On the classification of semifield flocks

Aart Blokhuis *Michel Lavrauw*
Technische Universiteit Eindhoven,
Postbox 513, 5600 MB Eindhoven,
The Netherlands

Simeon Ball *
Queen Mary, University of London,
London E1 4NS,
United Kingdom

31 January 2001: draft four

Abstract

It is shown that the only semifield flocks of the quadratic cone of $PG(3, q^n)$ with $q \geq 4n^2 - 8n + 2$ are the linear flocks and the Kantor-Knuth semifield flocks. This follows from the main theorem which states that there are no subplanes of order q contained in the set of internal points of a conic in $PG(2, q^n)$ for those q exceeding the bound.

1. Introduction

Let q be an odd prime power and let $\mathcal{K}$ be a quadratic cone of $PG(3, q^n)$ with vertex v. A *flock* $\mathcal{F}$ of $\mathcal{K}$ is a partition of $\mathcal{K} \setminus \{v\}$ into q^n conics. If all the planes that contain a conic of the flock share a line then the flock is called *linear*. 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 determined by the conics are called the planes of the flock and can be written as

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

where $t \in GF(q^n)$ and $f, \ g \ : \ GF(q^n) \to GF(q^n)$ and this flock is denoted $\mathcal{F}(f, g)$. If f and g are linear over a subfield then the flock is called *semifield*. The maximal subfield with this property is called the kernel of the (semifield) flock.

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 $GF(q^n)$.

*This author is supported by British EPSRC Fellowship No. AF/990-480

2. The Kantor-Knuth semifield flock ([5] or [12]) where $f(t) = mt^\sigma$, $g(t) = 0$, m is a non-square in $GF(q^n)$ and σ is an $GF(q)$-automorphism of $GF(q^n)$.

3. The Ganley semifield flock ([8]) where $q^n = 3^n$, $f(t) = m^{-1}t + mt^9$ and $g(t) = t^3$ with m a non-square in $GF(q^n)$.

4. The semifield flock ([1]) which comes from the Penttila-Williams ovoid ([10]) in $Q(4, q^n)$ (also denoted $O(5, q^n)$, see Section 4.) where $q^n = 3^5$, $f(t) = t^9$ and $g(t) = t^{27}$.

Let $\mathcal{F}(f, g)$ be a semifield flock of $\mathcal{K}$ with kernel containing $GF(q)$. In the dual space the lines of the cone $\mathcal{K}$ are a set of $q^n + 1$ lines in the plane π dual to v, no three of which are concurrent. Since q is odd they form a set of tangents to a conic $\mathcal{C}'$. Every intersection line of two planes of the flock is skew from every line of the cone $\mathcal{K}$. In the dual space the line joining two points of the flock (points dual to planes of the flock) meets π in an internal point of $\mathcal{C}'$ since the external points and the points of $\mathcal{C}'$ are incident with a tangent. Let $\mathcal{W}$ be this subset of the internal points. If we take the dual with respect to the standard inner product then

$$\mathcal{W} = \{\langle t, -f(t), g(t), 0\rangle \mid t \in GF(q^n)\}.$$

If $\mathcal{W}$ is contained in a line of π then the planes of the flock all share a common point. In [12], these flocks are shown to be either linear (in which case they share a line) or a Kantor-Knuth semifield flock.

If $\mathcal{W}$ is not contained in a line of π then it spans π over $GF(q^n)$. The subspace $\mathcal{W}$ is n-dimensional over $GF(q)$ and so $\mathcal{W}$ contains a subplane of order q which is contained in the internal points of a conic.

2. A lemma of Weil and some consequences

The following lemma is due to Weil and can be found in Schmidt ([11]).

Lemma 2.1 *The number of solutions N in $GF(q)$ of the hyperelliptic equation*

$$y^2 = g(x)$$

where $g \in GF(q)[X]$ is not a square and has degree $2m > 2$ satisfies

$$|N - q + 1| < (2m - 2)\sqrt{q}.$$

Lemma 2.2 *Let $f(X) = X^2 + uX + v \in GF(q^n)[X]$ be a non-zero square in $GF(q^n)$ for all $X = x \in GF(q)$, q odd and $q \geq 4n^2 - 8n + 2$. At least one of the following holds.*

1. *f is the square of a linear polynomial.*

2. *n is even and f has two distinct roots in $GF(q^{n/2})$.*

3. *The roots of f are α and α^σ for some σ a $GF(q)$-automorphism of $GF(q^n)$ and $\alpha \in GF(q^n)$.*

Proof : Let n_1 be the order of the smallest subfield such that $f(X) \in GF(q^{n_1})[X]$ and $f(x)$ is a non-zero square in $GF(q^{n_1})$ for all $x \in GF(q)$. If $n_1 \neq n$ simply replace n by n_1 and assume that no such subfield exists. Let f_i be the polynomial obtained from f by raising all coefficients to the power q^i. The roots of f_i are the roots of f raised to the power q^i. For all $x \in GF(q)$ we have that $f(x)$ is a square in $GF(q^n)$ precisely when

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

is a square in $GF(q)$. The degree of g is $2n$, $g(x) \in GF(q)[x]$ and by assumption

$$|2q - q + 1| > (2n - 2)\sqrt{q}.$$

The previous lemma implies that g is a square. Assume that f is not a square and let $\alpha, \beta \neq \alpha$ be the roots of f. The roots of g are

$$\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}, \beta, \beta^q, \ldots, \beta^{q^{n-1}}$$

and every value occurs in this list an even number of times. Therefore there exists σ, a $GF(q)$-automorphism of $GF(q^n)$, such that $\beta = \alpha^\sigma$ or there exists σ and τ, $GF(q)$-automorphisms of $GF(q^n)$, such that $\alpha = \alpha^\sigma$ and $\beta = \beta^\tau$. Let d be minimal such that $x^\sigma = x^{q^d}$.

If there is a σ such that $\alpha = \alpha^\sigma$, and there is no σ such that $\beta = \alpha^\sigma$, then each element of $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ occurs in the list $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ an even number of times, so the order m of σ is even. In particular n is even and $\alpha = \alpha^\sigma = \alpha^{\sigma^{m/2}} = \alpha^{q^{n/2}}$ and $\alpha \in GF(q^{n/2})$. Likewise $\beta \in GF(q^{n/2})$. This implies that f has two distinct roots in $GF(q^{n/2})$.

If there is a σ such that $\beta = \alpha^\sigma = \alpha^{q^d}$ where d is chosen to be minimal then the list $\{\beta, \beta^q, \ldots, \beta^{q^{n-d-1}}\}$ is equal to the list $\{\alpha^{q^d}, \alpha^{q^{d+1}}, \ldots, \alpha^{q^{n-1}}\}$. Therefore each value which occurs in the list

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}, \alpha^{q^n}, \alpha^{q^{n+1}}, \ldots, \alpha^{q^{n+d-1}}\}$$

occurs an even number of times. Let $e < 2n$ be minimal such that $\alpha = \alpha^{q^e}$. Now $e > d$ by the minimality of d and so the elements in the list $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ are all distinct. Hence

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\} = \{\alpha^{q^n}, \alpha^{q^{n+1}}, \ldots, \alpha^{q^{n+d-1}}\}$$

and

$$\{\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^d}\} = \{\alpha^{q^{n+1}}, \alpha^{q^{n+2}}, \ldots, \alpha^{q^{n+d}}\}$$

which by taking the symmetric difference implies $\{\alpha, \alpha^{q^d}\} = \{\alpha^{q^n}, \alpha^{q^{n+d}}\}$. If $\alpha \neq \alpha^{q^n}$ then $\alpha = \alpha^{q^{n+d}}$ and $\alpha^{q^d} = \alpha^{q^n}$ which combine to give $\alpha = \alpha^{q^{2d}}$ and therefore e divides $2d$. Moreover since $e > d$ we have that $e = 2d$ and since e divides $2n$ that d divides n. The coefficients of f are $-\alpha - \alpha^{q^d}$ and α^{q^d+1} respectively which are in the subfield $GF(q^d)$. Hence $f \in GF(q^d)[X]$. If n/d is even then $2d$ divides n and f has two roots α and α^σ where $\alpha \in GF(q^n)$. If n/d is odd then

$$1 = f(x)^{(q^n-1)/2} = f(x)^{(1+q^d+\ldots+q^{n-d})(q^d-1)/2} = f(x)^{(n/d)(q^d-1)/2} = f(x)^{(q^d-1)/2}$$

and $f(x)$ is a square in $GF(q^d)$. However we assumed at the start of the proof that this was not the case. □

3. The main theorem

Let Q be a quadratic form on $V(3,q)$ whose zeros are a non-degenerate conic $\mathcal{C}$. The value of Q on the internal points is either a non-zero square or a non-square in $GF(q)$ and after multiplying by a suitable scalar we can assume it is a non-zero square.

Theorem 3.1 *If there is a subplane of order q contained in the internal points of a non-degenerate conic $\mathcal{C}$ in $PG(2,q^n)$ then $q < 4n^2 - 8n + 2$.*

Proof : Let Q be the quadratic form

$$Q(X,Y,Z) = X^2 + aXY + bXZ + cY^2 + dYZ + eZ^2$$

that is square on the set $\{(x,y,z) \mid x,y,z \in GF(q)\}$ and whose set of zeros is the conic $\mathcal{C}$. Let n_1 be the order of the smallest subfield such that all the coefficients of Q are elements of $GF(q^{n_1})$. If $n_1 \neq n$ simply replace n by n_1 in the theorem and assume that all coefficients of Q do not lie in a subfield.

For a fixed y and z in $GF(q)$ not both zero let

$$f_{yz}(X) = Q(X,y,z).$$

The polynomial $f_{yz} \in GF(q^n)[X]$ is a square for all x in $GF(q)$.

If f_{yz} is a square of another polynomial then Q is a square for all points on the line $zY - yZ = 0$. However, the lines that contain internal points also contain external points on which Q is a non-square.

If f_{yz} has two distinct roots α and β in $GF(q^{n/2})$ then (α,y,z) and (β,y,z) are points of the conic $\mathcal{C}$. Moreover they are points of the conic $\mathcal{C}''$ defined by the quadratic form whose coefficients are the coefficients of Q raised to the power $q^{n/2}$. The coefficients of Q do not all lie in a subfield so $\mathcal{C} \neq \mathcal{C}''$. The conics $\mathcal{C}$ and $\mathcal{C}''$ meet in at most four points. Hence f_{yz} can have two distinct roots in $GF(q^{n/2})$ for at most two projective pairs (y,z). We assume henceforth that (y,z) are not one of these two.

By the lemma the roots of f are therefore α and α^σ for some $\alpha \in GF(q^n)$ and some $GF(q)$-automorphism σ of $GF(q^n)$. Let $g(Y,Z) = aY + bZ$ and $h(Y,Z) = cY^2 + dYZ + eZ^2$ so we have that

$$f_{yz}(X) = (X-\alpha)(X-\alpha^\sigma) = X^2 + g(y,z)X + h(y,z).$$

There are two cases to consider, namely when the order of σ is odd and when it is even.

Consider first the case that the order m of σ is odd. The identity

$$(\alpha+\alpha^\sigma)^2 = (\alpha^{1+\sigma})^{1-\sigma+\sigma^2-\ldots+\sigma^{m-1}} + 2\alpha^{1+\sigma} + (\alpha^{1+\sigma})^{\sigma(1-\sigma+\sigma^2-\ldots+\sigma^{m-1})}$$

implies

$$g(y,z)^2 = h(y,z)^{1-\sigma+\sigma^2-\ldots+\sigma^{m-1}} + 2h(y,z) + h(y,z)^{\sigma(1-\sigma+\sigma^2-\ldots+\sigma^{m-1})}.$$

There is such an automorphism σ for $q-1$ projective pairs (y,z) and hence there exists an automorphism $\tilde{\sigma}$ which occurs for at least

$$(q-1)/(n-1) > 2n \geq 2m$$

projective pairs. We modify our notation and let f_i be the polynomial obtained from f by raising all coefficients to the power $\tilde{\sigma}^i$. The above relation implies

$$h_1 h_2 \dots h_{m-1} g^2 = h_0 (h_2 h_4 \dots h_{m-1} + h_1 h_3 \dots h_{m-2})^2$$

which has total degree $2m$, holds for every projective pair (y, z), and is therefore an identity. For all $x \in GF(q)$

$$f_{yz}(X + x) = X^2 + (g + 2x)X + h + xg + x^2 = (X - (\alpha - x))(X - (\alpha^\sigma - x))$$

and we get the more general relation

$$w_1 w_2 \dots w_{m-1} (g + 2x)^2 = w_0 (w_2 w_4 \dots w_{m-1} + w_1 w_3 \dots w_{m-2})^2$$

where $w(x, y, z) = h(y, z) + g(y, z)x + x^2$. This equation is valid for all $(x, y, z) \in GF(q)^3$ and is of degree $2m$ and is again an identity. We may replace $w_0 = w$ by Q and it follows that

$$Q_1 \mid Q_0 Q_2 \dots Q_{m-1}.$$

Therefore either $Q_1 = Q_i$ for some i and the coefficients of Q lie in some subfield or Q_1 and hence Q splits into linear factors and Q is degenerate.

In the second case when the order m of σ is even

$$h(y, z)^{1+\sigma^2+\dots+\sigma^{m-2}} = h(y, z)^{\sigma+\sigma^3+\dots+\sigma^{m-1}}$$

and there exists an automorphism $\tilde{\sigma}$ for which this is an identity. We define $w(x, y, z)$ as before and obtain the more general relation

$$w_0 w_2 \dots w_{m-2} = w_1 w_3 \dots w_{m-1}$$

which is also an identity. We may replace $w_0 = w$ by Q and since

$$Q \mid Q_1 Q_3 \dots Q_{m-1}$$

either $Q = Q_i$ for some i and the coefficients of Q lie in some subfield or Q splits into linear factors and Q is degenerate.

□

Corollary 3.2 *The only semifield flocks of the quadratic cone of $PG(3, q^n)$ with $q \geq 4n^2 - 8n + 2$ are the linear flocks and the Kantor-Knuth semifield flocks.*

4. Equivalences and Applications

Let $\mathcal{F}(f, g)$ be a flock of the quadratic cone $\mathcal{K}$ of $PG(3, q^n)$ with vertex $\langle 0, 0, 0, 1 \rangle$ and base

$$\mathcal{C} \, : \, X_0 X_1 = X_2^2.$$

Let

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

be the planes of the flock. In the dual flock model (as described in the introduction) the set

$$\mathcal{W} = \{\langle t, -f(t), g(t), 0\rangle \mid t \in GF(q^n)\}$$

is contained in the set of internal points to the conic $\mathcal{C}'$ with equation $X_2^2 - 4X_0X_1 = 0$ in the plane $X_3 = 0$. Since $\langle 0,0,1,0\rangle$ lies on a tangent of $\mathcal{C}'$ and 1 is a square in $GF(q^n)$ it follows that $g^2 + 4xf$ is a non-square for all $x \in GF(q^n)$.

Let us assume throughout this section that f and g are functions with this property. We make a list of equivalent algebraic and geometric objects associated with a semifield flock.

1. Commutative semifields.

   A (finite) *semifield* is a (finite) set $\mathcal{S}$ on which two operations, addition and multiplication $(\cdot)$, are defined with the following properties.

   (S1) (S,+) is an abelian group with identity 0.
   (S2) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all a, b, $c \in \mathcal{S}$.
   (S3) There exists an element $1 \neq 0$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in \mathcal{S}$.
   (S4) If $a \cdot b = 0$ then either $a = 0$ or $b = 0$.

   The middle nucleus $\{x \in \mathcal{S} \mid (a \cdot x) \cdot b = a \cdot (x \cdot b) \text{ for all } a, b \in \mathcal{S}\}$ is a field and the semifield can be viewed as a left or right vector space over it's middle nucleus.

   A commutative semifield, two dimensional over it's middle nucleus $GF(q)$ always arises from the following construction ([3]). Let $\mathcal{S}(f, g)$ denote the set of ordered pairs of elements of $GF(q^n)$ with addition defined component-wise and multiplication by

   $$(a, b) \cdot (c, d) = (ac + g(bd), ad + bc + f(bd)).$$

   It is easy to check the axioms (S1)-(S3) hold and (S4) implies that $g^2 + 4xf$ is a non-square for all $x \in GF(q^n)$. The middle nucleus is the kernel of the corresponding semifield flock.

2. Spreads and spread sets.

   A *spread set* $\mathcal{D}$ is a set of q^{nd} $(d \times d)$-matrices with the following properties.

   (SS1) $O, I \in \mathcal{D}$
   (SS2) for all M, $N \in \mathcal{D}$ where $M \neq N$ implies $\det(M - N) \neq 0$

   The set

   $$\mathcal{D} = \left\{ \begin{pmatrix} y + g(x) & f(x) \\ x & y \end{pmatrix} \mid x, y \in GF(q) \right\}$$

   is a spread set. A spread set gives rise to a spread ([4]) and from $\mathcal{D}$ we get a spread of $PG(3, q^n)$ given by

   $$\{\langle (y, x, 1, 0), (f(x), y + g(x), 0, 1)\rangle \mid x, y \in GF(q^n)\} \cup \{\langle (1, 0, 0, 0), (0, 1, 0, 0)\rangle\}$$

   from which a translation plane of order q^{2n} with kernel $GF(q)$ can be constructed ([4]).

3. q^n-clans.

   A q^n*-clan* $\mathcal{Q}$ is a set of q^n (2×2)-matrices with the property that for all A_t, $A_s \in \mathcal{Q}$

   $$\mathbf{v}^T(A_t - A_s)\mathbf{v} = 0$$

implies that $\mathbf{v} = (0,0)$ or $t = s$. A q^n-clan is *additive* if $A_t + A_s = A_{t+s}$ for all t and s. The set

$$\left\{ \begin{pmatrix} x & g(x) \\ 0 & -f(x) \end{pmatrix} \mid x \in GF(q^n) \right\}$$

is an additive q^n-clan.

4. Eggs.

   An *egg* $\mathcal{E}$ of $PG(4n-1,q)$ is a set of $q^{2n}+1$ $(n-1)$-dimensional subspaces with the following properties.

   (E1) Any three elements of $\mathcal{E}$ span a $(3n-1)$-dimensional subspace.

   (E2) For all $E \in \mathcal{E}$ there exists a $(2n-1)$-dimensional subspace containing E which is skew from all other elements of $\mathcal{E}$.

   Given an additive q^n-clan one can construct an egg of $PG(4n-1,q)$ ([7] or [8]).

5. Translation generalised quadrangles.

   A *translation generalised quadrangle* is a generalised quadrangle ([2] or [9]) with the property that there is an abelian group T acting regularly on the points not collinear with a point P while fixing every line through P. For every egg of $PG(4n-1,q)$ one can construct a translation generalised quadrangle of order (q^n, q^{2n}) and conversely every translation generalised quadrangle of order (q^n, q^{2n}) gives rise to an egg of $PG(4n-1,q)$ ([9, 8.7.1]).

6. Ovoids of $O(5,q)$.

   An *ovoid* of a generalised quadrangle ([2] or [9]) is a set of points $\mathcal{O}$ such that each line contains exactly one point of $\mathcal{O}$.

   Let $Q(4,q^n)$ (sometimes denoted $O(5,q^n)$) denote the generalised quadrangle of order q^n whose points are the points of a non-singular quadric in $PG(4,q^n)$ and whose lines are the lines contained in that quadric. If we choose the quadratic form on $V(5,q^n)$ given by

$$X_0X_4 + X_1X_3 + X_2^2$$

   then the points of an ovoid in $O(5,q^n)$ can be written as

$$\left\{(1, x, y, -F(x,y), -y^2 + xF(x,y) \mid x, y \in GF(q^n)\right\} \cup \{(0,0,0,0,1)\}$$

   for some polynomial $F(x,y)$.

   The functions f and g are $GF(q)$-linear and so can be written in the form

$$f(X) = -\sum_{i=0}^{n-1} c_i X^{q^i} \text{ and } g(X) = \sum_{i=0}^{n-1} b_i X^{q^i}$$

   for some c_i, $b_i \in GF(q^n)$. The semifield flock $\mathcal{F}(f,g)$ is in one-to-one correspondence with the ovoid $\mathcal{O}$ of $O(5,q^n)$ ([13] and for details see [6]) given by

$$F(X,Y) = \sum_{i=0}^{n-1} (c_i X + b_i Y)^{q^{n-i}}.$$

5. Acknowledgements

The authors would like to thank Dr. Tim Penttila for highlighting the problem of finding subplanes contained in internal points of conics and suggesting that the authors should devote some time to finding a proof that it is not generally possible.

References

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

[2] P. J. Cameron, *Projective and Polar Spaces*, QMW Maths Notes 13, (1991). Updated version, http:www.maths.qmw.ac.uk/∼pjc/pps.

[3] S. D. Cohen and M. J. Ganley, Commutative semifields, two dimensional over their middle nuclei, *J. Algebra*, **75**, (1982), 373–385.

[4] P. Dembowski, *Finite Geometries*, Springer, 1968.

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

[6] M. Lavrauw, Semifield flocks, eggs and ovoids of generalised quadrangles, preprint.

[7] M. Lavrauw and T. Penttila, On eggs and translation generalised quadrangles, submitted.

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

[9] S. E. Payne and J. A. Thas, *Finite generalised quadrangles*, Research Notes in Mathematics 110, Pitman, 1984.

[10] T. Penttila and B. Williams, Ovoids of parabolic spaces, *Geom. Dedicata*, to appear.

[11] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Mathematics 536, Springer, 1976.

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

[13] J. A. Thas, Symplectic spreads in $PG(3, q)$, inversive planes and projective planes, *Discrete Math.*, **174**, (1997), 329–336.