Quasigroups and Related Systems **14** (2006), 61 – 72

Ranks of nets

G. Eric Moorhouse

Abstract

Let $\mathcal{N}$ be a k-net of prime order p. We find bounds on the p-rank of (the point-line incidence matrix of) $\mathcal{N}$ for $k \in \{3,4\}$, and observe connections between the p-rank and certain structural properties of $\mathcal{N}$. Implications for the study of finite projective planes are described.

1. Loops and 3-nets of prime order

Let $(L,*)$ be a loop of prime order p. The 3-*net* $\mathcal{N}=\mathcal{N}(L)$ coordinatized by L is the point-line incidence system having p^2 points $L^2 = L\times L$, and $3p$ lines given by

$\{a\}\times L$ for $a\in L$ (the lines "$x=a$");

$L\times\{b\}$ for $b\in L$ (the lines "$y=b$"); and

$\{(x,y)\in L^2 : x*y=c\}$ for $c\in L$ (the lines "$x*y=c$").

The point-line incidence matrix of $\mathcal{N}$ is the $p^2\times 3p$ matrix with rows and columns indexed by points and lines of $\mathcal{N}$ respectively; and having entries 0 and 1 corresponding to non-incident and incident point-line pairs respectively. We have

Theorem 1.1. (Main Theorem [5]**)** *The p-rank of the incidence matrix of $\mathcal{N}$ equals $3p{-}3$ if L is associative, and $3p{-}2$ otherwise.*

Our original proof [5], still the simplest proof available, uses loop theory. (Here for simplicity we consider only loops and nets of prime order, although

2000 Mathematics Subject Classification: 51A05, 20N05
Keywords: net, projective geometry, loop, web, p-rank

more arbitrary finite orders were considered in [5].) We reproduce this proof below; and we indicate three alternative proofs of the same result. Our (currently unrealized) goal is a generalization of Theorem 1.1 to k-nets for $k = 3, 4, \ldots, p{+}1$; possibly using techniques from nonassociative algebra, or possibly by generalizing some of the other techniques described in this paper. The desired generalization of this result is

Conjecture 1.2. [5] *Let $\mathcal{N}$ be any k-net of prime order p, and let $\mathcal{N}'$ be any $(k{-}1)$-subnet of $\mathcal{N}$ obtained by deleting one of the k parallel classes of lines of $\mathcal{N}$; here $k \in \{2, 3, \ldots, p{+}1\}$. Then the p-rank of the incidence matrix of $\mathcal{N}$ exceeds that of $\mathcal{N}'$ by at least $p{-}k{+}1$.*

The significance of Conjecture 1.2 lies in the fact [5] that this would imply that every projective plane of prime order is Desarguesian, thereby settling one of the most celebrated currently open problems in finite geometry. Extensions of this method to other finite orders would yield restrictions on the possible orders of finite projective planes, beyond the restrictions available through the Bruck-Ryser Theorem [2]. We believe that these finite geometric questions are worthy of the attention of researchers in nonassociative algebra. Indeed, Belousov [1] attributes the origins of quasigroup theory to the study of finite projective planes. (I am grateful to V.V. Goldberg for bringing this reference to my attention during our Mile High Conference.)

In Section 2, we describe the p-rank of a net in terms recognizable to researchers of webs. This leads to a reformulation of our main result Theorem 1.1 in equivalent terms as Theorem 2.3. In Sections 3, 4, 5 and 6 we provide proofs of this main result using loop theory, group theory, finite field theory, and number theory (specifically, exponential sums) respectively. Each of these approaches suggests different possibilities for generalization to k-nets. Finally in Section 7 we describe some recent progress towards Conjecture 1.2 in the case of 4-nets.

2. Nets and planes of prime order

Consider a field $F = \mathbb{F}_p$ of prime order p, and let $k \geqslant 2$. 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 $J' = \{1,2,\dots,k\} \setminus J$ so that in particular

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

A *k-net of order p* is a subset $\mathcal{N} \subseteq F^k$ such that for all $i \neq j$ in $\{1,2,\dots,k\}$, 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 $i \in \{1,2,\dots,k\}, a \in F$. For every $J \subseteq \{1,2,\dots,k\}$ 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 $i \in \{1,2,\dots,k\}$, 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 $(a_1,a_2,\dots,a_k) \mapsto (\alpha_1(a_{\sigma(1)}),\alpha_2(a_{\sigma(2)}),\dots,\alpha_k(a_{\sigma(k)}))$ for some $\alpha_1,\alpha_2,\dots,\alpha_k \in Sym(F)$ 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

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

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 $(f_1,f_2,\dots,f_k)$ of functions $F \to F$ such that

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

for all $(a_1,a_2,\dots,a_k) \in \mathcal{N}$. Also denote by $\mathcal{V}_0 = \mathcal{V}_0(\mathcal{N}) \leqslant \mathcal{V}$ the subspace consisting of all $(f_1,f_2,\dots,f_k) \in \mathcal{V}$ satisfying the additional condition $f_1(0) = f_2(0) = \cdots = f_k(0) = 0$. The map $\mathcal{V} \to F^k$, $(f_1,f_2,\dots,f_k) \mapsto (f_1(0),f_2(0),\dots,f_k(0))$ 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 $\mathcal{N}$, this gives

Proposition 2.1. *The p-rank of the incidence matrix A of $\mathcal{N}$ is given by*

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

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

Conjecture 2.2. *We have:*

(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 equivalent to Conjecture 1.2, 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, the corresponding incidence map has infinite rank, whereas the null space $\mathcal{V}$ is finite-dimensional. Indeed the bound $\dim(\mathcal{V}_0) \leqslant \frac{1}{2}(k{-}1)(k{-}2)$ holds for k-webs, with equality attainable in the case of algebraic webs; see [3,4]. We rephrase the Main Theorem as

Theorem 2.3. *Let $\mathcal{N}$ be a 3-net of order p. Then $\dim(\mathcal{V}_0) \leqslant 1$. 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.*

3. First proof of main theorem (using loop theory)

Let $\mathcal{N} \subset F^3$ be a 3-net of prime order p, in the notation of Section 2, and suppose $(f, g, h) \in \mathcal{V}_0(\mathcal{N})$ is nonzero. To within an isomorphism of nets, we have

$$\mathcal{N} = \{(x, y, x * y) : x, y \in F\}$$

where $(x, y) \mapsto x * y \in F$ is a loop operation on F with identity 0. By definition we have

$$f(0) = g(0) = h(0) = 0;$$
$$f(x) + g(y) + h(x * y) = 0 \quad \text{for all } x, y \in F.$$

This implies that $f(x) = g(x) = -h(x)$ for all $x \in F$ and that f is a nonzero homomorphism from the loop $(F, *)$ to the cyclic group $(F, +)$ of order p. These two loops are therefore isomorphic, so $\mathcal{N}$ is cyclic. Moreover every such homomorphism has the form cf for some $c \in F$, so $\mathcal{V}_0(\mathcal{N})$ is 1-dimensional. The result follows.

The same argument actually yields the stronger result

Theorem 3.1. [5] *Let L be a loop of order $n = p^r m$ where $gcd(p,m) = 1$. Then the p-rank of the incidence matrix of the 3-net $\mathcal{N}(L)$ equals $3p-2-e$ where $e \in \{0,1,2,\dots,r\}$. We have $|K| = p^e$ where $K \subseteq L$ is the largest normal subloop such that the quotient loop L/K is an elementary abelian p-group.*

4. Second proof of main theorem (using permutation groups)

An alternative proof of Theorem 3.1 is obtained by considering the left multiplication group of L. More generally, let Ω be a set of size $|\Omega| = n = p^r m$ where $gcd(p,m) = 1$, and let G be a group permuting Ω transitively. Let $H \leqslant G$ be the stabilizer of a point which we denote $1 \in \Omega$. For each $k \geqslant 0$, denote by C^k the vector space over F consisting of all functions $\Omega^{k+1} \to F$. Then G acts on C^k via

$$f^g(x_0, x_1, \dots, x_k) = f(x_0^g, x_1^g, \dots, x_k^g)$$

for $g \in G$, $f \in C^k$, $x_i \in \Omega$. Consider the F-linear map $\partial = \partial_k : C^k \to C^{k+1}$ defined by

$$(\partial f)(x_0, x_1, \dots, x_{k+1}) = \sum_{i=0}^{k+1} (-1)^{k+1-i} f(x_0, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{k+1})$$

for $f \in C^k$, $x_i \in \Omega$. Note that ∂ is G-equivariant: $\partial(f^g) = (\partial f)^g$. The image $B^1 = \partial C^0 \leqslant C^1$ consists of all functions $\partial\phi(x_0, x_1) = \phi(x_0) - \phi(x_1)$ for some $\phi : \Omega \to F$. Consider the subspace of G-invariants given by

$$(B^1)^G = \{f \in B^1 : f^g = f \text{ for all } g \in G\}.$$

In the following, $Hom(G/K, F)$ denotes the vector space over F consisting of homomorphisms from the multiplicative group G/K to the additive group of F.

Lemma 4.1. $(B^1)^G \cong Hom(G/K, F)$ *where K is the smallest normal subgroup of G containing H such that G/K is an elementary abelian p-group. In particular,* $\dim (B^1)^G = e \in \{0,1,2,\dots,r\}$ *where $|G/K| = p^e$.*

Proof. For each $\phi : G/K \to F$, define $\widehat{\phi} : \Omega \to F$ by $\widehat{\phi}(1^g) = \phi(Kg)$ for $g \in G$. Note that $\widehat{\phi} \in C^0$ is well-defined since K contains H. We claim that the map

$$\theta : Hom(G/K, F) \to (B^1)^G, \quad \phi \mapsto \partial\widehat{\phi}$$

is an isomorphism of vector spaces over F. Certainly if $\phi \in Hom(G/K, F)$ then

$$\begin{aligned}\partial\widehat{\phi}(1^{ug}, 1^{vg}) &= \phi(Kug) - \phi(Kvg) = \phi(Ku) + \phi(Kg) - \phi(Kv) - \phi(Kg)\\ &= \phi(Ku) - \phi(Kv) = \partial\widehat{\phi}(1^u, 1^v)\end{aligned}$$

for all $u, v, g \in G$. Since G is transitive on Ω, this implies that $\partial\widehat{\phi} \in (B^1)^G$. If $\partial\widehat{\phi} = 0$ then $\phi(Kg) = \phi(K) = 0$ for all $g \in G$, i.e. $\phi = 0$ so θ is injective. Finally, given $f \in (B^1)^G$, define $\phi(Kg) = f(1^g, 1)$. Since $f \in (B^1)^G$ we have

$$\begin{aligned}0 = \partial f(1^{gh}, 1^h, 1) &= f(1^h, 1) - f(1^{gh}, 1) + f(1^{gh}, 1^h)\\ &= f(1^h, 1) - f(1^{gh}, 1) + f(1^g, 1)\\ &= \phi(Kh) - \phi(Kgh) + \phi(Kg)\end{aligned}$$

for all $g, h \in G$ so that $\phi \in Hom(G/K, F)$ satisfying $\partial\widehat{\phi} = f$ and θ is surjective. □

Now suppose $(L, *)$ is a loop of order $n = p^r m$ where $gcd(p, m) = 1$. Let $1 \in L$ be the identity, and let G be the left multiplication group of L; i.e. $G \leqslant Sym(L)$ is generated by the permutations $x \mapsto a * x$, $a \in L$. We show that the map $(f, g, h) \mapsto \partial f$ gives an isomorphism $\mathcal{V}_0(\mathcal{N}) \xrightarrow{\cong} (B^1)^G$. For $(f, g, h) \in \mathcal{V}_0(\mathcal{N})$ we have

$$f(x) + g(y) + h(x * y) = 0$$

for all $x, y \in L$ and so $f(x) = g(x) = -h(x)$ and

$$\begin{aligned}\partial f(a * x, a * y) &= f(a * x) - f(a * y)\\ &= f(a) + f(x) - f(a) - f(y) = f(x) - f(y)\\ &= \partial f(x, y)\end{aligned}$$

so that $\partial f \in (B^1)^G$. If $\partial f = 0$ then $f(x) = \partial f(x, 1) = 0$. Also if $\phi : L \to F$ such that $\partial\phi \in (B^1)^G$ then we easily check that $(f, f, -f) \in \mathcal{V}_0(\mathcal{N})$ where

$f(x) = \partial\phi(x,1) = \phi(x) - \phi(1)$:

$$\begin{aligned} f(x) + f(y) - f(x*y) &= \partial\phi(x,1) + \partial\phi(y,1) - \partial\phi(x*y,1) \\ &= \partial\phi(x,1) - \partial\phi(x*y,1) + \partial\phi(x*y,x) \\ &= \partial^2(x*y,x,1) = 0. \end{aligned}$$

Theorem 3.1 follows.

5. Third proof of main theorem (using finite fields)

We require the following well-known result, whose proof is included for completeness. As before we fix $F = \mathbb{F}_p$ where p is prime, and we use the convention that $0^0 = 1$.

Proposition 5.1. *Let $f : F \to F$, and for every $r \geqslant 0$, write $\sigma_{f,r} = \sum_{a\in F} f(a)^r \in F$. Then*

(*a*) *The map f is a permutation of F, if and only if*

$$\sigma_{f,0} = \sigma_{f,1} = \cdots = \sigma_{f,p-2} = 0 \quad \textit{and} \quad \sigma_{f,p-1} = -1.$$

(*b*) *We have $\sigma_{f,0} = \sigma_{f,1} = \cdots = \sigma_{f,p-2} = 0$, if and only if $\left|f(F)\right|$ equals either 1 or p.*

Proof. First suppose that the map f is a permutation of F, so that $\sigma_{f,r} = \sum_{a\in F} a^r$. Clearly $\sigma_{f,0} = p = 0 \in F$ and $\sigma_{f,p-1} = p{-}1 = -1 \in F$. Now suppose $1 \leqslant r \leqslant p{-}2$. For every $c \in \{1, 2, \ldots, p-1\}$ we have $c^r\sigma_{f,r} = \sum_{a\in F}(ca)^r = \sum_{a\in F} a^r = \sigma_{f,r}$ since the map $a \mapsto ca$ is a permutation of F. Now the polynomial $\sigma_{f,r}X^r - \sigma_{f,r} \in F[X]$ has $p{-}1 > r$ zeroes in the field F, so $\sigma_{f,r} = 0$ as required.

In the general case, for every $a \in F$, let $n_a = \left|f^{-1}(a)\right|$, so that $\sigma_{f,r} = \sum_{a\in F} a^r n_a$. The linear system

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 2 & \cdots & p{-}2 & p{-}1 \\ 0 & 1 & 2^2 & \cdots & (p{-}2)^2 & (p{-}1)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 2^{p-2} & \cdots & (p{-}2)^{p-2} & (p{-}1)^{p-2} \\ 0 & 1 & 2^{p-1} & \cdots & (p{-}2)^{p-1} & (p{-}1)^{p-1} \end{bmatrix} \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ \vdots \\ n_{p-2} \\ n_{p-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ -1 \end{bmatrix}$$

over $\mathbb{Q}$ has a unique solution, since the coefficient matrix is a nonsingular Vandermonde matrix. We have seen that $n_0 = n_1 = \cdots = n_{p-1} = 1$ is a solution, so (a) follows. Moreover the linear system

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 2 & \cdots & p-2 & p-1 \\ 0 & 1 & 2^2 & \cdots & (p-2)^2 & (p-1)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 2^{p-2} & \cdots & (p-2)^{p-2} & (p-1)^{p-2} \end{bmatrix} \begin{bmatrix} n_0 \\ n_1 \\ n_2 \\ \vdots \\ n_{p-2} \\ n_{p-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

has as its general solution $n_0 = n_1 = \cdots = n_{p-1}$ since the coefficient matrix has rank $p-1$. Since $n_0 + n_1 + n_2 + \cdots + n_{p-1} = p$, we have either (i) $n_0 = n_1 = \cdots = n_{p-1} = 1$, or (ii) one of the n_k's is p and the others are zero. Conclusion (b) follows. □

Let $\mathcal{N}$ be a 3-net of odd prime order p, i.e. a set of p^2 triples $(x,y,z) \in F^3$ such that each point $(x,y,z) \in \mathcal{N}$ is uniquely determined by any two of its coordinates. We have $\operatorname{rank}_p \mathcal{N} = 3p-2-\dim \mathcal{V}_0$ where $\mathcal{V}_0$ is the set of all triples (f,g,h) of functions $F \to F$ such that $f(0) = g(0) = h(0) = 0$ and

$$f(x) + g(y) + h(z) = 0 \quad \text{for all } (x,y,z) \in \mathcal{N}.$$

We must show that $\dim \mathcal{V}_0 \leqslant 1$, and that equality holds iff the 3-net $\mathcal{N}$ is cyclic.

Suppose $(f,g,h) \in \mathcal{V}_0$ is nonzero. Using always the convention that $0^0 = 1$, we see that $\sigma_{f,0} = \sigma_{g,0} = \sigma_{h,0} = 0$. Note that for all $r \geqslant 0$ and all $(x,y,z) \in \mathcal{N}$, we have

$$h(z)^r = (-1)^r \sum_{s=0}^{r} \binom{r}{s} f(x)^{r-s} g(y)^s$$

by the Binomial Theorem. Summing over all p triples $(x,y,z) \in \mathcal{N}$ with a fixed value of y gives

$$\sigma_{h,r} = (-1)^r \sum_{s=0}^{r} \binom{r}{s} \sigma_{f,r-s} g(y)^s \tag{5.1}$$

for all $r \geqslant 0$, $y \in F$.

Summing (5.1) over all $y \in F$ gives

$$0 = \sum_{s=0}^{r} \binom{r}{s} \sigma_{f,r-s} \sigma_{g,s} \tag{5.2}$$

for all $r \geqslant 0$.

Theorem 5.2. *We have*

$$\sigma_{f,r} = \sigma_{g,r} = \sigma_{h,r} = \begin{cases} 0, & \textit{for } r = 0, 1, 2, \ldots, p{-}2, \textit{ and} \\ -1, & \textit{for } r = p{-}1. \end{cases}$$

Proof. As previously noted, the result holds for $r = 0$. Assume the conclusion of the Theorem holds for all $r \in \{0, 1, \ldots, t\}$ where $t \leqslant p{-}2$, and we will verify the conclusion in the case $r = t{+}1$. Applying (5.1) in the case $r = t{+}1$, we have $\sigma_{h,t+1} = (-1)^{t+1}\sigma_{f,t+1}$. Similarly, we obtain $\sigma_{f,t+1} = (-1)^{t+1}\sigma_{g,t+1}$ and $\sigma_{g,t+1} = (-1)^{t+1}\sigma_{h,t+1}$. Clearly the conclusion $\sigma_{f,t+1} = \sigma_{g,t+1} = \sigma_{h,t+1} = 0$ follows if t is even, but we proceed to obtain the same conclusion regardless of the parity of t.

We consider first the case $t \leqslant \frac{1}{2}(p{-}3)$. Applying (5.2) for $r = 2t{+}2$ yields

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

Since $2t{+}2 < p$, this implies that $\sigma_{f,t+1}\sigma_{g,t+1} = 0$. Combining this with the previous paragraph yields $\sigma_{f,t+1} = \sigma_{g,t+1} = \sigma_{h,t+1} = 0$. Thus the conclusion holds for $r = t{+}1$ as well.

Next consider the case $\frac{1}{2}(p{-}1) \leqslant t < p{-}2$. Multiplying both sides of (5.1) by $g(y)^{2t+3-p}$ and setting $r = p{-}1$ yields

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

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

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

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 (5.1) 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 5.1 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 $f(x) = g(x) = -h(x) = x$ for all $x \in F$; otherwise relabel the lines in each parallel class so that this is the case. Since $f(x) + g(y) + h(z) = 0$ for all $(x, y, z) \in \mathcal{N}$, we obtain $\mathcal{N} = \{(x, y, x{+}y) : x, y \in F\}$ and so the 3-net $\mathcal{N}$ is cyclic. □

6. Fourth proof of main theorem (using exponential sums)

Let $F = \mathbb{F}_p$ where p is 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*

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

Now suppose $\mathcal{N}$ is a 3-net of order p, and let $(f, g, h) \in \mathcal{V}_0(\mathcal{N})$. 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. □

7. 4-nets of prime order

Let $\mathcal{N}$ be a 4-net of prime order p, and let $(f, g, h, u) \in \mathcal{V}(\mathcal{N})$. In the notation of Section 6, we sum the quantity $\zeta^{f(x)+g(y)} = \zeta^{-h(z)-u(t)}$ over all $(x, y, z, t) \in \mathcal{N}$ to obtain $S_f S_g = \overline{S_h S_u}$. It is not hard to check that either

$$|S_f| = |S_g| = |S_h| = |S_u| > 0$$

or at least three of the exponential sums $\{S_f, S_g, S_h, S_u\}$ vanish, in which case the corresponding members of $\{f, g, h, u\}$ are permutations. With some further investigation we have shown

Theorem 7.1. [8] *Let $\mathcal{N}$ be a 4-net of order p. Then:*

(*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 $p = 7, 11$ are found at [6,7].

References

[1] **V. D. Belousov**: MR561712 (81g:20133), 1981. Review of *Kvasigrupe (Quasigroups)* by U. Janez, 1979.

[2] **R. H. Bruck and H. J. Ryser**: *The nonexistence of certain finite projective planes*, Canad. J. Math. **1** (1949), 88 – 93.

[3] **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.

[4] **P. A. Griffiths**: *Variations on a theorem of Abel*, Inventiones Math. **35** (1976), 321 – 390.

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

[6] **G. E. Moorhouse**: *Nets and Latin squares of order* 7, available at `http://www.uwyo.edu/moorhouse/pub/nets7/`.

[7] **G. E. Moorhouse**: *Nets and Latin squares of order* 11, available at `http://www.uwyo.edu/moorhouse/pub/nets11/`.

[8] **G. E. Moorhouse**: *Ranks of Nets and of Webs*, preliminary version, 2005.

Department of Mathematics
University of Wyoming
1000 E. University Ave.
Laramie, WY 82071
U.S.A.
e-mail: moorhous@uwyo.edu

Received January 2, 2006