Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 102 (2003) 143–162

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Finite Laguerre planes of order 8 are ovoidal

Günter F. Steinke

Department of Mathematics and Statistics, University of Canterbury, Private Bag 4800, Christchurch, New Zealand

Received 24 September 2002

Abstract

Using the uniqueness of the Desarguesian projective plane of order 8 and the classification of its ovals it is shown that a Laguerre of order 8 must be ovoidal.

1. Introduction and preliminaries

A *Laguerre plane* consists of a set P of points, a set $\mathscr{C}$ of circles and a set $\mathscr{G}$ of generators (subsets of P) such that the following four axioms on generators (G), joining (J), touching (T) and richness (R) are satisfied, compare [2, 5.6]:

(G) $\mathscr{G}$ partitions P and each circle intersects each generator in precisely one point.
(J) Three points no two of which are on the same generator can be uniquely joined by a circle.
(T) Given a point p on a circle C and a point q not on the same generator as p, there is a uniquely determined circle that contains both points and touches C at p, that is, intersects C only in p or coincides with C.
(R) There are at least two circles and each circle contains at least three points.

All known models of finite Laguerre planes are of the following form. Let $\mathscr{O}$ be an oval in the Desarguesian projective plane $\mathscr{P}_2 = \mathrm{PG}(2, q)$, q a prime power. Embed $\mathscr{P}_2$ into a 3-dimensional projective space $\mathscr{P}_3 = \mathrm{PG}(3, q)$ and let v be a point of $\mathscr{P}_3$ not belonging to $\mathscr{P}_2$. Then P consists of all points of the cone with base $\mathscr{O}$ and vertex v except the point v. Generators are the traces of lines of $\mathscr{P}_3$ through v that are contained in the cone. Circles are obtained by intersecting P with planes of $\mathscr{P}_3$ not

E-mail address: g.steinke@math.canterbury.ac.nz.

0097-3165/03/$ - see front matter
doi:10.1016/S0097-3165(03)00025-6

passing through v. In this way, one obtains an *ovoidal Laguerre plane of order q*. If the oval $\mathcal{O}$ one starts off with is a conic, one obtains the *Miquelian Laguerre plane of order q*. All known finite Laguerre planes of odd order are Miquelian and all known finite Laguerre planes of even order are ovoidal. In fact, it is a long-standing problem whether or not these are the only finite Laguerre planes.

The *internal incidence structure* $\mathscr{A}_p$ at a point p of a Laguerre plane has the collection of all points not on the generator through p as point set and, as lines, all circles passing through p (without the point p) and all generators not passing through p. From the definition of a Laguerre plane it readily follows that each internal incidence structure is an affine plane, the *derived affine plane at p*. We say that a Laguerre plane is finite if P is finite and that it has *order n* if a derived affine plane has order n. It now readily follows that a Laguerre plane of order n has $n+1$ generators, that every generator contains n points and every circle has $n+1$ points, that there are $n(n+1)$ points and n^3 circles. Hence, Laguerre planes of order n are precisely the transversal designs $\mathrm{TD}(3, n+1, n)$.

A circle K not passing through the distinguished point p at which the derived affine plane is formed induces an oval in the projective extension of the derived affine plane at p. This oval intersects the line at infinity in the point corresponding to lines that come from generators of the Laguerre plane; in $\mathscr{A}_p$ one has a *parabolic curve*. (The derived affine planes of the Miquelian Laguerre planes are Desarguesian and the parabolic curves are parabolae whose axes are the verticals, i.e., the lines that come from generators of the Laguerre plane.) A Laguerre plane can thus be described in one derived affine plane $\mathscr{A}$ by the lines of $\mathscr{A}$ and a collection of parabolic curves. This planar description of a Laguerre plane is then extended by the points of one generator where one has to adjoin a new point to each line and to each parabolic curve of the affine plane. We call the geometry induced on the complement of a generator the *affine part* of the Laguerre plane.

It follows from [8] that every parabolic curve in a finite Desarguesian affine plane of odd order is in fact a parabola. Furthermore, using this result, it was shown in [1] or [7, VII.2], that a finite Laguerre plane of odd order that admits a Desarguesian derivation is Miquelian. In particular, Laguerre planes of orders 3, 5 and 7 are Miquelian. The same argument applies for Laguerre planes of orders 2 and 4. Since there is no projective plane of order 6 (cf. [12]), there is no Laguerre plane of order 6 either. In [11], using the classification of projective planes of order 9 and their ovals, it was shown that a Laguerre plane of order 9 must be Miquelian.

In this note, we consider the case of order 8. From the classification of ovals in the Desarguesian projective plane of order 8 all ovoidal Laguerre planes of order 8 are well known. The same classification can even be used to show that all Laguerre planes of order 8 are indeed ovoidal. We prove the following.

Theorem 1. *A finite Laguerre plane $\mathscr{L}$ of order 8 is ovoidal. More precisely, $\mathscr{L}$ is Miquelian or isomorphic to the ovoidal Laguerre plane $\mathscr{L}^2$ over a proper translation oval, see Section 2 for a description of $\mathscr{L}^2$.*

As mentioned before all other finite Laguerre planes of order at most 9 are Miquelian. Since there is no affine plane of order 10 by [6], we have the following.

Theorem 2. *A finite Laguerre plane $\mathscr{L}$ of order at most* 10 *is ovoidal.*

2. The hyperovals in PG(2,8) and the ovoidal Laguerre planes of order 8

Let $\mathscr{L}$ be a finite Laguerre plane of order 8 and let p be a point of $\mathscr{L}$. The internal incidence structure $\mathscr{A}_p$ extends to a projective plane $\mathscr{P}$. By [3], a projective plane of order 8 is Desaguesian. Hence $\mathscr{P} = \mathrm{PG}(2,8)$ can be described over the Galois field $\mathbb{F}_8 = \mathrm{GF}(8)$ of order 8. We use the representation of $\mathscr{P}$ as an affine plane plus the line W at infinity, that is, $\mathscr{P}$ has point set $(\mathbb{F}_8 \times \mathbb{F}_8) \cup \{(m) \mid m \in \mathbb{F}_8 \cup \{\infty\}\}$, where (m) represents the point at infinity of lines of slope m. Then the generators of $\mathscr{L}$ are represented by the vertical lines.

Every circle not passing through p induces an oval in $\mathscr{P}$. An oval $\mathscr{O}$ in a finite projective plane of even order has a *nucleus*, that is, all the tangents to the oval pass through a common point v. Adjoining this point v leads to a *hyperoval* $\mathscr{O} \cup \{v\}$; cf. [5, Lemma 12.10], [13, Theorem 4.1], or [4, Sections 8.1, 8.4]. We can now remove any point of $\mathscr{O} \cup \{v\}$ and obtain again an oval. There are $2^6 \cdot 7 \cdot 73 = 32,704$ hyperovals and $2^6 \cdot 3^2 \cdot 7 \cdot 73 = 294,336$ ovals in $\mathrm{PG}(2,8)$, see [4, Table 14.10].

In fact, every hyperoval in $\mathrm{PG}(2,8)$ is a conic plus its nucleus, see [9,10], and thus all hyperovals in $\mathrm{PG}(2,8)$ are projectively equivalent. However, removing a point from such a hyperoval does not always yield a conic. Substituting a point of a conic by its nucleus yields a *translation oval* which is not a conic. Recall that an oval $\mathscr{O}$ of $\mathrm{PG}(2,8)$ is a translation oval if there is a point q of $\mathscr{O}$ such that the translations in $\mathrm{PG}(2,8)$ with axis the tangent to $\mathscr{O}$ at q that fix $\mathscr{O}$ are transitive on $\mathscr{O} \setminus \{q\}$, see [4, Section 8.5].

For our purpose, we are only interested in hyperovals that pass through a particular point, the point (∞), and there are three cases for such a hyperoval H to be written as a conic plus its nucleus v:

1. v is a point $\neq (\infty)$ on the line W at infinity; in this case, the affine part of the corresponding conic is a parabola in its usual representation and
$$H^2_{a,b,c} = \{(x, ax^2 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty), (b)\}$$
for $a, b, c \in \mathbb{F}_8$, $a \neq 0$.
2. $v = (\infty)$; in this case, the affine part of the corresponding conic is described by a parabola with axis a non-vertical line. Describing it in the usual way as the graph of a function one finds
$$H^4_{a,b,c} = \{(x, ax^4 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty), (b)\}$$
for $a, b, c \in \mathbb{F}_8$, $a \neq 0$. Note that $H \setminus \{(b)\}$ is a conic whereas $H \setminus \{(\infty)\}$ is not. In fact, the latter is a proper translation oval (i.e., not a conic).

3. v is a point not on W; in this case one finds the following algebraic description:

$$H^{6,d}_{a,b,c} = \{(x, a(x+d)^6 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty), (b)\}$$

for $a, b, c, d \in \mathbb{F}_8$, $a \neq 0$. The affine part of the corresponding conic is a 'hyperbola' with centre $(d, bd + c)$. (This point is also the nucleus.)

We call a hyperoval of *type n* if the highest power of x occurring as in the above list is n. In case $n = 6$, if we want to specify the parameter d, we more precisely say that the hyperoval is of *type* $(6, d)$ and call d the *subtype* of the hyperoval.

From the above description of hyperovals, one sees that there are 4480 hyperovals in PG(2, 8) through the point (∞). Of these 4480 hyperovals, we have to select 448 that together with the 64 lines not passing through (∞) basically form the circles of a Laguerre plane. Since the 448 hyperovals come from circles of a Laguerre plane, we have the following restriction on the number of points any two such hyperovals can have in common.

Lemma 1. *Two hyperovals in $\mathscr{P}$ that come from circles of the Laguerre plane intersect in at most three points of $\mathscr{P}$.*

Proof. Let H_1 and H_2 be two different hyperovals that come from circles C_1 and C_2. Since the circles intersect in at most two points, H_1 and H_2 can have at most two affine points in common. Both hyperovals pass through the point (∞) so there can be at most one further common point on the line W at infinity.

Suppose that H_1 and H_2 also pass through $(m) \in W$ and that they intersect in the affine point q. In the Laguerre plane, this means that C_1 and C_2 pass through q and touch a common circle at q. But then C_1 and C_2 touch each other at q and, because $C_1 \neq C_2$, thus have no point in common except q. This shows that $H_1 \cap H_2 = \{(\infty), (m), q\}$ consists of three points. $\square$

In the proof of Theorem 1, we are mainly interested in hyperovals through the points (∞), (0) and (0,0), that is, hyperovals of the form $H^2_{a,0,0}$, $H^4_{a,0,0}$ and $H^{6,d}_{a,0,ad^6}$, where $a \in \mathbb{F}_8^*$ and $d \in \mathbb{F}_8$. When dealing with these hyperovals and how they intersect, two kinds of collineations of $\mathscr{P}$ will prove to be useful. There is the collineation σ defined on the affine part of $\mathscr{P}$ by $(x, y) \mapsto (y, x)$. It fixes the point $(0, 0)$ and interchanges the points (∞) and (0). Therefore, the family of hyperovals through these points is left invariant. More precisely, hyperovals of types 2 and 4 get interchanged and

$$\sigma(H^2_{a,0,0}) = H^4_{a^3,0,0}, \quad \sigma(H^4_{a,0,0}) = H^2_{a^5,0,0}, \quad \sigma(H^{6,d}_{a,0,ad^6}) = H^{6,ad^6}_{a,0,d}.$$

The second kind of collineations are the collineations $\delta_{r,s}$ defined on the affine part of $\mathscr{P}$ by $(x, y) \mapsto (rx, sy)$, where $r, s \in \mathbb{F}_8^*$. Each $\delta_{r,s}$ fixes the points (∞), (0) and (0,0). A hyperoval of type n is mapped onto a hyperoval of the same type. In particular, for $s = r$ we obtain the homotheties $\delta_r = \delta_{r,r}$. Each δ_r fixes each point on W, and one finds that $\delta_r(H^{6,d}_{a,b,c}) = H^{6,rd}_{r^2a,b,rc}$.

We conclude this section with a brief description of the ovoidal Laguerre planes of order 8. We extend the spatial model of an ovoidal Laguerre plane by starting from a hyperoval $\mathscr{H}$ and a point v. We then consider the cone with base $\mathscr{H}$ and vertex v except the point v. Circles are obtained by intersecting this cone with planes of the 3-dimensional projective space not passing through v. Removing any generator of the cone yields a Laguerre plane. Each such Laguerre plane is ovoidal, but, in general, two Laguerre planes obtained in this way are not isomorphic. Alternatively, we can use the different ovals and construct the ovoidal Laguerre planes associated with them.

In coordinates, the point set of all these Laguerre planes is $P = (\mathbb{F}_8 \cup \{\infty\}) \times \mathbb{F}_8$ and generators are the verticals $\{c\} \times \mathbb{F}_8$ for $c \in \mathbb{F}_8 \cup \{\infty\}$. By starting from a conic we obtain the Miquelian Laguerre plane $\mathscr{L}^1$ whose circles are of the form

$$\{(x, ax^2 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty, a)\}$$

for $a, b, c \in \mathbb{F}_8$. By starting from the oval $H^4_{1,0,0}$, we obtain a non-Miquelian ovoidal Laguerre plane $\mathscr{L}^2$ whose circles are of the form

$$\{(x, ax^4 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty, a)\}$$

for $a, b, c \in \mathbb{F}_8$. Note that one can, essentially, also use parabolae to describe the circles of the latter Laguerre plane as

$$\{(x, ax^2 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty, b)\}$$

for $a, b, c \in \mathbb{F}_8$. In particular, this shows that the affine part consisting of the graphs of all polynomials of degree at most 2 can be extended in two ways to different Laguerre planes.

One obtains the seemingly different Laguerre plane $\mathscr{L}^{3,d}$ from the oval $H^{6,d}_{1,0,0}$, $d \in \mathbb{F}_8$, whose circles are of the form

$$\{(x, a(x+d)^6 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty, a)\}$$

for $a, b, c \in \mathbb{F}_8$. Clearly, $\mathscr{L}^{3,d}$ is isomorphic to $\mathscr{L}^3 = \mathscr{L}^{3,0}$. Furthermore, the transformation of P given by

$$(x, y) \mapsto \begin{cases} (x^2, xy), & \text{if } x \in \mathbb{F}_8, x \neq 0, \\ (\infty, y), & \text{if } x = 0, \\ (0, y), & \text{if } x = \infty, \end{cases}$$

takes a circle $\{(x, ax^6 + bx + c) \mid x \in \mathbb{F}_8\} \cup \{(\infty, a)\}$ of the Laguerre plane $\mathscr{L}^3$ to the circle $\{(u, cu^4 + bu + a) \mid u \in \mathbb{F}_8\} \cup \{(\infty, c)\}$ of $\mathscr{L}^2$ so that one obtains an isomorphism from $\mathscr{L}^3$ onto $\mathscr{L}^2$.

3. Proof of Theorem 1

Let $\mathscr{L}$ be a finite Laguerre plane of order 8, let p be a point of $\mathscr{L}$ and let G_p be the generator containing p. The internal incidence structure $\mathscr{A}_p$ is an affine plane of order 8 and extends to the Desarguesian projective plane $\mathscr{P} = \mathrm{PG}(2,8)$. We always denote the line at infinity by W. Every circle not passing through the distinguished point p induces an oval in $\mathscr{P}$ that passes through the point (∞) and extends to a hyperoval. We use the list of hyperovals through (∞) given in Section 2.

For the Galois field $\mathbb{F}_8$, we use

$$\begin{aligned}\mathbb{F}_8 &= \{c_0 + c_1\omega + c_2\omega^2 \mid c_i = 0,1\}\\ &= \{0\} \cup \{\omega^i \mid i = 0,1,\ldots,6\},\end{aligned}$$

where $\omega^3 = \omega + 1$. We further denote $\mathbb{F}_8 \backslash \{0\}$ by $\mathbb{F}_8^*$.

If $a \in \mathbb{F}_8$ and $a \neq 0, 1$, then a is a generator of the multiplicative group $\mathbb{F}_8^*$ and either $a^3 + a + 1 = 0$ or $a^3 + a^2 + 1 = 0$. The former case occurs for $a \in S$, where

$$S = \{\omega, \omega^2, \omega^4\}$$

and the latter for $a \in \{\omega^3, \omega^5, \omega^6\}$. Note that the latter set equals $S^{-1} = \{s^{-1} \mid s \in S\}$, that is,

$$S^{-1} = \{\omega^3, \omega^5, \omega^6\}$$

and that $(a+1)^3 + (a+1) + 1 = a^3 + a^2 + 1$ so that

$$1 + S = S^{-1}.$$

Furthermore, $S^2 = \{s^2 \mid s \in S\} = S$, $(S^{-1})^2 = S^{-1}$ and $\mathbb{F}_8^* = \{1\} \cup S \cup S^{-1}$. (Note that S and S^{-1} are the non-trivial orbits in the action of the automorphism group of $\mathbb{F}_8$ on $\mathbb{F}_8^*$.) To prove Theorem 1 we try to identify the circles in certain tangent bundles of circles. In particular, we look at collections of circles that touch a circle C at a point $q \in C \backslash G_p$. This bundle consists of eight circles, seven of which do not pass through p. In $\mathscr{P}$, we thus obtain one line L and seven hyperovals that in the affine part only intersect in the point q and have two points in common on W, the points (∞) and $L \cap W$. We call a collection of seven hyperovals a *tangent bundle* and more specifically an *$((m),(u,v))$-bundle*, where $m, u, v \in \mathbb{F}_8$ if each hyperoval contains (∞), (m) and (u,v) and any two of the hyperovals intersect in precisely these points.

The affine parts of hyperovals of type n in a ((0),(0,0))-bundle are described by

$$y = \begin{cases} ax^2 & (n = 2),\\ ax^4 & (n = 4),\\ ax^2(x^2 + dx + d^2)^2 & (n = 6)\end{cases}$$

for some $a, d \in \mathbb{F}_q$, $a \neq 0$.

For points of intersection, we frequently encounter one particular polynomial which we deal with in the following lemma; compare [4, 1.1.4]. Although the result of the lemma is well known we include a short proof.

Lemma 2. *The polynomial $x^2 + x + r$, where $r \in \mathbb{F}_8$ is irreducible over $\mathbb{F}_8$ if and only if $r \in \{1\} \cup S^{-1}$. For $r \in \{0\} \cup S$, the polynomial has the roots r^2 and $r^2 + 1$.*

Proof. The map $\mathbb{F}_8 \to \mathbb{F}_8$ given by $u \mapsto u^2 + u$ has range $\{0, \omega, \omega^2, \omega^4\} = \{0\} \cup S$. Hence, $u^2 + u + r \neq 0$ for any $u \in \mathbb{F}_8$ if r does not belong to the above set, that is, $r \in \mathbb{F}_8^* \backslash S = \{1\} \cup S^{-1}$.

If $r = 0$, then we clearly have the roots 0 and 1. For $r \in S$, one finds $(r^2)^2 + r^2 + r = r(r^3 + r + 1) = 0$ so that r^2 is a root. But then $r^2 + 1$ is also a root. $\square$

In case a ((0),(0,0))-bundle comes from a tangent bundle of circles in an ovoidal Laguerre plane all hyperovals are of the same type and have the same subtype d in case of type 6. We want to show that this is true for any such bundle of hyperovals. To this end we first show that types 2 and 4 cannot both occur in such a bundle.

Lemma 3. *Let H_n, $n = 2, 4$, be two hyperovals of type n through the points (∞), (0) and $(0,0)$. Then H_2 and H_4 intersect in two affine points.*

Proof. The affine part of H_n is given by $y = a_n x^n$ for some $a_n \in \mathbb{F}_8^*$. Then $a_2 x^2 = a_4 x^4$ has the solutions $x = 0$ and $x = (a_2/a_4)^4 \neq 0$. Hence, H_2 and H_4 intersect in the affine points $(0,0)$ and $((a_2/a_4)^4, a_2^2/a_4)$. $\square$

We are now ready to show that all hyperovals in a tangent bundle $\mathscr{B}$ must have the same type. The case of type 6 hyperovals and their subtypes will be dealt with separately.

Proposition 1. *Let $\mathscr{B}$ be a ((0),(0,0))-bundle. Then all members of $\mathscr{B}$ are of the same type.*

Proof. Lemma 3 shows that types 2 and 4 cannot both occur in $\mathscr{B}$. We first assume that only hyperovals of types 2 and 6 occur in $\mathscr{B}$ and that there is at least one of each type. If the affine points of these hyperovals are given by $y = a_2 x^2$ and $y = a_6 x^2 (x^2 + dx + d^2)^2$ for $a_2, a_6 \in \mathbb{F}_8^*$, the points of intersection of these affine parts are $(0,0)$ and $(u, a_2 u^2)$, where $u \neq 0$ is a root of $x^2 + dx + d^2 + r^2$ and $r = (a_2/a_6)^2 \neq 0$. Since by our assumption no such u can exist, this polynomial has no root except 0. This implies that $d \neq 0, r$, otherwise $r \neq 0$ is a root. Hence, $x^2 + dx + d^2 + r^2$ and thus $x^2 + x + 1 + (r/d)^2$ must be irreducible. By Lemma 2, we therefore obtain that $1 + (r/d)^2 \in \{1\} \cup S^{-1}$, that is, $(r/d)^2 \in S$. But then $(r/d)^4 \in S$ too. This yields $a_2 \in a_6 d^4 S$. In particular, there can be at most three a_2's, that is, $\mathscr{B}$ contains at most three type 2 hyperovals. Furthermore, $a_6 d^4 \in a_2 S^{-1}$ so that at most three values for $a_6 d^4$ can occur and there can be at most three hyperovals of subtype d for any given d.

Assume that there are $a_6, a'_6, d, d' \in \mathbb{F}_8^*$, $d \neq d'$, such that $a_6 d^4 = a'_6 (d')^4 = c$; in particular $d, d' \neq 0$. Then $a_6 = cd^3$ and $a'_6 = c(d')^3$ and the affine points of intersection of the associated type 6 hyperovals correspond to roots of $(d^5 + (d')^5)x^2 + (d^6 + (d')^6)x$, which has a non-zero root—a contradiction.

This shows that $d \neq d'$ for type 6 hyperovals in $\mathscr{B}$ implies $a_6 d^4 \neq a'_6 (d')^4$. Since at most three values for $a_6 d^4$ can occur, we see that at most three d's can occur. More precisely, if there is a d for which there are three hyperovals of that subtype in $\mathscr{B}$, then no other subtype can occur and we have three hyperovals of type 6 in $\mathscr{B}$. If there is a d, for which there are two hyperovals of that subtype in $\mathscr{B}$, then there is at most one further subtype possible and one associated hyperoval of type 6 and there are at most three hyperovals of type 6 in $\mathscr{B}$. If for each d, there is at most one hyperoval of that subtype in $\mathscr{B}$, then again $\mathscr{B}$ contains at most three type 6 hyperovals. In any case, we find that $\mathscr{B}$ has at most three type 6 hyperovals. But since there are also at most three type 2 hyperovals in $\mathscr{B}$, we cannot make up the seven hyperovals.

This shows that all hyperovals in $\mathscr{B}$ are either of type 2 or of type 6 if only types 2 and 6 occur in $\mathscr{B}$.

If only hyperovals of types 4 and 6 occur in $\mathscr{B}$ we use the collineation σ from Section 2. We then obtain a bundle containing only hyperovals of types 2 and 6. From the previous case, we know that all hyperovals are of the same type. Hence, all hyperovals in $\mathscr{B}$ are either of type 4 or of type 6. $\square$

Proposition 2. *Let $\mathscr{B}$ be a ((0),(0,0))-bundle all whose hyperovals are of type 6. Then there are $d \in \mathbb{F}_8$ and $m \in \{0, 1, 4\}$ such that $\mathscr{B} = \{H^{6,a^m d}_{a,0,a^{1-m}d^6} \mid a \in \mathbb{F}_8^*\}$.*

Proof. It is readily verified that the stated collections of type 6 hyperovals are indeed ((0),(0,0))-bundles.

Assume that the hyperovals $H^{6,d}_{a,0,ad^6}$ and $H^{6,c}_{b,0,bc^6}$ are in $\mathscr{B}$, where $a, b \in \mathbb{F}_8^*$ and $c, d \in \mathbb{F}_8$, $c \neq d$. Then the equation $ax^2(x^2 + dx + d^2)^2 = bx^2(x^2 + cx + c^2)^2$ has the only solution $x = 0$. Hence, the polynomial $a(x^2 + dx + d^2)^2 + b(x^2 + cx + c^2)^2$ and thus the polynomial

$$\begin{aligned} f(x) &= a^4(x^2 + dx + d^2) + b^4(x^2 + cx + c^2) \\ &= (a^4 + b^4)x^2 + (a^4 d + b^4 c)x + (a^4 d^2 + b^4 c^2) \end{aligned}$$

has no root except possibly 0.

Since $c \neq d$ no two of the coefficients of $f(x)$ can be equal to 0. If one of the coefficients is zero, then $f(x)$ has a non-zero root—a contradiction. This shows that $a \neq b, a^4 d \neq b^4 c, a^4 d^2 \neq b^4 c^2$ and thus

$$a \neq b, \quad ad^2 \neq bc^2, \quad ad^4 \neq bc^4. \tag{1}$$

In particular, 0 is not a root of $f(x)$ and $f(x)$ must be irreducible. Lemma 2 then implies that

$$\tfrac{a^4d^2+b^4c^2}{(a+b)^4}/(\tfrac{a^4d+b^4c}{(a+b)^4})^2 = \tfrac{(a+b)^4(a^4d^2+b^4c^2)}{(a^4d+b^4c)^2} = 1 + \tfrac{a^4b^4(c+d)^2}{(a^4d+b^4c)^2} \in \{1\} \cup S^{-1}.$$

But then

$$\frac{a^4b^4(c+d)^2}{(a^4d+b^4c)^2} \in S$$

because $a, b, c+d \neq 0$. However, S is invariant under squaring so that we further obtain

$$\frac{a^2b^2(c+d)}{a^4d+b^4c} \in S. \tag{2}$$

In fact, (2) implies (1) because in the case that $a=b$, $ad^2=bc^2$ or $ad^4=bc^4$, the expression $a^2b^2(c+d)/(a^4d+b^4c)$ becomes 1 or is undefined.

We first assume that a hyperoval of type (6,0) occurs in $\mathscr{B}$. If there also is a hyperoval of subtype $d \neq 0$ in $\mathscr{B}$, then (2) with $c=0$ becomes $b^2/a^2 \in S$ and thus $b/a \in S$. Hence,

$$b \in aS$$

and there can be at most three hyperovals of subtype 0 in $\mathscr{B}$.

It readily follows that the cosets of S in $\mathbb{F}_8^*$ form the lines of a projective plane of order 2. (The set of exponents $\{1,2,4\}$ is a cyclic (7,3,1) difference set modulo 7.) In particular, any two distinct cosets have exactly one point in common and the intersection of mutually distinct four cosets is empty. From this observation we see that, if there are at least two hyperovals of type $(6,0)$ in $\mathscr{B}$, then the 'leading coefficients' a of all the other hyperovals must be the same and there is at most one hyperoval of subtype d in $\mathscr{B}$ for each $d \neq 0$. However, $a \neq a'$ by (1)—a contradiction since there must be at least four different d's. If there is only one hyperoval of subtype 0 in $\mathscr{B}$ we may assume that $H^{6,0}_{1,0,0} \in \mathscr{B}$, that is, $b=1$. Then $a \in S^{-1}$ and for each $d \neq 0$ there are at most three hyperovals of type $(6,d)$ in $\mathscr{B}$. Furthermore, at least two different subtypes $d \neq 0$ must occur. But the leading coefficients for different d's are distinct by (1). This together with the above restrictions imply that there can be at most three hyperovals in $\mathscr{B}$ of type $(6,d)$ with $d \neq 0$. In total, we therefore obtain at most four hyperovals in $\mathscr{B}$—a contradiction.

This shows that either all hyperovals in $\mathscr{B}$ or none are of type $(6,0)$. In the former case, the bundle clearly has the stated form.

We now assume that no hyperoval of type (6,0) is in $\mathscr{B}$. Using a homothety δ_r from Section 2 we may assume that $\mathscr{B}$ contains a hyperoval of subtype 1. Then (1) and (2) for $c=1$ give us $a \neq b, bd^3, bd^5$ and $a^2b^2(d+1)/(a^4d+b^4) \in S$, where $a, d \in \mathbb{F}_8^*$, $d \neq 1$. Since d is a generator of $\mathbb{F}_8^*$, we find that $a \in b\{d, d^2, d^4, d^6\}$. We distinguish whether $d \in S$ or $d \in S^{-1}$. In the former case, we obtain $d^3+d+1=0$ and $d^5+d^4+1=0$. In the latter case, we find $d^3+d^2+1=0$ and $d^5+d+1=0$.

Evaluating $a^2b^2(d+1)/(a^4d+b^4)$ for all possible a's yields the values in the table below.

From this table we see that in any case

$$a \in b\{d, d^2\}.$$

a	$a^2b^2(d+1)/(a^4d+b^4)$	if $d \in S$	if $d \in S^{-1}$
bd	$d^2(d+1)/(d^5+1)$	$= d \in S$	$= d^6 \in S$
bd^2	$d^4/(d+1)$	$= d \in S$	$= d^6 \in S$
bd^4	$d(d+1)/(d^3+1)$	$= d^3 \in S^{-1}$	$= d^4 \in S^{-1}$
bd^6	$d^5/(d+1)^3$	$= d^3 \in S^{-1}$	$= d^4 \in S^{-1}$

In particular, there can be at most two hyperovals of type $(6, d)$ in $\mathscr{B}$ for each $d \neq 0$ and at least four different subtypes must occur in $\mathscr{B}$.

If there are two hyperovals of type (6,1) in $\mathscr{B}$, say without loss of generality, $H^{6,1}_{1,0,1}$ and $H^{6,1}_{b,0,b}$ for some $b \neq 0, 1$, then $\{d, d^2\} \cap b\{d, d^2\}$ is non-empty for each $d \neq 0, 1$ for which there is a hyperoval of that subtype in $\mathscr{B}$. But this condition implies that $d = bd^2$ or $d^2 = bd$, that is $d \in \{b, b^6\}$. This shows that there can be at most two such d's, that is, at most three different subtypes can occur in $\mathscr{B}$. This is a contradiction to what we found before. Hence, either all hyperovals in $\mathscr{B}$ are of type 1 or there is exactly one hyperoval of type (6,1) in $\mathscr{B}$. (After applying homotheties, the former case yields those bundles with $m = 0$.) Furthermore, using the homothety δ_r again, we see that in the latter case there must be exactly one hyperoval of type $(6, d)$ in $\mathscr{B}$ for each $d \neq 0$.

We may assume that the hyperoval $H^{6,1}_{1,0,1}$ is in $\mathscr{B}$. For each $d \neq 0, 1$ then there is precisely one $a \in \{d, d^2\}$ such that $H^{6,d}_{a,0,ad^6}$ is in $\mathscr{B}$.

If there is a $d \neq 0, 1$ such that $H^{6,d}_{d,0,1} \in \mathscr{B}$ (that is, $a = d$), we apply the collineation σ from Section 2. The bundle $\mathscr{B}$ is taken to a $((0), (0,0))$-bundle $\sigma(\mathscr{B})$ that contains $\sigma(H^{6,1}_{1,0,1}) = H^{6,1}_{1,0,1}$ and $\sigma(H^{6,d}_{d,0,1}) = H^{6,1}_{d,0,d}$. Thus, $\sigma(\mathscr{B})$ contains two hyperovals of type (6,1). From what we have seen above this implies that all hyperovals in $\sigma(\mathscr{B})$ must be of type (6,1), that is, $\sigma(\mathscr{B}) = \{H^{6,1}_{a,0,a} \mid a \in \mathbb{F}_8^*\}$, and thus $\mathscr{B} = \{H^{6,a}_{a,0,1} \mid a \in \mathbb{F}_8^*\}$. (After applying homotheties we obtain those bundles with $m = 1$.) If no such d exists we have $a = d^2$ for all $d \in \mathbb{F}_8^*$ and therefore $\mathscr{B} = \{H^{6,d}_{d^2,0,d} \mid d \in \mathbb{F}_8^*\} = \{H^{6,a^4}_{a,0,a^4} \mid a \in \mathbb{F}_8^*\}$. (After applying homotheties this case yields those bundles with $m = 4$.) $\square$

The two preceding Propositions 1 and 2 give us an explicit description of all possible $((0), (0,0))$-bundles of hyperovals which can readily be generalised to bundles that have a different tangent line at $(0,0)$.

Corollary 1. *Let $\mathscr{B}$ be a $((b),(0,0))$-bundle. Then $\mathscr{B}$ has the following form.*

- $\{H^2_{a,b,0} \mid a \in \mathbb{F}_8^*\}$ *in case of hyperovals of type* 2;
- $\{H^4_{a,b,0} \mid a \in \mathbb{F}_8^*\}$ *in case of hyperovals of type* 4;
- *there are* $d \in \mathbb{F}_8$ *and* $m \in \{0,1,4\}$ *such that* $\mathscr{B}$ *is*

$$\mathscr{B}^6_{d,m} = \{H^{6,a^m d}_{a,b,a^{1-m}d^6} \mid a \in \mathbb{F}_8^*\}$$

- *in case of hyperovals of type* 6.

Proof. The hyperovals in a ((0),(0,0))-bundle all have the same type by Proposition 1 and the bundles of type 6 are determined in Proposition 2. The collineation given on the affine part by $(x,y) \mapsto (x, y+bx)$ fixes (∞) and $(0,0)$ and maps (0) to (b) and the form of the hyperovals in bundle $\mathscr{B}$ follows. □

We say that a $((b),(0,0))$-bundle $\mathscr{B}$ is of type n if all hyperovals in $\mathscr{B}$ are of type n. In case of type 6, we further say that the bundle is of *co-type* $m \in \{0,1,4\}$ and *subtype* d, or simply of type $(6,d,m)$, if $\mathscr{B} = \mathscr{B}^6_{d,m}$ as in Corollary 1. Note that in the case of subtype 0 the bundle does not depend on the co-type, that is, $\mathscr{B}^6_{0,m} = \mathscr{B}^6_{0,0}$ for each $m \in \{0,1,4\}$. Apart from this case however, subtype and co-type uniquely determine the bundle.

We now compare different bundles and determine how the hyperovals contained in them intersect. Again we encounter a particular kind of polynomial in the process.

Lemma 4. *The polynomial* $x^5 + \alpha x^3 + \beta x + 1$ *has at least two roots in* $\mathbb{F}_8$ *for* $\alpha = 0$, $\beta = 1$, *or* $\alpha \in S$, $\beta \in \{0, \alpha\}$, *or* $\alpha \in S^{-1}$, $\beta \in \{\alpha, \alpha^3\}$.

Proof. For $\alpha = \beta \neq 0, 1$, the above polynomial has the two roots 1 and α^2 in $\mathbb{F}_8$ and in case $\alpha \in S$, $\beta = 0$ one finds the roots α and α^3. In the remaining two cases where $\alpha = 0$, $\beta = 1$ or $\alpha \in S^{-1}$, $\beta = \alpha^3$, the polynomial has the three roots $\omega^3, \omega^5, \omega^6$ and $\alpha^3, \alpha^4, \alpha^5$, respectively. □

In fact, in all other cases for α and β not listed in the lemma, the polynomial $x^5 + \alpha x^3 + \beta x + 1$ has no or precisely one root in $\mathbb{F}_8$. Note that $\alpha = 1$ does not occur among the possible coefficients for which the polynomial has more than one root. This is at the core of the problem that leads to the exceptional cases in the following proposition.

Proposition 3. *Let $\mathscr{B}$ be a ((0),(0,0))-bundle and $\mathscr{B}'$ be a $((1),(0,0))$-bundle. Assume that each hyperoval in $\mathscr{B}$ intersects each hyperoval in $\mathscr{B}'$ in at most three points. Then all members of $\mathscr{B} \cup \mathscr{B}'$ are of the same type unless one bundle is of type* (6,1,4) *and the other bundle is of type* 2.

Proof. Note that all hyperovals in $\mathscr{B}$ and $\mathscr{B}'$ have the points (∞) and $(0,0)$ in common. Hence, by our assumption each member of $\mathscr{B}$ intersects each member of $\mathscr{B}'$ in at most one affine point different from (0,0).

From Proposition 1, we know that all members of $\mathscr{B}$ are of the same type n and all members of $\mathscr{B}'$ are of the same type n' and we also know the explicit form of the hyperovals in $\mathscr{B}$ and $\mathscr{B}'$ by Corollary 1. We distinguish several cases depending on the types n and n' and exclude all situations except the ones in the statement. Since the collineation given on the affine part by $(x,y)\mapsto(x,y+x)$ fixes $(0,0)$ and (∞) and interchanges the points (0) and (1), we can interchange the roles of $\mathscr{B}$ and $\mathscr{B}'$, that is, we may assume that $n\geqslant n'$. Finally note that, irrespective of the co-type m, a bundle of the form $\mathscr{B}^6_{d,m}$ contains the hyperoval $H^{6,d}_{1,0,d^6}$.

Case 1: $n=4$ and $n'=2$.

In this case $H^4_{1,0,0}\in\mathscr{B}$ and $H^2_{1,1,0}\in\mathscr{B}'$ by Corollary 1. The affine points of intersection of these hyperovals correspond to the roots of

$$x^4+x^2+x=x(x^3+x+1)=x(x+\omega)(x+\omega^2)(x+\omega^4).$$

Hence, $H^4_{1,0,0}\cap H^2_{1,1,0}$ contains five points—four affine points associated with the roots and the point (∞). This contradicts our assumption on the number of points of intersection members of $\mathscr{B}$ with members of $\mathscr{B}'$. Therefore, types 2 and 4 both occurring is not possible.

Case 2: $n=6$ and $n'=2$.

By Corollary 1, there is a $d\in\mathbb{F}_8$ such that $H^{6,d}_{1,0,d^6}\in\mathscr{B}$ and $H^2_{a',1,0}\in\mathscr{B}'$ for all $a'\in\mathbb{F}_8^*$. The affine points of intersection of these hyperovals correspond to the roots of

$$x^2(x^2+dx+d^2)^2+a'x^2+x=x(x^5+d^2x^3+(d^4+a')x+1).$$

We distinguish the cases $d=0$, $d=1$, $d\in S$ and $d\in S^{-1}$. In the first and last cases, we let $a'=1$ and in the third cases, we let $a'=d$. The resulting polynomials then have at least three different roots by Lemma 4 (root 0 and at least two roots from the quintic factor). Hence, the hyperovals intersect in at least four points.

Finally, in the case $d=1$ we have to use the full bundle $\mathscr{B}$. There is an $m\in\{0,1,4\}$ such that $\mathscr{B}=\mathscr{B}^6_{1,m}$. The affine points of intersection of $H^{6,a^m}_{a,0,a^{1-m}}\in\mathscr{B}$ with $H^2_{a',1,0}$ correspond to the roots of

$$\begin{aligned}&x(ax^5+a^{2m+1}x^3+(a^{4m+1}+a')x+1)\\&\quad=x((bx)^5+a^{2m-1}(bx)^3+(a^{4m-2}+a^4a')(bx)+1),\end{aligned}$$

where $a=b^5$, that is, $b=a^3$. If $r=a^{2m-1}$ the second factor on the right-hand side becomes

$$u^5+ru^3+(r^2+t)u+1,$$

where $u=bx$ and $t=a^4a'$. Note that for $m=0,1,4$ we obtain $r=a^6,a,1$, respectively. Therefore, the map $a\mapsto r$ is a permutation of $\mathbb{F}_8^*$ for $m=0,1$ and is constant for $m=4$.

For $r \in S$ we let $t = r^2$ and for $r \in S^{-1}$ we let $t = 1$. Then the resulting quintic polynomial in u has at least two roots by Lemma 4. Hence, the corresponding hyperovals have at least four points in common. This shows that $m = 0$ or 1 is not possible.

For $m = 4$ however, we obtain $u^5 + u^3 + (1 + t)u + 1$ which has precisely one zero for each $t \in \mathbb{F}_8$, $t \neq 1$ and is irreducible for $t = 1$.

This shows that types 2 and 6 both occurring is not possible except when $d = 1$ and $m = 4$.

Case 3: $n = 6$ and $n' = 4$.

By Corollary 1, there is a $d \in \mathbb{F}_8$ such that $H^{6,d}_{1,0,d^6} \in \mathscr{B}$ and $H^4_{a',1,0} \in \mathscr{B}'$ for all $a' \in \mathbb{F}_8^*$. The affine points of intersection of these hyperovals correspond to the roots of

$$x^2(x^2 + dx + d^2)^2 + a'x^4 + x = x(x^5 + (d^2 + a')x^3 + d^4x + 1).$$

We distinguish the cases $d = 0$, $d = 1$, $d \in S$ and $d \in S^{-1}$. In the respective cases, we let $a' \in S$, $a' = 1$, $a' = d$ and $a' = d + 1$. The resulting polynomials then have at least three roots, 0 and at least two roots from the quintic factor, by Lemma 4. Hence, the hyperovals have at least four points in common.

This shows that types 4 and 6 both occurring is not possible. □

We next show that in case of two type 6 bundles only co-types 0 and 4 can occur and that all hyperovals in the two bundles must have the same subtype. Note that since, in the notation of Section 2, the Laguerre planes $\mathscr{L}^{3,d}$ exist, the bundles of co-type 0 exist as stated in the following proposition.

Proposition 4. *Let $\mathscr{B}$ be a ((0),(0,0))-bundle and $\mathscr{B}'$ be a ((1),(0,0))-bundle, both of type 6. Assume that each hyperoval in $\mathscr{B}$ intersects each hyperoval in $\mathscr{B}'$ in at most three points. Then $\mathscr{B}$ and $\mathscr{B}'$ are both of co-type 0 and subtype d for some $d \in \mathbb{F}_8$ or both bundles are of co-type 4 and have subtypes d and d', where either $d = d' = 1$ or $(d + 1)(d' + 1) = 1$, $d, d' \neq 0$.*

Proof. From Corollary 1, we know the explicit form of the hyperovals in $\mathscr{B}$ and $\mathscr{B}'$. We assume that $\mathscr{B}$ and $\mathscr{B}'$ are of type $(6, m, d)$ and $(6, m', d')$, respectively. As in the proof of Proposition 3 we see that the roles of $\mathscr{B}$ and $\mathscr{B}'$ can be interchanged and that each member of $\mathscr{B}$ intersects each member of $\mathscr{B}'$ in at most one affine point different from $(0, 0)$. Hence, we may assume that $d' = 0$ if one of d, d' is 0 or that $m \geqslant m'$. Also note that a $(6, m', d')$ bundle is taken by a homothety δ_r to a $(6, m', r^{1-2m'}d')$ bundle so that we may assume that $d' = 0, 1$ for $m' \neq 4$.

The affine points of intersection of $H^{6,a^m d}_{a,0,a^{1-m}d^6} \in \mathscr{B}$ and $H^{6,a^{m'}d'}_{a',1,(a')^{1-m'}(d')^6} \in \mathscr{B}'$ correspond to the roots of

$$x((a + a')x^5 + (a^{2m+1}d^2 + (a')^{2m'+1}(d')^2)x^3 + (a^{4m+1}d^4 + (a')^{4m'+1}(d')^4)x + 1)$$

so that by our assumptions on the number of points of intersection the polynomial

$$(a+a')x^5 + (a^{2m+1}d^2 + (a')^{2m'+1}(d')^2)x^3 + (a^{4m+1}d^4 + (a')^{4m'+1}(d')^4)x + 1 \tag{3}$$

can have at most one root in $\mathbb{F}_8$.

If $a \neq a'$ we let $u = (a+a')^3 x$. Then the above polynomial (3) becomes

$$u^5 + \alpha u^3 + \beta u + 1,$$

where

$$\alpha = (a^{2m+1}d^2 + (a')^{2m'+1}(d')^2)(a+a')^5,$$
$$\beta = (a^{4m+1}d^4 + (a')^{4m'+1}(d')^4)(a+a')^4.$$

This polynomial too can have at most one root in $\mathbb{F}_8$.

Similarly, if $a = a'$ and $t = a^{2m+1}d^2 + a^{2m'+1}(d')^2 \neq 0$ we let $v = t^5 x$. Then the polynomial (3) becomes

$$v^3 + \gamma v + 1,$$

where

$$\gamma = (a^{4m+1}d^4 + a^{4m'+1}(d')^4)(a^{2m+1}d^2 + a^{2m'+1}(d')^2)^2.$$

This polynomial in v has more than one root in $\mathbb{F}_8$ if and only if γ is equal to 1.

We distinguish several cases depending on the co-types and subtypes and exclude all situations except the ones in the statement. The strategy is to find suitable a's and a's in those cases we want to exclude so that polynomial (3) has at least two roots, that is, $\gamma = 1$ if $a = a'$ or α and β satisfy the conditions from Lemma 4 for $a \neq a'$.

Case 1: $m < 4$, $d \neq 0 = d'$.

Let $a = a' = d^{3m+2}$. Then $t = d^{6-m} \neq 0$ and $\gamma = 1$.

Case 2: $m = 4$, $d \neq 0 = d'$.

If $d = 1$, we let $a = a' = 1$. Then $t = 1 \neq 0$ and $\gamma = 1$. For $d \neq 1$ we let $a = 1$ and $a' = 1 + d^2$. Then $a' \neq 0, a$ and $\alpha = \beta = d^5 \neq 0, 1$.

Case 3: $m = 4 > m'$, $d \neq 0$, $d' = 1$.

We choose $a \in (d^{5-3m'} + dS)$, $a \neq 0$. Let $a' = (a^3 d^4)^{2m'+1} = a^{3-m'} d^{m'+4}$. Then $a' \neq 0$ and $a + a' = ad^{4+m'}(a^{2-m'} + d^{3-m'}) = ad^{4+m'}(a + d^{5-3m'})^{2-m'}) \neq 0$. (Note that $(m')^2 = m'$ in this case.) Furthermore, $\alpha = d^{3+2m'}(a + (d^{5-3m'})^{4-2m'} \in S$, $\beta = 0$.

Case 4: $m = 1$, $m' = 0$, $d \neq 0$, $d' = 1$.

We choose $r \in d^6 S \cap S$. Such an r exists because the cosets of S in $\mathbb{F}_8^*$ form the lines of a projective plane of order 2; compare the proof of Proposition 2. Let $a = r^2 d^6$ and $a' = r^3 d^6$. Then $a, a' \neq 0$ and $a + a' = r^2(r+1)d^6 = r^5 d^6 \neq 0$. Moreover, $\alpha = rd \in S$ and $\beta = 0$.

Case 5: $m = m' = 0$, $d \neq d'$.

Let $a = a' = (d+d')^2$. Then $a \neq 0$, $t = (d+d')^6 \neq 0$ and $\gamma = 1$.

Case 6: $m = m' = 1$, $d \neq 0$, $d' = 1$.

We choose $r \in S$ such that $r \neq d^2, d^4, d^6$. Such an r exists because S has three members of which at most two are excluded. (Note that d^2 and d^6 cannot be both in S.) Let $a' = (r+1)(r^3 + d^5)(r^5 + d^3)^6 d^5$ and $a = ra'$. By our choice of r we have $a, a', a + a' \neq 0$. Furthermore, $\alpha = \beta = (r+1)^6 (r^3 + d^5)^2 (r^5 + d^3)^6 \neq 0, 1$.

Case 7: $m = m' = 4$, $d = d' \neq 0, 1$.

Let $a' = 1$ and $a = d^5$ if $d \in S$ or $a = d^2$ if $d \in S^{-1}$. Then $\alpha = d^2$ and $\beta = \alpha$ for $d \in S$ and $\beta = \alpha^3$ for $d \in S^{-1}$.

Case 8: $m = m' = 4$, $d, d' \neq 0$, $d \neq d'$, $(d+1)(d'+1) \neq 1$.

For $d + d' = 1$ we let $a = a' = 1$. Then $t = (d + d')^2 \neq 0$ and $\gamma = d + d' = 1$. For $d + d' \in S$ we let $a' = 1$ and $a = d(d')^6$. Then $a + a' = (d + d')(d')^6 \neq 0$ and $\alpha = (d + d')^2 \in S$, $\beta = 0$. If $d + d' \in S^{-1}$, we distinguish the cases $d = 1$, $d' = 1$, $dd' = 1$. In the first case, we have $d' \in S$ and we let $a = (d')^3$, $a' = 1$. Then $a + a' \neq 0$ and $\alpha = \beta = (d')^5 \in S$. If $d' = 1$, we have $d \in S$ and we let $a = d^2$, $a' = 1$. Then $a + a' \neq 0$ and $\alpha = \beta = d^4 \in S$. In the last case where $dd' = 1$ we let $a = d^4$, $a' = 1$. Then $\alpha = d^3(d+1) \in S^{-1}$ and $\beta = \alpha^3$. The remaining possibilities for d and d' such that $d + d' \in S^{-1}$ then are $(d+1)(d'+1) = 1$.

Note that conversely $(d+1)(d'+1) = 1$ implies that either $d = d' = 0$ or $d, d' \neq 0$, $d \neq d'$ and $d + d' \in S^{-1}$. □

The existence of the exceptional cases of co-type 4 bundles in the two preceding propositions is intriguing and remarkable. In fact, we can form bundles of hyperovals and lines through (0,0) that look like the collection of all circles through a point in a Laguerre plane. We call a collection $\mathscr{B}_0$ of hyperovals a *point bundle* or more specifically a *p-bundle*, where p is an affine point if $\mathscr{B}_0$ is made up of $((b), p)$-bundles such that $\mathscr{B}_0$ contains a $((b), p)$-bundle for each $b \in \mathbb{F}_8$ and such that any two distinct members of $\mathscr{B}_0$ intersect in at most three points.

Proposition 5. *Let $\mathscr{B}_0$ be a* (0,0)*-bundle. Then all tangent bundles in $\mathscr{B}_0$ are of the same type or there is a $c \in \mathbb{F}_8$ such that $\mathscr{B}_0$ consists of all hyperovals*

$$\{(x, x^2(a^6 + b^6 x)^6 + cx) \mid x \in \mathbb{F}_8\} \cup \{(\infty), (b + c)\}$$

for $a, b \in \mathbb{F}_8$, $a \neq 0$.

Proof. By applying a collineation $\gamma_{t,s}$ given on the affine part by $(x, y) \mapsto (x, ty + sx)$ for $s, t \in \mathbb{F}_8$, $t \neq 0$ we can achieve that any particular tangent bundle in $\mathscr{B}_0$ passes through the points at infinity (0) and (1), respectively. Such a transformation does not change the type or co-type of a tangent bundle and a $(6, 4, d)$-type bundle is taken to a bundle of type $(6, 4, t^3 d)$. Hence, by Proposition 3, any two tangent bundles in $\mathscr{B}_0$ are of the same type or one of the transformed tangent bundles is of type 2 and the other is of type (6,4,1).

We first exclude the case that $\mathscr{B}_0$ contains two type 2 bundles and one tangent bundle of type 6. Using a transformation $\gamma_{t,s}$ we may assume that the $((0), (0,0))$-bundle in $\mathscr{B}_0$ is of type 6 and that the $((1), (0,0))$- and $((r), (0,0))$-bundles for some

$r \neq 0, 1$ in $\mathscr{B}_0$ are of type 2. The $((0),(0,0))$-bundle then is of type (6,4,1) and using $\gamma_{r^6,0}$ we see that the $((0),(0,0))$-bundle must also be of type $(6,4,r^3)$—a contradiction because $r \neq 1$.

This shows that if different types occur in $\mathscr{B}_0$, then one tangent bundle must be of type 2 and all the others must be of type 6. We may assume that the $((0),(0,0))$-bundle is of type 2. An $((r),(0,0))$-bundle, where $r \neq 0$ is taken under $\gamma_{r^6,0}$ to an $((1),(0,0))$-bundle which then must be of type (6,4,1) by Proposition 3. Hence, the original $((r),(0,0))$-bundle has type $(6,4,r^4)$. The hyperovals in these tangent bundles are then of the form $H^{6,a^4r^4}_{a,r,a^4r^3}$. In the affine part, these bundles are described by

$$\begin{aligned} y &= a(x + a^4r^4)^6 + rx + a^4r^3 \\ &= ax^6 + a^2rx^4 + a^3r^2x^2 + rx^8 \\ &= x^2(rx^6 + ax^4 + a^2r^2x^2 + a^3r^2) \\ &= x^2(r^6x + a^4r^5)^6. \end{aligned}$$

Hence, we obtain the form as stated. $\square$

Note that $x^2(a^6 + b^6x)^6 + cx = ax^2 + a^3b^5x^5 + a^5b^3x^6 + (b+c)x$ for $x \in \mathbb{F}_8$. Hence, we obtain the hyperoval $H^2_{a,c,0}$ for $b = 0$ and $H^{6,a^6b}_{a^5b^3,b+c,a^6b^2} \in \mathscr{B}^6_{b^3,4}$ for $b \neq 0$. Furthermore, for $a = 0$ we obtain on the affine part the line $y = (b+c)x$. So $\mathscr{B}_0$ extended by the lines through $(0,0)$ looks very much like the bundle of circles through (0,0). Indeed, the transformation $(x,y) \mapsto (x^6, x(y+cx)^6)$ for $x \in \mathbb{F}_8^*$ maps $y = x^2(a^6 + b^6x)^6 + cx$ onto $y = a^6x + b^6$ so that lines and hyperovals in the extended bundle intersect in the right number of points.

Proposition 6. *Let $\mathscr{B}_0$ be a* (0,0)*-bundle such that all tangent bundles in $\mathscr{B}_0$ are of type* 6. *Then all tangent bundles are of co-type* 0 *and have the same subtype.*

Proof. Let $(6, m_r, d_r)$ be the type of the $((r),(0,0))$-bundle in $\mathscr{B}_0$ for $r \in \mathbb{F}_8$. By Proposition 4, the tangent bundles are either all of co-type 0 or all of co-type 4.

Suppose the latter. The transformation δ_{1,r^6}, where $r \neq 0$, takes the $((r),(0,0))$-bundle to a ((1),(0,0))-bundle of subtype r^4d_r and the ((0),(0,0))-bundles is transformed into one of subtype r^4d_0. By applying Proposition 2, we obtain that either $d_r = d_0 = r^3$ or $(r^4d_r + 1)(r^4d_0 + 1) = 1$, that is, $d_r = d_0 + d_0^2(r^3 + d_0)^6$ in both cases. Note that the map $r \mapsto d_r$ is injective so that the d_r's are mutually distinct for $r \neq 0$.

Let $s \in \mathbb{F}_8^*$ be the unique element such that $d_0 = s^3$. The transformation $\gamma_{(r+s)^6,s}$ given on the affine part by $(x,y) \mapsto (x, (r+s)^6y + sx)$ for $r \neq 0, s$ maps the $((s),(0,0))$-and $(r),(0,0))$-bundles onto ((0),(0,0))- and ((1),(0,0))-bundles, respectively. For the transformed subtypes we thus have by Proposition 4 that $((r+s)^4 d_s+1)((r+s)^4 d_r+1)=1$. Since $d_s=d_0=s^3$ we find $(r+s)^4 d_r = 1+r^3s^4 = r^3(r+s)^4$, that is, $d_r=r^3$. However, the formula for d_r found above yields $d_r = s^3+s^6(r^3+s^3)^6=(r+s)^3 \neq r^3$. This shows that co-type 4 is not possible.

Hence, all tangent bundles in $\mathscr{B}_0$ are of co-type 0. In this case, $\delta_{1/r,1}$ does not change the subtype and Proposition 4 finally yields that all tangent bundles have the same subtype. □

We call a circle of $\mathscr{L}$ an *H-circle* if it does not pass through the distinguished point p and an *L-circle* if it passes through p. Such a circle then induces a hyperoval and a line in $\mathscr{P}$, respectively. In transferring the notions of type, subtype and co-type to circles we say that an H-circle of $\mathscr{L}$ is of type $n \in \{2,4,6\}$, subtype d or co-type $m \in \{0,1,4\}$ if the associated hyperoval in $\mathscr{P}$ is of that type, subtype or co-type. With this notation, we have the following.

Proposition 7. *All H-circles are of the same type. In case of type* 6 *all H-circles are furthermore of the same subtype and of co-type* 0.

Proof. Let C be a circle of type n not passing through p and let $q \in C$ be a point of $\mathscr{A}_p$. We consider the collection $\mathscr{B}_q$ of all H-circles in $\mathscr{L}$ through q. In $\mathscr{A}_p$, any two of these circles intersect in q and at most one further point. Furthermore, for each such circle $C' \in \mathscr{B}_q$ there is a circle L through p and q that touches C' at q. Hence, $\mathscr{B}_q$ is the union of tangent bundles $\mathscr{B}_L$ to L-circles through q.

We now look at the situation induced in $\mathscr{P}$. We obtain a bundle $\mathscr{B}'_q$ of hyperovals through q and this bundle contains an hyperoval of type n (associated with the circle C). Using an elation of $\mathscr{P}$ with axis W, we may assume that $q=(0,0)$. Note that collineations of $\mathscr{P}$ that fix (∞) and W preserve the type. Hence, $\mathscr{B}'_q$ represents a (0,0)-bundle in $\mathscr{P}$. By Propositions 5 and 6, all hyperovals in $\mathscr{B}'_q$ are of type n unless we have the exceptional point bundle from Proposition 5.

Suppose that there is a point q such that the point bundle $\mathscr{B}'_q$ is of mixed type. Then every point bundle $\mathscr{B}_{q'}$ must be of mixed type. In particular, we have $(0,i)$-bundles $\mathscr{B}_i$, $i=0,1$, in $\mathscr{P}$. Using the translation $(x,y)\mapsto(x,y+1)$, we see from Proposition 5 that there must be $c_i \in \mathbb{F}_8$ such that the hyperovals in $\mathscr{B}_i$ are given by

$$H^i_{a,b} = \{(x, x^2(a^6+b^6x)^6+c_ix+i) \mid x \in \mathbb{F}_8\} \cup \{(\infty),(b+c_i)\}$$

for $a,b \in \mathbb{F}_8$, $a \neq 0$.

We first assume that $c_0 \neq c_1$. Let $c=c_0+c_1 \neq 0$ and $s \in S$. But then $H^0_{c^2s^4,cs^3} \cap H^1_{c^2s,cs} = \{(\infty),(cs+c_1),(c^6s^5,c_1c^6s^5),(c^6s^3,s^2+c_1c^6s^3)\}$ in contradiction to Lemma 1. This shows that $c_0=c_1$. However, then $H^0_{1,1}$ and $H^1_{1,0}$ have the five points (∞), (1,0) and (s,s^6) for $s \in S$ in common—again a contradiction to Lemma 1.

This shows that no point bundles of mixed type can occur, that is, all hyperovals in $\mathscr{B}'_q$ are of the same type. In case of type 6, Proposition 6 further shows that all hyperovals in $\mathscr{B}'_q$ must have co-type 0 and the same subtype.

Let C be a circle not passing through p. All H-circles that intersect C in at least one point of $\mathscr{A}_p$ have the same type as C by what we have seen above. Now every H-circle intersects at least one of these circles in at least one point and thus must have the same type as C again by the above. The same argument applies for subtypes and co-types in case of type 6. $\square$

Proposition 7 gives us an explicit description of the affine part of a Laguerre plane with respect to a point p. The Laguerre plane 'almost' looks like an ovoidal Laguerre plane.

Corollary 2. *Let $\mathscr{L}$ be a Laguerre plane of order* 8 *and let G be a generator of $\mathscr{L}$. Then the geometry $\mathscr{L}\backslash G$ induced by $\mathscr{L}$ on the complement of G is isomorphic to the geometry induced by an ovoidal Laguerre plane $\mathscr{L}^k$, $k = 1, 2, 3$, see Section* 2, *on the complement of the generator $\{\infty\} \times \mathbb{F}_8$.*

Proof. Let p be a point on G. From Proposition 7, we know that all H-circles of $\mathscr{L}$ have the same type and, in case of type 6, the same subtype and co-type 0. Together with the non-vertical lines of the derived affine plane $\mathscr{A}_p$ at p we thus find that the traces of circles on $\mathscr{A}_p$ are represented by the sets $C_{a,b,c} = \{a(x+d)^n + bx + c \mid x \in \mathbb{F}_8\}$ for $a, b, c \in \mathbb{F}_8$, where $n = 2, 4$ or 6 and $d \in \mathbb{F}_8$ are fixed and $d = 0$ unless $n = 6$. There are $8^3 = 512$ of these sets and there are 512 circles in $\mathscr{L}$. Since any two of these sets intersect in at most two points, we obtain that each $C_{a,b,c}$ in fact occurs as the trace of a circle of $\mathscr{L}$. But the collection of all $C_{a,b,c}$'s is just the affine part of an ovoidal Laguerre plane $\mathscr{L}^1$, $\mathscr{L}^2$ or $\mathscr{L}^{3,d}$ as described in Section 2 when the generator $G_\infty = \{\infty\} \times \mathbb{F}_8$ is deleted.

As already mentioned at the end of Section 2, in case $n = 6$ the transformation of $\mathbb{F}_8 \times \mathbb{F}_8$ given by $(x, y) \mapsto (x + d, y)$ provides and isomorphism from $\mathscr{L}^{3,d}\backslash G_\infty$ onto $\mathscr{L}^{3,0}\backslash G_\infty$. Hence, we can assume that $d = 0$ and we obtain the affine part of the Laguerre plane $\mathscr{L}^3 = \mathscr{L}^{3,0}$. $\square$

The remaining problem now is how the affine part extends to a Laguerre plane, that is, how the extra generator fits in. From Section 2, we know that, in general, this can be done in at least two ways for $\mathscr{L}^k$, where $k = 1, 2$. In our situation however, we already know from the way we obtained the affine part what the H- and the L-circles are.

We use the notation

$$C^k_{a,b,c} = \{ax^{2k} + bx + c \mid x \in \mathbb{F}_8\}$$

for $a, b, c \in \mathbb{F}_8$, where $k = 1, 2$ or 3 and call $C^k_{a,b,c}$ a *trace of a circle* or simply a *T-circle*. Then $\{C^k_{0,b,c} \mid b, c \in \mathbb{F}_8\}$ is the collection of traces of L-circles so that each $C^k_{0,b,c}$ is to be augmented by the point at infinity $(\infty, 0)$.

Lemma 5. *The polynomial* $ax^{2k} + bx + c$*, where* $a, b, c \in \mathbb{F}_8$ *and* $k \in \{1, 2, 3\}$ *has precisely one root in* $\mathbb{F}_8$ *if and only if* $a = 0$*,* $b \neq 0$ *or* $a \neq 0$*,* $b = 0$*.*

Proof. Since the map $u \mapsto u^{2k}$ is a permutation of $\mathbb{F}_8$ it readily follows that $f(x) = ax^{2k} + bx + c$ has precisely one root in $\mathbb{F}_8$ if $a = 0$, $b \neq 0$ or $a \neq 0$, $b = 0$.

For $a, b \neq 0$, let $d \in \mathbb{F}_8^*$ be defined by $d^{2k-1} = b/a$. Then

$$f(x) = ad^{2k}\left(\left(\frac{x}{d}\right)^{2k} + \frac{x}{d} + \frac{c}{bd}\right).$$

The map $\mathbb{F}_8 \to \mathbb{F}_8$ given by $u \mapsto u^{2k} + u$ has range $\{0\} \cup S$ for $k \in \{1, 2\}$ and $\{1\} \cup S^{-1}$ for $k = 3$. Moreover, each value occurs precisely twice. (For $k = 1$ or 2, the map is additive and u and $u + 1$ have the same image.) Hence, $f(x)$ has either two roots or none if $a, b \neq 0$. $\square$

From Corollary 1, we know that the collection $\{C^k_{a,0,0} \mid a \in \mathbb{F}_8\}$ of T-circles forms a tangent bundle to $C^k_{0,0,0}$ at the point $(0, 0)$. Since the corresponding circles in $\mathscr{L}$ cannot intersect in any point other than $(0, 0)$, each $C^k_{a,0,0}$ must be augmented by a different point at infinity and there is no loss of generality to assume that $C^k_{a,0,0}$ is augmented by the point (∞, a).

Proposition 8. *Under the assumptions above a* T*-circle,* $C^k_{a,b,c}$ *must be augmented by the point at infinity* (∞, a)*.*

Proof. The statement is certainly true for $a = 0$ or $b = c = 0$.

For $a \neq 0$, all H-circles through (∞, a) essentially form the lines of an affine plane, the derived affine plane $\mathscr{A}_{(\infty,a)}$ at that point. In particular, all these lines except the eight lines parallel to $C^k_{a,0,0}$ intersect $C^k_{a,0,0}$ in precisely one point. Furthermore, of these, different lines have at most one point in common.

From Lemma 5, we obtain that there are precisely two kinds of T-circles that intersect $C^k_{a,0,0}$ in precisely one point. The first kind consists of the T-circles $C^k_{a,b,c}$ for $b, c \in \mathbb{F}_8$, $b \neq 0$ and then there are the T-circles, $C^k_{a',0,c}$ for $a', c \in \mathbb{F}_8$, $a' \neq a$. For the latter kind of T-circles we further obtain that $a' \neq 0$ so that there are $6 \cdot 8 = 48$ circles of this kind.

There must be 56 T-circles that have precisely one point in common with $C^k_{a,0,0}$. Since there are only 48 T-circles of the second kind we need at least eight T-circles of the first kind. Suppose that there is a T-circle $C^k_{a',0,c}$ of the second kind in $\mathscr{A}_{(\infty,a)}$. Lemma 5 then shows that $C^k_{a',0,c}$ meets each T-circle of the first kind in no or two points. Since the latter alternative cannot occur in the derived affine plane we see that $C^k_{a',0,c}$ must have no point in common with any T-circle of the first kind in $\mathscr{A}_{(\infty,a)}$, that is, each T-circle of the first kind in $\mathscr{A}_{(\infty,a)}$ is a parallel to $C^k_{a',0,c}$. From what we said before this implies that there are at least eight lines $\neq C^k_{a',0,c}$ parallel to $C^k_{a',0,c}$.

Since this cannot occur in an affine plane of order 8, we conclude that there cannot be any T-circle of the second kind in $\mathscr{A}_{(\infty,a)}$. Hence, each of the 56 T-circles of the second kind must belong to $\mathscr{A}_{(\infty,a)}$, that is, each $C^k_{a,b,c}$ for $b, c \in \mathbb{F}_8$, $b \neq 0$ must be augmented by (∞, a).

Regarding the remaining lines in $\mathscr{A}_{(\infty,a)}$, that is, the lines parallel to $C^k_{a,0,0}$, we repeat the argument above for the T-circle $C^k_{a,1,0}$ to conclude that $C^k_{a,0,c}$ for $c \in \mathbb{F}_8$ is also augmented by (∞, a). $\square$

Proof of Theorem 1. Let $\mathscr{L}$ be a Laguerre plane of order 8 and let p be a point of $\mathscr{L}$. Corollary 2 shows that $\mathscr{L} \setminus G$ is isomorphic to $\mathscr{L}^k \setminus G_\infty$ for some $k \in \{1, 2, 3\}$, where G is the generator in $\mathscr{L}$ that contains the point p. On the complement of G circles of $\mathscr{L}$ are therefore represented as T-circles $C^k_{a,b,c}$ for $a, b, c \in \mathbb{F}_8$. Given that the point p has coordinates $(\infty, 0)$, Proposition 8 then shows that $C^k_{a,b,c}$ passes through the point at infinity (∞, a) and we obtain the same circles as in the ovoidal Laguerre plane $\mathscr{L}^k$, that is, $\mathscr{L}$ is isomorphic to $\mathscr{L}^k$. As seen in Section 2, the plane $\mathscr{L}^3$ is isomorphic to $\mathscr{L}^2$. In summary, this shows that $\mathscr{L}$ is isomorphic to either $\mathscr{L}^1$, the Miquelian Laguerre plane of order 8, or the ovoidal Laguerre plane $\mathscr{L}^2$. In particular, $\mathscr{L}$ itself is ovoidal. $\square$

References

[1] Y. Chen, G. Kaerlein, Eine Bemerkung über endliche Laguerre- und Minkowski-Ebenen, Geom. Dedicata 2 (1973) 193–194.

[2] A. Delandtsheer, Dimensional linear spaces, in: F. Buekenhout (Ed.), Handbook of Incidence Geometry, Buildings and Foundations, Elsevier, Amsterdam, 1995, pp. 193–294.

[3] M. Hall, J.D. Swift, R.J. Walker, Uniqueness of the projective plane of order eight, Math. Tables Aids Comput. 10 (1956) 186–194.

[4] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, Oxford, 1979.

[5] D.R. Hughes, F.C. Piper, Projective Planes, Springer, New York, 1973.

[6] C.W.H. Lam, L. Thiel, S. Swiercz, The nonexistence of finite projective planes of order 10, Canad. J. Math. 41 (1989) 1117–1123.

[7] S.E. Payne, J.A. Thas, Generalized quadrangles with symmetry, Part II, Simon Stevin 49 (1976) 81–103.

[8] B. Segre, Ovals in a finite projective plane, Canad. J. Math. 7 (1955) 414–416.

[9] B. Segre, Sui k-archi nei piani finiti di caratteristica due, Rev. Math. Pures Appl. 2 (1957) 289–300.

[10] B. Segre, Ovali e curve σ nei piani di Galois di carattersitica due, Atti Accad. Naz. Lincei Rend. 32 (1962) 785–790.

[11] G.F. Steinke, A remark on Benz planes of order 9, Ars Combin. 34 (1992) 257–267.

[12] M.G. Tarry, Le problème des 36 officiers, Comptes rendus Ass. Franc. Advanc. Sci. natur 1 (1900) 122–123; 2 (1901) 170–203.

[13] J.A. Thas, Complete arcs and algebraic curves in PG$(2, q)$, J. Algebra 106 (1987) 451–464.