On Monomial Flocks

LAURA BADER\textsuperscript{1}, DINA GHINELLI AND TIM PENTTILA

We study monomial flocks of quadratic cones of $PG(3, q)$, with emphasis on the case where the flock is semifield, providing some nonexistence and some uniqueness results. In addition, we give a computer-free proof of the existence of the sporadic semifield flock of the quadratic cone of $PG(3, 3^5)$ (and hence of the sporadic translation ovoid of $Q(4, 3^5)$), and relate that flock to the sporadic simple group $M_{11}$.

\begin{center}
\begin{tabular}{c}
$^{\dagger}$Author to whom correspondence should be addressed.
\end{tabular}
\end{center}

1. Introduction

Let $K$ be the quadratic cone of $PG(3, q)$ with equation $x_0x_1 = x_2^2$ and vertex $v = (0, 0, 0, 1)$. A flock $\mathcal{F}$ of $K$ is a partition of $K \setminus \{v\}$ into $q$ conics.

Without loss of generality, we can suppose $\mathcal{F}$ consists of the planes $\pi_t$ with equations $tx_0 - f(t)x_1 + g(t)x_2 + x_3 = 0$ respectively, for suitable maps $f, g$ from $GF(q)$ to itself such that $f(0) = g(0) = 0$. We write $\mathcal{F} = \mathcal{F}(f, g)$.

Equivalent to flocks are some translation planes of order $q^2$ and kernel containing $GF(q)$, which are constructed as follows: embed the cone in the Klein quadric $Q^+(5, q)$ as a section with a tangent three-dimensional space, and consider the $q$ planes which are polars of the planes of the flock with respect to $Q^+(5, q)$. These planes intersect the Klein quadric in $q$ irreducible conics with a common point (the vertex of the cone) and their union is an ovoid mapped, under the Klein correspondence, to a line spread of $PG(3, q)$ consisting of $q$ reguli sharing a line, which define, as usual, a translation plane \cite{9, 28}; the spread consists of the line $x_1 = x_2 = 0$ and the lines $(y_1, y_2) = \left( g(t) + u / f(t), t / u \right) (x_1, x_2)$ for $t, u \in GF(q)$ \cite{10}.

In addition, flocks define elation generalized quadrangles with parameters $(q^2, q)$, which are constructed algebraically as coset geometries starting with the $q$–clan associated with the flock, i.e., the set of matrices $\left( \begin{array}{cc} t & g(t) \\ 0 & -f(t) \end{array} \right)$ \cite{13, 18, 24}. For $q$ odd, these quadrangles can also be defined starting with the lines of the BLT-set associated with the flock with a geometric construction \cite{5, 15} or, for any $q$, with the procedure of \cite{27}. For more details, see \cite{17, 20, 25}.

If all the planes of the flock share a common line, then $\mathcal{F}$ is called linear. If both $f$ and $g$ are monomial functions, then $\mathcal{F}$ is called of monomial type or, more briefly, monomial. We explicitly remark that there exist collineations of $PG(3, q)$ which fix the cone and map the planes of a monomial flock to planes having equations $sx_0 - F(s)x_1 + G(s)x_2 + x_3 = 0$ with $F$ and/or $G$ which may not be monomial. Hence, there exist isomorphisms mapping a flock with monomial $f$ and $g$ to one with nonmonomial $f$ and/or $g$, and conversely; in other words: given a flock it might be not easy to decide whether it is monomial or not.

For $q$ even, monomial flocks have been completely classified by T. Penttila and L. Storme \cite{22}, proving that they are either linear, or Kantor–Payne or Fisher–Thas–Walker. The herd of hyperovals of $PG(2, q)$ associated with the flock plays an essential role in their argument, and the herd exists only when $q$ is even. For more details on herds, see \cite{8, 17, 25}.

For $q$ odd, apart from a sporadic example, four classes of monomial flocks are known, which will be listed in Section 2. A geometric construction of these flocks is given in \cite{1}, via the osculating planes to a certain curve.
From now on, we always assume \( q \) is an odd prime power.

In Section 2 we discuss some generalities on monomial flocks.

In Section 3 we study sporadic semifield monomial flocks, proving that no examples exist up to certain, quite big, values for the characteristic and/or the exponents. In addition, the sporadic BLT-set of \( Q(4, 3^5) \) constructed in [4] using the ovoid of [21] is described in terms of the sporadic Mathieu group \( M_{11} \).

Finally, in Section 4, we show that new infinite classes of monomial flocks with \( f(t) = at^{2k+1} \) and \( g(t) = bt^{k+1} \), which in some sense generalize the known examples, do not exist for small \( k \), and, in general, if they exist, there are strong restrictions on the characteristic and they are necessarily unique for each particular odd \( k \), while at most two classes of examples exist for each particular even \( k \).

The authors wish to thank the referees for their helpful comments.

2. Generalities on Monomial Flocks

Let \( q = p^s \), \( p \) any odd prime, and let \( K \) be the cone with equation \( x_0x_1 = x_2^3 \) and vertex \((0, 0, 0, 1)\). Let \( \mathcal{F} = \mathcal{F}(f, g) = \{ \pi_t : t x_0 - f(t)x_1 + g(t)x_2 + x_3 = 0 \mid t \in GF(q) \} \). Recall that \( \mathcal{F} \) is a flock if and only if
\[
H(t, s) = (g(t) - g(s))^2 + 4(t - s) (f(t) - f(s)) \text{ is a nonsquare} \tag{1}
\]
for all \( t, s \in GF(q) \) with \( t \neq s \) [24]. In particular, if \( \mathcal{F} \) is a flock, then \( f \) is a bijection. Here we follow the notation of [10]. For all the results not explicitly mentioned, one can refer, for example, to the excellent surveys [17, 25].

Four classes of monomial flocks are known.

Linear flocks. For \( f(t) = ct \) and \( g(t) = bt \), \( X^2 + bX - c \) an irreducible polynomial over \( GF(q) \), the \( q \) planes \( \pi_t \), with equation \( t x_0 - ct x_1 + bt x_2 + x_3 = 0 \), \( t \in GF(q) \), define a flock which is linear, since all the planes contain the points \((c, 1, 0, 0)\) and \((-b, 0, 1, 0)\).

Kantor–Knuth flocks. For \( f(t) = mt^\sigma \) and \( g(t) = 0 \), \( m \) a given nonsquare of \( GF(q) \), and \( \sigma \neq 1 \) a given automorphism of \( GF(q) \), the \( q \) planes \( \pi_t \), with equation \( t x_0 - mt^\sigma x_1 + x_3 = 0 \), \( t \in GF(q) \), define a flock of \( K \) [10, 24]. All planes \( \pi_t \) contain the point \((0, 0, 1, 0)\). (This flock is linear if and only if \( \sigma = 1 \).) Conversely, every flock of \( K \) for which the planes of the \( q \) conics all contain a unique common point, is of the type just described [24]. The translation planes associated with these flocks have coordinates in some Knuth semifields.

Fisher–Thas–Walker flocks. Let \( q \equiv 2 \pmod{3} \), \( q > 2 \). For \( f(t) = -\frac{1}{2}t^3 \) and \( g(t) = -t^2 \), the \( q \) planes \( \pi_t \), with equation \( t x_0 - \frac{1}{2}t^3 x_1 - t^2 x_2 + x_3 = 0 \), \( t \in GF(q) \), define a flock. This is associated with the generalized quadrangle constructed by W. M. Kantor in [13] even before the relationship between flocks and quadrangles was found. For more details, see [9].

Kantor–Payne flocks. Let \( q \equiv \pm 2 \pmod{5} \), \( q > 3 \). For \( f(t) = -\frac{n^2}{5}t^5 \) and \( g(t) = nt^3 \), with \( n \in GF(q) \), the \( q \) planes \( \pi_t \), with equation \( t x_0 + \frac{n^2}{5}t^5 x_1 + nt^3 x_2 + x_3 = 0 \), \( t \in GF(q) \), define a flock which was independently found by W. M. Kantor [14] for \( q \) odd and by S. E. Payne [19] for \( q \) even. As here \( q \) is odd, we can put \( q = p^r \), \( r \) odd and \( p \equiv \pm 2 \pmod{5} \), \( n = 1 \).

Note that all these examples of monomial flocks have \( f(t) = at^{2k+1} \) and \( g(t) = bt^{k+1} \) for some \( a, b \in GF(q) \) and a suitable integer \( k \). These flocks will be studied in detail in Section 4.

In addition, there exists an example of a monomial flock that is not of the above type.

Sporadic semifield flock. Let \( q = 3^5 \). For \( f(t) = t^q \) and \( g(t) = t^{27} \), the \( q \) planes \( \pi_t \), with equation \( t x_0 - t^q x_1 + t^{27} x_2 + x_3 = 0 \), \( t \in GF(q) \), define a flock which was constructed...
On monomial flocks

by L. Bader, G. Lunardon and I. Pinna [4], using the Penttila–Williams ovoid of $Q(4, 3^5)$
defined in [21]. We will give further details on this flock in Section 3.

If $\mathcal{F} = \mathcal{F}(\alpha t^a, \beta t^b)$ is a monomial flock, with $\alpha, \beta \in GF(q)$, $a, b$ integers such that
$0 < a, b < q - 1$, note that $\alpha \neq 0$ because $f$ is a bijection, and if $\beta = 0$ then the flock is
either linear or Kantor–Knuth.

For $\beta \neq 0$, the following proposition proves that, without loss of generality, we can reduce
the number of parameters to three.

**Proposition 1.** Let $\mathcal{F} = \mathcal{F}(\alpha t^a, \beta t^b)$ be a flock with $\beta \neq 0$. Then there exists $\gamma \in
GF(q)$ such that $\mathcal{F} = \mathcal{F}(\alpha t^a, \beta t^b)$ is isomorphic to $\mathcal{F} = \mathcal{F}(\gamma t^a, t^b)$.

**Proof.** Let $\theta$ be the collineation of $PG(3, q)$ defined as $(x_0, x_1, x_2, x_3)^\theta = (x_0, \beta^{-2} x_1, \beta^{-1} x_2, x_3)$. Then $\theta$ fixes the cone $K$ and maps $\mathcal{F} = \mathcal{F}(\alpha t^a, \beta t^b)$ to $\mathcal{F} = \mathcal{F}(\gamma t^a, t^b)$, with
$\gamma = a \beta^{-2}$.

**Proposition 2.** Let $\mathcal{F} = \mathcal{F}(\gamma t^a, t^b)$ be a flock. Then, $(a, q - 1) = 1$, thus, since we are
taking $q$ to be odd, $a$ is odd.

**Proof.** If $(a, q - 1) \neq 1$, then $f$ is not bijective: a contradiction.

Throughout the rest of this paper, we fix $k = \frac{a - 1}{q - 2}$. Since $1 < a < q - 2$ and $q$ is odd, we have

$$0 \leq k \leq \frac{q - 3}{2}. \quad (2)$$

We explicitly require $a, b < q - 1$, since we want both $f$ and $g$ to be polynomials reduced
modulo the fundamental polynomial of the field. If not, problems such as the following might
arise: $\mathcal{F} = \mathcal{F}(\gamma t^a, t^{\frac{k - 1}{2}})$ is linear because $f(t) = \gamma t^a = \gamma t$ and $g(t) = t^{\frac{k - 1}{2}} = -t$, yet it is
not in the standard form given above, namely $\mathcal{F}(\gamma t, t)$.

We conclude this section with the following proposition.

**Proposition 3.** If $\mathcal{F} = \mathcal{F}(\gamma t^{2k+1}, t^{k+1+c})$ is a flock, then $c$ and $q - 1$ have a nontrivial
common divisor.

**Proof.** Since $\mathcal{F}$ is a flock, we have by (1): $H(t, 0) = g(t)^2 + 4tf(t) = t^{2k+2}(t^{2c} + 4\gamma)$, which is
a nonsquare for all nonzero $t \in GF(q)$ if and only if $(t^{2c} + 4\gamma)$ is. The map
$GF(q) \mapsto GF(q), x \mapsto x^2 + 4\gamma$, takes on $\frac{q+1}{2}$ nonzero values, but there are only $\frac{q+1}{2}$
nonsquares in $GF(q)$. This implies that $GF(q) \mapsto GF(q), t \mapsto t^4$ is not a bijection, hence $c$
and $q - 1$ have a nontrivial common divisor.

3. **Sporadic semifield monomial flocks**

A flock is **semifield** if the associated translation plane is coordinatized by a semifield. This
is equivalent to $f$ and $g$ being additive. Also, semifield flocks are equivalent to some trans-
lation generalized quadrangles (for more details, see, e.g., [20]) and to translation ovoids of
$Q(4, q)$ [6, 16, 17, 26]. This makes the class of semifield flocks a very special one, and it is
almost completely classified.

In fact, semifield flocks which are not linear do not exist for $q$ even by [12], and, in addition
to the known classes (linear, Kantor, Ganley) only sporadic examples may exist for $q$ odd
by [3]; a unique example is known: the sporadic semifield flock for $q = 3^5$, which happens
to be monomial, and it is computed and completely studied in [4].

The general construction for semifield flocks which gives back, in particular, the sporadic
semifield flock of the quadratic cone of $PG(3, 3^5)$, is the following.
Theorem 1. Let \( p \) be an odd prime and \( q = p^s \). Suppose there exist: \( \delta \in GF(q) \) and an integer \( c \) such that \( t^{2c} + \delta \) is a non-square in \( GF(q) \) for all \( t \in GF(q) \) and \( t \neq 0 \), an integer \( k \) such that \( k + c + 1 = p^i \) and \( 2k + 1 = p^j \) for some integers \( 1 \leq i, j \leq n - 1 \). Then \( F = F^i\left(2k+1, t^{k+c+1}\right) \) is a sporadic monomial semifield flock. Conversely, any sporadic monomial semifield flock is constructed as above.

Proof. Recall that for semifield flocks the exponents of \( t \) in both \( f \) and \( g \) must be powers of the characteristic \( p \), as these maps are additive.

A direct computation shows that \( H(t, s) = (t - s)^{2k+2}(t - s)^{2c} + \delta \) is a non-square for all \( t, s \in GF(q) \) with \( t \neq s \). Conversely, if such a flock exists, \( c \) can be computed. \( \square \)

Example. The sporadic semifield (monomial) flock is defined by \( p = 3, n = 5, k = 4, c = 22, \delta = 1, i = 3, j = 2 \).

Computer Results. Using the software MAGMA [7], we showed that
1. for \( p = 3, n \leq 100 \) and \( n \neq 5 \), no sporadic semifield monomial flocks exist;
2. for \( p \leq 100, n \leq 10 \) and \( (p, n) \neq (3, 5) \), no sporadic semifield monomial flocks exist;
3. for \( p = 3 \) and \( n = 5 \), there are the following 22 possibilities for the values satisfying the hypotheses of Theorem 1. They are

\[
\begin{align*}
c &= -11, \quad k = 13, \quad j = 3, \quad i = 1, \quad f(t) = \delta t^{27}, \quad g(t) = t^3 \\
c &= 22, \quad k = 4, \quad j = 2, \quad i = 3, \quad f(t) = \delta t^9, \quad g(t) = t^{27}
\end{align*}
\]

with \( \delta \) in the cyclic group \( G \) of order 11 generated by \( \gamma^{22} \), \( \gamma \) a primitive element of \( GF(3) \).

Denote by \( F_3 \), respectively \( F_3' \), the above flock corresponding to \( c = -11 \), respectively \( c = 22 \), and \( \delta \), so that \( F_3 \) consists of the planes \( \pi_1 : tx_0 - \delta t^{27}x_1 + t^3x_2 + x_3 = 0 \) with \( t \in GF(3^5) \) and \( F_3' \) consists of the planes \( \pi'_1 : tx_0 - \delta t^9x_1 + t^{27}x_2 + x_3 = 0 \) with \( t \in GF(3^5) \). Note that \( F_3' \) is the sporadic semifield flock.

In the following theorem it is shown all these flocks are isomorphic, so that semifield mono-

Theorem 2. Any of the flocks \( F_3 \) and \( F_3' \) is isomorphic to the sporadic semifield flock constructed in [4] using the ovoid of [21].

Proof. With the substitution \( t = s^9 \), since \( s \in GF(3^5) \), we can rewrite \( F_3 \) as the set of the planes with equation \( s^9x_0 - \delta s x_1 + s^{27}x_2 + x_3 = 0 \); now the collineation \( (x_0, x_1, x_2, x_3) \mapsto (-\delta x_1, -\delta^{-1}x_0, x_2, x_3) \) fixes the cone and maps the planes of \( F_3' \) to the planes of \( F_3 \). Thus \( F_3' \cong F_3 \), and there are at most 11 nonequivalent examples.

To complete the proof, we write the translation ovoids of \( O(4, 3^5) \) associated with these flocks. Recall that by [16, Theorem 4] the flocks are isomorphic if and only if the ovoids are.

Following the computation of [4] with a few slight changes, one obtains that associated with the flock \( F_3' \) is the ovoid \( O_3 = \{(0, 0, 0, 0, 1)\} \cup \{(1, x, y, -\delta x^9 - y^{81}, -y^2 + \delta x^{10} + xy^{81}) | x, y \in GF(3^5)\} \), and \( O = O_1 \) is the Penttila–Williams ovoid of [21].

To conclude, we show that \( O \cong O_3 \) for all \( \delta \in G \). We adapt to our case some ideas of the proof of the existence of a \( C_{22} \) in the stabilizer of the ovoid of [21]. If there is an element \( \tau \) of \( PT\mathcal{O}(5, 3^{5}) \) mapping \( O \mapsto O_3 \), we can suppose \( (0, 0, 0, 0, 1) \) is fixed because it is the special point of the ovoid, and \((1, 0, 0, 0, 0) \) may be fixed as well because \( PT\mathcal{O}(5, 3^{5})\{(0,0,0,0,1)\} \)
is transitive on the remaining points of the translation ovoid $O_3$. Then, $\tau$ is $\tau_{a,b,c}$ with the companion automorphism $\sigma$ as it is defined in [21], i.e., $\tau_{a,b,c}(1, x, y, \gamma = -x^9 - yx^8, -y^2 + x^{10} + x^8y^3)$ = $(b^2, c^{-1}x^\sigma + ay^\sigma + a^2cx^9y^\sigma, by^\sigma - abcxy^81\sigma, -b^2cx^9y^\sigma - b^2cy^81\sigma, -y^2\sigma + x^{10}\sigma + x^7y^{81}\sigma)$. Because this last is a point of $O_3$, then $\delta(c^{-1}x^\sigma + ay^\sigma + a^2cx^9y^\sigma + b^{-144}(by^\sigma - abcxy^81\sigma))^2 = b^{18}(y^9\sigma + y^81\sigma)$ for all $x, y \in GF(3^5)$. As the last equation holds for $x = 0$ and any $y \in GF(3^5)$, we get $a = 0$ and $c = b^{-81}$. On the other hand, substituting $a = 0$, for $y = 0$ we get $\delta c^{-9}x^9 = -b^{18}cx^9y^\sigma$ for all $x \in GF(3^5)$, hence $\delta = b^{96}$ and $c = b^{-81}$. Therefore, if $\delta = \gamma^{22i}$, with $\gamma$ a generator of the multiplicative group of $GF(3^5)$, then $a = 0, b = \gamma^{81i},$ and $c = \gamma^{27i}$. In addition, it is clear that such a $\tau_{a,b,c}$ exists and provides the required isomorphism.

We conclude this section with the construction of the sporadic semifield flock. This flock was computed by L. Bader, G. Lunardon and I. Pinneri [4] from the Penttila–Williams ovoid of $Q(4, 3^3)$ constructed with a little help from a computer in [21]. The results of [6, 16, 26] may also be applied to construct the Penttila–Williams ovoid from the sporadic semifield flock. Thus, giving a computer-free proof of the existence of the sporadic semifield flock below also leads to a computer-free proof of the existence of the Penttila–Williams ovoid.

**Theorem 3.** Let $q = 3^5$. For $f(t) = t^9$ and $g(t) = t^{27}$, the $q$ planes $\pi_t$ with equation $tx_0 - t^3x_1 + t^2x_2 + x_3 = 0, t \in GF(q)$, define a flock.

**Proof.** We must show that $H(t, s) = (g(t) - g(s))^2 + 4(t-s)(f(t) - f(s))$ is a nonsquare for all $t, s \in GF(q)$ with $t \neq s$, that is, $(t-s)^5 + (t-s)^4$ is a nonsquare for all $t, s \in GF(q)$ with $t \neq s$. It is therefore sufficient to show that $x^{44} + 1$ is a nonsquare for all $x \in GF(3^5)$ with $x \neq 0$. Now $(q-1)/2 = 121$ and $(x^{44} + 1)^{21} = (x^{44} + 1)^{1+3+3^2+3^3+3^4}$. Let $y = x^{44}$. Then $(y + 1)^{1+3+3^2+3^3+3^4} = (y + 1)(y^3 + 1)(y^{3^2} + 1).$ We are only interested in $(x^{44} + 1)^{121} modulo x^{242} - 1$ and so we are only interested in $(y + 1)^{121} modulo y^{11} - 1$, and thus we are concerned with the behavior of $\{1, 3, 3^2, 3^3, 3^4\}$ modulo 11. Of course, these are the quadratic residues modulo 11, giving rise to the biplane with automorphism group $PSL(2, 11)$, associated with $M_{11}$.

$(y + 1)(y^3 + 1)(y^{3^2} + 1)(y^{3^3} + 1)(y^{3^4} + 1) = -1$ modulo $y^{11} - 1$, since every nonzero element of the integers modulo 11 can be expressed as a sum of a subset of $\{1, 3, 3^2, 3^3, 3^4\}$ in exactly three ways, as each is the sum of two distinct elements of $\{1, 3, 3^2, 3^3, 3^4\}$ in exactly one way, and the sum of three distinct elements of $\{1, 3, 3^2, 3^3, 3^4\}$ in exactly one way and is either the sum of one element of $\{1, 3, 3^2, 3^3, 3^4\}$ or the sum of four distinct elements of $\{1, 3, 3^2, 3^3, 3^4\}$ (but not both). Thus $(y + 1)(y^3 + 1)(y^{3^2} + 1)(y^{3^3} + 1)(y^{3^4} + 1) = y^{121} + 1 = -1$ modulo $y^{11} - 1$. Hence $(x^{44} + 1)^{121} = -1$ modulo $x^{242} - 1$, implying $(x^{44} + 1)^{121} = -1$ for all nonzero $x \in GF(3^5)$. Hence $x^{44} + 1$ is a nonsquare, for all nonzero $x \in GF(3^5)$.

We remark that the 11th roots of unity in $GF(3^5)$ also played a role in the original proof of the existence of the Penttila–Williams ovoid in [21], and that the stabilizer of the set of 11th roots of unity of $GF(3^5)$ in $PGL(5, 3)$ in $M_{11}$. Presumably, the remarkable properties of the quadratic residues modulo 11 used in the proof above are related to the sharp 4-transitivity of $M_{11}$.

**4. The Case** $f(t) = a\gamma^{1+2k}, \ g(t) = \beta \gamma^{1+k}$

Apart from the sporadic semifield flock, all the known examples of monomial flocks have $f(t) = a\gamma^{1+2k}, \ g(t) = \beta \gamma^{1+k}$. In addition, flocks with these $f, g$ are related to a class of
translation planes studied by Y. Hiramine and N. L. Johnson in [11]. By Proposition 1, we can restrict ourselves to flocks \( F = \mathcal{F}(\gamma t^{1+2k}, t^{1+k}) \), with \( \gamma \in GF(q) \).

Put \( H(t,s) = dm^2(t,s) \) for \( d \) a fixed nonsquare in \( GF(q) \) and \( m(t,s) \) a reduced polynomial over \( GF(q) \). Suppose \( H(t,s) = dm^2(t,s) \) holds as a polynomial identity. For any odd integer \( r \), let \( f_r \) and \( g_r \) be the extensions to \( GF(q^s) \) of \( f \) and \( g \) respectively; note that \( \mathcal{F}(f_r, g_r) \) is a flock of the quadratic cone of \( PG(3, q^s) \). Hence, following [3, 4], we say that \( F = \mathcal{F}(\gamma t^{1+2k}, t^{1+k}) \) is a nonsporadic monomial flock if equality \( H(t,s) = dm^2(t,s) \) holds as a polynomial identity.

Let \( a_0, a_1, \ldots, a_{k-1} \in GF(q) \) be defined by \( \frac{H(t,1)}{(1+4\gamma)(q-1)^2} = h^2(t) \) with \( h(t) = t^k + a_{k-1}t^{k-1} + \cdots + a_1t + a_0 \).

The proofs of the following results are obtained by tedious computation, which are given in detail in [2].

**Theorem 4.** Let \( k \) be odd. If a nonsporadic flock \( F = \mathcal{F}(\gamma t^{1+2k}, t^{1+k}) \) exists, then both \( \gamma \) and \( 1+4\gamma \) are nonsquares in \( GF(q) \) and

\[
a_0 = -1, \quad a_i = -a_{k-i} \quad \forall i = 1, \ldots, k-1.
\]

Furthermore, the flock is unique with

\[
\gamma = \frac{-(k+1)^2}{4(2k+1)},
\]

so that \(-(2k+1)\) is a nonsquare in \( GF(q) \). \( \square \)

**Theorem 5.** Let \( k \) be even. At most two nonsporadic flocks \( F = \mathcal{F}(\gamma t^{1+2k}, t^{1+k}) \) exist, for \( a_0 = \pm 1 \), and in both cases \( 1+4\gamma \) is a nonsquare in \( GF(q) \). If, furthermore, we assume \( a_0 = -1 \), then \( \gamma \) has the expression (4), and thus \(-(2k+1)\) is a nonsquare in \( GF(q) \). \( \square \)

**Theorem 6.** Let \( k \) be an integer such that \( 1 \leq k \leq 6 \). Then, a nonsporadic flock \( F = \mathcal{F}(\gamma t^{1+2k}, t^{1+k}) \) exists only if \( k = 1 \), and the flock is the Fisher–Thas–Walker flock, or \( k = 2 \), and the flock is the Kantor–Payne flock. \( \square \)

**Remark.** Doing by hand the computation of Theorem 6 for small \( k \) makes clear that, if any example exists, all equations involving either the \( a_i \) or \( b_i \) coefficients imply, at least for each particular \( k \), many strong restrictions on the characteristic of \( GF(q) \).

Moreover a computer search using GAP [23] has shown that in \( GF(q) \) with \( q < 450 \) no example for \( k \) odd exist apart from the known ones.

**Acknowledgements**

This research is partially supported by GNSAGA and by the Italian Ministry for University, Research and Technology (project: *Strutture geometriche, combinatoria e loro applicazioni*).

**References**

On monomial flocks


Received 12 May 2000 and accepted 12 March 2001

LAURA BADER
Dipartimento di Matematica e Applicazioni,
Università di Napoli ‘Federico II’,
Complesso di Monte S. Angelo-Edificio T,
Via Cintia,
I-80126 Napoli, Italy
E-mail: laura.bader@dma.unina.it
DINA GHINELLI
Dipartimento di Matematica,
Università di Roma ‘La Sapienza’,
Piazzale Aldo Moro 2,
I-00185 Roma, Italy
E-mail: dina@mat.uniroma1.it
AND

TIM PENTTILA
Department of Mathematics and Statistics,
University of Western Australia,
WA 6907 Australia
E-mail: penttila@maths.uwa.edu.au