

Flocks of cones of higher degree

Peter Sziklai

Received: 27 February 2006 / Accepted: 1 August 2006 /
Published online: 4 October 2006
© Springer Science + Business Media, LLC 2007

Abstract It is known that in $\text{PG}(3, q)$, $q > 19$, a partial flock of a quadratic cone with $q - \varepsilon$ planes, can be extended to a unique flock if $\varepsilon < \frac{1}{4}\sqrt{q}$, and a similar and slightly stronger theorem holds for the case q even. In this paper we prove the analogue of this result for cones with base curve of higher degree.

Keywords Flock · Cone

1 Introduction

A *flock* of a cone of $\text{PG}(3, q)$ is a partition of the points of the cone different from the vertex into q disjoint plane sections. The case of the quadratic cone was investigated by several researchers. Associated with flocks of the quadratic cone are some line spreads of $\text{PG}(3, q)$ and translation planes; q -clans and some elation generalised quadrangles of order (q^2, q) ; hyperbolic fibrations; BLT-sets (when q is odd); and, when q is even, families of ovals in $\text{PG}(2, q)$, called herds.

Parts (i) and (ii) of the following theorem were proved in [10] in a short way, while part (iii) is due to Storme and Thas [11].

Theorem 1. *Let $q > 19$. Assume that the planes E_i , $i = 1, \dots, q - \varepsilon$ intersect the quadratic cone $C \subset \text{PG}(3, q)$ in disjoint irreducible conics.*

- (i) *If $\varepsilon < \frac{1}{4}\sqrt{q}$ then one can find additional ε planes (in a unique way), which extend the set $\{E_i\}$ to a flock.*

Research is supported by OTKA F-043772, T-043758, T-049662, TÉT Hungarian-Spanish and Magyary grants.

P. Sziklai (✉)

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

- (ii) If $q = p$ is a prime and $\varepsilon < \frac{1}{40}p + 1$ then the partial flock can be extended to a unique flock.
- (iii) If q is even and $\varepsilon \leq \sqrt{q}$ if q is a square and $\varepsilon < \sqrt{2}\sqrt{q}$ if q is a nonsquare then the partial flock can be extended to a unique flock.

In Section 2 of this paper we prove the following analogue of this result for cones with base curve of higher degree. The proof will be more complicated than in the quadratic case.

Theorem 2. For $2 \leq d \leq \sqrt[3]{q}$ consider the cone $\{(1, t, t^d, z) : t, z \in \text{GF}(q)\} \cup \{(0, 0, 1, z) : z \in \text{GF}(q)\} \cup \{(0, 0, 0, 1)\} = C \subset \text{PG}(3, q)$ and let $C^* = C \setminus \{(0, 0, 0, 1)\}$. Assume that the planes $E_i, i = 1, \dots, q - \varepsilon, E_i \not\ni (0, 0, 0, 1)$, intersect C^* in pairwise disjoint curves. If $\varepsilon < \lfloor \frac{1}{d^2}\sqrt{q} \rfloor$ then one can find additional ε planes (in a unique way), which extend the set $\{E_i\}$ to a flock, (i.e. q planes partitioning C^*).

The proof (see below) starts like in the quadratic case. Using elementary symmetric polynomials we find an algebraic curve $G(X, Y)$, which “contains” the missing planes in some sense. The difficulties are (i) to show that G splits into ε factors, and (ii) to show that each of these factors corresponds to a missing plane. For (i) we use our new Lemma 3. For (ii) we have to show that most of the possible terms of such a factor do not occur, which needs a linear algebra argument on a determinant with entries being elementary symmetric polynomials; this matrix may be well-known but the author could not find a reference for it. To be self-contained we include that half of the proof which is common with the one in [10].

2 Proof

Lemma 3. Choose three constants $1 \leq d \leq \sqrt[3]{q}, \alpha \geq \frac{1}{d+1} + \frac{1+d(d-1)\sqrt{q}}{(d+1)q}$ and $n \leq \frac{1}{d}\sqrt{q} - d + \frac{3}{2}$. Let C_n be a curve of order n defined over $\text{GF}(q)$, and denote by N the number of its points in $\text{PG}(2, q)$. Suppose that C_n does not contain a component defined over $\text{GF}(q)$ of degree $\leq d$. Then $N \leq nq\alpha$.

For curves without linear component a similar lemma can be found in Sziklai [9], which is a variant of a lemma by Szőnyi [12]. For curves without quadratic component see [10].

Proof: (i) Suppose first that C_n is absolutely irreducible. Then Weil’s theorem ([15], [6]) gives $N \leq q + 1 + (n - 1)(n - 2)\sqrt{q}$. We want $q + 1 + (n - 1)(n - 2)\sqrt{q} \leq nq\alpha$. As it is quadratic in n it is enough to check it for $n = d + 1$ and $n = \frac{1}{d}\sqrt{q} - d + \frac{3}{2}$, and it holds indeed.

If C_n is not absolutely irreducible, then it can be written as $C_n = \mathcal{D}_1 \cup \dots \cup \mathcal{D}_s$, where \mathcal{D}_j is an absolutely irreducible component of order i_j , so $\sum_{j=1}^s i_j = n$. If \mathcal{D}_j can not be defined over $\text{GF}(q)$, then it has at most $N_j \leq (i_j)^2 \leq i_j q\alpha$ points in $\text{PG}(2, q)$ (see [6], Lemma 2.24). If \mathcal{D}_j is defined over $\text{GF}(q)$, then the Weil-bound implies again

that $N_j \leq i_j q \alpha$. Hence

$$N = \sum_{j=1}^s N_j \leq \sum_{j=1}^s i_j q \alpha = n q \alpha.$$

□

Proof of Theorem 2. Suppose that the plane E_i has the equation $X_4 = a_i X_1 + b_i X_2 + c_i X_3$, for $i = 1, 2, \dots, q - \varepsilon$.

Define $f_i(T) = a_i + b_i T + c_i T^d$, then $E_i \cap C = \{(1, t, t^d, f_i(t)) : t \in \text{GF}(q)\} \cup \{(0, 0, 1, c_i)\}$. Let $\sigma_k(T) = \sigma_k(\{f_i(T) : i = 1, \dots, q - \varepsilon\})$ denote the k -th elementary symmetric polynomial of the polynomials f_i , then $\text{deg}_T(\sigma_k) \leq dk$. As for any fixed $T = t \in \text{GF}(q)$ 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 $\text{GF}(q) \setminus \{f_i(t) : i = 1, \dots, q - \varepsilon\}$.

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

$$X^q - X = (X^{q-\varepsilon} - \sigma_1(t)X^{q-\varepsilon-1} + \sigma_2(t)X^{q-\varepsilon-2} - \dots \pm \sigma_{q-\varepsilon}(t)) \times (X^\varepsilon - \sigma_1^*(t)X^{\varepsilon-1} + \sigma_2^*(t)X^{\varepsilon-2} - \dots \pm \sigma_\varepsilon^*(t));$$

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

$$\begin{aligned} \sigma_1^*(t) &= -\sigma_1(t); & \sigma_2^*(t) &= \sigma_1(t)^2 - \sigma_2(t); \\ \sigma_3^*(t) &= -\sigma_1(t)^3 + 2\sigma_1(t)\sigma_2(t) - \sigma_3(t); \dots \end{aligned} \tag{1}$$

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

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

$$\begin{aligned} \sigma_1^*(T) &= -\sigma_1(T); & \sigma_2^*(T) &= \sigma_1(T)^2 - \sigma_2(T); \\ \sigma_3^*(T) &= -\sigma_1(T)^3 + 2\sigma_1(T)\sigma_2(T) - \sigma_3(T); \dots \end{aligned} \tag{1^*}$$

up to σ_ε^* . Note that $\text{deg}_T(\sigma_j^*) \leq dj$. From the definition

$$\begin{aligned} &(X^{q-\varepsilon} - \sigma_1(T)X^{q-\varepsilon-1} + \sigma_2(T)X^{q-\varepsilon-2} - \dots \pm \sigma_{q-\varepsilon}(T)) \times \\ &(X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - \dots \pm \sigma_\varepsilon^*(T)) \end{aligned}$$

is a polynomial, which is $X^q - X$ for any substitution $T = t \in \text{GF}(q)$, so it is of the form $X^q - X + (T^q - T)(\dots)$. Now define

$$G(X, T) = X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - \dots \pm \sigma_\varepsilon^*(T), \tag{2}$$

from the recursive formulae it is a polynomial in X and T , of total degree $\leq d\varepsilon$ and X -degree ε .

For any $T = t \in \text{GF}(q)$ the polynomial $G(X, t)$ has ε roots in $\text{GF}(q)$ (i.e. the missing elements $\text{GF}(q) \setminus \{f_i(t) : i = 1, \dots, q - \varepsilon\}$), so the algebraic curve $G(X, T)$ has at least $N \geq \varepsilon q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$. Suppose that G has no component (defined over $\text{GF}(q)$) of degree $\leq d$. Let's apply the Lemma with a suitable $\frac{1}{d+1} + \frac{1+d(d-1)\sqrt{q}}{(d+1)q} \leq \alpha < \frac{1}{d}$, $n = \deg G \leq d\varepsilon \leq \frac{1}{d}\sqrt{q} - d + \frac{3}{2}$, we have

$$\varepsilon q \leq N \leq d\varepsilon q \alpha < \varepsilon q,$$

which is false, so $G = H_1 G_1$, where H_1 is an irreducible factor over $\text{GF}(q)$ of degree at most d . If $\deg_X H_1 = d_X \geq 2$ then $\deg_X G_1 = \varepsilon - d_X$, which means that H_1 has at most $q + 1 + (d_X - 1)(d_X - 2)\sqrt{q}$ and G_1 has at most $(\varepsilon - d_X)q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$ (at most $\varepsilon - d_X$ for each $T = t \in \text{GF}(q)$), so in total G has

$$\varepsilon q \leq N \leq (\varepsilon - d_X + 1)q + 1 + (d_X - 1)(d_X - 2)\sqrt{q},$$

a contradiction if $2 \leq d_X \leq \sqrt{q} + 1$, so $\deg_X H_1 = 1$.

One can suppose w.l.o.g. that both H_1 and G_1 , expanded by the powers of X , are of leading coefficient 1. So H_1 is of the form $H_1(X, T) = X - f_{q-\varepsilon+1}(T)$, where

$$f_{q-\varepsilon+1}(T) = a_{q-\varepsilon+1} + b_{q-\varepsilon+1}T + c_{q-\varepsilon+1}T^d + \delta_{q-\varepsilon+1}(T),$$

where $\delta_{q-\varepsilon+1}(T)$ is an ‘‘error polynomial’’ with terms of degree between 2 and $d - 1$. At the end of the proof we will show that $\delta_{q-\varepsilon+1}$ and other error polynomials are zero.

Now one can repeat everything for G_1 , which has at least $(\varepsilon - 1)q$ distinct points in $\text{GF}(q) \times \text{GF}(q)$ (as H_1 has exactly q and $H_1 G_1$ has at least εq). A similar reasoning gives $G_1 = H_2 G_2$, where $H_2(X, T) = X - f_{q-\varepsilon+2}(T)$ with $f_{q-\varepsilon+2}(T) = a_{q-\varepsilon+2} + b_{q-\varepsilon+2}T + c_{q-\varepsilon+2}T^d + \delta_{q-\varepsilon+2}(T)$. Going on we get $f_{q-\varepsilon+3}, \dots, f_q$ (where for $j = q - \varepsilon + 1, \dots, q$ we have $f_j(T) = a_j + b_j T + c_j T^d + \delta_j(T)$, where $\delta_j(T)$ contains terms of degree between 2 and $(d - 1)$ only). Hence

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

For any $t \in \text{GF}(q)$ the values $f_1(t), \dots, f_q(t)$ are all distinct, this is obvious from

$$\begin{aligned} & (X^{q-\varepsilon} - \sigma_1(t)X^{q-\varepsilon-1} + \sigma_2(t)X^{q-\varepsilon-2} - \dots \pm \sigma_{q-\varepsilon}(t)) \times \\ & ((X - f_{q-\varepsilon+1}(t)) \cdots (X - f_q(t))) = X^q - X. \end{aligned}$$

For $j = q - \varepsilon + 1, \dots, q$ let the plane E_j be defined by $X_4 = a_j X_1 + b_j X_2 + c_j X_3$. We are going to prove that $\{E_j : j = 1, \dots, q\}$ is a flock.

First we check the case “ $t = \infty$ ”: we have to check whether the intersection points $E_i \cap C$ on the plane at infinity $X_1 = 0$, i.e. the values $\underbrace{c_1, \dots, c_{q-\varepsilon}}_{\Gamma}; \underbrace{c_{q-\varepsilon+1}, \dots, c_q}_{\Gamma^*}$ are all distinct (for Γ we know it). (Note that even 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

$$\begin{aligned} \sigma_1(\Gamma^*) &= -\sigma_1(\Gamma); \quad \sigma_2(\Gamma^*) = \sigma_1(\Gamma)^2 - \sigma_2(\Gamma); \\ \sigma_3(\Gamma^*) &= -\sigma_1(\Gamma)^3 + 2\sigma_1(\Gamma)\sigma_2(\Gamma) - \sigma_3(\Gamma); \end{aligned}$$

etc., so

$$\begin{aligned} X^q - X &= (X^{q-\varepsilon} - \sigma_1(\Gamma)X^{q-\varepsilon-1} + \sigma_2(\Gamma)X^{q-\varepsilon-2} - \dots \pm \sigma_{q-\varepsilon}(\Gamma)) \\ &\quad \times (X^\varepsilon - \sigma_1(\Gamma^*)X^{\varepsilon-1} + \sigma_2(\Gamma^*)X^{\varepsilon-2} - \dots \pm \sigma_{q-\varepsilon}(\Gamma^*)), \end{aligned}$$

which we wanted to prove.

Now we want to get rid of the δ_j 's, i.e. we are going to prove that $\delta_{q-\varepsilon+1}, \dots, \delta_q = 0$. Let s be the maximal T -exponent appearing in any of $\delta_{q-\varepsilon+1}, \dots, \delta_q$, so each $\delta_j(T) = d_j T^s + \dots$ (for $j = q - \varepsilon + 1, \dots, q$; also $2 \leq s \leq d - 1$ and there exists a $d_j \neq 0$). In the equation

$$\begin{aligned} G(X, T) &= X^\varepsilon - \sigma_1^*(T)X^{\varepsilon-1} + \sigma_2^*(T)X^{\varepsilon-2} - \dots \pm \sigma_\varepsilon^*(T) \\ &= \prod_{i=1}^\varepsilon (X - a_{q-\varepsilon+i} - b_{q-\varepsilon+i}T - c_{q-\varepsilon+i}T^d - \delta_{q-\varepsilon+i}(T)), \end{aligned}$$

the coefficient of $X^{\varepsilon-j} T^{d(j-1)+s}$, $j = 1, \dots, \varepsilon$, is zero on the left hand side (i.e. the coefficient of $T^{d(j-1)+s}$ in σ_j^* , it can be seen by induction from (1*) for instance), and it is

$$\sigma_{j-1}(\Gamma^* \setminus \{c_{q-\varepsilon+1}\})d_{q-\varepsilon+1} + \sigma_{j-1}(\Gamma^* \setminus \{c_{q-\varepsilon+2}\})d_{q-\varepsilon+2} + \dots + \sigma_{j-1}(\Gamma^* \setminus \{c_q\})d_q$$

on the right hand side. Hence we have a system of homogeneous linear equations for $d_{q-\varepsilon+1}, \dots, d_q$ with the elementary symmetric determinant

$$\begin{aligned} &\begin{vmatrix} 1 & 1 & \dots & 1 \\ \sigma_1(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_1(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & \dots & \sigma_1(\Gamma^* \setminus \{c_q\}) \\ \sigma_2(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_2(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & \dots & \sigma_2(\Gamma^* \setminus \{c_q\}) \\ \vdots & \vdots & \dots & \vdots \\ \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_{q-\varepsilon+1}\}) & \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_{q-\varepsilon+2}\}) & \dots & \sigma_{\varepsilon-1}(\Gamma^* \setminus \{c_q\}) \end{vmatrix} \\ &= \prod_{1 \leq i < j \leq \varepsilon} (c_{q-\varepsilon+i} - c_{q-\varepsilon+j}), \end{aligned}$$

which is non-zero as the c_i 's are pairwise distinct. Hence the unique solution is $d_{q-\varepsilon+1}, \dots, d_q = 0$ and $f_j(T) = a_j + b_j T + c_j T^d$ for each $j = 1, \dots, q$.

Our final and the last missing argument we need is that for $j = 1, \dots, q$ the plane E_j intersects C in $\{(1, t, t^d, f_j(t)) : t \in \text{GF}(q)\} \cup \{(0, 0, 1, c_j)\}$, so these intersections are pairwise disjoint, E_1, \dots, E_q is a flock of C . \square

References

1. L. Bader, Flocks of cones and related structures, *lecture notes*.
2. R.D. Baker, G.L. Ebert, and T. Penttila, "Hyperbolic fibrations and q -clans," *Des. Codes Crypt.* **34** (2005), 295–305.
3. L. Bader, G. Lunardon, and J.A. Thas, "Derivation of flocks of quadratic cones," *Forum Math.* **2** (1990), 163–174.
4. J.C. Fisher and J.A. Thas, "Flocks in $\text{PG}(3, q)$," *Math. Z.* **169** (1979), 1–11.
5. H. Gevaert and N.L. Johnson, "Flocks of quadratic cones, generalised quadrangles and translation planes," *Geom. Dedicata* **27** (1988), 301–317.
6. J.W.P. Hirschfeld, *Projective geometries over finite fields, 2nd edition*, Oxford University Press, 1998.
7. N. Knarr, "A geometric construction of generalized quadrangles from polar spaces of rank three," *Resultate Math.* **21** (1992), 332–344.
8. W.M. Kantor, "Note on generalized quadrangles, flocks and BLT-sets," *J. Comb. Theory Ser. (A)* **58** (1991), 153–157.
9. P. Sziklai, "On subsets of $\text{GF}(q^2)$ with d -th power differences," *Discrete Math.* **208–209** (1999), 547–555.
10. P. Sziklai, "Partial flocks of the quadratic cone," *J. Combin. Th. Ser. A* **113** (2006), 698–702.
11. L. Storme, and J. A. Thas, " k -arcs and partial flocks," *Linear Algebra Appl.* **226/228** (1995), 33–45.
12. T. Szőnyi, "On the number of directions determined by a set of points in an affine Galois plane," *J. Combin. Th. Ser. A* **74** (1996), 141–146.
13. J.A. Thas, "Generalized Quadrangles and Flock of Cones," *Europ. J. Combin.* **8** (1987), 441–451.
14. M. Walker, "A class of translation planes," *Geom. Dedicata* **5** (1976), 135–146.
15. A. Weil, "Sur les Courbes Algébrique et les varietés qui s'en déduisent," *Actualités Scientifiques et Industrielles* **1041**, Herman & Cie, Paris, 1948.