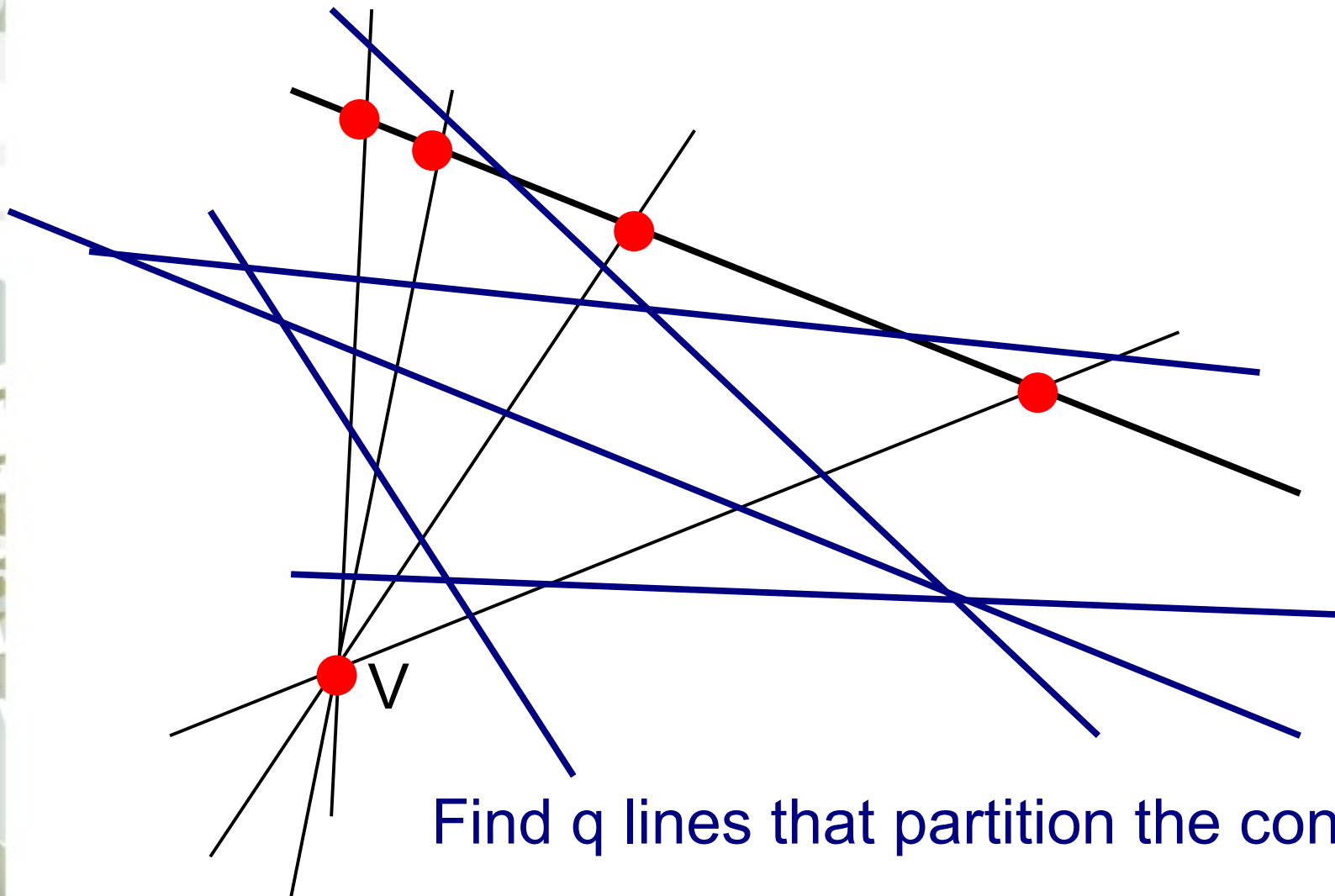


Permutation Polynomials, Flocks and Flokki

Bill Cherowitzo
UC Denver
May 8, 2009

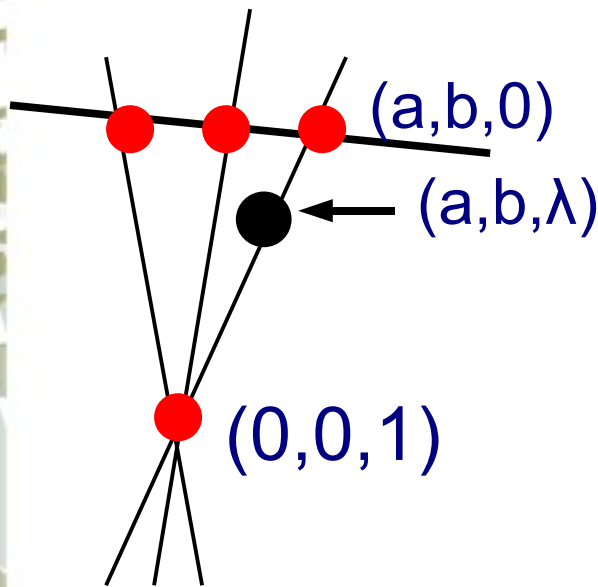
A Simple Geometric Problem



Find q lines that partition the cone - $\{V\}$

A Simple Geometric Problem

We can assume that the line is $z = 0$ and that $V=(0,0,1)$.
Bijectively assign elements of $GF(q)$ to any set of q lines that do not pass through V . This defines functions f and g so that the equations of the lines can be written as $f(t)x + g(t)y - z = 0$ for each $t \in GF(q)$.



The point (a,b,λ) is on each line for which $f(t)a + g(t)b = \lambda$. So, if the function $f(t)a + g(t)b$ is a permutation, no two lines can meet at a point of this generator.

If this condition is met for each generator, we will have a solution.

The Real Result

Theorem 1: Let \mathcal{S} be any set of points in $PG(n,q)$ not including $V = (0,0,\dots,1)$. Let \mathcal{S}^* be the set of points in the hyperplane $x_n = 0$ obtained by projecting \mathcal{S} from V . The points of the cone $V\mathcal{S}^* - \{V\}$ can be partitioned by q hyperplanes if and only if there exist n functions f_0, f_1, \dots, f_{n-1} over $GF(q)$ such that

$$f_0(t)a_0 + f_1(t)a_1 + \dots + f_{n-1}(t)a_{n-1}$$

is a permutation polynomial for each $(a_0, a_1, \dots, a_{n-1}, 0)$ in \mathcal{S}^* .

Dickson Permutation Polynomials

The Dickson polynomials (of the first kind) are:

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

They satisfy the recursion:

$$D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a) \quad \text{with } D_0 = 2, D_1 = x.$$

Theorem: A Dickson polynomial $D_n(x, a)$ is a permutation polynomial (in x , for all a) over $GF(q)$ iff $(n, q^2-1) = 1$.

OK – So what do we really want?

The main interest has always been in the 3-dimensional case of Theorem 1 when the cone is a quadratic cone.

The planes (or their conic intersections) that partition the quadratic cone are called a **flock**. The set of permutation polynomials defined by the flock is called a **herd** (only in even characteristic - if you are Tim!).

If the planes of a flock are given by :

$$\pi_t : f(t)x + g(t)y + h(t)z - w = 0 \quad \forall t \in GF(q)$$

the set of q 2×2 matrices given by
is called a **q -clan** (– if you are Stan!) $\begin{pmatrix} f(t) & g(t) \\ 0 & h(t) \end{pmatrix}$

Kantor/Payne Flocks

Consider the Dickson permutation polynomial $D_5(t,-a) = t^5 + 5at^3 + 5a^2t$ for odd $q \equiv \pm 2 \pmod{5}$.

By Theorem 1, $\pi_t : t^5x + 5t^3y + 5tz - w = 0$ is a flock of the quadratic cone $xz = y^2$. This is the Kantor monomial flock (K_2) [Kantor, '86].

When we restrict this example to even q we get: $D_5(t,a) = t^5 + at^3 + a^2t$ for $q = 2^{2k+1}$. Since in these fields $t \rightarrow t^{1/6}$ is a permutation, we have that $\pi_t : t^{5/6}x + t^{3/6}y + t^{1/6}z + w = 0$ is a flock of the quadratic cone $xz = y^2$. This is the Payne flock. [Payne, '85]

Notation

I have made pains to represent these flocks in a form that would make them easily recognizable, but it is not necessary to do this.

Also, there is an arbitrary choice about where to place the constants in this representation of the pp's, either in the flock functions or in the cone coordinates. My preference is for the latter.

Thus, I would denote the Kantor/Payne flock by:

$$\mathcal{F} = [t^5, t^3, t] \text{ for } q \equiv \pm 2 \pmod{5}$$

where the cone is $5xz = y^2$.

Tim's Flokki

But now, there is more interest in non-quadratic cones (Thanks, Tim).

Consider the Dickson permutation polynomial
 $D_7 = x^7 - 7ax^5 + 14a^2x^3 - 7a^3x$ $q \not\equiv \pm 1 \pmod{7}$
which for even q becomes,

$$D_7(x,a) = x^7 + ax^5 + a^3x \quad q = 2^e, 3 \nmid e$$

By Theorem 1, $[t^7, t^5, t]$ is a “flokki” of the cone $xz = y^3$.

β - clans

As Tim just mentioned, these are not flokki.

When I found them [WEC '97] I called them **3-clans**.

Let Σ_β be the cone in $PG(3,q)$ with vertex $(0,0,0,1)$ given by $y^\beta = xz^{\beta-1}$ where $(\beta - 1, q-1) = 1$.

A “flock” of Σ_β is called a **β -clan**.

By Theorem 1, a β -clan is equivalent to the set of q permutation polynomials given by:

$$F(t,x) = x^\beta f(t) + xg(t) + h(t) \text{ when } f \text{ is a pp.}$$

Monomial β - clans

To simplify the discussion, consider the special case where the clan functions are monomial, i.e., let

$$f(t) = At^a \quad g(t) = Bt^b \quad h(t) = Ct^c \quad \text{where } B \neq 0.$$

The condition that $F(t,x)$ is a pp for any $x \in GF(q)$ is:

$$x^\beta + x \neq -\kappa \frac{(t^a - s^a)^{\frac{1}{\beta-1}} (t^c - s^c)}{(t^b - s^b)^{\frac{\beta}{\beta-1}}} \quad \forall t \neq s \quad \text{where } \kappa = \frac{A^{\frac{1}{\beta-1}} C}{B^{\frac{\beta}{\beta-1}}}$$

Note that the constant $-\kappa$ is not of the form $x^\beta + x$ (set $t = 1$ and $s = 0$).

A Dumb Little Result

Theorem 2 [WEC '97] : Let $q = p^h$. If $\beta = p^i + 1$, then $[t^a, t^b, \kappa t^c]$ is a β -clan iff $[t^{(\beta-1)c}, t^b, \kappa t^{a/(\beta-1)}]$ is a β -clan.

Proof: Since $\beta-1$ corresponds to an automorphism we have:

$$-K \frac{(t^a - s^a)^{\frac{1}{p^i}} (t^c - s^c)}{(t^b - s^b)^{\frac{\beta}{\beta-1}}} = -K \frac{(t^{p^i c} - s^{p^i c})^{\frac{1}{p^i}} (t^{\frac{a}{p^i}} - s^{\frac{a}{p^i}})}{(t^b - s^b)^{\frac{\beta}{\beta-1}}}$$

Note: This works in the non-monomial case as well.

... with some consequences

Example: Let $q = 2^e$ and $\beta = 3$. Then if $[t^a, t^b, t^c]$ is a 3-clan, so is $[t^{2c}, t^b, t^{a/2}]$. So, for instance, when $3 \nmid e$ $[t, t^5, t^7]$ is a 3-clan and so is $[t^{14}, t^5, t^{1/2}]$.

For all q and all β we have that the linear flock $[t, t, \kappa t]$ is a β -clan. Thus, applying Theorem 2 to the linear flock gives:

Corollary: $[t^{p^i}, t, t^{p^{-i}}]$ is a (p^i+1) -clan over $\text{GF}(p^e)$ for each $0 \leq i < e$.

Another 3-clan is thus $[t^2, t, t^{1/2}]$ over $\text{GF}(2^e)$.

Linearized Polynomials

A rich source of pp are the *linearized polynomials*:

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in GF(q^r)[x]$$

A linearized polynomial is a pp when $L(x) = 0$ iff $x = 0$.

Equivalently,

$$\begin{vmatrix} a_0 & a_{r-1}^q & a_{r-2}^{q^2} & \cdots & a_1^{q^{r-1}} \\ a_1 & a_0^q & a_{r-1}^{q^2} & \cdots & a_2^{q^{r-1}} \\ a_2 & a_1^q & a_0^{q^2} & \cdots & a_3^{q^{r-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{r-1} & a_{r-2}^q & a_{r-3}^{q^2} & \cdots & a_0^{q^{r-1}} \end{vmatrix} \neq 0$$

Prequasifields

A finite **prequasifield** is a finite vector space K over the prime field, together with a binary operation $*$ on K that is left distributive and such that

$$x * t_1 = x * t_2 \Rightarrow x = 0 \text{ or } t_1 = t_2.$$

This produces a translation plane in a standard manner.

We can obtain prequasifields easily by defining

$$x * t = L(x,t)$$

where $L(x,t)$ is a linearized polynomial in x (this gives the left distributivity) and $(1/x)L(x,t)$ is a pp for all t (this satisfies the condition above).

β -clans \rightarrow Translation planes

Tim uses $L(x,t) = x^4a(t) + x^2b(t) + xc(t)$ and shows that the 3-clans $[a(t),b(t),c(t)] = [t,t^5,t^7]$ and $[t^{14},t^5,t^{1/2}]$ produce prequasifields over $GF(2^e)$ when $3 \nmid e$.

Theorem 3 : Any (2^i-1) -clan defines a prequasifield (and hence a translation plane) over $GF(2^e)$ when $(i-1, e) = 1$.

Proof: Let $L(x,t) = x^{2^i}f(t) + x^2g(t) + xh(t)$.

$x^{2^i-1}f(t) + xg(t) + h(t)$ is a pp $\forall t \Leftrightarrow [f(t),g(t),h(t)]$ is a (2^i-1) -clan.

“Real” Flokki

Using the cone $xy^\alpha = z^{\alpha+1}$ with vertex $(0,0,0,1)$ where $t \rightarrow t^\alpha$ is any automorphism of $GF(q)$, any $(-\alpha)$ -clan [without the $(\beta-1, q-1)=1$ condition] is called a **flokki**.

Putting the $(-\alpha)$ -clan into the form $[f(t), t, g(t)]$ then

$$\begin{pmatrix} u + [g(t)]^{\frac{1}{\alpha}} & -[f(t)]^{\frac{1}{\alpha}} \\ t & u^\alpha \end{pmatrix} \quad \forall u, t \in GF(q)$$

is a spread set and the corresponding translation plane is called a **flokki plane**.

Flokki

The function f of a flokki must be a permutation (since the point $(1,0,0,0)$ is in the cone – this can also be seen from the spread set when $u = 0$) but the function g need not be.

All the examples of flokki in odd characteristic have $g \equiv 0$, a condition which implies that all the planes meet in a point (I call these ***star flocks***).

~~I suspect that all flokki in odd characteristic may be star flocks. [Note that the $(\beta-1, q-1)=1$ condition always fails in odd characteristic.]~~

I have a family of non-star flokki in odd characteristic. 5/12/09

Other Flokki (a.k.a. $(-\alpha)$ - clans)

Even characteristic provides a richer source of flokki, even after imposing the $(\beta-1, q-1)=1$ condition.

For instance, if $q = 2^{2^k-1}$ and $\sigma = 2^k$, it will follow from our next result that

$[t^2, t, \kappa t^\sigma]$ is always a $(-\sigma)$ – clan.

A special class of β -clans

Theorem 4: Let $\mathbb{F} = \text{GF}(p^r)$ be a proper subfield of $\mathbb{K} = \text{GF}(q)$ and let $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. With $0, a$ and b distinct, $[t^{pa}, t, \kappa t^{pb}]$ is a β -clan for

$$\beta \equiv \frac{j(q-1) + (p^r-1)(p^b-p^a)}{(p^b-1)(p^r-1)} \pmod{q-1} \quad \text{where } 0 \leq j < p^r-1,$$

whenever $(\beta-1, q-1) = 1$ and no element of $-\kappa\mathbb{F}^*$ is of the form $z^\beta + z$.

Note: The herd functions (pp's) of these clans are linearized polynomials. Any flocki of this form will give rise to semifield flocki planes.

But wait – there's more

A computer search for β -clans in even characteristic over the fields $GF(2^i)$, $i = 1, \dots, 8$ and partially for $i = 9$ [WEC '97] (under the additional assumption that $(\beta, q-1) = 1$) found, besides the special family and the 3-clans already mentioned, only two other examples.

For $q = 2^{2h+1}$,

$$\left[t^h, t, t^{\frac{5^h-1}{4(5^{h-1})}} \right]$$

and its mate by Theorem 2 are 5-clans for $h = 1, 2, 3$ but not 4.

Odds and Ends

Other families of pp's are known. Some, giving flocks, are:

As t^3 is a pp when $q \equiv 2 \pmod{3}$, so is $(t+a)^3 - a^3 = t^3 + 3at^2 + 3a^2t \quad \forall a$. Thus, $[t^3, t^2, t]$ is a flock (2-clan) for all $q \equiv 2 \pmod{3}$. These are the FTW flocks.

$f(t) = t^5 + 2\eta t^3 + \eta^2 t$, where η is a non-square is a pp when $q = 5^e$. Thus, $f(t+a) - (2\eta a^3 + \eta^2 a) = t^5 + 2\eta t^3 + \eta^2 t + 6\eta a t^2 + 6\eta a^2 t$ is a pp $\forall a$. This gives the flock $[t^5 + 2\eta t^3 + \eta^2 t, 6\eta t^2, 6\eta t]$ for $q = 5^e$. These are the Kantor "likeable" flocks due to Gevaert and Johnson.

And by the way ...

β -clans are equivalent to q - β clans (that is, they are in the same orbit of $\text{P}\Gamma\text{L}(4,q)_{v,w=0}$).

The Cardano flokki are (-2) -clans over $\text{GF}(2^e)$ and $-2 \equiv q - 3 \pmod{q - 1}$.

Thus, Tim's 3-clans are equivalent to the Cardano flokki, so my use of "flokki" is perfectly correct!