Planes, Nets and Webs

G. Eric Moorhouse, University of Wyoming

Two big open problems in finite geometry:

Q1. Must every finite (affine or projective) plane have prime power order?

Q2. Must every plane of prime order be Desarguesian?

The best progress to date on Q2:

Theorem. *Every* transitive *affine plane of prime order is Desarguesian.*

This result is a corollary of

Theorem. *Every planar polynomial over* $\mathbb{F}_p$ *is quadratic.*

Note: A polynomial $f(X) \in \mathbb{F}_p[X]$ is *planar* if for every nonzero $k \in \mathbb{F}_p$, the polynomial $f(X+k) - f(X)$ is a permutation of $\mathbb{F}_p$.

This result was proven independently by Gluck (1990); Rónyai and Szőnyi (1989); and Hiramine (1989).

Gluck's proof used exponential sums. These arise when applying characters to an elementary abelian collineation group.

My hope is to apply similar methods *without assuming any collineation group.* For us, exponential sums arise when applying characters to the dual code of a net.

Henceforth $F = \mathbb{F}_p$, p an odd prime.

Nets

Let $k \geq 2$.

$\pi_i : F^k \to F, \quad (a_1, \ldots, a_k) \mapsto a_i$

$\pi_{ij} : F^k \to F, \quad (a_1, \ldots, a_k) \mapsto (a_i, a_j)$

A *k-net of order p* is a subset $\mathcal{N} \subset F^k$ such that for all $i \neq j$ in $\{1, 2, \ldots, k\}$, the map

$$\mathcal{N} \xrightarrow{\pi_{ij}} F^2$$

is bijective.

p^2 **points**: elements of $\mathcal{N}$

pk **lines**: fibres $\mathcal{N} \cap \pi_i^{-1}(a)$, $a \in F$, $1 \leq i \leq k$

Examples

Cyclic 3-nets: $\mathcal{N} = \{(a, b, a+b) : a, b \in F\}$

Affine plane of order p	$\longleftrightarrow$	$(p+1)$-net of order p

Desarguesian affine plane of order p:

$$\mathcal{N} = \{(a, b, a+b, 2a+b, 3a+b, \ldots, (p-1)a+b) : a, b \in F\}$$

A k-net $\mathcal{N}$ gives rise to linear codes (vector spaces):

$\mathcal{V} = \mathcal{V}(\mathcal{N}) =$ the set of all k-tuples $(f_1, f_2, \ldots, f_k)$ of functions $f_i : F \to F$ such that

$$f_1(a_1) + f_2(a_2) + \cdots + f_k(a_k) = 0$$

for all $(a_1, a_2, \ldots, a_k) \in \mathcal{N}$.

$\mathcal{V}_0 \leq \mathcal{V}$ is the subspace satisfying the additional condition $f_1(0) = f_2(0) = \cdots = f_k(0) = 0$.

Clearly $\dim(\mathcal{V}/\mathcal{V}_0) = k - 1$.

The *rank* of $\mathcal{N}$ is $\dim(\mathcal{V}_0)$.

Compare: the *nullity* of the $p^2 \times pk$ incidence matrix of the design is

$$\dim(\mathcal{V}) = k - 1 + \dim(\mathcal{V}_0).$$

Let $\mathcal{N}$ be a k-net of order p.

Conjecture. *(i)* $\dim \pi_1(\mathcal{V}) \le k-1$.

(ii) $\dim(\mathcal{V}_0) \le (k-1)(k-2)/2$, *and equality holds iff* $\mathcal{N}$ *is Desarguesian.*

Note: $\dim \pi_1(\mathcal{V}) = 1 + \dim \pi_1(\mathcal{V}_0)$ for $k \ge 2$.

In the Desarguesian case ($2 \le k \le p+1$), $\pi_1(\mathcal{V})$ is a $[p, k-1, p-k+2]$ Reed Solomon code.

If the Conjecture (i) or (ii) is true, then *every* affine plane of prime order is Desarguesian.

The upper bound $(k-1)(k-2)/2$ appearing in (ii) is the upper bound for the arithmetic genus of an algebraic plane curve of degree k.

Webs are the smooth analogues of nets, defined over $\mathbb{C}$ or $\mathbb{R}$.

Theorem. *For webs over $\mathbb{C}$, we have* $\dim(\mathcal{V}_0) \leq (k-1)(k-2)/2$*, and equality holds iff the web arises from an algebraic curve of maximal genus* $(k-1)(k-2)/2$*.*

S. Lie, H. Poincaré, N. Abel,
W. Blaschke, S.S. Chern and P. Griffiths

Analogous results hold when the field $\mathbb{C}$ is replaced by $\mathbb{R}$ and $\mathbb{F}_p((X))$.

I want a similar result over $\mathbb{F}_p$.

Theorem (M. 1991). *Let $\mathcal{N}$ be a 3-net of prime order p. Then* $\dim(\mathcal{V}_0) \le 1$, *and equality holds iff $\mathcal{N}$ is cyclic.*

Original (and easiest) proof used loop theory. I now have several proofs of this result, including a proof using exponential sums.

Also using exponential sums:

Theorem (M. 2005). *Let $\mathcal{N}$ be a 4-net of prime order p.*

- *(i)* *The number of* cyclic *3-subnets of $\mathcal{N}$ is 0, 1, 3 or 4.*
- *(ii)* *$\mathcal{N}$ has* four *cyclic 3-subnets iff $\mathcal{N}$ is Desarguesian.*
- *(iii)* *Suppose $\mathcal{N}$ has* at least one *cyclic 3-subnet. Then* $\dim(\mathcal{V}_0) \le 3$, *and equality holds iff $\mathcal{N}$ is Desarguesian.*

Remarks. (i) and (ii) are best possible.
I expect the additional hypothesis in (iii) can be dropped, and this will verify our original conjecture in the case of 4-nets of prime order.

Exponential Sums

Let $F = \mathbb{F}_p$, p prime.

$\zeta = \zeta_p \in \mathbb{C}$ a primitive p-th root of unity.

$e : F \to \langle \zeta \rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\}$, $a \mapsto \zeta^a$.

$e(a+b) = e(a)e(b)$

Given $f : F \to F$, define the *exponential sum*

$$S_f = \sum_{a \in F} e(f(a)) = \sum_{a \in F} \zeta^{f(a)} \in \mathbb{Z}[\zeta].$$

Clearly $|S_f| \leq p$, and equality holds iff f is constant. Moreover

Theorem (Hasse-Davenport-Weil Bound). $|S_f| \leq (d-1)\sqrt{p}$ *whenever* f *is expressible as a polynomial* $f(X) \in F[X]$ *of degree* $d \geq 1$.

Theorem. *Let* $f : F \to F$.

(i) *If* $|S_{f(X)+cX}| = \sqrt{p}$ *for all* $c \in F$, *then* f *is quadratic.*

(ii) *If* $|S_{f(X)+cX}| \in \{0, \kappa\}$ *for all* $c \in F$, *then* f *has degree* ≤ 2.

(iii) *If* $|S_{X^2+cf(X)}| = \sqrt{p}$ *for all* $c \in F$, *then* f *is either constant or bijective.*

(iv) *Let* $C_f = \{c \in F : S_{f(X)+cX} \neq 0\}$. *If* $|C_f| \leq (p-1)/2$ *then* $|C_f| = 1$ *and* f *has degree* ≤ 1.

Proofs use:

Standard facts about exponential sums and cyclotomic fields.

Techniques similar to Gluck (1990), including use of Segre's theorem.

Rédei's lower bound $\frac{1}{2}(p+3)$ for the number of slopes determined by p noncollinear points in $AG_2(p)$.

Theorem (M. 1991). *Let $\mathcal{N}$ be a 3-net of prime order p. Then* $\dim(\mathcal{V}_0) \leq 1$*, and equality holds iff $\mathcal{N}$ is cyclic.*

Proof. Let $(f, g, h) \in \mathcal{V}_0$, i.e.

$$f, g, h : F \to F;$$
$$f(0) = g(0) = h(0) = 0;$$
$$f(a) + g(b) + h(c) = 0 \quad \text{for all } (a, b, c) \in \mathcal{N}.$$

Summing $\zeta^{f(a)+g(b)} = \zeta^{-h(c)}$ over all $(a, b, c) \in \mathcal{N}$ gives

$$S_f S_g = p\overline{S_h}$$

and similarly

$$S_g S_h = p\overline{S_f}, \qquad S_h S_f = p\overline{S_g}\ .$$

Thus

$$|S_f|^2 = |S_g|^2 = |S_h|^2 = \tfrac{1}{p} S_f S_g S_h\ .$$

Case I: $|S_f| = |S_g| = |S_h| \neq 0$.

In this case $|S_f| = |S_g| = |S_h| = p$ so $f, g, h : F \to F$ are constant functions; but then the condition $f(0) = g(0) = h(0) = 0$ forces $(f, g, h) = (0, 0, 0)$.

Case II: $S_f = S_g = S_h = 0$.

In this case $f, g, h : F \to F$ are permutations, so we may assume

$$f(a) = a, \quad g(b) = b, \quad h(c) = -c.$$

Now

$$0 = f(a) + g(b) + h(c) = a + b - c$$

for all $(a, b, c) \in \mathcal{N}$, i.e.

$$\mathcal{N} = \{(a, b, a+b) : a, b \in F\}. \qquad \square$$

4-Nets

Let $\mathcal{N}$ be a 4-net of prime order p, and let $(f, g, h, t) \in \mathcal{V}$; that is,

$$f, g, h, u : F \to F;$$
$$f(a)+g(b)+h(c)+u(d) = 0 \text{ for all } (a, b, c, d) \in \mathcal{N}.$$

Summing $\zeta^{f(a)+g(b)} = \zeta^{-h(c)-u(d)}$ over all $(a, b, c, d) \in \mathcal{N}$ gives

$$S_f S_g = \overline{S_h S_u}$$

and similarly

$$S_f S_h = \overline{S_g S_u}, \quad S_f S_u = \overline{S_g S_h}\ .$$

Then

$$(|S_f|^2 - |S_g|^2) S_h = 0$$

and similarly for all permutations of f, g, h, u.

This yields:

Lemma. *For every* $(f, g, h, u) \in \mathcal{V}$, *one of the following must hold:*

(i) $S_f = S_g = S_h = S_u = 0$;

(ii) $S_f = S_g = S_h = 0 \neq S_u$ *(up to a permutation of* f, g, h, u*); or*

(iii) $|S_f| = |S_g| = |S_h| = |S_u| > 0$.

Theorem (M. 2005). *Let* $\mathcal{N}$ *be a 4-net of prime order* p.

(i) *The number of* cyclic *3-subnets of* $\mathcal{N}$ *is 0, 1, 3 or 4.*

(ii) $\mathcal{N}$ *has* four *cyclic 3-subnets iff* $\mathcal{N}$ *is Desarguesian.*

(iii) *Suppose* $\mathcal{N}$ *has* at least one *cyclic 3-subnet. Then* $\dim(\mathcal{V}_0) \leq 3$, *and equality holds iff* $\mathcal{N}$ *is Desarguesian.*