Codes of Nets and Projective Planes

G. Eric Moorhouse

Abstract. In the study of finite projective planes, two of the most prominent open questions are: do there exist finite planes of finite order other than prime powers? and, must every plane of prime order be Desarguesian? Coding theory has played a prominent role in traditional approaches to these problems. These approaches, although fruitful, have not resolved the two key problems to which we refer. We suggest some promising alternative ways that coding theory may be applied to these problems, focusing on codes of nets.

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 dimension of its p-ary code), and structural properties of $\mathcal{N}$ that are deducible from the 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.

1. Introduction

This study is motivated by 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?

Coding theory figures prominently in traditional approaches to these problems, particularly (Q1). Let Π be a projective plane of order n, and suppose that p is a prime sharply dividing n (i.e. n is divisible by p but not by p^2). The p-ary code of Π, suitably extended, is self-dual, and the MacWilliams relations impose strong constraints on the weight enumerator of this code. The hope is that further combinatorial reasoning may restrict the possible shape of low-weight codewords, thereby resolving (Q1) for particular small choices of n. This description provides a very rough outline of the result of Lam et. al. [**LTS**] that projective planes of order 10 do not exist. The success of this method, however, depends heavily upon computer—a computational tour de force is required for $n = 10$; and the computation requirements are currently not within reach for any value of $n > 10$. The problems (Q1) and (Q2) are currently awaiting some fresh ideas.

We have proposed [**M91a**] an approach to (Q1) and (Q2) based on codes of nets. The limitations of this approach remain unclear, but the progress has been

2000 *Mathematics Subject Classification.* Primary 51E14; Secondary 11T23, 51E14, 05B25.
Key words and phrases. Code, net, finite projective plane, exponential sum.

encouraging. In this work, we focus on codes of k-nets of prime order p, with particular attention to the case $k = 4$.

The best progress to date on (Q2) is:

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

This result is a corollary of

THEOREM 1.2. *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 [**G**], Rónyai and Szőnyi [**RS**], and Hiramine [**H**]. 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 [**M91a**] 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*, where $k \leqslant p + 1$. Less formally [**M91a**], $\mathcal{N}$ 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. Note that the case $k = p + 1$ yields precisely an affine plane of order p. 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 $p^2 \times pk$ incidence matrix. We have posed

CONJECTURE 1.3 ([**M91a**]). Let $\mathcal{N}$ be a k-net of order p, and let $\mathcal{N}'$ be any of its $(k{-}1)$-subnets. Then $\operatorname{rank}_p(\mathcal{N}) - \operatorname{rank}_p(\mathcal{N}') \geqslant p - k + 1$.

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

CONJECTURE 1.4. Let $\mathcal{N}$ be a k-net of order p. Then $pk - \operatorname{rank}_p(\mathcal{N}) \leqslant \frac{1}{2}(k - 1)(k - 2)$.

Note that the quantity $pk - \operatorname{rank}_p(\mathcal{N})$ is simply the *nullity* of the $p^2 \times pk$ incidence matrix of the net $\mathcal{N}$. It is significant that the conjectured upper bound $\frac{1}{2}(k - 1)(k - 2)$ is also an upper bound for the arithmetic genus of an algebraic plane curve of degree k. Indeed the most natural analogue of Conjecture 1.4, in the infinite case, is a bound on the rank of a *web* (more precisely, a 2-dimensional k-web) which in the infinite case is a theorem. Moreover, examples of k-webs attaining this bound are obtainable from extremal curves of degree k, i.e. plane curves of maximal genus $\frac{1}{2}(k-1)(k-2)$ for the given degree k.

We also showed

Theorem 1.5 ([**M91a**]). *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 [**M91a**] using loop theory. Below (see Theorem 3.3) we provide an easy alternative proof of this fact using exponential sums. Moreover, the method of exponential sums provides further information in the case of 4-nets. This progress, stated in Theorem 1.6 below, is proved in Section 3. Here a Desarguesian 3-net is called simply a *cyclic* 3-net, since it is the unique isomorphism type of 3-net of order p corresponding to the cyclic Latin square of order p.

Theorem 1.6. *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 exactly 0, 1 or 3 cyclic subnets. Examples of these for $p = 7$ are found at [**M**]. Further partial results in the direction of Conjecture 1.3 are found in [**M91b**], [**M93**].

We have verified by computer that Conjecture 1.3 holds for $p \leqslant 11$. For $p \leqslant 7$, this is easily checked using a complete classification of all nets of order p; see [**M**]. We have also verified Conjecture 1.3 for 4-nets of order $p = 11$; although the actual nets are probably too numerous to classify, the methods of Section 3 bring the problem within the reach of practical computation. The case $p = 11$ is significant since 11 is the smallest order for which projective planes have yet to be classified.

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).

Lemma 2.1. *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*

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

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 [**G**]. 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. □

LEMMA 2.2. *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

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

LEMMA 2.3. *Suppose $|A_f| \leqslant \frac{1}{2}(p+1)$. 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 the affine plane $AG_2(F)$, i.e. the set of all values of the difference quotient $(f(y) - f(x))/(y - x)$ for all pairs (x, y) of distinct elements of F. The result follows by a theorem of Rédei [**R**]; see also [**B**], [**LS**]. □

LEMMA 2.4. *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, i.e. a set of $q + 1$ points with no three collinear. 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.

Lemma 2.5. *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 $\varepsilon = (1,1,\dots,1)^T \in \mathbb{C}^p$; 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, $k \geqslant 1$ 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. □

Lemma 2.6. *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. □

We have seen that nets yield relations between exponential sums, and it is natural to compare factorizations of these expressions (or of the principal ideals which they generate) in the ring $\mathbb{Z}[\zeta]$. (Here we must remember that $\mathbb{Z}[\zeta]$ does not have unique factorization for $p > 19$.) We will see (Theorem 3.4) that the functions arising from codes of nets satisfy the following condition with $m = 1$.

Lemma 2.7. *Let $f : F \to F$. Then S_f lies in the ideal $(1-\zeta) \subset \mathbb{Z}[\zeta]$. If moreover $\sum_{a\in F} f(a)^j = 0 \in F$ for $j = 0, 1, \ldots, m$ where $m \leqslant p-2$, then $S_f \in (1-\zeta)^{m+1}$.*

Proof. The ideal $(p) \subset \mathbb{Z}[\zeta]$ ramifies as $(p) = (\varepsilon)^{p-1}$ where $\varepsilon = \zeta-1$ and $\mathbb{Z}[\zeta]/(\varepsilon) \cong \mathbb{F}_p$. Now suppose $m \leqslant p-2$ such that $\sum_{a\in F} f(a)^j = 0$ for $j = 0, 1, \ldots, m$. (The latter condition always holds for $j = 0$.) Re-interpreting the values of f as integers in the range $0, 1, 2, \ldots, p-1$, we have

$$\begin{aligned} S_f &= \textstyle\sum_{a\in F} \zeta^{f(a)} = \sum_{a\in F} (1+\varepsilon)^{f(a)} \\ &\equiv \textstyle\sum_{0\leqslant j\leqslant m} \frac{\varepsilon^j}{j!} \sum_{a\in F} f(a)\big(f(a)-1\big)\big(f(a)-2\big)\cdots\big(f(a)-j+1\big) \mod (\varepsilon)^m. \end{aligned}$$

For $j \leqslant m$, the innermost sum lies in $(p) \subseteq (\varepsilon)^{m+1}$ by hypothesis. The remaining terms (for $j \geqslant m+1$) also clearly lie in $(\varepsilon)^{m+1}$. □

3. Nets

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

$$\pi_J : F^k \to F^{|J|}, \qquad (a_1, a_2, \ldots, a_k) \mapsto (a_j : j \in J).$$

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 $i \neq j$ 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 $\mathcal{V}_0=\mathcal{V}_0(\mathcal{N})\leqslant\mathcal{V}$ 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), i.e. the dual of the $\mathbb{F}_p$-space spanned by rows, this gives

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

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

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

CONJECTURE 3.2. (i) $\dim\pi_1(\mathcal{V})\leqslant k{-}1$.
(ii) $\dim(\mathcal{V}_0)\leqslant\frac{1}{2}(k{-}1)(k{-}2)$, and equality holds iff $\mathcal{N}$ is Desarguesian.

Statement (i) is a simple restatement of 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. Some indication that $\mathcal{V}_0$ is more natural to consider than the row or column space of A itself, is found in remarks following Conjecture 1.4. The case $k=3$ of Conjecture 3.2(i) was settled in[**M91a**] using loop theory. See [**M06**] for a collection of proofs of this fact using a variety of techniques. Here we use exponential sums to prove this case:

THEOREM 3.3. *Let $\mathcal{N}$ be a 3-net of order p. Then* $\dim(\mathcal{V}_0)\leqslant1$. *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 $S_fS_g=p\overline{S_h}$, and similarly $S_gS_h=p\overline{S_f}$ and $S_hS_f=p\overline{S_g}$. Thus

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

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. □

Theorem 3.4. *Let $\mathcal{N}$ be a k-net of order p where $k\in\{2,3,\ldots,p\}$, and let $(f_1,f_2,\ldots,f_k)\in\mathcal{V}(\mathcal{N})$. Then for every $i\in\{1,2,\ldots,k\}$ we have $\sum_{a\in F}f_i(a)=0$. In particular the corresponding exponential sums S_{f_i} lie in the ideal $(1{-}\zeta)^2\subseteq\mathbb{Z}[\zeta]$.*

We remark that the conclusion fails for $k=p{+}1$.

Proof. For every $(x_1,\ldots,x_k)\in\mathcal{N}$ we have

$$f_1(x_1)+f_2(x_2)+\cdots+f_k(x_k)=0.$$

Summing over all $(x_1,\ldots,x_k)\in\mathcal{N}$ with fixed first coordinate $x_1=b\in F$ gives

$$\sum_{a\in F}\bigl(f_2(a)+f_3(a)+f_4(a)+\cdots+f_k(a)\bigr)=0.$$

A similar argument gives

$$\sum_{a\in F}\bigl(f_1(a)+f_3(a)+f_4(a)+\cdots+f_k(a)\bigr)=0.$$

The difference of these last two sums yields $\sum_{a\in F}f_1(a)=\sum_{a\in F}f_2(a)$. Similar arguments yield

$$\sum_{a\in F}f_1(a)=\sum_{a\in F}f_2(a)=\cdots=\sum_{a\in F}f_k(a)$$

and then substituting into the earlier sum yields

$$0=\sum_{a\in F}\bigl(f_2(a)+f_3(a)+\cdots+f_k(a)\bigr)=(k-1)\sum_{a\in F}f_1(a).$$

Since $k-1$ is not divisible by p the first conclusion holds, and the fact that $S_{f_i}\in(1{-}\zeta)^2$ follows from Lemma 2.7. □

Lemma 3.5. *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 $S_fS_g=\overline{S_hS_u}$, and similarly $S_fS_h=\overline{S_gS_u}$ and $S_fS_u=\overline{S_gS_h}$. This yields

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

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

Lemma 3.6. *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 3.5 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 3.5, 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 $|A_g| \leqslant |A_h| \leqslant |A_u|$. This implies that $|A_g| \leqslant |A_h| \leqslant \frac{1}{3}p \leqslant \frac{1}{2}(p-1)$. 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. □

Theorem 3.7. *Let $\mathcal{N}$ be a 4-net of prime order p. 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 3.6, 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. □

Theorem 3.8. *Suppose $\mathcal{N}$ is a 4-net of prime order p, all four of whose 3-subnets are cyclic. Then $\mathcal{N}$ is Desarguesian.*

Proof. As in the proof of Theorem 3.7, 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 3.6, 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. □

Theorem 3.9. *Let $\mathcal{N}$ be a 4-net of prime order p having at least one cyclic 3-subnet. Then* $\dim(\mathcal{V}_0) \leqslant 3$, *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 $\dim(\pi_1\mathcal{V}_0)\geqslant 2$. By Lemma 3.6 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 3.6 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 3.6 that $u(X){+}r(X)$ is quadratic, whence $r(X)$ itself has degree $\leqslant 2$. 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 3.8. □

This completes the proof of Theorem 1.6.

References

[B] A. Blokhuis, ‘Polynomials in finite geometries and combinatorics’, in *Surveys in Combinatorics, 1993,* ed. Keith Walker, Camb. Univ. Press, 1993, pp. 35–52.

[G] D. Gluck, ‘A note on permutation polynomials and finite geometries’, *Discrete Math.* **80** (1990), 97–100.

[H] Y. Hiramine, ‘A conjecture on affine planes of prime order’, *J. Combin. Theory Ser. A* **52** (1989) no.1, 44–50.

[LTS] C. W. H. Lam, L. Thiel and S. Swiercz, ‘The non-existence of finite projective planes of order 10’, *Canad. J. Math* **41** (1989), 1117-1123.

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

[M91a] G. E. Moorhouse, ‘Bruck nets, codes, and characters of loops’, *Des. Codes Cryptogr.* **1** (1991), 7–29.

[M91b] G. E. 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.

[M93] G. E. 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.

[M] G. E. Moorhouse, ‘Nets and Latin squares of small order’.
http://www.uwyo.edu/moorhouse/pub/nets/

[M06] G. E. Moorhouse, ‘Ranks of Nets’, *Quasigroups Rel. Systems* **14** (2006), 61–72.

[R] L. Rédei, *Lückenhafte Polynome über endlichen Körpern,* Birkhäuser Verlag, Basel, 1970.

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WYOMING, LARAMIE, WYOMING 82071
E-mail address: moorhous@uwyo.edu