have seen that this is impossible for $q > 7$. The following combinatorial proof works for all q.

Theorem 8.1. *Let q be odd, K an ellipse in $\mathrm{AG}(2, q^2)$, then K does not remain an oval in $\mathrm{Hall}(q^2)$.*

Proof. Here we essentially just count. Consider the line ℓ_∞ together with the partition $E \cup I$ into external and internal points. The subgroup of $\mathrm{PGL}(2, q^2)$ stabilizing this partition has order $2(q^2 + 1)$, there is a dihedral group of order $q^2 + 1$ fixing the set E and an extra factor 2 because we may interchange E and I. Now how does this group act on the set of Baer-sublines, or better, how large are the orbits? The stabilizer of a Baer-subline has order $(q + 1)q(q - 1)$, and the greatest common divisor of $(q^2 + 1)$ and $(q + 1)q(q - 1)$ is 2, this means that if we find a Baer-subline contained in E, we find $(q^2 + 1)/2$, and an additional set of this size in I. Now let us count the number N of triples (P_e, P_i, B), of an external point P_e, an internal point P_i and a Baer-subline B containing them. Since every pair of points is contained in $(q^2 - 1)/(q - 1) = (q + 1)$ Baer-sublines, we find $N = \frac{1}{4}(q^2 + 1)^2(q + 1)$. Now we count in the other way, the total number of Baer-sublines is $(q^2 + 1)q^2(q^2 - 1)/((q + 1)q(q - 1)) = (q^2 + 1)q$, but if we assume that there is a Baer-subline contained in E, then at least (q^2+1) of them do not contribute to our counts, so we find $N \leq \frac{1}{4}(q^2+1)(q-1)(q+1)^2 < \frac{1}{4}(q^2+1)^2(q+1)$, contradiction. $\square$

Remark 8.2. *(i) If s denotes the number of external points in our derivation set D, then as in the hyperbola case the total number of collinear triples in the Hall plane is $2s\binom{q+1-s}{2}+2\binom{s}{3}$, roughly $7q^3/48$, using the bound on s from Proposition 5.4.*

(ii) Also, we do not have collinear sets of size 5 or more, since 5 points in of our Baer-subplanes extend to a conic with points at infinity.

We finish this section with an open problem concerning the exact number of 3-secant new lines.

Question 8.3. *Let q be odd, K an ellipse or a hyperbola with non-conjugate infinite points in $\mathrm{AG}(2,q^2)$. Let s denote the number of external points of K in the derivation set D. Find a formula for the number a_3 of 3-secant new lines in terms of q and s.*

In the last section, we answer this question for the even q case.

9. Inherited ellipses and hyperbolas for q even

In Theorem 4.2, we showed that if q is even and K is either an ellipse or a hyperbola having two non-conjugate infinite points, then in the Hall plane K has $\binom{q+1}{3}$ collinear triples. In this section, we give an explicit formula for the number a_3 of 3-secant new lines. By $a_3+4a_4=\binom{q+1}{3}$ this also determines the number a_4 of 4-secant new lines.

Theorem 9.1. *Let q be even, and D a derivation set on ℓ_∞ of $\mathrm{AG}(2,q^2)$. Let K be either an ellipse or a hyperbola such that the infinite points of K are non-conjugate and none of them is contained in D. Then, the number of 3-secant new lines is $a_3=q(q-1)/2$.*

Lemma 9.2. *Let $u_1,u_2 \in \mathrm{GF}(q^4)$ be the roots of the quadratic polynomial $f(X)=X^2+\beta X+\gamma \in \mathrm{GF}(q^2)[X]$ and assume $u_i \notin \{u_i^q, u_j, u_j^q\}$, where $\{i,j\}=\{1,2\}$. Then there is a $\mathrm{GF}(q)$-rational map $z \mapsto \frac{az+b}{cz+d}$ which brings $f(X)$ to the form X^2+X+w with some $w \in \mathrm{GF}(q^2)\setminus\mathrm{GF}(q)$.*

Proof. The fact $u_i \neq u_j$ implies $\beta \neq 0$. Straightforward calculation shows

$$f(u(z)) = \frac{(a^2+\beta ac+\gamma c^2)z^2+\beta(cb+ad)z+b^2+\beta db+\gamma d^2}{(cz+d)^2}.$$

Assume first that $\beta \in \mathrm{GF}(q^2)\setminus\mathrm{GF}(q)$. If $\gamma = t\beta$ with $t \in \mathrm{GF}(q)$ then $u(z)=t/z$ brings $f(Z)$ to the form X^2+X+t/β. If $\gamma/\beta \notin \mathrm{GF}(q)$, then β,γ

forms a GF(q)-basis of GF(q^2) and there are unique elements $t_1, t_2 \in$ GF(q), $t_2 \neq 0$, such that

$$1 = t_1\beta + t_2\gamma.$$

Define $a = b = 1$, $c = \sqrt{t_2}$, $d = 1 + \sqrt{t_2}$. Then

$$a^2 + \beta ac + \gamma c^2 = (t_1 + \sqrt{t_2})\beta, \quad (1)$$

$$\beta(cb + ad) = \beta, \quad (2)$$

$$b^2 + \beta bd + \gamma d^2 = \beta(1 + t_1 + \sqrt{t_2}) + \gamma. \quad (3)$$

By (1), $t_1 + \sqrt{t_2} = 0$ implies that $c/a = \sqrt{t_2}$ is a root of $f(X)$, which contradicts to $u_i \neq u_i^q$. Hence, u brings $f(X)$ to the form $f_0(X) = X^2 + \beta_0 X + \gamma_0$, with

$$\beta_0 = \frac{1}{t_1 + \sqrt{t_2}} \in GF(q)^*.$$

Now, $v(z) = \beta_0 z$ brings $f_0(X)$ to the desired form $X^2 + X + w$, where $w \notin$ GF(q) follows from $u_i \neq u_j^q$. □

Lemma 9.2 implies that AG($2, q^2$) has an affine coordinate frame in which $D = \{(x, y, 0) \mid x, y \in \text{GF}(q)\}$ and the equation of K has the form

$$K : X^2 + XY + cY^2 + uX + vY + w,$$

with $c \in \text{GF}(q^2) \setminus \text{GF}(q)$, $u, v, w \in \text{GF}(q^2)$. All dilations (=translations and homotheties) preserve D and the quadratic component $X^2 + XY + cY^2$ of K.

We use the notation t_P for the tangent line of K at the point $P \in K$.

Lemma 9.3. *Let B be a new line.*

(i) If $|B \cap K| = 3$ then there is a unique $P \in B \cap K$ such that the tangent t_P intersects D.

(ii) If t_P intersects D for an element $P \in B \cap K$ then $|B \cap K| \leq 3$.

Proof. Up to dilatations we can assume that $B = \{(x, y) \mid x, y \in \text{GF}(q)\}$, which means that $B \cap K$ consists of the GF(q)-rational points of K. Equivalently, $B \cap K = K \cap \bar{K}$, where

$$\bar{K} : X^2 + XY + c^q Y^2 + u^q X + v^q Y + w^q$$

is the conjugate of K. Counting with multiplicities, K and $\bar{K}$ have 4 points in common over the algebraic closure of GF(q). (Cf. Bézout's Theorem [5, Theorem 3.14]). If $|B \cap K| = 3$ then there is a unique $P \in B \cap K$ such that K and $\bar{K}$ have intersection multiplicity 2. In particular, K and $\bar{K}$ have a common tangent t at P (see [5, Proposition 3.6]). This means that t is defined over GF(q) and the infinite point of t is in D. This proves (i).

Conversely, if $t_P \cap D \neq \emptyset$ for some $P \in B \cap K$, then t_P is a common tangent of K and $\bar{K}$. Hence, K and $\bar{K}$ have a common tangent at P, which implies an intersection multiplicity at least 2. Thus, (ii) follows. □

Proof of Theorem 9.1. Fix a point $A = (u, v, 0) \in D$. Let t be the tangent from A to K, with tangent point $T \in K$. We want to determine the 3-secant new lines through T. Lemma 9.3 shows that if A runs through D, then this enumerates all 3-secant new lines for K.

Up to dilations, we can have $T = (0, 0)$ and let K have equation

$$K : X^2 + XY + cY^2 + vX + uY.$$

Moreover, any new line through T has the form

$$B_\lambda = \{(\lambda^{-1}x, \lambda^{-1}y) \mid x, y \in \mathrm{GF}(q)\}$$

for some $\lambda \in \mathrm{GF}(q^2)$. More precisely, since λ is given up to a nonzero $\mathrm{GF}(q)$-rational scalar multiple, w.l.o.g. $\lambda = 1$ or $\lambda = \lambda_0 + c$ with $\lambda_0 \in \mathrm{GF}(q)$. By substituting the generic point of B_λ in the equation of K, we find a $1-1$ correspondence between $B_\lambda \cap K$ and the set of $\mathrm{GF}(q)$-rational points of the conic

$$K_\lambda : X^2 + XY + cY^2 + v\lambda X + u\lambda Y.$$

Case 1: $\lambda = 1$. Then $K_\lambda + \bar{K}_\lambda : Y^2 = 0$, This implies $Y = 0$ and $X^2 + vX = 0$. The only rational points of K_λ are $(0, 0)$ and $(v, 0)$. Thus, $|B_\lambda \cap K| \leq 2$.

Case 2: $\lambda \neq 1$ and $(u, v) = (1, 0)$. As $\lambda = \lambda_0 + c$, we have $\lambda + \lambda^q = c + c^q$ and $K_\lambda + \bar{K}_\lambda : (c + c^q)(Y^2 + Y) = 0$. If $Y = 0$ then $X = 0$. In order to have $|B_\lambda \cap K| = 3$, we need two more rational points, which holds if $Y = 1$ and $X^2 + X + \lambda_0$ has two distinct roots in $\mathrm{GF}(q)$. This happens if and only if $\mathrm{Tr}_{\mathrm{GF}(q)/\mathrm{GF}(2)}(\lambda_0) = 0$. Therefore, we found exactly $q/2$ new lines B_λ through $T = (0, 0)$ such that $|B_\lambda \cap K| = 3$.

Case 3: $\lambda \neq 1$ and $v = 1$. Again, $\lambda = \lambda_0 + c$ and

$$K_\lambda + \bar{K}_\lambda : (c + c^q)(Y^2 + X + uY) = 0.$$

Substituting $X = Y^2 + uY$ into K_λ, we have

$$Y^2(Y^2 + Y + u^2 + u + \lambda_0) = 0.$$

If $Y = 0$ then $X = 0$. If

$$\mathrm{Tr}_{\mathrm{GF}(q)/\mathrm{GF}(2)}(u^2 + u + \lambda_0) = \mathrm{Tr}_{\mathrm{GF}(q)/\mathrm{GF}(2)}(\lambda_0) = 1$$

then $B_\lambda \cap K = \{(0, 0)\}$. If $\lambda_0 = u^2 + u$ then $Y = 0$ or $Y = 1$, and $B_\lambda \cap K = \{(0, 0), (u + 1, 1)\}$. Finally, if $\mathrm{Tr}_{\mathrm{GF}(q)/\mathrm{GF}(2)}(\lambda_0) = 0$ and $\lambda_0 \neq u^2 + u$, then $Y^2 + Y + u^2 + u + \lambda_0$ has two roots in $\mathrm{GF}(q) \setminus \{0, 1\}$, giving rise to two rational points of K_λ, different from $(0, 0)$. Hence, we found $q/2 - 1$ new lines B_λ through $T = (0, 0)$ such that $|B_\lambda \cap K| = 3$.

Resuming the results, we found $q/2 + q(q/2 - 1) = q(q - 1)/2$ new lines which intersect K in exactly 3 points. □

References

[1] S.G. Barwick, D.J. Marshall, Conics and multiple derivation, *Discrete Math.* **312** (2012), 1623–1632.

[2] W. Cherowitzo, The classification of inherited hyperconics in Hall planes of even order, *Europ. J. Comb.* **31** (2011), 81–86.

[3] D.G. Glynn, G. Steinke, On conics that are ovals in a Hall plane, *Europ. J. Comb.* **14** (1993), 521–528.

[4] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed. Clarendon Press, Oxford (1999).

[5] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic curves over a finite field.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ (2008).

[6] J.W.P. Hirschfeld, T. Szőnyi, Sets in a finite plane with few intersection numbers and a distinguished point, *Discrete Mathematics* **97** (1991), 229–242.

[7] G. Korchmáros, Ovali nei piani di Hall di ordine dispari, *Atti Accad. Naz. Lincei Rend.* **56** (1974), 315–317.

[8] G. Korchmáros, Inherited arcs in finite affine planes, *J. Combin. Theory A* **42** (1986), 140–143.

[9] D.J. Marshall, *Conics, Unitals and Net Replacement*, PhD thesis, Adelaide (2010).

[10] G. Menichetti, q-archi completi nei piani di Hall di ordine $q = 2^k$, *Rend. dell'Accad. Naz. Lincei* **56** (1974), 518–525.

[11] G. Mészáros, *Configurations in non-Desarguesian planes*, MSc Thesis, Eötvös Loránd University (2011).

[12] C.M. O'Keefe, A.A. Pascasio, Images of conics under derivation, *Discrete Math.* **151** (1996), 189–199.

[13] C.M. O'Keefe, A.A. Pascasio, T. Penttila, Hyperovals in Hall planes, *Europ. J. Comb.* **13** (1992), 195–199.

[14] B. Segre, Introduction to Galois geometries, *Acta Accad. Naz. Lincei Mem.* **8** (edited by J.W.P. Hirschfeld) (1967), 133-236.

[15] B. Segre, G. Korchmáros, Una proprieta degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica, *Atti Accad. Naz. Lincei Rend.* (8)) **62** (1977), 363–369.

[16] T. Szőnyi, Complete arcs in non-Desarguesian planes, *Conf. Sem Mat. Univ. Bari* **233** (1989).

[17] T. Szőnyi, Arcs and k-sets with large nucleus-set in Hall planes, *J. Geom.* **34** (1989), 187–194.

[18] T. Szőnyi, Zs. Weiner, On the stability of sets of even type, *Adv. Math.* **267** (2014), 381–394.

[19] F. Wettl, On the nuclei of a point set of a finite projective plane, *J. Geom.* **30** (1987), 157–163.