Sublines of prime order contained in the set of internal points of a conic

Michel Lavrauw

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Jordi Girona 1-3, Mòdul C3, Campus Nord, 08034 Barcelona, Espanya
lavrauw@mat.upc.es

Keywords Internal points of a conic, flock, ovoid, egg, semifield.

Abstract

In [2] it was shown that if $q \geq 4n^2-8n+2$ then there are no subplanes of order q contained in the set of internal points of a conic in $\mathrm{PG}(2,q^n)$, q odd, $n \geq 3$. In this article we improve this bound in the case where q is prime to $q > 2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$, and prove a stronger theorem by considering sublines instead of subplanes. We also explain how one can apply this result to flocks of a quadratic cone in $\mathrm{PG}(3,q^n)$, ovoids of $Q(4,q^n)$, rank two commutative semifields, and eggs in $PG(4n-1,q)$.

1 Introduction

Consider a non-degenerate conic $\mathcal{C}$ in a projective plane $\mathrm{PG}(2,q)$ of order q. If q is even, then all the tangents of the conic meet in a common point, called *the nucleus*, and hence every other point of the plane is contained in exactly one tangent line to $\mathcal{C}$. If q is odd then a point of the plane not contained in $\mathcal{C}$ is either contained in two tangent lines of $\mathcal{C}$, in which case the point is called an *external point*, or is not contained in a tangent line of $\mathcal{C}$, and we call such a point an *internal point*. We denote the set of internal points of $\mathcal{C}$ by $\mathcal{I}(\mathcal{C})$. If $Q(X,Y,Z)$ is the quadratic form defining the conic $\mathcal{C}$ in $\mathrm{PG}(2,q)$, q odd, then either $\mathcal{I}(\mathcal{C})$ is the set of points of $\mathrm{PG}(2,q)$ defined by the vectors (x,y,z) for which $Q(x,y,z)$ is a non-zero square in $\mathrm{GF}(q)$ or the set of points defined by the vectors (x,y,z) for which $Q(x,y,z)$ is a non-square in $\mathrm{GF}(q)$, see [10].

Let $\mathcal{C}$ be a non-degenerate conic of $\mathrm{PG}(2,q^n)$, q odd, $n \geq 3$, defined by the quadratic form $Q(X,Y,Z)$. If $\mathcal{I}(\mathcal{C})$ contains a subplane π isomorphic to $\mathrm{PG}(2,q)$, then without loss of generality we may assume that the subplane is the set of points defined by all non-zero vectors (x,y,z) with $x,y,z \in \mathrm{GF}(q)$, and that $Q(x,y,z)$ is a non-zero square for all $x,y,z \in \mathrm{GF}(q)$. In particular, $f(X) := Q(X,1,0)$ will only take non-zero square values for all $x \in \mathrm{GF}(q)$. In [2] such polynomials $f(X)$ were characterised and as a corollary it was

shown that such subplanes cannot exist if $q \geq 4n^2 - 8n + 2$. We will show that if q is a prime, then this bound can be improved (roughly by a factor $1/2$), using the same techniques and an estimate on the sum of the Legendre symbols of polynomials by Mit'kin [11]. In fact we will show that in that case there does not exist an external line containing a subline contained in $\mathcal{I}(\mathcal{C})$ or contained in the set of external points of $\mathcal{C}$, and show that this implies the non-existence of such a subplane. This result has immediate implications for the existence of semifield flocks of a quadratic cone in $\mathrm{PG}(3, q^n)$, translation ovoids of $Q(4, q^n)$, eggs of $\mathrm{PG}(4n, 1, q)$ and translation generalized quadrangles. However, because of the weaker hypotheses, it turns that the result can also be applied to flocks different from semifield flocks, and ovoids different from translation ovoids. These applications will be explained in section 3.

2 On the existence of sublines contained in $\mathcal{I}(\mathcal{C})$

In this section we prove the main theorem. We start with a result on the estimate of the sum of the Legendre symbol of polynomials over a finite field of odd prime order. If q is even then every element of $\mathrm{GF}(q)$ is a square in $\mathrm{GF}(q)$. If q is odd, this is not the case and if $q = p$ is prime, we use the so called Legendre symbol $\left(\frac{a}{p}\right)$ defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p, \\ -1 & \text{if } a \text{ is a non-square mod } p, \end{cases}$$

to indicate if a is a square in $\mathrm{GF}(p)$ or not. In 1973 Mit'kin improved Weil's estimate for the Hasse invariant.

Theorem 2.1 (D. A. Mit'kin [11]) *Let $n \geq 4$ be even, $p > (n^2 - n)/2$ simple odd, $f(X) = a_0 + a_1 X + \ldots + a_n X^n$ be a polynomial with integral coefficients that is not quadratic over $\mathrm{GF}(p)$, $(a_n, p) = 1$. Then the following estimate holds:*

$$\left| \sum_{x=1}^{p} \left(\frac{f(x)}{p} \right) \right| \leq (n-2)\sqrt{p + 1 - \frac{n(n-4)}{4}} + 1.$$

We now apply this estimate to characterise polynomials of $\mathrm{GF}(p^n)[X]$ of degree two, which always give a non-zero square when evaluated at elements of $\mathrm{GF}(p)$. The proof is similar to the proof of [2, Lemma 2.2].

Lemma 2.2 *Suppose $f(X) = aX^2 + bX + c \in \mathrm{GF}(p^n)[X]$, $a \neq 0$, p an odd prime, $n \geq 2$, $f(x)$ is a non-zero square for all $x \in \mathrm{GF}(p)$, and $p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$. Then one of the following holds.*

1. *f is the square of a linear polynomial in X over $\mathrm{GF}(p^n)$.*
2. *n is even and f has two distinct roots in $\mathrm{GF}(p^{n/2})$.*
3. *The roots of f are α and α^σ for some $\mathrm{GF}(p)$- automorphism of $\mathrm{GF}(p^n)$ σ, and α in $\mathrm{GF}(p^n)$.*

Proof. Let $f_i(X)$ denote the polynomial obtained from $f(X)$ by raising all coefficients to the power p^i. The roots of $f_i(X)$ are the roots of $f(X)$ raised to the power p^i. For all $x \in \mathrm{GF}(p)$ we have that $f(x)$ is a square in $\mathrm{GF}(p^n)$ precisely when

$$g(x) = \prod_{i=0}^{n-1} f_i(x)$$

is a square in $\mathrm{GF}(p)$. Then $g(X) \in \mathrm{GF}(p)[X]$, which implies that the equation $Y^2 - g(X) = 0$ has $2p$ solutions in $\mathrm{GF}(p)^2$. Suppose $g(X)$ is not a square in $\mathrm{GF}(p)[X]$. Since $p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3}) > 2n^2 - 2n$, and the degree of $g(X)$ is $2n \geq 4$, we can apply Theorem 2.1 and obtain

$$p = \left| \sum_{x=1}^{p} \left(\frac{g(x)}{p} \right) \right| \leq (2n-2)\sqrt{p + 1 - n^2 + 2n} + 1.$$

It follows that $(p-1)^2 - (2n-2)^2(p - (n^2 - 2n - 1)) \leq 0$, contradicting $p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$. Hence $g(X)$ is a square of a polynomial in $\mathrm{GF}(p)[X]$. The rest of the proof is exactly the same as in the proof of [2, Lemma 2.2]. ∎

Remark 2.3 *In [2, Lemma 2.2] the X^2-term in $f(X)$ has coefficient 1. However it is easily seen that the arguments used in the proof also work for an arbitrary coefficient $a \in \mathrm{GF}(q^n)^*$.*

We are now ready to prove the following theorem.

Theorem 2.4 *Let $\mathcal{C}$ be a non-degenerate conic in $\mathrm{PG}(2, q^n)$, q odd, $n \geq 2$. Let L be an external line with respect to $\mathcal{C}$ containing a subline ℓ of order q. If ℓ is contained in the set of internal points of $\mathcal{C}$, or contained in the set of external points of $\mathcal{C}$ then $q < 4n^2 - 8n + 2$, and $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime.*

Proof. Suppose ℓ is a subline of $\mathrm{PG}(2, q^n)$ isomorphic to $\mathrm{PG}(1, q)$ contained in the external line $L : Z = 0$ with respect to the non-degenerate conic $\mathcal{C}$ with equation

$$Q(X, Y, Z) = aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0$$

and contained in the set of internal points or the set of external points of $\mathcal{C}$. Without loss of generality we may assume that ℓ consists of the points $\{\langle x, y, 0\rangle : (x, y) \in (\mathrm{GF}(q)^2)^*\}$. Then $g(X) := Q(X, 1, 0)$ is a polynomial in $\mathrm{GF}(q^n)[X]$ of the form $aX^2 + bX + c$ with $a, b, c \in \mathrm{GF}(q^n)$, which has no roots in $\mathrm{GF}(q^n)$, since L is an external line with respect to $\mathcal{C}$. If c is a non-zero square in $\mathrm{GF}(q^n)$ then $g(x)$ is a non-zero square in $\mathrm{GF}(q^n)$ for all $x \in \mathrm{GF}(q)$, since ℓ is contained in the set of internal points or the set of external points of $\mathcal{C}$. But then [2, Lemma 2.2] implies that $q < 4n^2 - 8n + 2$, and Lemma 2.2 implies that $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime. If c is a non-square then consider the polynomial $cg(X)$. ∎

Using Theorem 2.4 we can now prove Theorem 3.1 in [2] in a less complicated way and avoiding the problem which occurs in the original proof when $n = 3$. In the case when q is prime, we obtain a better bound.

Theorem 2.5 *If there is a subplane of order q contained in the set of internal points of a non-degenerate conic $\mathcal{C}$ in $\mathrm{PG}(2, q^n)$, q odd, $n \geq 3$, then $q < 4n^2 - 8n + 2$ and $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime.*

Proof. It follows from Theorem 2.4 that if a line of $\mathrm{PG}(2, q^n)$ generated by two points of the subplane is external with respect to the conic, then $q < 4n^2 - 8n + 2$, and $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime. Suppose that every line generated by two points of the subplane is a bisecant with respect to the conic. Let P be a point of the subplane and consider the $q + 1$ lines $\ell_0, \ldots, \ell_q$ of the subplane through P. Let ν denote the polarity induced by the conic $\mathcal{C}$. Then P^ν is an external line containing the subline isomorphic to $\mathrm{PG}(1, q)$ consisting of the external points $\ell_0^\nu, \ldots, \ell_q^\nu$ with respect to the conic. Theorem 2.4 implies that $q < 4n^2 - 8n + 2$ and $q \leq 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, if q is prime. ∎

3 Applications

Assume for the rest of the paper that q is an odd prime power, and $\mathcal{W}$ is an $(n-1)$-space over $\mathrm{GF}(q)$ contained in the set of internal points of a non-degenerate conic $\mathcal{C}$ of $\mathrm{PG}(2, q^n)$. In this section we explain some of the consequences of the (non-) existence of such a subspace $\mathcal{W}$. It follows that our result has many corollaries.

We will start with the connection with flocks of a quadratic cone. Although it is not the oldest mathematical object related to $\mathcal{W}$, it is probably the most straightforward one, see Section 3.1 for the construction. It is part of a construction due to Thas [19] (see Lunardon [14] for more details) who observed the equivalence of semifield flocks of a quadratic cone and translation ovoids of $Q(4, q)$ (see Section 3.2). However, it will turn out that Theorem 2.4 does not only imply restrictions for the existence of semifield flocks, resp. translation ovoids, see Theorem 3.2, resp. Theorem 3.5.

3.1 Flocks

Consider the set $\mathcal{U}$ of affine points of an n-dimensional space contained in $\mathrm{PG}(3, q^n)$ and intersecting $\mathrm{PG}(2, q^n)$ in $\mathcal{W}$. In the dual space of $\mathrm{PG}(3, q^n)$ the set of tangents of $\mathcal{C}$ becomes the set of lines on a quadratic cone in $\mathrm{PG}(3, q^n)$, and the set of points $\mathcal{U}$ becomes a set of q^n planes not through the vertex of the cone, such that each point of the cone minus the vertex is on at most one of these planes, and hence defining a partition of the cone minus its vertex into q^n conics. Such a set of conics is called a *flock of a*

quadratic cone in $\mathrm{PG}(3,q^n)$. The planes containing the conics are called the *planes of the flock*. If all planes of the flock share a line then the flock is called *linear*. Conversely one can start with a flock of a quadratic cone in $\mathrm{PG}(3,q^n)$, and obtain a set of q^n affine points $\mathcal{U}$ with the property that the line joining any two of these points meets the plane corresponding to the vertex of the cone in an internal point w.r.t. a non-degenerate conic. If the set $\mathcal{W}'$ of internal points obtained in this way forms a projective space over some subfield $\mathrm{GF}(q')$ of $\mathrm{GF}(q^n)$ then the flock we started with is called a *semifield flock*, and the maximal subfield with this property is called the *kernel* of the semifield flock. Hence the flock we obtained from $\mathcal{W}$ is a semifield flock with kernel containing $\mathrm{GF}(q)$.

Let v be the point $\langle 0,0,0,1\rangle$ and let the conic $\mathcal{C}'$ in the plane π with equation $X_3=0$ be the base of the cone $\mathcal{K}$. The planes of the flock can be written as

$$\pi_t \;:\; tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0$$

where $t \in \mathrm{GF}(q^n)$ and $f,\ g\ :\ \mathrm{GF}(q^n) \to \mathrm{GF}(q^n)$ and this flock is denoted $\mathcal{F}(f,g)$. If $\mathcal{F}(f,g)$ is a semifield flock then f and g are linear over the kernel of $\mathcal{F}(f,g)$. The known semifield flocks of $\mathcal{K}$ where the conic $\mathcal{C}'$ is defined by the equation $X_0X_1 = X_2^2$ are the following.

1. The linear flock where $f(t) = mt$ and $g(t) = 0$, m is a non-square in $\mathrm{GF}(q^n)$.
2. The Kantor-Knuth semifield flock ([9] or [19]) where $f(t) = mt^\sigma$, $g(t) = 0$, m is a non-square in $\mathrm{GF}(q^n)$ and σ is an $\mathrm{GF}(q)$-automorphism of $\mathrm{GF}(q^n)$.
3. The Cohen-Ganley semifield flock (from [6], see [15]) where $q^n = 3^n$, $f(t) = m^{-1}t + mt^9$ and $g(t) = t^3$ with m a non-square in $\mathrm{GF}(q^n)$.
4. The semifield flock ([1]) arising from the Penttila-Williams ovoid ([17]) in $Q(4,q^n)$ where $q^n = 3^5$, $f(t) = t^9$ and $g(t) = t^{27}$.

We will often use the following theorem. The first part is trivial, the second part follows from Thas [19].

Theorem 3.1 (From [5]) *If $\mathcal{F}(f,g)$ is a semifield flock of a quadratic cone in $\mathrm{PG}(3,q^n)$, q odd, with kernel $\mathrm{GF}(q)$. If $n=1$ then $\mathcal{F}(f,g)$ is linear, and if $n=2$ then $\mathcal{F}(f,g)$ is of Kantor-Knuth type.*

If there exists an external line w.r.t. $\mathcal{C}$ intersecting $\mathcal{W}'$ in a subline over $\mathrm{GF}(q)$, then we can apply Theorem 2.4, and this does not require that $\mathcal{W}'$ is an $(n-1)$-space over $\mathrm{GF}(q)$. It follows that our result does not only apply to semifield flocks, but to all flocks with the property that in the dual flock model the set of points $\mathcal{W}'$ contains a subline of order q contained in

an external line w.r.t. the conic $\mathcal{C}$. Before we state the next theorem we introduce the following notation. Let $\mathcal{L}(\mathcal{F})$ denote the set of lines contained in at least two planes of the flock $\mathcal{F}$ of a quadratic cone $\mathcal{K}$, and let $\mathcal{P}(\mathcal{F})$ denote the set of planes through the vertex of the cone and containing a line of $\mathcal{L}(\mathcal{F})$.

Theorem 3.2 *If $\mathcal{F}$ is a flock of a quadratic cone $\mathcal{K}$ in $\mathrm{PG}(3,q^n)$, q odd, and $\mathcal{P}(\mathcal{F})$ contains a dual subline of order q on a line not contained in a tangent plane to $\mathcal{K}$ then $q < 4n^2 - 8n + 2$ and $q \leq 2n^2 - (4-2\sqrt{3})n + (3-2\sqrt{3})$ if q is prime.*

Proof. Suppose L^D is a dual subline of order q not on a tangent plane to $\mathcal{K}$. Then in the dual flock model L is a subline of order q consisting of internal points of a non-degenerate conic $\mathcal{C}$ contained in an external line w.r.t. $\mathcal{C}$. Applying Theorem 2.4 concludes the proof. ■

Remark 3.3 *Note that if $\mathcal{F}$ is a linear flock then $|\mathcal{L}(\mathcal{F})| = 1$ and hence $\mathcal{F}$ does not satisfy the hypotheses of Theorem 3.2. If $\mathcal{F}$ is the Kantor-Knuth semifield flock, then $\mathcal{P}(\mathcal{F})$ is contained in a dual line of order q^n. Since these flocks exist for any odd prime power q, $n \geq 2$, it must follow that the dual line is on a line contained in some tangent plane to the cone. One easily verifies this using the explicit description of the Kantor-Knuth flocks given before.*

If $\mathcal{F}$ is a semifield flock we obtain the following.

Corollary 3.4 *If $\mathcal{F}$ is a non-linear semifield flock of a quadratic cone $\mathcal{K}$ in $\mathrm{PG}(3,q^n)$, q odd, with kernel $\mathrm{GF}(q)$, and $\mathcal{F}$ is not of Kantor-Knuth type then $q < 4n^2 - 8n + 2$, and $q \leq 2n^2 - (4-2\sqrt{3})n + (3-2\sqrt{3})$ if q is prime.*

Proof. Since $\mathcal{F}$ is not linear and not of Kantor-Knuth type, it follows that $n \geq 3$ and $\mathcal{F}$ induces a subplane of order q contained in the set of internal points of a non-degenerate conic. The result follows from Theorem 2.5. ■

3.2 Ovoids of $Q(4,q^n)$

The *generalized quadrangle* $Q(4,q^n)$ is the incidence structure of points and lines of a non-degenerate quadratic form over $\mathrm{PG}(4,q^n)$ (see [16]). An *ovoid of* $Q(4,q^n)$ is a set of $q^{2n}+1$ points no two of which are collinear in $Q(4,q^n)$. As usual we denote the generalized quadrangle constructed from a conic $\mathcal{C}$ by Tits (see [16]) by $T_2(\mathcal{C})$. It is well known that $T_2(\mathcal{C}) \cong Q(4,q^n)$, see [16], or [13, Section 3.5] for more details.

Dualising $\mathrm{PG}(2,q^n)$ w.r.t. $\mathcal{C}$ over $\mathrm{GF}(q)$ one obtains a $(2n-1)$-space $\mathcal{W}^D$

over GF(q) skew from $\mathcal{C}$. Consider $T_2(\mathcal{C})$ in PG$(3,q^n)$ and let $\mathcal{V}$ be the set of affine points of a $2n$-space over GF(q) of PG$(3,q^n)$ intersecting PG$(2,q^n)$ in $\mathcal{W}^D$. Then $\mathcal{V}\cup\{(\infty)\}$ (where (∞) denotes as usual the translation point of $T_2(\mathcal{C})$, see [16]) is a set of $q^{2n}+1$ points of $T_2(\mathcal{C})$ no two points of which are collinear, and hence defines an ovoid of $Q(4,q^n)$. Conversely suppose $\mathcal{O}$ is an ovoid of $Q(4,q^n)$. Then for every point P_i $(i=1,\ldots,q^{2n}+1)$ of $\mathcal{O}$ we might consider the $T_2(\mathcal{C}_i)$ model of $Q(4,q^n)$, where $\mathcal{C}_i$ is the base of the cone $\mathcal{K}_i$ obtained by intersecting $Q(4,q^n)$ with the polar space of P_i, and in every one of these $\mathcal{O}$ induces a set $\mathcal{V}_i$ of q^{2n} affine points, such that every line containing two of these points is skew from $\mathcal{C}_i$. Let $\mathcal{W}_i^D$ denote the set of points of the plane π_i containing the conic $\mathcal{C}_i$ obtained in this way. If one of the sets $\mathcal{V}_i$ is the set of affine points of a projective space over a subfield of GF(q^n), then the ovoid is called a *translation ovoid*; the point P_i is called the *translation point* of the ovoid, and the maximal subfield of GF(q^n) with this property is called the *kernel* of the translation ovoid. If this is the case and if GF(q) is the kernel of the ovoid then the set $\mathcal{W}_i^D$ is a $(2n-1)$-space over GF(q), skew from $\mathcal{C}_i$ and induces an $(n-1)$-space $\mathcal{W}_i$ contained in the set of internal points of $\mathcal{C}_i$.

The list of known translation ovoids follows from the list of known semifield flocks; the linear flock corresponds to an elliptic quadric of PG$(3,q^n)$ contained in $Q(4,q^n)$. We call an ovoid corresponding to a Kantor-Knuth semifield flock, an ovoid of Kantor-Knuth type.

If there exists an external line w.r.t. $\mathcal{C}_i$ intersecting $\mathcal{W}_i$ in a subline of order q, then we can apply Theorem 2.4. If follows that our result does not only apply to translation ovoids, but to all ovoids of $Q(4,q^n)$ with the property that one of the sets ${\mathcal{W}_i}^D$ contains a dual subline of order q on an internal point of $\mathcal{C}_i$. We have proved the following theorem.

Theorem 3.5 *If $\mathcal{O}$ is an ovoid of $Q(4,q^n)$, q odd, and ${\mathcal{W}_i}^D$ contains a dual subline of order q on an internal point of $\mathcal{C}_i$, for some $i\in\{1,\ldots,q^{2n}+1\}$ then $q<4n^2-8n+2$, and $q\leq 2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$ if q is prime.*

If $\mathcal{O}$ is a translation ovoid of $Q(4,q^n)$ we obtain the following.

Corollary 3.6 *If $\mathcal{O}$ is a translation ovoid of $Q(4,q^n)$, q odd, with kernel* GF(q)*, and $\mathcal{O}$ is not an elliptic quadric and not of Kantor-Knuth type then $q<4n^2-8n+2$ and $q\leq 2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$ if q is prime.*

Proof. Since $\mathcal{O}$ is not an elliptic quadric and not of Kantor-Knuth type, it follows that $n\geq 3$ and $\mathcal{O}$ induces a subplane contained in the set of internal points of a conic. Applying Theorem 2.5 concludes the proof. ■

3.3 Semifields

A *semifield* is an algebra satisfying the axioms for a skew field except (possibly) associativity. The study of finite semifields was initiated almost a century ago by Dickson in [8]. Their relevance in the theory of translation planes (class V.1 in the Lenz-Barlotti classification) is well known and can be found in Dembowski [7], where the properties of the collineation group of the plane correspond to the properties of the ternary ring obtained by coordinatising the plane. The *middle nucleus* of a semifield $\mathcal{S}$ is the set $\{x \in \mathcal{S} \parallel a(xb) = (ax)b \ \forall a, b \in \mathcal{S}\}$. If a semifield is commutative and of rank two over its middle nucleus then $\mathcal{S}$ is called a *rank two commutative semifield*. These are the kind of semifields which are connected with a subspace contained in the set of internal points of a conic, see e.g. [4], [3].

For more on semifields and the connections with the previous two sections we refer to [4], [2], [3]. Here we only state the following corollary. It improves [2, Theorem 1.1] in the case q is a prime.

Corollary 3.7 *Let $\mathcal{S}$ be a commutative semifield of rank $2n$ over $\mathrm{GF}(p)$, p an odd prime, and of rank 2 over its middle nucleus $\mathrm{GF}(p^n)$. If $p > 2n^2 - (4-2\sqrt{3})n + (3-2\sqrt{3})$ then $\mathcal{S}$ is either a Dickson semifield or a field.*

Proof. Completely analogous to the proof of [2, Theorem 1.1]. ■

3.4 Eggs and Translation Generalized Quadrangles

An *egg* $\mathcal{E}(n, m, q)$ in $\mathrm{PG}(2n + m - 1, q)$ is a partial $(n-1)$-spread of size $q^m + 1$ such that every 3 egg elements span a $(3n-1)$-space and for every egg element E there exists an $(n+m-1)$-space, denoted by T_E and called the *tangent space of $\mathcal{E}$ at E*, containing E but disjoint from every other egg element. The idea of eggs was introduced by Thas in 1971 [18] and it turned out later, see Payne and Thas [16], that the theory of eggs is equivalent to the theory of translation generalized quadrangles (TGQ's). If $n = m$ then $\mathcal{E}(n, m, q)$ is called a *pseudo-oval* and if $2n = m$ then $\mathcal{E}(n, m, q)$ is called a *pseudo-ovoid*. If we take an oval in $\mathrm{PG}(2, q^n)$, respectively an ovoid in $\mathrm{PG}(3, q^n)$, and consider the ambient space over $\mathrm{GF}(q)$, then we obtain a pseudo-oval, respectively a pseudo-ovoid, and hence the motivation to use that name. The examples constructed in this way are called *elementary*. In a similar way one can construct an egg $\mathcal{E}(n', m', q')$ from an egg $\mathcal{E}(n, m, q)$ for every q' dividing q. We assume from now on that the notation $\mathcal{E}(n, m, q)$ implies that $\mathcal{E}$ can not be constructed from an egg $\mathcal{E}(n', m', q')$, with $q < q'$, and in this case we say that $\mathrm{GF}(q)$ is the *kernel of the egg* $\mathcal{E}(n, m, q)$. A pseudo-ovoid is called *good at an element E* if every $(3n-1)$-space containing E and two other egg elements contains exactly $q^n + 1$ egg elements, and in that case E is called the *good element*.

It follows from [20] that good eggs of $\mathrm{PG}(4n-1,q)$, q odd, are equivalent to semifield flocks (see also [12]). In [13, Section 3.7] a geometrical construction was given of a good egg of $\mathrm{PG}(4n-1,q)$ starting from a semifield flock, in particular from $\mathcal{W}$. It follows that we can list the known examples as we did for semifield flocks. The linear flock corresponds to an elementary egg arising from an elliptic quadric of $\mathrm{PG}(3,q^n)$; we call an egg corresponding to a Kantor-Knuth semifield flock, and egg of Kantor-Knuth type. We immediately have the following.

Corollary 3.8 *If $\mathcal{E}$ is a good egg of $\mathrm{PG}(4n-1,q)$, with kernel $\mathrm{GF}(q)$, q odd, and $\mathcal{E}$ is not elementary and not of Kantor-Knuth type then $q < 4n^2-8n+2$ and $q \leq 2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$ if q is prime.*

Without assuming that the egg has a good element we get the following.

Corollary 3.9 *Let $\mathcal{E}$ be an egg of $\mathrm{PG}(4n-1,q)$, q odd. If there exists a $(3n-1)$-space ρ containing an elementary pseudo-oval $\mathcal{O}_q$ contained in $\mathcal{E}$, corresponding to an oval $\mathcal{O}$ of $\mathrm{PG}(2,q^n)$, and there is a tangent space intersecting ρ in a $(2n-1)$-space $\mathcal{U}$ containing a dual subline of order q on an internal point w.r.t. $\mathcal{O}$ then $q < 4n^2-8n+2$ and $q \leq 2n^2-(4-2\sqrt{3})n+(3-2\sqrt{3})$ if q is prime.*

Proof. First note that $\mathcal{E}$ cannot be elementary nor of Kantor-Knuth type since in these cases $\mathcal{U}$ does not contain a dual subline of order q on an internal point w.r.t. $\mathcal{O}$. This follows from Remark 3.3 and the geometric between semifield flocks and good eggs from [13, Section 3.7]. Suppose $\mathcal{O}_q$ is an elementary pseudo-oval contained in $\mathcal{E}$. Then since q is odd, the corresponding oval $\mathcal{O}$ of $\mathrm{PG}(2,q^n)$ is a conic of $\mathrm{PG}(2,q^n)$. If there is a tangent space intersecting ρ in a $(2n-1)$-space $\mathcal{U}$ containing a dual subline of order q on an internal point w.r.t. $\mathcal{O}$ then it follows from the definition of an egg that $\mathcal{U}$ is skew from $\mathcal{O}$, and hence we obtained a $(2n-1)$-space over $\mathrm{GF}(q)$ skew from a conic $\mathcal{O}$ of $\mathrm{PG}(2,q^n)$, containing a dual subline of order q on an internal point w.r.t. $\mathcal{O}$. After dualising w.r.t. $\mathcal{O}$ over $\mathrm{GF}(q)$ we get an external line of $\mathrm{PG}(2,q^n)$ containing a subline of order q contained in the set of internal points of a conic in $\mathrm{PG}(2,q^n)$. Applying Theorem 2.4 concludes the proof. ■

Remark 3.10 *Since the theory of eggs is equivalent to the theory of translation generalized quadrangles (TGQ), Corollary 3.8 immediately has its consequences in the theory of TGQ's. For the definition of a TGQ we refer to [16].*

Acknowledgements

I would like to thank Prof. S. E. Payne for his interest in this work and his helpful comments on the original manuscript.
This research has been supported by a Marie Curie Fellowship of the European Community programme "Improving the Human Research Potential and the Socio-Economic Knowledge Base" under the contract number HMPF-CT-2001-01386.

References

[1] L. Bader, G. Lunardon and I. Pinneri, A new semifield flock, *J. Combin. Theory Ser. A*, **86**, (1999), 49–62.

[2] Simeon Ball, Aart Blokhuis, Michel Lavrauw; On the classification of semifield flocks. *Adv. Math.* **180** (2003).

[3] Simeon Ball, Matthew R. Brown; The six semifields corresponding to a semifield flock. To appear in Adv. Math.

[4] Simeon Ball, Michel Lavrauw; Commutative semifields of rank 2 over their middle nucleus, Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Mullen, G. L. (ed) et al, Springer-Verlag, 1–21, 2002.

[5] I. Bloemen, J. A. Thas, H. Van Maldeghem; Translation ovoids of generalized quadrangles and hexagons. *Geom. Dedicata* **72** (1998), no. 1, 19–62.

[6] Stephen D. Cohen, Michael J. Ganley; Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra* **75** (1982), no. 2, 373–385.

[7] P. Dembowski; *Finite geometries.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44 Springer-Verlag, Berlin-New York 1968 xi+375 pp.

[8] L. E. Dickson; Linear algebra in which division is always uniquely possible, *Trans. Amer. Math. Soc.* **7** (1906), 514–527.

[9] H. Gevaert and N. L. Johnson, Flocks of quadratic cones, generalized quadrangles and translation planes, *Geom. Dedicata*, **27**, (1988), 301–317.

[10] J. W. P. Hirschfeld; *Projective geometries over finite fields.* Second edition. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. xiv+555 pp. ISBN: 0-19-850295-8.

[11] D. A. Mit'kin; Estimation of the sum of Legendre symbols of polynomials of even degree. (Russian) *Mat. Zametki* **14** (1973), 73–81.

[12] Michel Lavrauw, Tim Penttila; On eggs and translation generalised quadrangles. *J. Combin. Theory Ser. A* **96** (2001), no. 2, 303–315.

[13] Michel Lavrauw; Scattered spaces with respect to spreads, and eggs in finite projective spaces. Dissertation, Technische Universiteit Eindhoven, Eindhoven, 2001. Eindhoven University of Technology, Eindhoven, 2001. viii+115 pp.

[14] Guglielmo Lunardon; Flocks, ovoids of $\mathrm{Q}(4,q)$ and designs. *Geom. Dedicata* **66** (1997), no. 2, 163–173.

[15] S. E. Payne, An essay on skew translation generalized quadrangles, *Geom. Dedicata*, **32**, (1989), 93–118.

[16] S. E. Payne, J. A. Thas; *Finite generalized quadrangles*. Research Notes in Mathematics, 110. Pitman (Advanced Publishing Program), Boston, MA, 1984. vi+312 pp. ISBN 0-273-08655-3

[17] T. Penttila and B. Williams, Ovoids of parabolic spaces, *Geom. Dedicata* **82** (2000), no. 1-3, 1–19.

[18] J. A. Thas; The m-dimensional projective space $S_m(M_n(\mathrm{GF}(q)))$ over the total matrix algebra $M_n(\mathrm{GF}(q))$ of the $n \times n$-matrices with elements in the Galois field $\mathrm{GF}(q)$. *Rend. Mat.* (6) **4** (1971), 459–532.

[19] J. A. Thas, Generalized quadrangles and flocks of cones, *European J. Combin.*, **8**, (1987), 441–452.

[20] J. A. Thas; Generalized quadrangles of order (s, s^2). III. *J. Combin. Theory Ser. A* **87** (1999), 247–272.