Ranks of Nets and of Webs

G. Eric Moorhouse, University of Wyoming

Abstract. Let p be an odd prime, and let $\mathcal{N}$ be a 4-net of order p. In many cases we obtain bounds on the p-rank of $\mathcal{N}$ (i.e. the rank of its incidence matrix over $\mathbb{F}_p$), and structural properties of $\mathcal{N}$ that are deducible from its p-rank. The main tool in this investigation is the use of exponential sums over $\mathbb{F}_p$. Implications for the study of finite projective planes are described. Finally we highlight the analogy between our conjectured bounds for the p-rank of a net of prime order, and the known bounds for the rank of a web.

1. Introduction

Our interest in nets arises from the following two 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) is:

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

This result is a corollary of

1.2 Theorem. *Let p be prime. Then every planar polynomial over $\mathbb{F}_p$ is quadratic.*

Recall that a polynomial $f(X) \in \mathbb{F}_p[X]$ is called *planar* if for every nonzero $k \in \mathbb{F}_p$, the polynomial $f(X+k)-f(X)$ induces a permutation of $\mathbb{F}_p$. Theorem 1.2 was proven independently by Gluck [3], Rónyai and Szőnyi [14], and Hiramine [5]. Gluck's proof of this result made use of exponential sums, which arise naturally when applying characters of the elementary abelian collineation group of the plane. It is our hope that similar arguments may lead to an extension of Theorem 1.2 without the assumption of any collineation group, thereby providing an answer to (Q2). We show that exponential sums arise naturally in the study of nets, when characters are applied to the additive group of a certain code obtained from the net (the dual of the row space of the point-line incidence matrix of the net). By Theorem 1.5 below, we may assume that this group is large, and so we may reasonably hope that it provides a satisfactory substitute for a collineation group. It is in fact reasonable to hope that this method may provide some answers to (Q1), inasmuch as we have shown [9] that codes of nets provide a natural tool for addressing both questions. In this paper, however, we fix an odd prime p and consider only nets of order p.

In Section 3 we formally define a *k-net $\mathcal{N}$ of order p.* Less formally [9], $\mathcal{N}$ is an incidence system consisting of p^2 points and pk lines in which every line has p points; two lines are called *parallel* if they are either equal or disjoint; and parallelism of lines is an equivalence relation on the set of lines, with k parallel classes. Each parallel class is a partition of the point set into p lines, and any two non-parallel lines meet in a unique point. Every k-net $\mathcal{N}$ of order p gives rise to $(k{-}1)$-subnets of order p; in fact, k such subnets, each obtained by omitting one of the parallel classes of lines of $\mathcal{N}$. The *p-rank of* $\mathcal{N}$ is the $\mathbb{F}_p$-rank of its $p^2 \times kp$ incidence matrix. We have conjectured

1.3 Conjecture [9]**.** *Let $\mathcal{N}$ be a k-net of order p, and let $\mathcal{N}'$ be any of its $(k{-}1)$-subnets. Then $\mathrm{rank}_p(\mathcal{N}) - \mathrm{rank}_p(\mathcal{N}') \geq p - k + 1$.*

By taking the sum of a finite arithmetic series, the preceding conjecture implies

1.4 Conjecture. *Let $\mathcal{N}$ be a k-net of order p. Then $pk - \mathrm{rank}_p(\mathcal{N}) \leq \frac{1}{2}(k-1)(k-2)$.*

Note that the quantity $pk - \mathrm{rank}_p(\mathcal{N})$ is simply the *nullity* of the $pk \times p^2$ incidence matrix of the net $\mathcal{N}$. The significance of the conjectured upper bound $\frac{1}{2}(k-1)(k-2)$ is that this is also an upper bound for the arithmetic genus of an algebraic curve of degree k. This connection becomes evident in Section 4 where we indicate the theorem (in the case of infinite webs) which provides the analogue of Conjecture 1.4 (for the finite case). However, the finite case differs from the infinite case in several important respects, for example: In every known case where the upper bound of Conjecture 1.4 holds, then net is *Desarguesian,* i.e. a subnet of a Desarguesian affine plane (see Section 3); in the case of infinite webs, many examples are known. Furthermore the analogue of Conjecture 1.3 fails for infinite webs, as we shall see in Section 4. Thus while it is possible that the infinite case may provide some further inspiration for the finite case, we see that the finite case is 'tighter'. We also showed

1.5 Theorem [9]**.** *If Conjecture 1.3 holds then every plane of prime order is Desarguesian.*

The validity Conjecture 1.3 for $k = 3$ (the smallest nontrivial case) was established in [9] using loop theory. Here we offer two new proofs of this result (Theorem 3.3), the first using exponential sums, and the second (Section 6) using finite field arguments only. Now in addition to a two-line proof, we have two longer proofs; but these alternative approaches lead to further progress against Conjecture 1.3. In particular the method of exponential sums leads to a proof (in Section 3) of the following Theorem 1.6. A Desarguesian 3-net is called simply a *cyclic* 3-net since it is the unique 3-net of order p corresponding to the cyclic Latin square of order p.

1.6 Theorem. *Let $\mathcal{N}$ be a 4-net of 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 $\mathcal{N}$ has rank at least $4p{-}3$, and equality holds iff $\mathcal{N}$ is Desarguesian.

We remark that (i) and (ii) are best possible in the sense that there exist (necessarily non-Desarguesian) 4-nets of prime order p having 0, 1 or 3 cyclic subnets. Examples of these for $p=7$ are found at [12]. Further partial results in the direction of Conjecture 1.3 are found in [10], [11].

2. Exponential Sums

Let $F=\mathbb{F}_p$ where p is an odd prime, and let $\zeta\in\mathbb{C}$ be a primitive p-th root of unity. We have a well-defined map

$$e:F\to\mathbb{Z}[\zeta],\quad a\mapsto\zeta^a$$

satisfying $e(a+b)=e(a)e(b)$ for all $a,b\in F$. Each function $f:F\to F$ gives rise to an *exponential sum*

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

In the following we call a function $f:F\to F$ *linear* (respectively, *quadratic*) if it is represented by a polynomial in $F[X]$ of degree 1 (resp. 2).

2.1 Lemma. *Let $f:F\to F$ and suppose $|S_f|=\sqrt{p}$. Then there exists a quadratic polynomial $g(X)\in F[X]$ such that the sequence $(f(0),f(1),\ldots,f(p-1))$ is a permutation of $(g(0),g(1),\ldots,g(p-1))$. In particular, the fibre size $|f^{-1}(a)|$ equals*

$$\begin{cases}0, & \text{for exactly } (p-1)/2 \text{ choices of } a\in F;\\ 1, & \text{for exactly } 1 \text{ choice of } a\in F; \text{ and}\\ 2, & \text{for exactly } (p-1)/2 \text{ choices of } a\in F.\end{cases}$$

If moreover $f(0)=0$ then $f(X)=a\pi(X)^2+b\pi(X)$ for some $a,b\in F$ and some permutation $\pi:F\to F$ satisfying $\pi(0)=0$.

Proof. See Gluck [3]. To obtain the last assertion we assume that $f(0)=0$. By the previous conclusion there exist constants $a,b,c\in F$ and a permutation $\sigma:F\to F$ such that $f(X)=a\sigma(X)^2+b\sigma(X)+c$. Setting $\pi(X)=\sigma(X)-\sigma(0)$ gives the final conclusion. □

2.2 Lemma. *Let $f:F\to F$ and suppose $|S_{f(X)+cX}|=\sqrt{p}$ for all $c\in F$. Then f is quadratic.*

Proof. Consider the point set in the projective plane over F defined by

$$\mathcal{O}=\{(x,f(x),1):x\in F\}\cup\{(0,1,0)\}.$$

Note that $|\mathcal{O}|=p+1$; we will show that no three points of $\mathcal{O}$ are collinear. Suppose that three points of $\mathcal{O}$ lie on the line $aX+bY+cZ=0$ where $a,b,c\in F$ are not all zero. We cannot have $b = 0$, for then the line $aX + cZ = 0$ meets $\mathcal{O}$ in only two points including $(0, 1, 0)$. We may therefore assume $b = 1$ and that the line $aX + Y + cZ = 0$ meets $\mathcal{O}$ in three distinct points $(x_i, f(x_i), 1)$ for $i = 1, 2, 3$. This means that $f(X)+aX$ attains the value $-c \in F$ at least three times. However, $|S_{f(X)+aX}| = \sqrt{p}$, and by Lemma 2.1 we obtain a contradiction. □

For every function $f : F \to F$ we denote

$$A_f = \{a \in F : S_{f(X)+aX} \neq 0\}.$$

2.3 Lemma. *Suppose $|A_f| \leq \frac{1}{2}(p+1)$. Then $|A_f| = 1$ and f is either constant or linear.*

Proof. There exist distinct $x, y \in F$ such that $f(x)+ax = f(y)+ay$, if and only if $-a \in A_f$. Thus the subset $-A_f = \{-a : a \in A_f\} \subseteq F$ coincides with the set of all slopes to the graph of f in $AG_2(F)$, i.e. the set of difference quotients $(f(y) - f(x))/(y - x)$ for all pairs (x, y) of distinct elements of F. The result follows by a theorem of Rédei [13] (see also [1], [8]). □

2.4 Lemma. *Let $f : F \to F$ such that $f(0) = 0$ and $f(1) = 1$, and suppose that $|S_{X^2+cf(X)}| = \sqrt{p}$ for all $c \in F$. Then f is a permutation satisfying $f(t) = \pm t$ for all $t \in F$.*

Proof. Consider the projective plane $PG_2(F)$ with homogeneous coordinates (X, Y, Z) for points, in which we consider those points with $Z \neq 0$ as the 'affine points'. Every line other than the 'line at infinity' $Z = 0$ is either a 'vertical line' $X = aZ$ for some $a \in F$, or a 'non-vertical line' $Y = aX + bZ$ for some $a, b \in F$.

Consider the point set $\mathcal{O} = \mathcal{O}_1 \cup \{(0, 1, 0)\}$ in $PG_2(F)$ where

$$\mathcal{O}_1 = \{(f(t), t^2, 1) : t \in F\}.$$

We will show that $\mathcal{O}$ is an oval. Clearly the line $Z = 0$ meets $\mathcal{O}$ only in $(0, 1, 0)$.

Fix $a \in F$ and consider those affine lines passing through $(1, -a, 0)$, these being the nonvertical lines of slope a, i.e. lines of the form $Y = aX + cZ$ for some $c \in F$. Such a line meets $\mathcal{O}$ precisely in those points $(f(t), t^2, 1) \in \mathcal{O}_1$ such that $t^2 - af(t) = c$. By Lemma 2.1 (and since $|S_{X^2-af(X)}| = \sqrt{p}$), among such lines there is exactly one tangent to $\mathcal{O}$ and $(p-1)/2$ secants to $\mathcal{O}$. Since every point of the form $(1, -a, 0)$ (for $a \in F$) lies on a unique affine tangent to $\mathcal{O}$, but no two points of $\mathcal{O}_1$ lie on the same tangent, it follows that every point $P \in \mathcal{O}_1$ lies on a unique tangent line ℓ_P to $\mathcal{O}$. Since every non-vertical line through P meets $\mathcal{O}$ in at most two points, this means that of the $p+1$ lines through P, one is tangent and the other p are secants. In particular the vertical line through P

meets $\mathcal{O}$ only in P and $(0,1,0)$. This means that $f : F \to F$ is bijective and that $\mathcal{O}$ is an oval as claimed. By Segre's Theorem, $\mathcal{O}$ is a conic. Since $\mathcal{O}$ passes through $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$ and has both lines $Y=0$ and $Z=0$ as tangents, the conic $\mathcal{O}$ must be given by the equation $X^2 = YZ$ and the result follows. □

Note that for any $f : F \to F$, the value $|S_f|^2 = S_f\overline{S_f} \in \mathbb{Z}[\zeta]$ is an algebraic integer, and so in fact $|S_f|$ is an algebraic integer.

2.5 Lemma. *Let $f : F \to F$. Suppose there exists a real constant $\kappa > 0$ such that for all $c \in F$ we have $|S_{f(X)+cX}| \in \{0, \kappa\}$. Then either*

(a) f is quadratic and $|S_{f(X)+cX}| = \sqrt{p}$ for all $c \in F$, or

(b) f is constant or linear, i.e. $f(X) = a_1X + a_0$ for some $a_0, a_1 \in F$, and

$$|S_{f(X)+cX}| = \begin{cases} 0, & \text{if } c \neq -a_1; \\ p, & \text{if } c = a_1. \end{cases}$$

Proof. For each $c \in F$, define $\alpha_c \in \mathbb{C}$ by

$$\alpha_c = \begin{cases} \kappa^{-1} S_{f(X)+cX} & \text{if } S_{f(X)+cX} \neq 0; \\ 1, & \text{if } S_{f(X)+cX} = 0. \end{cases}$$

Note that $|\alpha_c| = 1$ for all $c \in F$. Consider the complex $p \times p$ matrix defined by

$$M = \left[\overline{\alpha_i}\zeta^{ij+f(j)}\right]_{i,j\in F}.$$

We easily check that $MM^* = pI$ where I is the $p \times p$ identity matrix, so that the matrix $p^{-1/2}M$ is unitary, and every eigenvalue of M has magnitude $\sqrt{p}$. Let $\varepsilon = (1,1,\ldots,1)^T \in \mathbb{C}^p$; then the hypothesis means that $M\varepsilon$ is a vector having k entries equal to κ and the remaining $p-k$ entries zero, where k is the number of $c \in F$ such that $|S_{f(X)+cX}| = \kappa$. Now

$$k\kappa^2 = \|M\varepsilon\|^2 = p\|\varepsilon\|^2 = p^2.$$

In particular, $k \geq 1$ and so $\kappa = |S_{f(X)+cX}|$ for some $c \in F$. Now $p^2/k = \kappa^2 \in \mathbb{Z}[\zeta]$ is an algebraic integer, so $k = 1$ or p.

If $k = p$ then $|S_{f(X)+cX}| = \kappa = \sqrt{p}$ for all $c \in F$, so $f(X)$ is quadratic by Lemma 2.2. Hence assume $k = 1$, so that $|S_{f(X)-a_1X}| = \kappa = p$ for some $a_1 \in F$, which implies that $f(X) - a_1X = a_0 \in F$ is constant. □

2.6 Lemma. *Let $f, g : F \to F$ be linearly independent functions satisfying $f(0) = g(0) = 0$, and suppose that $|S_{af+bg}| \in \{0, \sqrt{p}, p\}$ for all $a, b \in F$. Then there exists a permutation $\sigma : F \to F$ such that f and g are linear combinations of $\sigma(X)$ and $\sigma(X)^2$.*

Proof. We first assume that $f : F \to F$ is a permutation. In this case we may assume that $f(X) = X$; otherwise substitute $f^{-1}(X)$ for X in both $f(X)$ and $g(X)$. Now $|S_{aX+g(X)}| \in \{0, \sqrt{p}, p\}$ for all $a \in F$, and the value p cannot arise since $g(0) = 0$ and $g(X)$ is not a scalar multiple of X. Now Lemma 2.5 gives $g(X) = a_2X^2 + a_1X$ for some $a_1, a_2 \in F$ and we are done.

We may henceforth assume that no linear combination of f and g is a permutation; thus $|S_{af+bg}| \in \{\sqrt{p}, p\}$ for all $a, b \in F$, and in fact $|S_{af+bg}| = \sqrt{p}$ unless $a = b = 0$.

Since $|S_f| = \sqrt{p}$, Lemma 2.1 gives $f(X) = a_2\pi(X)^2 + a_1\pi(X)$ for some permutation $\pi : F \to F$ satisfying $\pi(0) = 0$. There is no loss of generality in assuming $\pi(X) = X$ and $a_2 = 1$, so that $f(X) = X^2 + a_1X$ and $|S_{X^2+a_1X+bg(X)}| = \sqrt{p}$ for all $b \in F$. Writing $h(X) = g\big(X - \frac{a_1}{2}\big)$, we have $|S_{X^2+bh(X)}| = \sqrt{p}$ for all $b \in F$ and so $h : F \to F$ is bijective by Lemma 2.4; but then g is bijective, a contradiction. □

3. Nets

Denote $F = \mathbb{F}_p$ where p is an odd prime, and let $k \ge 2$. For every $J \subseteq \{1, 2, \ldots, k\}$ we consider the projection $F^k \to F^{|J|}$ defined by

$$(a_1, a_2, \ldots, a_k) \mapsto (a_j : j \in J).$$

We simply write $\pi_i = \pi_{\{i\}}$, $\pi_{ij} = \pi_{\{i,j\}}$, and we denote $J' = \{1, 2, \ldots, k\} \smallsetminus J$ so that in particular

$$\pi_{i'}(a_1, a_2, \ldots, a_k) = (a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k).$$

We consider only nets of order p. A *k-net of order p* is a subset $\mathcal{N} \subseteq F^k$ such that for all $i \ne j$ in $\{1, 2, \ldots, k\}$, the map $\mathcal{N} \xrightarrow{\pi_{ij}} F^2$ is bijective. The members of $\mathcal{N}$ are called *points,* and the *lines* of $\mathcal{N}$ are the fibres

$$\mathcal{N} \cap \pi_i^{-1}(a) = \{v \in \mathcal{N} : \pi_i(v) = a\}$$

for $i \in \{1, 2, \ldots, k\}, a \in F$. For every $J \subseteq \{1, 2, \ldots, k\}$ of cardinality at least 2, clearly $\pi_J(\mathcal{N})$ is a $|J|$-net of order p; we call this a *$|J|$-subnet* of $\mathcal{N}$. In particular for each $i \in \{1, 2, \ldots, k\}$, we have that $\pi_{i'}(\mathcal{N})$ is a $(k-1)$-subnet of $\mathcal{N}$, obtained by simply deleting from $\mathcal{N}$ the i-th parallel class of lines. An *isomorphism* of nets $\phi : \mathcal{N} \to \mathcal{N}'$ is a map of the form $(a_1, a_2, \ldots, a_k) \mapsto (\alpha_1(a_{\sigma(1)}), \alpha_2(a_{\sigma(2)}), \ldots, \alpha_k(a_{\sigma(k)}))$ for some $\alpha_1, \alpha_2, \ldots, \alpha_k \in Sym(F)$

and $\sigma \in S_k$; this simply says that the corresponding point-line incidence structures are isomorphic.

An *affine plane* of order p is simply a $(p+1)$-net of order p. The *Desarguesian affine plane* is the $(p+1)$-net

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

A *Desarguesian net* is any subnet of $\mathcal{D}$. A Desarguesian 3-net is known simply as a *cyclic 3-net.* Every cyclic 3-net of order p is isomorphic to $\{(a, b, a{+}b) : a, b \in F\}$.

Denote by $\mathcal{V} = \mathcal{V}(\mathcal{N})$ the vector space consisting of all k-tuples $(f_1, f_2, \ldots, f_k)$ of functions $F \to F$ such that

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

for all $(a_1, a_2, \ldots, a_k) \in \mathcal{N}$. Also denote by $\mathcal{V}_0 = \mathcal{V}_0(\mathcal{N}) \leq \mathcal{V}$ the subspace consisting of all $(f_1, f_2, \ldots, f_k) \in \mathcal{V}$ satisfying the additional condition $f_1(0) = f_2(0) = \cdots = f_k(0) = 0$. The map $\mathcal{V} \to F^k$, $(f_1, f_2, \ldots, f_k) \mapsto (f_1(0), f_2(0), \ldots, f_k(0))$ induces an isomorphism from $\mathcal{V}/\mathcal{V}_0$ to a $(k{-}1)$-dimensional subspace of F^k; thus $\dim(\mathcal{V}) = \dim(\mathcal{V}_0) - k + 1$, and so we may focus our attention on $\mathcal{V}_0$ rather than on $\mathcal{V}$ itself. Since $\mathcal{V}$ may be interpreted as the right null space of the point-line incidence matrix A of $\mathcal{N}$ (a $p^2 \times pk$ matrix of 0's and 1's), this gives

3.1 Theorem. *The p-rank of $\mathcal{N}$ is given by*

$$\mathit{rank}_p\,\mathcal{N} = \mathit{rank}_p\,A = pk - \dim\mathcal{V} = (p{-}1)k + 1 - \dim\mathcal{V}_0.$$

Rephrasing our conjectured bounds for the rank of A in terms of the nullity gives

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

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

Statement (i) is equivalent to Conjecture 1.3; and the first assertion of (ii) is implied by (i). If either (i) or (ii) holds then every plane of prime order is Desarguesian. As indication that $\mathcal{V}_0$ is more natural to consider than the row or column space of A itself, we observe that in the case of webs (Section 4), the corresponding incidence map has infinite rank, whereas the null space $\mathcal{V}$ is finite-dimensional; moreover the analogue of Conjecture 3.2(ii) is a theorem (see Theorem 4.1). The case $k = 3$ was settled in [9] using loop theory, and here we provide an alternative proof using exponential sums:

3.3 Theorem. *Let $\mathcal{N}$ be a 3-net of order p. Then $\dim(\mathcal{V}_0) \leq 1$. Moreover, equality holds iff $\mathcal{N}$ is cyclic, in which case $\mathcal{V}_0$ is spanned by a triple (f, g, h) in which the maps $f, g, h : F \to F$ are permutations.*

Proof. Let $(f, g, h) \in \mathcal{V}_0$. Summing $\zeta^{f(a)+g(b)} = \zeta^{-h(c)}$ over all $(a, b, c) \in \mathcal{N}$ gives $S_f S_g = \overline{S_h}$, and similarly $S_g S_h = \overline{S_f}$ and $S_h S_f = \overline{S_g}$. Thus

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

Now if $|S_f| = |S_g| = |S_h| = p$ then $f, g, h : F \to F$ are constant functions, but then the condition $f(0) = g(0) = h(0) = 0$ forces $(f, g, h) = (0, 0, 0)$.

Otherwise we must have $S_f = S_g = S_h = 0$, so that $f, g, h : F \to F$ are permutations. After permuting labels, we may assume that

$$f(X) = X, \quad g(X) = X, \quad h(X) = -X.$$

Now

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

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

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

which is the cyclic 3-net of order p. □

3.4 Lemma. *Let $\mathcal{N}$ be a 4-net of order p. Then for every $(f, g, h, u) \in \mathcal{V}$, either*

(a) three or more of S_f, S_g, S_h, S_u are zero; or
(b) $|S_f| = |S_g| = |S_h| = |S_u| > 0$.

Proof. Let $(f, g, h, u) \in \mathcal{V}$. 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 $S_f S_h = \overline{S_g S_u}$ and $S_f S_u = \overline{S_g S_h}$. This yields

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

and similarly for all permutations of f, g, h, u. The result follows. □

3.5 Lemma. *Let $\mathcal{N}$ be a 4-net of prime order p, and suppose $(0, X, X, X)$ and (f, g, h, u) are linearly independent members of $\mathcal{V}_0$. Then either*

(i) $|S_f| = |S_g| = |S_h| = |S_u| = \sqrt{p}$ and the functions g, h, u are quadratic, or
(ii) $S_f = 0$ and at least two of g, h, u are scalar multiples of X.

Proof. Suppose first that $S_f \neq 0$. Then for all $a \in F$, Lemma 3.4 implies that either

$$S_{g(X)+aX} = S_{h(X)+aX} = S_{u(X)+aX} = 0$$

or

$$|S_{g(X)+aX}| = |S_{h(X)+aX}| = |S_{u(X)+aX}| = |S_f| > 0.$$

By Lemma 2.5, and using the fact that $g(0) = h(0) = u(0) = 0$, we obtain either conclusion (i) or $g(X) = h(X) = u(X) = aX$ for some $a \in F$; but in the latter case we have $(f, 0, 0, 0) = (f, g, h, u) - a(0, X, X, X) \in \mathcal{V}_0$ which forces $f = 0$ and $(f, g, h, u) = a(0, X, X, X)$ for some $a \in F$, a contradiction.

Hence we may assume that $S_f = 0$, so that f is a permutation; without loss of generality, $f(X) = X$. By Lemma 3.4, the sets A_g, A_h and A_u (defined as in Section 2) are mutually disjoint; but after permuting the 2nd, 3rd and 4th coordinates of $\mathcal{N}$ if necessary, we may assume that $|A_g| \le |A_h| \le |A_u|$. This implies that $|A_g| \le |A_h| \le p/3 \le \frac{1}{2}(p-1)$. By Lemma 2.3 and the condition $g(0) = h(0) = 0$, we have $g(X) = aX$ and $h(X) = bX$ for some $a, b \in X$, so conclusion (ii) follows. □

3.6 Theorem. *Suppose $\mathcal{N}$ has at least two cyclic 3-subnets. Then $\mathcal{N}$ has at least three cyclic 3-subnets.*

Proof. Without loss of generality, $\mathcal{V}_0$ contains $(0, X, X, X)$ and $(f, g, h, 0)$ where the functions $f, g, h : F \to F$ are permutations. By Lemma 3.5, we may suppose that $g(X) = aX$ for some $a \in F$. Now

$$(f, 0, h(X){-}aX, -aX) = (f, g, h, 0) - a(0, X, X, X) \in \mathcal{V}_0$$

so that $\mathcal{N}$ has a third cyclic 3-subnet. □

3.7 Theorem. *Suppose $\mathcal{N}$ has four cyclic 3-subnets. Then $\mathcal{N}$ is Desarguesian.*

Proof. As in the proof of Theorem 3.6, we may assume that $\mathcal{V}_0$ contains $(0, X, X, X)$, $(f(X), aX, h(X), 0)$ and $(f(X), 0, h(X){-}aX, -aX)$ where $S_f = S_h = S_{h(X)-aX} = 0$. Without loss of generality, $f(X) = X$. There also exists $(r(X), s(X), 0, v(X)) \in \mathcal{V}_0$ where the functions $r, s, v : F \to F$ are bijective. By Lemma 3.5, either $s(X) = bX$ or $v(X) = bX$ for some $b \in F$. We may assume that $s(X) = bX$, for otherwise we may interchange coordinates 2 and 4 of $\mathcal{N}$, replacing also $(a, h(X))$ by $(-a, h(X){-}aX)$. Now

$$(r(X), 0, -bX, v(X){-}bX) = (r(X), bX, 0, v(X)) - b(0, X, X, X) \in \mathcal{V}_0$$

so this is a scalar multiple of $(X, 0, h(X){-}aX, -aX)$, and without loss of generality

$$(r(X), 0, -bX, v(X){-}bX) = (X, 0, h(X){-}aX, -aX).$$

This forces

$$\mathcal{N} = \{(bx{+}ay, -x{-}y, x, y) : x, y \in F\}$$

where $a \neq b$ and the result follows. $\square$

3.8 Theorem. *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.*

Proof. We may suppose that $\pi_{1'}\mathcal{N}$ is cyclic and that $(0, X, X, X) \in \mathcal{V}_0$; also that $\dim(\pi_1\mathcal{V}_0) \geq 2$. By Lemma 3.5 we have $|S_f| \in \{0, \sqrt{p}, p\}$ for all $f \in \pi_1\mathcal{V}_0$, so by Lemma 2.6 we may assume $\pi_1(\mathcal{V}_0)$ contains X and X^2. By Lemma 3.5 we may assume that $(X, aX, bX, r(X))$, $(X^2, g(X), h(X), u(X)) \in \mathcal{V}_0$ for some $a, b \in F$, where $g, h, u : F \to F$ are quadratic. In particular

$$(X, 0, (b{-}a)X, r(X){-}aX),\ (X, (a{-}b)X, 0, r(X){-}bX) \in \mathcal{V}_0$$

and so the 3-subnets $\pi_{2'}\mathcal{N}$ and $\pi_{3'}\mathcal{N}$ are cyclic. Since

$$(X^2, g(X), h(X), u(X)) + (X, aX, bX, r(X)) \in \mathcal{V}_0\,,$$

we see by Lemma 3.5 that $u(X){+}r(X)$ is quadratic, whence $r(X)$ itself has degree ≤ 2. This means that $r(X) = cu(X) + dX$ for some $c, d \in F$, and so

$$(cX^2{-}X,\ cg(X){+}(d{-}a)X,\ ch(X){+}(d{-}b)X,\ 0) \in \mathcal{V}_0$$

so that the 3-subnet $\pi_{4'}\mathcal{N}$ is also cyclic. The result follows by Theorem 3.7. $\square$

4. Webs

We consider here not the most general notion of a web (see e.g. [2]) but rather what may be described as 2-dimensional k-webs over $\mathbb{C}$. Let $\mathcal{W} \subseteq \mathbb{C}^2$ be a connected open neighbourhood of 0, and consider a k-tuple of holomorphic functions

$$u_i : \mathcal{W} \to \mathbb{C}, \quad i = 1, 2, \ldots, k$$

such that at every point $w \in \mathcal{W}$, any two of the gradients $u_1'(w), u_2'(w), \ldots, u_k'(w) \in \mathbb{C}^2$ are linearly independent over $\mathbb{C}$. We regard $\mathcal{W}$ as the point set of an incidence structure whose 'lines' are the level curves $u_i^{-1}(a) \subset \mathcal{W}$ for every $a \in u_i(\mathcal{W})$. (The condition on the derivatives $u_i'(w)$ ensures that these curves intersect transversely; and assuming $\mathcal{W}$ is sufficiently small, every point $w \in \mathcal{W}$ is uniquely determined by any two of its 'coordinates' $u_1(w), u_2(w), \ldots, u_k(w)$.) We may assume that $u_i(0) = 0$ for all i. The resulting structure $(\mathcal{W}, u_1, u_2, \ldots, u_k)$, denoted simply $\mathcal{W}$, is called a *k-web*. Just as in the finite case (Section 3) we define the complex vector space $\mathcal{V} = \mathcal{V}(\mathcal{W})$ as the set of all k-tuples $(f_1, f_2, \ldots, f_k)$ of holomorphic functions such that

$$f_1(u_1(w)) + f_2(u_2(w)) + \cdots + f_k(u_k(w)) = 0$$

for all $w \in \mathcal{W}$. Also consider the subspace $\mathcal{V}_0 = \mathcal{V}_0(\mathcal{W})$ consisting of those k-tuples of functions satisfying the additional condition that $f_i(0) = 0$ for all i. As before, the quotient space $\mathcal{V}/\mathcal{V}_0$ has dimension $k{-}1$. The *rank* of the web $\mathcal{W}$ is by definition the $\mathbb{C}$-dimension of $\mathcal{V}_0$. We have

Next consider the case $\frac{1}{2}(p-1) \le t \le p{-}2$. Multiplying both sides of (6.2) by $g(j)^{2t+3-p}$ and setting $r = p{-}1$ yields

$$\begin{aligned}\sigma_{h,p-1}g(j)^{2t+3-p} &= \sum_{s=0}^{p-1}\binom{p-1}{s}\sigma_{f,p-1-s}g(j)^{s+2t+3-p}\\ &= \sum_{s=0}^{p-t-2}\binom{p-1}{s}\sigma_{f,p-1-s}g(j)^{s+2t+3-p}.\end{aligned}$$

Note that $2t{+}3{-}p \ge 2$, so all exponents are non-negative. Now observe that $2t{+}3{-}p < t$ and sum over $j \in F$ to obtain

$$0 = \sigma_{g,p-1}\sigma_{g,2t+3-p} = \sum_{s=0}^{p-t-2}\binom{p-1}{s}\sigma_{f,p-1-s}\sigma_{g,s+2t+3-p} = \binom{p-1}{p-t-2}\sigma_{f,t+1}\sigma_{g,t+1}.$$

Since the latter binomial coefficient is not divisible by p, we obtain $\sigma_{f,t+1}\sigma_{g,t+1} = 0$. This yields $\sigma_{f,t+1} = \sigma_{g,t+1} = \sigma_{h,t+1} = 0$ as before.

Applying (6.2) for $r = p{-}1$ gives $\sigma_{h,p-1} = \sigma_{f,p-1}$; and similarly, $\sigma_{h,p-1} = \sigma_{g,p-1}$. By assumption, $(f,g,h) \in \mathcal{V}_0$ is nonzero; therefore by Proposition 6.1 we have $\sigma_{f,p-1} = \sigma_{g,p-1} = \sigma_{h,p-1} = -1$ and each of the maps f,g,h is a permutation of F. We may assume that $f(k) = g(k) = -h(k) = k$ for all $k \in F$; otherwise relabel the lines in each parallel class so that this is the case. Since $f(i) + g(j) + h(k) = 0$ for all $(i,j,k) \in \mathcal{N}$, we obtain $\mathcal{N} = \{(i,j,i{+}j) : i,j \in F\}$ and so the 3-net $\mathcal{N}$ is cyclic.

This completes our proof of Theorem 3.3 by the method of moments. While this method presumably also leads to a proof of Theorem 1.1 without using exponential sums, this approach seems much more technical and not particularly advantageous.

7. References

1. A. Blokhuis, ‘Polynomials in finite geometries and combinatorics’, in *Surveys in Combinatorics, 1993,* ed. Keith Walker, Camb. Univ. Press, 1993, pp.35–52.
2. S.S. Chern and P. Griffiths, ‘Abel’s theorem and webs’, *Jahresberichte der Deut. Math. Ver.* **80** (1978), 13–110; also, ‘Corrections and addenda to our paper: Abel’s theorem and webs’, same Journal, **83** (1981), 78–83.
3. D. Gluck, ‘A note on permutation polynomials and finite geometries’, *Discrete Math.* **80** (1990), 97–100.
4. P.A. Griffiths, ‘Variations on a theorem of Abel’, *Inventiones Math.* **35** (1976), 321–390.
5. Y. Hiramine, ‘A conjecture on affine planes of prime order’, *J. Combin. Thoery Ser. A* **52** (1989) no.1, 44–50.

6. J. Little, ‘Translation manifolds and the converse of Abel’s theorem’, *Compositio Math.* **49** (1983), 147–171.

7. J.B. Little, ‘On the converse of Abel’s theorem in characteristic p’, *Manuscripta Math.* **46** (1984), 27–63.

8. L. Lovász and A. Schrijver, ‘Remarks on a theorem of Rédei’, *Studia Scient. Math. Hungar.* **16** (1981), 449–454.

9. G.E. Moorhouse, ‘Bruck nets, codes, and characters of loops’, *Des. Codes Cryptogr.* **1** (1991), 7–29.

10. G. Eric Moorhouse, ‘Codes of Nets with Translations’, in *Advances in Finite Geometries and Designs,* ed. J. Hirschfeld et. al., Oxford Univ. Press, 1991, pp.327–336.

11. G. Eric Moorhouse, ‘On codes of Bruck nets and projective planes’, in *Coding Theory, Design Theory, Group Theory (Proceedings of the Marshall Hall Conference),* ed. D. Jungnickel and S.A. Vanstone, Wiley, 1993, pp.237–242.

12. G.E. Moorhouse, ‘Nets and Latin squares of order 7’. `http://www.uwyo.edu/moorhouse/pub/nets7/`

13. L. Rédei, *Lückenhafte Polynome über endlichen Körpern,* Birkhäuser Verlag, Basel, 1970.

14. L. Rónyai and T. Szőnyi, ‘Planar functions over finite fields’, *Combinatorica* **9** (1989) no.3, 315–320.