Partial flocks of the quadratic cone

PETER SZIKLAI

Department of Computer Science
Eötvös University, Budapest
Pázmány P. s. 1/c, Budapest, H-1117,
Hungary
sziklai@cs.elte.hu

Abstract: We prove that in PG(3, q), q > 19, a partial flock of a quadratic cone
with q − ε planes, can be extended to a unique flock if ε < \frac{\sqrt{q}}{4}.

Keywords: flock, cone

A flock of the quadratic cone of PG(3, q) is a partition of the points of the cone different from
the vertex into q irreducible conics. Associated with flocks are some line spreads of PG(3, q) and
translation planes [4, 5]; q-clans and some elation generalised quadrangles [8, 14]; hyperbolic
fibrations [2]; BLT-sets (when q is odd) [1, 7]; and, when q is even, families of ovals in PG(2, q),
called herds [3]. In [12] Storme and Thas remark that this idea can be applied to partial flocks
(i.e. sets of pairwise disjoint conics on the cone), obtaining a correspondence between partial
flocks of order k and (k + 2)-arcs of PG(2, q), and constructing herds of (k + 2)-arcs. Using this
correspondence, they can prove that, for q > 2 even, a partial flock with > q − \sqrt{q} − 1 planes if
q is a square and > q − \sqrt{2q} if q is a nonsquare, is extendable to a unique flock. (For q odd
the case of 1 missing conic was solved by Payne and Thas [9].)

Applying this result, Storme and Thas could give new and shorter proofs of some known
theorems, e.g., they can show directly that if the planes of the flock have a common point then
the flock is linear (this originally was proved by Thas relying on a theorem by D.G. Glynn on
inversive planes, and is not true in general if q is odd). Here we prove the following

Theorem 1 Let q > 19. Assume that the planes E_i, i = 1, ..., q − ε intersect the quadratic cone
C ⊂ PG(3, q) in disjoint irreducible conics. If ε < \frac{\sqrt{q}}{4} then one can find additional ε planes
(in a unique way), which extend the set \{E_i\} to a flock.

We note that a similar theorem holds for cones with base curve of higher degree, the proof is
far more complicated though, see [11]. However, the proof below works for cones with any base
curve in the case ε = 1.

Lemma 2 Let C_n be a curve of order n defined over GF(q), and denote by N the number of its
points in PG(2, q). Suppose that C_n does not contain a component defined over GF(q) of degree
≤ 2. Choose a constant \frac{1}{3} + \frac{2\sqrt{q} + 1}{3q} ≤ α and assume that n ≤ α\sqrt{q}. Then N ≤ nα\alpha.

For curves without linear component a similar lemma can be found in Sziklai [10], which is
a variant of a lemma by Szőnyi [13].

*Research was supported by OTKA F043772, T043758, T049662, TÉT Hungarian-Spanish and Magyary grants
Proof: Suppose first that \( C_n \) is absolutely irreducible. Then the Hasse-Weil theorem ([16], [6], Cor. 2.30) gives \( N \leq q + 1 + (n - 1)(n - 2)\sqrt{q} \leq nqa. \) (As \( q + 1 + (n - 1)(n - 2)\sqrt{q} - nqa \leq 0 \) holds for both \( n = 3 \) and \( n = \alpha \sqrt{q} \)).

If \( C_n \) is not absolutely irreducible, then it can be written as \( C_n = D_{n_1} \cup \ldots \cup D_{n_s}, \) where \( D_{n_j} \) is an absolutely irreducible component of order \( n_j, \) so \( \sum_{j=1}^{s} n_j = n. \) If \( D_{n_j} \) cannot be defined over \( GF(q), \) then it has at most \( N_{n_j} \leq (n_j)^2 \leq n_jqa \) points in \( PG(2, q) \) (see [6], Lemma 2.24).

If \( D_{n_j} \) is defined over \( GF(q), \) then the Weil-bound implies again that \( N_{n_j} \leq n_jqa. \) Hence

\[
N = \sum_{j=1}^{s} N_{n_j} \leq \sum_{j=1}^{s} n_jqa = nqa.
\]

Proof of the Theorem. Let \( C \) be the quadratic cone \( C = \{(1, t, t^2, z) : t, z \in GF(q) \} \cup \{(0, 0, 1, z) : z \in GF(q) \} \cup \{(0, 0, 0, 1) \} \) and \( C^* = C \setminus \{(0, 0, 0, 1) \}. \) Suppose that the planes \( E_i \) intersect \( C^* \) in disjoint conics, and \( E_i \) has equation \( X_4 = a_iX_1 + b_iX_2 + c_iX_3 \) for \( i = 1, 2, \ldots, q - \varepsilon. \)

Define \( f_i(T) = a_i + b_iT + c_iT^2, \) then \( E_i \cap C^* = \{(1, t, t^2, f_i(t)) : t \in GF(q) \} \cup \{(0, 0, 1, c_i) \}. \) (By a little abuse of notation) let \( \sigma_k(T) = \sigma_k(f_i(T) : i = 1, \ldots, q - \varepsilon) \) denote the \( k \)-th elementary symmetric polynomial of the polynomials \( f_i, \) then \( \deg_T(\sigma_k) \leq 2k. \) As for any fixed \( T = t \in GF(q) \) the values \( f_i(t) \) are all distinct, we would like to find

\[
\frac{X^q - X}{\prod_i (X - f_i(t))},
\]

the roots of which are the missing values \( GF(q) \setminus \{f_i(t) : i = 1, \ldots, q - \varepsilon\}. \)

In order to do so, we define the elementary symmetric polynomials \( \sigma_j^*(t) \) of the “missing elements” with the following formula:

\[
X^q - X = \left(X^{q-\varepsilon} - \sigma_1(t)X^{q-\varepsilon-1} + \sigma_2(t)X^{q-\varepsilon-2} - \ldots \pm \sigma_{q-\varepsilon}(t)\right)\left(X^\varepsilon - \sigma_1^*(t)X^{\varepsilon-1} + \sigma_2^*(t)X^{\varepsilon-2} - \ldots \pm \sigma_\varepsilon^*(t)\right);
\]

from which \( \sigma_j^*(t) \) can be calculated recursively from the \( \sigma_k(t) \)-s, as the coefficient of \( X^{q-j}, j = 1, \ldots, q - 2 \) is 0 = \(-\sigma_j^*(t) + \sigma_{j-1}^*(t)\sigma_1(t) - \ldots \pm \sigma_1^*(t)\sigma_{j-1}(t) \mp \sigma_j(t); \) for example

\[
\sigma_1^*(t) = -\sigma_1(t); \quad \sigma_2^*(t) = \sigma_1(t)^2 - \sigma_2(t); \quad \sigma_3^*(t) = -\sigma_1(t)^3 + 2\sigma_1(t)\sigma_2(t) - \sigma_3(t);
\]

etc. Note that we do not need to use all the coefficients/equations, it is enough to do it for \( j = 1, \ldots, \varepsilon. \)

Using the same formulae, obtained from the coefficients of \( X^{q-j}, j = 1, \ldots, \varepsilon, \) one can define the polynomials

\[
\sigma_1^*(T) = -\sigma_1(T); \quad \sigma_2^*(T) = \sigma_1(T)^2 - \sigma_2(T); \quad \sigma_3^*(T) = -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T);
\]

up to \( \sigma_\varepsilon^*. \) Note that \( \deg_T(\sigma_j^*) \leq 2j. \) From the definition

\[
\left(X^{q-\varepsilon} - \sigma_1(T)X^{q-\varepsilon-1} + \sigma_2(T)X^{q-\varepsilon-2} - \ldots \pm \sigma_{q-\varepsilon}(T)\right)\left(X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - \ldots \pm \sigma_\varepsilon^*(T)\right)
\]

is a polynomial, which is \( X^q - X \) for any substitution \( T = t \in GF(q), \) so it is \( X^q - X + (T^q - T)\ldots. \)

Now define

\[
G(X, T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - \ldots \pm \sigma_\varepsilon^*(T),
\]
from the recursive formulae it is a polynomial in $X$ and $T$, of total degree $\le 2\varepsilon$ and $X$-degree $\varepsilon$.

For any $T = t \in \text{GF}(q)$ the polynomial $G(X, t)$ has $\varepsilon$ roots in $\text{GF}(q)$ (i.e. the missing elements $\text{GF}(q) \setminus \{f_i(t) : i = 1, \ldots, q - \varepsilon\}$), so the algebraic curve $G(X, T)$ has at least $N \ge \varepsilon q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$. Suppose that $G$ has no component (defined over $\text{GF}(q)$) of degree $\le 2$.

Let’s apply the Lemma with $\alpha = \max(\frac{1}{3} + \frac{2\sqrt{q+1}}{q^2}, \frac{2}{\sqrt{q}}) < \frac{1}{2}$ if $q > 19$; we have

$$
\varepsilon q \le N \le 2\varepsilon \alpha q < \varepsilon q,
$$

which is false, so $G = G_1 G_2$, where $G_1$ is an irreducible factor over $\text{GF}(q)$ of degree at most 2. If deg$_X G_1 = 2$ then deg$_X G_2 = \varepsilon - 2$, which means that $G_1$ has at most $q+1$ and $G_2$ has at most $(\varepsilon - 2)q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$ (at most $\varepsilon - 2$ for each $T = t \in \text{GF}(q)$), contradiction (as $G$ has at least $\varepsilon q$).

Both $G_1$ and $G_2$, expanded by the powers of $X$, are of leading coefficient 1. So $G_1$ is of the form $G_1(X, T) = X - f_{\varepsilon-1}(T)$, where $f_{\varepsilon-1}(T) = a_{\varepsilon-1} + b_{\varepsilon-1} T + c_{\varepsilon-1} T^2$. Let the plane $E_{\varepsilon-1}$ be defined by $X_4 = a_{\varepsilon-1} X_1 + b_{\varepsilon-1} X_2 + c_{\varepsilon-1} X_3$.

The plane $E_{\varepsilon-1}$ intersects $C^*$ in $\{(1, t^2, f_{\varepsilon-1}(t)) : t \in \text{GF}(q)\} \cup \{(0, 0, 1, c_{\varepsilon-1})\}$. Now we prove that for any $t \in \text{GF}(q)$ the points $\{(1, t^2, f_i(t)) : i = 1, \ldots, q-\varepsilon\}$ and $(1, t^2, f_{\varepsilon-1}(t))$, in other words, the values $f_1(t), \ldots, f_{\varepsilon-1}(t)$: $f_{\varepsilon-1}(t)$ all distinct. But this is obvious from

$$
\left(X^q - \sigma_1(t) X^{q-\varepsilon} + \sigma_2(t) X^{q-2\varepsilon} - \ldots - \pm \sigma_{q-\varepsilon}(t)\right)(X - f_{\varepsilon-1}(t)) \mid X^q - X.
$$

Now one can repeat all this above and get $f_{\varepsilon-2}, \ldots, f_1$, so we have

$$
G(X, T) = \prod_{q-\varepsilon+1}^q (X - f_i(T))
$$

and the values $f_i(t), i = 1, \ldots, q$ are all distinct for any $t \in \text{GF}(q)$. The only remaining case is $\varepsilon = \infty$: we have to check whether the intersection points $E_1 \cap C^*$ on the plane at infinity $X_1 = 0$, i.e. the values $c_1, \ldots, c_{q-\varepsilon}; c_{q-\varepsilon+1}, \ldots, c_q$ are all distinct (for $\Gamma$ we know it). (Note that if $q$ planes partition the affine part of $C^*$ then this might be false for the infinite part of $C^*$.) From (1), considering the leading coefficients in each defining equality, we have

$$
\sigma_1(\Gamma) = -\sigma_1(\Gamma); \quad \sigma_2(\Gamma^*) = \sigma_1(\Gamma) - \sigma_2(\Gamma); \quad \sigma_3(\Gamma^*) = -\sigma_1(\Gamma)^3 + 2\sigma_1(\Gamma)\sigma_2(\Gamma) - \sigma_3(\Gamma);
$$

etc.,

($\sigma_k(\Gamma)$ has its original meaning, the $k$-th elementary symmetric polynomial of the elements of $\Gamma$), so $X^q - X =

\left(X^q - \sigma_1(\Gamma) X^{q-\varepsilon} \pm \sigma_2(\Gamma) X^{q-2\varepsilon} \ldots \pm \sigma_{q-\varepsilon}(\Gamma)\right)(X^q - \sigma_1(\Gamma) X^{q-\varepsilon} + \sigma_2(\Gamma) X^{q-2\varepsilon} - \ldots \pm \sigma_1(\Gamma^*) X^{q-\varepsilon} + \sigma_2(\Gamma^*) X^{q-2\varepsilon} - \ldots \pm \sigma_1(\Gamma^*)\right),

which completes the proof. (As it was pointed out by one of the referees, there is an alternative nice geometrical argument to handle the case “$t = \infty$”.)

Remark. Using other results instead of the Hasse-Weil bound on the number $N$ of $\text{GF}(q)$-rational points of a curve in Lemma 2, one may strengthen the result above. For example, when $q = p$ is a prime then the Stöhr-Voloch bound [15] saying that $N \le 2n(n - 2) + \frac{2}{3}n p$ yields

3
Theorem 3 In PG(3, p), p prime, if $\varepsilon < \frac{1}{4p}p + 1$ then a partial flock of $q - \varepsilon$ irreducible conics on the quadratic cone can be extended to a (unique) flock.

I am grateful to Aart Blokhuis and András Gács for the discussions on the case “$\varepsilon = 1$” at La Roche; and to Laura Bader for drawing my attention to the links and various applications at Capomulini. I would like to thank Tamás Szőnyi and the referees for their suggestions.

References


