BRUCK NETS, CODES, AND CHARACTERS OF LOOPS

G. Eric Moorhouse

Abstract. Numerous computational examples suggest that if $\mathcal{N}_{k-1} \subset \mathcal{N}_k$ are $(k-1)$- and k-nets of order n, then $\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \ge n-k+1$ for any prime p dividing n at most once. We conjecture that this inequality always holds. Using characters of loops, we verify the conjecture in case $k=3$, proving in fact that if $p^e \,\big|\big|\, n$, then $\operatorname{rank}_p \mathcal{N}_3 \ge 3n-2-e$, where equality holds if and only if the loop G coördinatizing $\mathcal{N}_3$ has a normal subloop K such that G/K is an elementary abelian group of order p^e. Furthermore if n is squarefree, then $\operatorname{rank}_p \mathcal{N}_3 = 3n-3$ for every prime $p \,\big|\, n$, if and only if $\mathcal{N}_3$ is cyclic (i.e. $\mathcal{N}_3$ is coördinatized by a cyclic group of order n).

The validity of our conjectured lower bound, would imply that any projective plane of squarefree order, or of order $n \equiv 2 \bmod 4$, is in fact desarguesian of prime order.

Finally, our conjectured lower bound holds with equality in the case of desarguesian nets (i.e. subnets of $\mathrm{AG}(2,p)$), which leads to an easy description of an explicit basis for the $\mathbb{F}_p$-code of $\mathrm{AG}(2,p)$.

1. Introduction

A **k-net of order** n is an incidence structure consisting of n^2 points and nk distinguished subsets called lines, such that

(i) every line has exactly n points;

(ii) parallelism (the property of being either equal or disjoint) is an equivalence relation on the lines;

(iii) there are k parallel classes, each consisting of n lines, and

(iv) any two non-parallel lines meet exactly once.

(See [2], [3], [5], [8], [11], [16].) Thus an $(n+1)$-net of order n is the same thing as an affine plane of order n. For example the 4-net (affine plane, in this case desarguesian) of order 3 is shown in Figure 1.

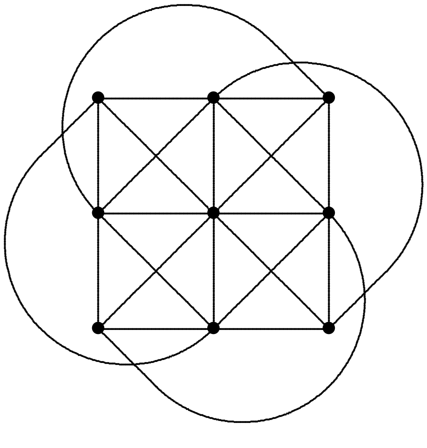


Figure 1. Affine plane of order 3

In Section 2 we shall give a formal description of the $\mathbb{F}_p$-code of such a net, as the span of the characteristic functions of the line sets. But for this first example we choose a more graphic approach as follows. The lines of the above net $\mathcal{N}$ are represented in an obvious way by the matrices

$$\begin{aligned}
M_{11}&=\begin{pmatrix}1&1&1\\0&0&0\\0&0&0\end{pmatrix}, & M_{12}&=\begin{pmatrix}0&0&0\\1&1&1\\0&0&0\end{pmatrix}, & M_{13}&=\begin{pmatrix}0&0&0\\0&0&0\\1&1&1\end{pmatrix},\\
M_{21}&=\begin{pmatrix}1&0&0\\1&0&0\\1&0&0\end{pmatrix}, & M_{22}&=\begin{pmatrix}0&1&0\\0&1&0\\0&1&0\end{pmatrix}, & M_{23}&=\begin{pmatrix}0&0&1\\0&0&1\\0&0&1\end{pmatrix},\\
M_{31}&=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, & M_{32}&=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, & M_{33}&=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\\
M_{41}&=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}, & M_{42}&=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}, & M_{43}&=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}.
\end{aligned}$$

The four parallel classes are represented by $\{M_{r1}, M_{r2}, M_{r3}\}$, $1 \le r \le 4$. The $\mathbb{F}_3$-code of $\mathcal{N}$ is the $\mathbb{F}_3$-span of these twelve matrices, denoted by $\mathcal{C}_3(\mathcal{N})$. Its dimension is easily found: $\operatorname{rank}_3 \mathcal{N} = \dim \mathcal{C}_3(\mathcal{N}) = 6$. We list six independent relations between the matrices M_{rs} with coefficients in $\mathbb{F}_3$:

$$M_{11}+M_{12}+M_{13} = M_{21}+M_{22}+M_{23} = M_{31}+M_{32}+M_{33} = M_{41}+M_{42}+M_{43},$$
$$M_{12}-M_{13}-M_{22}+M_{23} = M_{32}-M_{33}, \qquad M_{12}-M_{13}+M_{22}-M_{23} = M_{42}-M_{43},$$
$$M_{12}+M_{13}-M_{23}-M_{32} = M_{43}.$$

In fact if $\mathcal{N}_k$ denotes the k-subnet of $\mathcal{N}$ consisting of the first k parallel classes, as represented by $\{M_{r1}, M_{r2}, M_{r3}\}$, $1 \le r \le k$, then the above relations show that

$$\operatorname{rank}_3 \mathcal{N}_1 = 3, \qquad \operatorname{rank}_3 \mathcal{N}_2 = 5, \qquad \operatorname{rank}_3 \mathcal{N}_3 = 6.$$

(A **subnet** $\mathcal{N}' \subseteq \mathcal{N}$ consists of the same points as $\mathcal{N}$, and some subset of the parallel classes of $\mathcal{N}$.) There is a pattern here which becomes more apparent if we consider instead ranks of quotients of codes in the chain

$$\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \mathcal{N}_3 \subset \mathcal{N}_4 = \mathcal{N};$$

namely, write

$$\rho_k = \operatorname{rank}_3 \mathcal{N}_k - \operatorname{rank}_3 \mathcal{N}_{k-1} = \dim\big(\mathcal{C}_3(\mathcal{N}_k)/\mathcal{C}_3(\mathcal{N}_{k-1})\big).$$

Then $(\rho_1, \rho_2, \rho_3, \rho_4) = (3, 2, 1, 0)$, a decreasing arithmetic progression. We show in Section 6 that this arithmetic progression is typical of desarguesian nets. Numerous examples of nets gathered from the literature (see Section 3) suggest that when $p^2 \not| \, n$, the value $\rho_k = \operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1}$ is minimized in the case of desarguesian nets, which leads us to the following conjecture.

1.1 Conjecture. *Let $\mathcal{N}_k$ be any k-net of order n, and let $\mathcal{N}_{k-1}$ be any $(k-1)$-subnet thereof. If p is any prime such that $p^2 \not| \, n$, then*

$$\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \geq n - k + 1.$$

It is easily shown (see Proposition 2.1) that for $k \geq 2$ the upper bound $\rho_k = \operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \leq n - 1$ is attained whenever $p \not| \, n$, so in scrutinizing Conjecture 1.1 we may assume that $p \,||\, n$, i.e. p divides n exactly once. Conjecture 1.1 holds trivially for $k \leq 2$, and its validity for $k = 3$ is one conclusion of Theorem 4.2. Moreover we show that cyclic 3-nets (those coördinatized by cyclic groups) may be characterized by their p-ranks in special cases, namely when n is squarefree, or when the coördinatizing loop is a nilpotent group; see Corollaries 4.5–7.

Our main interest in this investigation is that Conjecture 1.1 implies that any projective plane of order $n \equiv 2 \mod 4$, or of *squarefree* order n (i.e. n is a product of distinct primes) is in fact desarguesian of prime order (see Theorem 5.1). To date, the only criterion for non-existence of a projective plane of a given order (aside from the recent computer-dependent result of C. Lam and J. McKay which announces the non-existence of a plane of order 10), is the celebrated Bruck-Ryser Theorem [6]. Furthermore for primes $p > 7$, no proof currently exists that every projective plane of order p is desarguesian.

It perhaps should be pointed out that our notion (see Section 2) of the code of a net $\mathcal{N}$, is equivalent to the usual notion of the row space of an incidence matrix of $\mathcal{N}$ over $\mathbb{F}_p$, as quite distinct from the orthogonal array codes found in [8,p.355], [14,p.328], which are (in general) nonlinear n-ary codes.

It is well known (see eg. [13]) that any $(p+1)$-net (i.e. affine plane) of prime order p has p-rank equal to $\frac{1}{2}p(p+1)$. We show (Theorem 6.1) that Conjecture 1.1 holds with equality, in the case of subnets of the desarguesian affine plane $\mathcal{N}_{p+1} = \mathrm{AG}(2,p)$, i.e. for arbitrary **desarguesian nets** of prime order. Moreover the arguments following the proof of Theorem 6.1 show how to construct an explicit basis for the code of $\mathcal{N}_{p+1}$: take all p lines in some parallel class, plus any $p-1$ lines from some other parallel class, plus any $p-2$

lines from yet another parallel class, and so on, finally taking 0 lines from the last remaining parallel class. Altogether this gives $p+(p-1)+(p-2)+\ldots+1+0=\frac{1}{2}p(p+1)$ lines as required.

We stress that Conjecture 1.1 is posed for *any* net $\mathcal{N}$, regardless of whether $\mathcal{N}$ is completable to an affine plane. Indeed, among the examples offered in Section 3 in support of the Conjecture, the nets of orders 14, 26, 33 and 38 do not even fulfill the Bruck-Ryser criterion for completability. The question of whether a given net may be completed (or even extended), so predominant in much of the literature on nets, is not relevant to an assessment of the veracity of Conjecture 1.1. The reader is challenged to verify Conjecture 1.1 at least for 4-nets, which after all "just" correspond to two orthogonal Latin squares!

The author is grateful to D. Jungnickel for numerous suggestions which were helpful in revising the original manuscript.

2. Defining the Code

Let $\mathcal{N}$ be a k-net of order n, with point set $\mathcal{P}$ and parallel classes $\{\ell_{rs} : 1\le s\le n\}$, $1\le r\le k$, and let p be a prime. To each line ℓ_{rs} of $\mathcal{N}$ there corresponds the characteristic function

$$\chi_{rs}:\mathcal{P}\to\mathbb{F}_p,\qquad \chi_{rs}(P)=\begin{cases}1, & P\in\ell_{rs};\\ 0, & P\notin\ell_{rs}.\end{cases}$$

The set $\mathbb{F}_p^{\mathcal{P}}$ of all functions $\mathcal{P}\to\mathbb{F}_p$ is an n^2-dimensional vector space over $\mathbb{F}_p$, and we define the **$\mathbb{F}_p$-code** of $\mathcal{N}$ as

$$\mathcal{C}_p(\mathcal{N})=\sum_{r=1}^{k}\sum_{s=1}^{n}\mathbb{F}_p\chi_{rs},$$

which is the subspace of $\mathbb{F}_p^{\mathcal{P}}$ spanned by the characteristic functions of the line sets of $\mathcal{N}$. The **p-rank** of $\mathcal{N}$ is

$$\operatorname{rank}_p\mathcal{N}=\dim\mathcal{C}_p(\mathcal{N}).$$

Two k-nets $\mathcal{N}_k$, $\mathcal{N}_k'$ are **isomorphic** (and we write $\mathcal{N}_k\cong\mathcal{N}_k'$) if there exists a bijection of the respective point sets, say $\theta:\mathcal{P}\to\mathcal{P}'$, taking the lines of $\mathcal{N}_k$ to those of $\mathcal{N}_k'$. (Here we deviate from other authors, eg. [1] and [16], in that we do *not* distinguish the parallel classes of $\mathcal{N}_k$ and $\mathcal{N}_k'$ with labels $1,2,\ldots,k$, requiring θ to preserve the labels on the parallel classes.) Clearly $\operatorname{rank}_p\mathcal{N}_k=\operatorname{rank}_p\mathcal{N}_k'$ whenever $\mathcal{N}_k\cong\mathcal{N}_k'$.

The following gives an upper bound for p-ranks of nets, which in general is the best possible. It also indicates that the only primes of interest are those dividing n.

2.1 Proposition. *Let $\mathcal{N}$ be a k-net of order n, and let p be a prime. Then*

$$\operatorname{rank}_p \mathcal{N} \le (n-1)k+1,$$

in which equality holds if $p \not| \, n$.

Proof. Define $\gamma \in \mathbb{F}_p^{\mathcal{P}}$ by $\gamma(P)=1$ for all $P \in \mathcal{P}$. Then

$$\gamma = \sum_{s=1}^{n} \chi_{1s} = \sum_{s=1}^{n} \chi_{2s} = \ldots = \sum_{s=1}^{n} \chi_{ks},$$

and so $\mathcal{C}_p(\mathcal{N})$ is spanned by

$$\{\gamma\} \cup \{\chi_{rs} : 1 \le r \le k,\ 2 \le s \le n\},$$

which proves that $\operatorname{rank}_p \mathcal{N} \le (n-1)k+1$. Now suppose that $p \not| \, n$. Let $\alpha \in \mathbb{F}_p$ such that $n\alpha = 1 \in \mathbb{F}_p$. Define a symmetric bilinear form on $\mathbb{F}_p^{\mathcal{P}}$ by

$$(\chi,\psi) = \alpha \sum_{P \in \mathcal{P}} \chi(P)\psi(P), \qquad \chi,\psi \in \mathbb{F}_p^{\mathcal{P}}.$$

Then $(\chi_{rs}, \chi_{r's'}) = \alpha \big| \ell_{rs} \cap \ell_{r's'} \big|$, and so

$$\left.\begin{array}{l} \big(\chi_{rs}\,,\ \chi_{r's'} - \chi_{r'1}\big) = \delta_{rr'}\delta_{ss'} \\ \big(\gamma\,,\ \chi_{r's'} - \chi_{r'1}\big) = 0 \\ \big(\chi_{rs}\,,\ \chi_{11}+\chi_{21}+\ldots+\chi_{k1}+\alpha(1-k)\gamma\big) = 0 \\ \big(\gamma\,,\ \chi_{11}+\chi_{21}+\ldots+\chi_{k1}+\alpha(1-k)\gamma\big) = 1 \end{array}\right\} \quad 1 \le r, r' \le k, \quad 2 \le s, s' \le n.$$

This shows that our original set of size $(n-1)k+1$ is a basis for $\mathcal{C}_p(\mathcal{N})$, and at the same time provides a dual basis with respect to our bilinear form. □

3. Computational Examples

Let $\mathcal{N}$ be a k-net of order n, and choose a maximal chain of subnets

$$\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \ldots \subset \mathcal{N}_{k-1} \subset \mathcal{N}_k = \mathcal{N}$$

where $\mathcal{N}_i$ is an i-subnet of order n. For each prime $p \,\big|\, n$ we have a sequence

$$(\rho_1, \rho_2, \ldots, \rho_k), \qquad \rho_i = \operatorname{rank}_p \mathcal{N}_i - \operatorname{rank}_p \mathcal{N}_{i-1}, \quad 1 \le i \le k.$$

This sequence depends not only on the choice of prime $p \,\big|\, n$, but also on the choice of chain of subnets. A given k-net $\mathcal{N}$ has exactly $k!$ such maximal chains of subnets, each chain being determined by one of the $k!$ possible orderings of the k parallel classes within $\mathcal{N}$. In general, distinct chains may yield distinct sequences $(\rho_1, \rho_2, \ldots, \rho_k)$, yet $\rho_1 + \rho_2 + \ldots + \rho_k = \operatorname{rank}_p \mathcal{N}$ is independent of the choice of chain $\{\mathcal{N}_i\}$ in $\mathcal{N}$.

For selected k-nets found in the literature, we have listed in Tables 1–3 all $k!$ sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ which occur, as we have determined by computer. (Most of the nets listed in these Tables, are presented in [2] and [11], although we have referred to the primary source in most cases.) For example, for the 4-net $\mathcal{N}^{7\mathrm{b}}$ of order 7, the sequences $(7, 6, 5, 5)$ and $(7, 6, 6, 4)$ occur 18 and 6 times respectively, where $18 + 6 = 24 = 4!$. Note how closely these examples corroborate Conjecture 1.1: $\rho_i \ge n - i + 1$, with equality in several cases. Actually, all the nets listed in Tables 1–3 are constructed (or constructible) from difference matrices over finite groups. Such nets are special in that they admit a group of order n consisting of central translations with a common direction (see [10], [11]), and this apparently accounts for their low rank.

We also tested a variety of nets not admitting such a group of central translations. These cases, listed in Table 4, most with $p \,\big|\big|\, n$, attain the upper bound of Proposition 2.1, which perhaps makes such examples less interesting for our purpose. Most of the examples of nets listed in Table 4 are constructed using quasi-difference matrices (see [2]). A given quasi-difference matrix, however, determines not always a unique net, but often a large number of possible nets, of which we sampled only a few at random due to computer time limitations. Our random choices always yielded the rank sequence (n, $n{-}1$, $n{-}1$, $\ldots$, $n{-}1$); nevertheless in Table 4 we do *not* assert that *every* net obtained from the indicated source yields the same rank sequence.

As an 'experimental control', in Table 5 we list rank sequences using primes p such that $p^2 \,\big|\, n$. Whereas the seven examples $\mathcal{N}^{24\mathrm{a}}$, $\mathcal{N}^{24\mathrm{b}}$, $\ldots$, $\mathcal{N}^{24\mathrm{g}}$ yielded the same rank sequences for $p = 3$ (see Table 3), for $p = 2$ only $\mathcal{N}^{24\mathrm{b}}$, $\mathcal{N}^{24\mathrm{d}}$ and $\mathcal{N}^{24\mathrm{f}}$ yielded the same rank sequences (not shown). In particular at least five of $\mathcal{N}^{24\mathrm{a}}$, $\mathcal{N}^{24\mathrm{b}}$, $\ldots$, $\mathcal{N}^{24\mathrm{g}}$ are nonisomorphic.

Table 1: Rank sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ with $p \,||\, n$

Net	Source	n	k	p	$(\rho_1, \rho_2, \ldots, \rho_k)$	
$\mathcal{N}^3$	affine plane of order 3	3	4	3	(3,2,1,0)	24×
$\mathcal{N}^5$	affine plane of order 5	5	6	5	(5,4,3,2,1,0)	720×
$\mathcal{N}^{7a}$	affine plane of order 7	7	8	7	(7,6,5,4,3,2,1,0)	40320×
$\mathcal{N}^{7b}$	Jungnickel and Grams [12]	7	4	7	(7,6,5,5)	18×
					(7,6,6,4)	6×
$\mathcal{N}^{12a}$	Wallis and Zhu [21]	12	6	3	(12,11,10,10,10,10)	360×
					(12,11,11, 9,10,10)	120×
					(12,11,11,11, 8,10)	120×
					(12,11,11,11,11, 7)	120×
$\mathcal{N}^{12b}$	Johnson, Dulmage and Mendelsohn [9]	12	7	3	(12,11,10,10,10,10,10)	2160×
					(12,11,11, 9,10,10,10)	720×
					(12,11,11,11, 8,10,10)	720×
					(12,11,11,11,11, 7,10)	720×
					(12,11,11,11,11,11, 6)	720×
$\mathcal{N}^{15}$	Schellenberg, van Rees and Vanstone [18]	15	6	3	(15,14,13,13,13,13)	360×
					(15,14,14,12,13,13)	120×
					(15,14,14,14,11,13)	120×
					(15,14,14,14,14,10)	120×
$\mathcal{N}^{15}$	”	15	6	5	(15,14,13,13,12,12)	324×
					(15,14,14,13,13,10)	108×
					(15,14,14,13,11,12)	108×
					(15,14,14,12,12,12)	108×
					(15,14,13,12,13,12)	48×
					(15,14,13,14,13,10)	12×
					(15,14,13,14,11,12)	12×

Table 2: More rank sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ with $p \,||\, n$

Net	Source	n	k	p	$(\rho_1, \rho_2, \ldots, \rho_k)$	
$\mathcal{N}^{13a}$	Todorov [20]	13	8	13	(13,12,11,11,10, 9, 8, 6)	8352×
					(13,12,12,11,10, 9, 7, 6)	5568×
					(13,12,11,10,11, 9, 8, 6)	3072×
					(13,12,12,10,10, 9, 8, 6)	2784×
					(13,12,12,11, 9, 9, 8, 6)	2784×
					(13,12,12,11,10, 8, 8, 6)	2784×
					(13,12,11,10, 9,11, 8, 6)	2400×
					(13,12,11,12,10, 9, 7, 6)	1536×
					(13,12,11,10, 9, 8,11, 6)	1440×
					(13,12,11,11,10, 8, 9, 6)	1152×
					(13,12,11,10,12, 9, 7, 6)	960×
					(13,12,11,11, 9,10, 8, 6)	864×
					(13,12,12,11, 9,10, 7, 6)	768×
					(13,12,12,11, 9, 8, 9, 6)	768×
					(13,12,11,12,10, 8, 8, 6)	768×
					(13,12,11,12, 9, 9, 8, 6)	768×
					(13,12,12,10,11, 9, 7, 6)	576×
					(13,12,12,10, 9,10, 8, 6)	576×
					(13,12,11,10,12, 8, 8, 6)	480×
					(13,12,11,10, 9,12, 7, 6)	480×
					(13,12,11,10,11, 8, 9, 6)	384×
					(13,12,12,10,10, 8, 9, 6)	384×
					(13,12,12,10,11, 8, 8, 6)	288×
					(13,12,11,12, 9,10, 7, 6)	192×
					(13,12,11,12, 9, 8, 9, 6)	192×
$\mathcal{N}^{13b}$ $\mathcal{N}^{13c}$	”	13	8	13	rank distributions similar (but not identical) to those of $\mathcal{N}^{13a}$ above	
$\mathcal{N}^{21}$	Schellenberg, van Rees and Vanstone [18]	21	6	3	(21,20,19,19,19,19)	360×
					(21,20,20,18,19,19)	120×
					(21,20,20,20,17,19)	120×
					(21,20,20,20,20,16)	120×
$\mathcal{N}^{21}$	”	21	6	7	(21,20,19,19,19,19)	360×
					(21,20,20,18,19,19)	120×
					(21,20,20,20,17,19)	120×
					(21,20,20,20,20,16)	120×

TABLE 3: More rank sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ with $p \,||\, n$

Net	Source	n	k	p	$(\rho_1, \rho_2, \ldots, \rho_k)$	
$\mathcal{N}^{24\text{a}}$	Roth and Peters [17]	24	6	3	(24,23,22,22,22,22)	360×
					(24,23,23,21,22,22)	120×
					(24,23,23,23,20,22)	120×
					(24,23,23,23,23,19)	120×
$\mathcal{N}^{24\text{b}}$ $\mathcal{N}^{24\text{c}}$ $\mathcal{N}^{24\text{d}}$ $\mathcal{N}^{24\text{e}}$ $\mathcal{N}^{24\text{f}}$ $\mathcal{N}^{24\text{g}}$	”	24	6	3	same rank distributions as $\mathcal{N}^{24\text{a}}$ above	
$\mathcal{N}^{33}$	Schellenberg, van Rees and Vanstone [18]	33	5	3	(33,32,31,31,31)	72×
					(33,32,32,32,29)	24×
					(33,32,32,30,31)	24×
$\mathcal{N}^{33}$	”	33	5	11	(33,32,31,31,30)	54×
					(33,32,31,30,31)	24×
					(33,32,32,30,30)	18×
					(33,32,32,31,29)	18×
					(33,32,31,32,29)	6×
$\mathcal{N}^{39}$	Schellenberg, van Rees and Vanstone [18]	39	5	3	(39,38,37,37,37)	72×
					(39,38,38,38,35)	24×
					(39,38,38,36,37)	24×
$\mathcal{N}^{39}$	”	39	5	13	(39,38,37,37,36)	54×
					(39,38,37,36,37)	24×
					(39,38,38,36,36)	18×
					(39,38,38,37,35)	18×
					(39,38,37,38,35)	6×

TABLE 4: Rank sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ achieving the upper bound for ρ_i

Net	Source	n	k	p	$(\rho_1, \rho_2, \ldots, \rho_k)$
$\mathcal{N}^{10}$	Parker [15]	10	4	2	(10, 9, 9, 9) 24×
$\mathcal{N}^{10}$	”	10	4	5	(10, 9, 9, 9) 24×
$\mathcal{N}^{14a}$	Zhu [23,p.2]	14	4	2	(14,13,13,13) 24×
$\mathcal{N}^{14a}$	”	14	4	7	(14,13,13,13) 24×
$\mathcal{N}^{14b}$	Zhu [23,p.3]	14	4	2	(14,13,13,13) 24×
$\mathcal{N}^{14b}$	”	14	4	7	(14,13,13,13) 24×
$\mathcal{N}^{14c}$	Todorov [19]	14	5	2	(14,13,13,13,13) 120×
$\mathcal{N}^{14c}$	”	14	5	7	(14,13,13,13,13) 120×
$\mathcal{N}^{14d}$ $\mathcal{N}^{14e}$ $\}$	”	14	5	2,7	same rank distribution as $\mathcal{N}^{14c}$ above
$\mathcal{N}^{18}$	Wang [22]; [2,p.402]	18	5	2	(18,17,17,17,17) 120×
$\mathcal{N}^{22}$	Wang [22]; [2,p.403]	22	5	2	(22,21,21,21,21) 120×
$\mathcal{N}^{22}$	”	22	5	11	(22,21,21,21,21) 120×
$\mathcal{N}^{26}$	Wang [22]; [2,p.404]	26	5	2	(26,25,25,25,25) 120×
$\mathcal{N}^{26}$	”	26	5	13	(26,25,25,25,25) 120×
$\mathcal{N}^{30}$	Wang [22]; [2,p.404]	30	5	2	(30,29,29,29,29) 120×
$\mathcal{N}^{30}$	”	30	5	3	(30,29,29,29,29) 120×
$\mathcal{N}^{30}$	”	30	5	5	(30,29,29,29,29) 120×
$\mathcal{N}^{38}$	Todorov [20]	38	6	2	(38,37,37,37,37,37) 720×
$\mathcal{N}^{38}$	”	38	6	19	(38,37,37,37,37,37) 720×
$\mathcal{N}^{44}$	Todorov [20]	44	6	2	(44,43,43,43,43,43) 720×
$\mathcal{N}^{44}$	”	44	6	11	(44,43,43,43,43,43) 720×

TABLE 5: Rank sequences $(\rho_1, \rho_2, \ldots, \rho_k)$ with $p^2 \,\big|\, n$

Net	Source	n	k	p	$(\rho_1, \rho_2, \ldots, \rho_k)$
$\mathcal{N}^{12a}$	Wallis and Zhu [21]	12	6	2	(12,11, 9, 9, 9, 5) 300×
					(12,11,11, 7, 9, 5) 108×
					(12,11,11,11, 5, 5) 144×
					(12,11,11, 9, 7, 5) 36×
					(12,11, 9, 9, 7, 7) 84×
					(12,11,11, 7, 7, 7) 36×
					(12,11, 9,11, 7, 5) 12×
$\mathcal{N}^{12b}$	Johnson, Dulmage and Mendelsohn [9]	12	7	2	(12,11, 9, 9, 9, 9, 3) 1464×
					(12,11, 9, 9, 9, 5, 7) 600×
					(12,11, 9, 9, 7, 7, 7) 168×
					(12,11,11, 7, 9, 9, 3) 504×
					(12,11,11,11, 5, 9, 3) 576×
					(12,11,11,11,11, 3, 3) 720×
					(12,11,11,11, 9, 5, 3) 144×
					(12,11,11, 7, 9, 5, 7) 216×
					(12,11,11,11, 5, 5, 7) 288×
					(12,11,11, 9, 7, 9, 3) 72×
					(12,11,11, 9, 7, 5, 7) 72×
					(12,11,11, 9,11, 5, 3) 72×
					(12,11,11, 7, 7, 7, 7) 72×
					(12,11, 9,11, 7, 9, 3) 24×
					(12,11, 9,11, 7, 5, 7) 24×
					(12,11, 9,11,11, 5, 3) 24×
$\mathcal{N}^{16}$	Example 3.1	16	5	2	(16,15,11,11, 5) 72×
					(16,15,15,11, 1) 24×
					(16,15,15, 7, 5) 24×
$\mathcal{N}^{24a}$	Roth and Peters [17]	24	6	2	(24,23,20,20,20,20) 360×
					(24,23,23,17,20,20) 96×
					(24,23,23,22,15,20) 72×
					(24,23,23,22,22,13) 72×
					(24,23,23,23,14,20) 24×
					(24,23,23,23,21,13) 24×
					(24,23,22,18,20,20) 24×
					(24,23,22,23,15,20) 24×
					(24,23,22,23,22,13) 24×
$\mathcal{N}^{24b}$ ⋮ $\mathcal{N}^{24g}$	”	24	6	2	rank distributions similar (but not identical) to those of $\mathcal{N}^{24a}$ above

In Table 5 we also include the following example, noteworthy for attaining the particularly small value $\rho_5 = 1$:

3.1 Example. *$\mathcal{N}^{16}$ is the 5-net of order 16 constructed as in [2] from the difference matrix*

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
0 & 4 & 15 & 10 & 14 & 11 & 2 & 1 & 9 & 5 & 8 & 12 & 3 & 6 & 13 & 7 \\
0 & 5 & 13 & 9 & 10 & 14 & 4 & 6 & 1 & 12 & 2 & 7 & 15 & 11 & 3 & 8
\end{pmatrix}$$

over the elementary abelian group of order 16. Here the group elements $0, 1, 2, \ldots, 15$ *are added by first converting to binary representation, then adding 'without carrying'.*

This example refutes any hope of extending Conjecture 1.1 to $\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \geq n-(k-2)e-1$ in case $k \geq 2$, $p^e \,\|\, n$, as might well have been suggested by the other examples of Table 5, as well as by Theorem 4.2.

The computer programs we used in producing Tables 1–5 would first convert each example (whether defined by an explicitly printed list of orthogonal Latin squares, or by difference matrices, or by orthomorphisms, or by quasi-difference matrices) to the matrix representation of a net. These nets were then uniformly checked by a common program to ensure that they satisfied the defining properties of a net, in order to screen for input errors, before computing rank sequences.

4. Loops, 3-Nets and Their Ranks

A **loop** is a set G together with a binary operation $* : G \times G \to G$ such that

(i) for all $a, c \in G$ the equation $a * x = c$ has a unique solution $x \in G$;

(ii) for all $b, c \in G$ the equation $x * b = c$ has a unique solution $x \in G$; and

(iii) G contains a two-sided **identity** element, i.e. there exists $1 \in G$ such that $1 * x = x * 1 = x$ for all $x \in G$.

The **order** of a loop G is $|G|$. We proceed to review the correspondence between 3-nets of order n and loops of order n. (For more details see [1], [3] or [16].)

Given a loop G of order n, we define a 3-net $\mathcal{N} = \mathcal{N}(G)$ of order n on the points $G \times G = \{(x, y) : x, y \in G\}$ by choosing the following three parallel classes of lines:

$$\ell_{1g} = \{(g, y) : y \in G\}, \quad g \in G;$$

$$\ell_{2g} = \{(x, g) : x \in G\}, \quad g \in G;$$

$$\ell_{3g} = \{(x, y) : x * y = g\}, \quad g \in G.$$

(Here we deviate slightly from the notation of Section 2 by using subscripts from G rather than 1, 2, …, n.)

Conversely, given a 3-net $\mathcal{N}$ of order n with parallel classes $\{\ell_{rs} : 1 \le s \le n\}$, $1 \le r \le 3$, we may construct (although not uniquely) a loop G of order n such that $\mathcal{N}(G) \cong \mathcal{N}$, as follows. Arbitrarily label the three parallel classes of $\mathcal{N}$ as classes 1, 2 and 3. Arbitrarily choose a point $(1,1)$ of $\mathcal{N}$ as the 'origin', and let $(1,1) = \ell_{11} \cap \ell_{21}$ where ℓ_{11} and ℓ_{21} are lines of class 1 and 2 respectively. Arbitrarily label the remaining points of ℓ_{11} as $(1,2)$, $(1,3)$, …, $(1,n)$. Let ℓ_{2i} (resp. ℓ_{3i}) be the unique line of class 2 (resp. class 3) through $(1,i)$. Let $(i,1) = \ell_{21} \cap \ell_{3i}$, ℓ_{1i} = the unique line of class 1 through $(i,1)$, and $(i,j) = \ell_{1i} \cap \ell_{2j}$. Finally define $G = \{1,2,\ldots,n\}$, with binary operation $* : G \times G \to G$, $i * j = s$ where $\ell_{1i} \cap \ell_{2j} \in \ell_{3s}$. Then $(G,*)$ is a loop with identity 1, such that $\mathcal{N}(G) \cong \mathcal{N}$, and we say that G **coördinatizes** $\mathcal{N}$. Although $\mathcal{N}$ itself does not determine G uniquely, G is specified up to loop isomorphism once the three parallel classes of $\mathcal{N}$ are distinguished and a point of $\mathcal{N}$ is distinguished as the 'origin'.

While it is possible for nonisomorphic loops to coördinatize isomorphic 3-nets, it is well known that this cannot happen for a 3-net coördinatized by an associative loop (i.e. a group). But to extract this fact from the existing literature requires some care as to what is meant by 'net isomorphism' (recall our definition in Section 2), and so we present a direct proof of this assertion here.

4.1 Proposition. *Let G_1 be a group of order n, and G_2 a loop of order n. Then $G_1 \cong G_2$ if and only if $\mathcal{N}(G_1) \cong \mathcal{N}(G_2)$.*

Proof. If $G_1 \cong G_2$ then clearly $\mathcal{N}(G_1) \cong \mathcal{N}(G_2)$.

Conversely, let $\mathcal{N} = \mathcal{N}(G_1)$ with point set $G_1 \times G_1$ and lines ℓ_{1g}, ℓ_{2g}, ℓ_{3g} $(g \in G_1)$ defined as above. Then $\mathcal{N}$ admits an automorphism $\theta : (x,y) \mapsto (y^{-1}, x^{-1})$, which maps $\ell_{1g} \mapsto \ell_{2,g^{-1}}$, $\ell_{2g} \mapsto \ell_{1,g^{-1}}$, $\ell_{3g} \mapsto \ell_{3,g^{-1}}$ and an automorphism $\rho : (x,y) \mapsto (xy, y^{-1})$, which maps $\ell_{1g} \mapsto \ell_{3g}$, $\ell_{2g} \mapsto \ell_{2,g^{-1}}$, $\ell_{3g} \mapsto \ell_{1g}$. Thus $\operatorname{Aut}\mathcal{N}$ induces all $3! = 6$ permutations of the three parallel classes. Furthermore $\operatorname{Aut}\mathcal{N}$ has a subgroup of order n^2 acting transitively on the points, while preserving each parallel class: for any $u, v \in G_1$ we have $\tau_{uv} : (x,y) \mapsto (ux, yv)$, which maps $\ell_{1g} \mapsto \ell_{1,ug}$, $\ell_{2g} \mapsto \ell_{2,gv}$, $\ell_{3g} \mapsto \ell_{3,ugv}$. Consequently any choice of labels 1, 2, 3 for the three parallel classes of $\mathcal{N}$, and any choice of point as 'origin' for $\mathcal{N}$, will yield the same (i.e. isomorphic) coördinatizing loop for $\mathcal{N}$. □

For our purposes, a p**-character** of a loop G shall mean a loop homomorphism $G \to \mathbb{F}_p$, i.e. a map $\phi : G \to \mathbb{F}_p$ such that $\phi(g * h) = \phi(g) + \phi(h)$ for all $g, h \in G$. Clearly the set $\mathrm{Hom}(G, \mathbb{F}_p)$ of all p-characters of G, is a vector space over $\mathbb{F}_p$. In proving the following results we shall assume some basic facts concerning loops (eg. Lagrange's Theorem for normal subloops, homomorphisms of loops, and isomorphism theorems) as recorded in [4].

4.2 Theorem. *Let G be a loop of order n, with corresponding 3-net $\mathcal{N}_3 = \mathcal{N}(G)$, and let p be a prime such that $p^e \,\big|\big|\, n$. Then*

$$\mathrm{rank}_p \mathcal{N}_3 = 3n - 2 - \dim \mathrm{Hom}\,(G, \mathbb{F}_p) = 3n - 2 - s \geq 3n - 2 - e$$

where $p^s = [G : K]$ and K is the unique minimal normal subloop of G such that G/K is an elementary abelian p-group.

Proof. Corresponding to the lines $\ell_{1g}, \ell_{2g}, \ell_{3g}$ $(g \in G)$ of $\mathcal{N}_3$, we have the characteristic functions $\chi_{1g}, \chi_{2g}, \chi_{3g} \in \mathbb{F}_p^{\mathcal{P}}$ where $\mathcal{P} = G \times G$ is the point set of $\mathcal{N}_3$. Since $\sum\limits_{g\in G} \chi_{1g} = \sum\limits_{g\in G} \chi_{2g} = \sum\limits_{g\in G} \chi_{3g}$, the code $\mathcal{C}_p(\mathcal{N}_3)$ spanned by $\{\chi_{ig} : 1 \leq i \leq n,\ g \in G\}$ has dimension $\leq$ $3n - 2$, and in fact

$$\dim \mathcal{C}_p(\mathcal{N}_3) = 3n - 2 - \dim \mathcal{V},$$

where $\mathcal{V}$ is the vector space (over $\mathbb{F}_p$) consisting of all sequences $\big(a_g : g \in G\big)$ in $\mathbb{F}_p$ such that $a_1 = 0$ (where $1 \in G$ is the two-sided identity) and

$$\sum_{g\in G} a_g \chi_{3g} \in \sum_{i=1}^{2} \sum_{g\in G} \mathbb{F}_p \chi_{ig}.$$

If $\chi \in \sum\limits_{i=1}^{2} \sum\limits_{g\in G} \mathbb{F}_p \chi_{ig}$, then clearly $\chi(1,1) - \chi(x,1) - \chi(1,y) + \chi(x,y) = 0$ for all $(x,y) \in \mathcal{P}$. It follows that for $\big(a_g : g \in G\big) \in \mathcal{V}$, we have $a_1 - a_x - a_y + a_{x*y} = 0$. But $a_1 = 0$, so the map $G \to \mathbb{F}_p,\ g \mapsto a_g$ is a p-character of G. Conversely, if $\phi \in \mathrm{Hom}\,(G, \mathbb{F}_p)$, then $\phi(1) = 0$ and

$$\sum_{g\in G} \phi(g) \chi_{3g} = \sum_{i=1}^{2} \sum_{g\in G} \phi(g) \chi_{ig},$$

since the values of both sides agree at an arbitrary point $(x,y) \in \mathcal{P} = G \times G$. Thus we may identify $\mathcal{V}$ with $\mathrm{Hom}\,(G, \mathbb{F}_p)$, which proves that $\mathrm{rank}_p \mathcal{N}_3 = 3n - 2 - \dim \mathrm{Hom}\,(G, \mathbb{F}_p)$.

If H_1 and H_2 are normal subloops of G such that each quotient G/H_i is an elementary abelian p-group, then $H_1 \cap H_2$ is a normal subloop of G, and the natural loop homomorphism

$$\pi : G \to \big(G/H_1\big) \times \big(G/H_2\big), \quad g \mapsto (gH_1, gH_2)$$

has kernel $H_1 \cap H_2$, so that $G/H_1 \cap H_2$ is isomorphic to a subgroup of $\big(G/H_1\big) \times \big(G/H_2\big)$. This means that the class of all normal subloops $H \subseteq G$ such that G/H is an elementary abelian p-group, has a unique minimal member, say K, and $\big|G/K\big| = |G|\big/|K| = p^s,\ \ s \le e$.

If $\phi \in \mathrm{Hom}\,(G, \mathbb{F}_p)$ is nonzero, then $\ker\phi$ is a normal subloop of G such that $G/\ker\phi$ is a cyclic group of order p, so that $\ker\phi \supseteq K$; thus there is a unique $\overline{\phi} \in \mathrm{Hom}\,\big(G/K, \mathbb{F}_p\big)$ such that $\phi(g) = \overline{\phi}(gK)$ for all $g \in G$. Conversely any p-character of G/K, after composing with the natural homomorphism $G \to G/K$, gives a p-character of G. This gives a bijection between $\mathrm{Hom}\,(G, \mathbb{F}_p)$ and $\mathrm{Hom}\,\big(G/K, \mathbb{F}_p\big)$. Thus $\dim \mathrm{Hom}\,(G, \mathbb{F}_p) = \dim \mathrm{Hom}\,\big(G/K, \mathbb{F}_p\big) = s \le e$, from which the result follows. □

Bruck, in his beautiful 1951 paper [3], encountered a normal subloop condition similar to the definition of K above, when considering extendability of nets, using some basic notions (if not strictly the modern language) of coding theory. Combining Bruck's results with ours gives the following.

4.3 Corollary. *Let $\mathcal{N}_3$ be a 3-net of order $n \equiv 2 \mod 4$. If $\mathcal{N}_3$ is extendable to a 4-net, then* $\mathrm{rank}_2\,\mathcal{N}_3 = 3n-2$.

Proof. Let G be a loop coördinatizing $\mathcal{N}_3$. If $\mathrm{rank}_2\,\mathcal{N}_3 = 3n-3$ then G has a normal subloop of order $n/2$ by Theorem 4.2, in which case by [3], $\mathcal{N}_3$ cannot be extended by a single additional line, much less by a fourth parallel class. □

Corollary 4.3 explains why the examples of Table 4 with $2\,\big|\big|\,n$, have $\rho_3 = n-1$.

4.4 Theorem. *Let G be a loop of order $n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$, where $p_1, p_2, \ldots, p_m$ are distinct primes, and let $\mathcal{N}_3 = \mathcal{N}(G)$. Then the following four conditions are equivalent.*

(i) *G is a direct product of elementary abelian groups of order $p_i^{e_i}$, $\ i = 1, 2, \ldots, m$.*

(ii) $\mathrm{rank}_{p_i}\,\mathcal{N}_3 = 3n - 2 - e_i$ *for $i = 1, 2, \ldots, m$.*

(iii) $\dim \mathrm{Hom}\,(G, \mathbb{F}_{p_i}) = e_i$ *for $i = 1, 2, \ldots, m$.*

(iv) *For $i = 1, 2, \ldots, m$, G has a normal subloop K_i such that G/K_i is an elementary abelian group of order $p_i^{e_i}$.*

Proof. By the previous results, it remains only to assume (iv) and prove (i). The natural homomorphism

$$\pi : G \to \big(G/K_1\big) \times \big(G/K_2\big) \times \big(G/K_m\big), \quad g \mapsto (gK_1, gK_2, \ldots, gK_m)$$

has kernel $K_1 \cap K_2 \cap \ldots \cap K_m$, a normal subloop of G, with order dividing $n/p_i^{e_i}$ for each i, and so $\ker \pi = 1$, i.e. π is one-to-one. Comparing orders, we see that π is an isomorphism.□

A 3-net is **cyclic** if one (and hence each) of its coördinatizing loops is a cyclic group.

4.5 Corollary. *Let $\mathcal{N}_3$ be a 3-net of squarefree order n, coördinatized by a loop G. Then $\mathcal{N}_3$ is cyclic, if and only if* $\text{rank}_p \mathcal{N}_3 = 3n - 3$ *for every prime* $p \,\big|\, n$.

With the interest of characterizing cyclic 3-nets of *arbitrary* order by their p-ranks, D. Jungnickel has observed the following (which is invalid with 'solvable' in place of 'nilpotent', as the example of $\mathrm{S}_3 \times \mathrm{C}_3$ shows):

4.6 Corollary. *Let $\mathcal{N}_3 = \mathcal{N}(G)$ where G is a nilpotent group of order n. Then $\mathcal{N}_3$ is cyclic if and only if* $\text{rank}_p \mathcal{N}_3 = 3n - 3$ *for every prime* $p \,\big|\, n$.

This actually follows from the more general result

4.7 Corollary. *Let $\mathcal{N}_3 = \mathcal{N}(G)$, where G is a nilpotent loop of order n. Then G is generated by a single element, if and only if* $\text{rank}_p \mathcal{N}_3 \geq 3n - 3$ *for every prime* $p \,\big|\, n$.

Proof of Corollary 4.7. Let $n = p_1^{e_1} p_2^{e_2} \ldots p_m^{e_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes. Let $\Phi(G)$ be the Frattini subloop of G (see [4]). Since G is nilpotent, $G/\Phi(G)$ is a direct product of cyclic groups of prime order, and furthermore $\Phi(G)$ is the unique minimal normal subloop of G with this property.

Suppose that $\text{rank}_{p_i} \mathcal{N}_3 \geq 3n - 3$ for $i = 1, 2, \ldots, m$. Then $|G/\Phi(G)|$ divides $p_1 p_2 \ldots p_m$ by Theorem 4.4, and in particular $G/\Phi(G)$ is cyclic. Let $g \in G$ such that $g\Phi(G)$ generates $G/\Phi(G)$; then $G = \langle g, \Phi(G) \rangle = \langle g \rangle$. The converse follows by reversing these steps. □

Note that if G is a nilpotent group of order n and the prime $p \,\big|\, n$, then G necessarily has a normal subgroup of index p, so Theorem 4.4 yields $\text{rank}_p \mathcal{N}(G) \leq 3n - 3$; this explains why the inequality in the statement of 4.7 was replaced with equality in 4.6. The situation for loops is different; eg. the loop G of order 6 with multiplication table

1	2	3	4	5	6
2	1	4	3	6	5
3	4	5	6	1	2
4	3	6	5	2	1
5	6	1	2	4	3
6	5	2	1	3	4

is nilpotent; we have $G = \langle 3\rangle$, $\Phi(G) = \mathrm{Z}(G) = \{1,2\}$, $\mathrm{rank}_3\,\mathcal{N}(G) = 3n-3 = 15$, $\mathrm{rank}_2\,\mathcal{N}(G) = 3n-2 = 16$.

5. Implications for Projective Planes

Our main result is as follows.

5.1 Theorem. *Suppose that* Π *is a projective plane of order* n*, where* n *is squarefree or* $n \equiv 2 \mod 4$*. If Conjecture 1.1 holds for* n*, then* n *is prime and* Π *is Desarguesian.*

Before proving Theorem 5.1, we require the following two propositions, in which n is an arbitrary integer, not necessarily satisfying the hypotheses of Theorem 5.1.

5.2 Proposition. *Let* G *be a cyclic group of order* $n > 1$*.*
(i) If n *is odd, then every element of* G *is a product of two generators of* G*.*
(ii) If n *is even, then every square in* G *is a product of two generators.*

As a corollary,
(iii) every non-generator of G *is expressible as the product of two generators.*

Proof of Proposition 5.2. (i) We proceed by induction on the number of distinct prime divisors of n. First suppose that n is a power of an odd prime p. Let x be a generator for G. For any element $x^e \in G$, at most one of $\{x^{e-1}, x^{e+1}\}$ belongs to $\langle x^p\rangle$ (i.e. fails to generate G). Thus at least one of the two factorizations $x^e = x^{e-1}x = x^{e+1}x^{-1}$ suffices.

Now suppose that $n = n_1n_2$ where n_1 and n_2 are relatively prime odd integers exceeding 1. We have $G = G_1G_2 \cong G_1 \times G_2$ where G_i is cyclic of order n_i. The generators of G

are of the form x_1x_2 where x_i generates G_i. Let $a \in G$. Then $a = a_1a_2$, $a_i \in G_i$. We may suppose by induction that $a_i = x_iy_i$ where $\langle x_i\rangle = \langle y_i\rangle = G_i$. Then $a = (x_1x_2)(y_1y_2)$ is a factorization as required.

(ii) Write $n = n_1n_2$, $n_1 = 2^s$, n_2 odd, $G = G_1G_2 \cong G_1 \times G_2$, G_i cyclic of order n_i. Since the squares in G are of the form a_1a_2 where $a_i \in G_i$ and a_1 is a square, it suffices (cf. (i)) to prove the result for G_1. Let x generate G_1. If $a \in G_1$ is a square, then ax is a nonsquare, so $\langle ax\rangle = G_1$, and the factorization $a = (ax)(x^{-1})$ suffices.

(iii) Follows directly from (i) and (ii). □

Let G be a loop of order n, with corresponding 3-net $\mathcal{N}_3 = \mathcal{N}(G)$. It is convenient to assume that $G = \{1, 2, \ldots, n\}$ with binary operation $* : G \times G \to G$. With respect to the lexicographical ordering of the lines as $\ell_{11}, \ell_{12}, \ldots, \ell_{1n}$, $\ell_{21}, \ell_{22}, \ldots, \ell_{2n}$, $\ell_{31}, \ell_{32}, \ldots, \ell_{3n}$, and the points as $(1,1), (1,2), \ldots, (1,n)$, $(2,1), (2,2), \ldots, (2,n)$, $\ldots$, $(n,1), (n,2), \ldots, (n,n)$, the line-point incidence matrix of $\mathcal{N}_3$ is

$$(5.3) \qquad A = \begin{pmatrix} R_1 & R_2 & R_3 & \cdots & R_n \\ I & I & I & \cdots & I \\ I & \Sigma_2 & \Sigma_3 & \cdots & \Sigma_n \end{pmatrix}$$

where $\Sigma_2, \Sigma_3, \ldots, \Sigma_n$ are $n \times n$ permutation matrices such that $I + \Sigma_2 + \Sigma_3 + \ldots + \Sigma_n = J$ (the $n \times n$ matrix of 1's), the $(s,1)$-entry of Σ_s is 1, and the $n \times n$ matrices R_s are given by

$$(5.4) \qquad R_1 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \ldots, \; R_n = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

An n**-cycle matrix** is an $n \times n$ permutation matrix of the form $\big(\delta_{i,\sigma(j)} \,:\, 1 \le i, j \le n\big)$ where the permutation $\sigma \in \mathrm{S}_n$ is an n-cycle, i.e. σ is conjugate in S_n to $(1\,2\,3\,\ldots\,n)$.

5.5 Proposition. *A 3-net $\mathcal{N}_3$ of order n having incidence matrix given by (5.3), is a cyclic 3-net if and only if $\{I, \Sigma_2, \Sigma_3, \ldots, \Sigma_n\} = \{I, Q, Q^2, \ldots, Q^{n-1}\}$ for some n-cycle matrix Q.*

Proof. Suppose that $\{\Sigma_1 = I, \Sigma_2, \Sigma_3, \ldots, \Sigma_n\} = \{I, Q, Q^2, \ldots, Q^{n-1}\}$ for some n-cycle matrix Q. Then $Q = M^{-1}Q_0M$ for some $n \times n$ permutation matrix M, where

$$Q_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

With no loss of generality, we may assume that $Q = Q_0$, for otherwise replace A by the equivalent incidence matrix

$$\begin{pmatrix} I & 0 & 0 \\ 0 & M^{-1} & 0 \\ 0 & 0 & M^{-1} \end{pmatrix} A \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix}.$$

Without loss of generality the $(s,1)$-entry of Σ_s is 1; otherwise permute the $3n \times n$ blocks $\left(\begin{smallmatrix} R_s \\ I \\ \Sigma_s \end{smallmatrix}\right)$ appropriately, then permute rows 2, 3, ..., n of A to restore the first n rows to $\big(R_1\, R_2\, \cdots\, R_n\big)$. Then $\Sigma_s = Q_0^{s-1}$. Labelling the rows of A by the lines lexicographically ordered as $\ell_{11}, \ell_{12}, \ldots, \ell_{1n}$, $\ell_{21}, \ell_{22}, \ldots, \ell_{2n}$, $\ell_{31}, \ell_{32}, \ldots, \ell_{3n}$, we have $i{*}j = k \iff \ell_{1i} \cap \ell_{2j} \in \ell_{3k} \iff$ the (k,j)-entry of $\Sigma_i = Q_0^{i-1}$ is 1 $\iff (i-1) + (j-1) \equiv (k-1) \bmod n$. Thus $G = \{1, 2, \ldots, n\}$ under the operation $*$, is a cyclic group of order n, which coördinatizes $\mathcal{N}_3$. The converse is easy, and is left to the reader. $\square$

Proof of Theorem 5.1. Let (P_0, ℓ_0) be an arbitrary incident point-line pair in Π. We may label the remaining points $\{P_i : 1 \le i \le n^2 + n\}$ and lines $\{\ell_i : 1 \le i \le n^2 + n\}$ of Π in such a way (see [8,p.287]) that the resulting incidence matrix

$$A = \big(a_{ij} : 0 \le i, j \le n^2 + n\big), \qquad a_{ij} = \begin{cases} 1, & \text{if } P_j \in \ell_i; \\ 0, & \text{otherwise} \end{cases}$$

has the form

$$A = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 1\,1\cdots 1 & 0 & 0 & 0 & \cdots & 0 \\ \hline \begin{matrix} 1 \\ 1 \\ \vdots \\ 1 \end{matrix} & 0 & R_1 & R_2 & R_3 & \cdots & R_n \\ \hline 0 & R_1^{\mathrm{T}} & I & I & I & \cdots & I \\ \hline 0 & R_2^{\mathrm{T}} & I & \Sigma_{22} & \Sigma_{23} & \cdots & \Sigma_{2n} \\ \hline 0 & R_3^{\mathrm{T}} & I & \Sigma_{32} & \Sigma_{33} & \cdots & \Sigma_{3n} \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline 0 & R_n^{\mathrm{T}} & I & \Sigma_{n2} & \Sigma_{n3} & \cdots & \Sigma_{nn} \\ \hline \end{array}$$

where the $n \times n$ matrices R_s are as defined in (5.4), and the Σ_{ij}'s are $n \times n$ permutation matrices. Then

$$\begin{pmatrix} R_1 & R_2 & R_3 & \cdots & R_n \\ I & I & I & \cdots & I \\ I & \Sigma_{22} & \Sigma_{23} & \cdots & \Sigma_{2n} \\ I & \Sigma_{32} & \Sigma_{33} & \cdots & \Sigma_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & \Sigma_{n2} & \Sigma_{n3} & \cdots & \Sigma_{nn} \end{pmatrix}$$

is the incidence matrix of an $(n+1)$-net $\mathcal{N}$ of order n, i.e. an affine plane of order n (namely, the residual of Π with respect to ℓ_0). For any prime $p \,\big|\big|\, n$ it is well known that

$$\operatorname{rank}_p \mathcal{N} = \tfrac{1}{2}\big(n^2 + n\big)$$

(since $\operatorname{rank}_p \Pi = \frac{1}{2}\big(n^2 + n + 2\big)$; see eg. [13,p.57]). Let

$$\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \ldots \subset \mathcal{N}_{n+1} = \mathcal{N}$$

be any chain of subnets of subsets of $\mathcal{N}$, as in Sections 1,3. Then assuming Conjecture 1.1, we have

$$\begin{aligned} \tfrac{1}{2}\big(n^2+n\big) = \operatorname{rank}_p \mathcal{N} &= \operatorname{rank}_p \mathcal{N}_1 + \sum_{k=2}^{n+1} \big(\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1}\big) \\ &\geq n + (n-1) + (n-2) + \ldots + 2 + 1 + 0 \\ &= \tfrac{1}{2}\big(n^2+n\big). \end{aligned}$$

This means that equality must hold for each summand:

$$\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} = n - k + 1.$$

In particular we obtain $\operatorname{rank}_p \mathcal{N}_3 = 3n - 3$. If $n \equiv 2 \mod 4$ and $p = 2$ then the result follows by Corollary 4.3. Hence assume that n is squarefree, so the above holds for any prime $p \,\big|\, n$. By Corollary 4.5, this means that every 3-subnet $\mathcal{N}_3 \subseteq \mathcal{N}$ is cyclic. By Proposition 5.5, for $2 \leq i \leq n$ the set $\{I, \Sigma_{i2}, \Sigma_{i3}, \ldots, \Sigma_{in}\}$ consists of all n powers of some n-cycle matrix, and the same is true of $\{I, \Sigma_{2i}, \Sigma_{3i}, \ldots, \Sigma_{ni}\}$ by the dual argument. Moreover whenever $i \neq i'$, $2 \leq i, i' \leq n$, $\mathcal{N}$ has a 3-subnet with incidence matrix

$$\begin{pmatrix} R_1 & R_2 & R_3 & \cdots & R_n \\ I & \Sigma_{i2} & \Sigma_{i3} & \cdots & \Sigma_{in} \\ I & \Sigma_{i'2} & \Sigma_{i'3} & \cdots & \Sigma_{i'n} \end{pmatrix}.$$

Another incidence matrix for this 3-subnet is found by permuting columns:

$$\begin{pmatrix} R_1 & R_2 & R_3 & \cdots & R_n \\ I & I & I & \cdots & I \\ I & \Sigma_{i'2}\Sigma_{i2}^{\mathrm{T}} & \Sigma_{i'3}\Sigma_{i3}^{\mathrm{T}} & \cdots & \Sigma_{i'n}\Sigma_{in}^{\mathrm{T}} \end{pmatrix}.$$

Again by Proposition 5.5, the set $\{I, \Sigma_{i'2}\Sigma_{i2}^{\mathrm{T}}, \Sigma_{i'3}\Sigma_{i3}^{\mathrm{T}}, \ldots, \Sigma_{i'n}\Sigma_{in}^{\mathrm{T}}\}$ consists of all n powers of some n-cycle matrix.

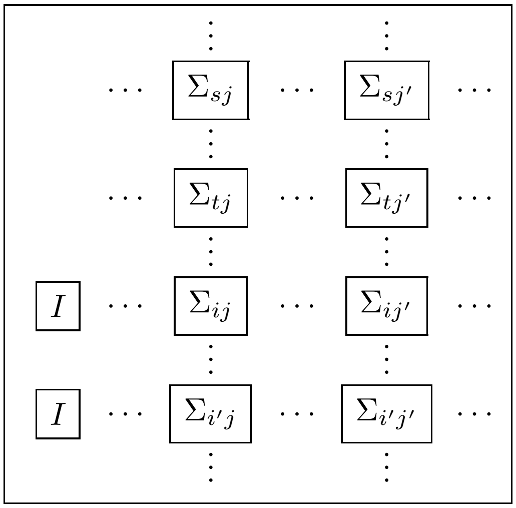
We claim that all Σ_{ij}'s are powers of *the same* n-cycle matrix. The alert reader will see that this already follows from the above remarks if n is prime; however we proceed to prove the claim in the general case (n is squarefree) using Proposition 5.2. If our claim is false, then we may choose $i \neq i'$ and $j \neq j'$ such that Σ_{ij} and $\Sigma_{i'j'}$ are both n-cycle matrices, but

$$\Sigma_{i'j'} \notin \langle \Sigma_{ij} \rangle = \{\Sigma_{ij}^r : 0 \le r < n\} = \{I\} \cup \{\Sigma_{rj} : 2 \le r \le n\}.$$

However $\Sigma_{i'j} \in \langle \Sigma_{ij} \rangle \cap \langle \Sigma_{i'j'} \rangle$. This implies that $\Sigma_{i'j}$ is a *non-generator* of $\langle \Sigma_{ij} \rangle$. By Proposition 5.2(iii), $\Sigma_{i'j}$ is a product of two generators of $\langle \Sigma_{ij} \rangle$, say

$$\Sigma_{i'j} = \Sigma_{sj}\Sigma_{tj}, \qquad \langle \Sigma_{sj} \rangle = \langle \Sigma_{tj} \rangle = \langle \Sigma_{ij} \rangle.$$

Figure 2. A portion of the incidence matrix of $\mathcal{N}$



(Refer to Figure 2.) Since $\Sigma_{i'j}\Sigma_{tj}^{\mathrm{T}} = \Sigma_{sj}$ is an n-cycle matrix, by the above remarks

$$\Sigma_{i'j'}\Sigma_{tj'}^{\mathrm{T}} \in \langle \Sigma_{i'j}\Sigma_{tj}^{\mathrm{T}} \rangle = \langle \Sigma_{sj} \rangle = \langle \Sigma_{ij} \rangle.$$

However we also have $\Sigma_{tj'} \in \langle \Sigma_{tj} \rangle = \langle \Sigma_{ij} \rangle$. Together this implies that $\Sigma_{i'j'} \in \langle \Sigma_{ij} \rangle$, a contradiction.

We have verified our claim: there exists an n-cycle $\sigma \in \mathrm{S}_n$ such that every Σ_{ij} is a power of the n-cycle matrix $Q = \big(\delta_{i,\sigma(j)} \;:\; 1 \le i, j \le n\big)$, and in particular Σ_{ij} commutes with Q. This implies that the mapping

$$\begin{array}{ll} P_i \mapsto P_i, \quad 0 \le i \le n; & \ell_i \mapsto \ell_i, \quad 0 \le i \le n; \\ P_{sn+i} \mapsto P_{sn+\sigma(i)}, \quad 1 \le s, i \le n; & \ell_{sn+i} \mapsto \ell_{sn+\sigma(i)}, \quad 1 \le s, i \le n \end{array}$$

is an automorphism of Π, in fact an elation of order n with centre P_0 and axis ℓ_0 (see [7]). However (P_0, ℓ_0) was an arbitrarily chosen incident point-line pair in Π. Thus Π is (P, ℓ)-transitive for every flag (P, ℓ) of Π. It is well known (see eg. [7]) that any finite plane satisfying this condition is desarguesian. Moreover this implies that n is a prime power, and hence prime. □

6. Desarguesian Nets of Prime Order

6.1 Theorem. *Conjecture 1.1 holds with equality in the case of desarguesian nets (necessarily of prime order).*

Proof. Let p be a prime. A desarguesian net of order p is by definition a subnet of a desarguesian $(p+1)$-net $\mathcal{N}_{p+1}$ (i.e. affine plane) of order p. Consider a maximal chain of subnets

$$\mathcal{N}_0 \subset \mathcal{N}_1 \subset \mathcal{N}_2 \subset \ldots \subset \mathcal{N}_p \subset \mathcal{N}_{p+1}$$

where $\mathcal{N}_i$ is an i-subnet. Then

$$\tfrac{1}{2}p(p+1) = \operatorname{rank}_p \mathcal{N}_{p+1} = \sum_{k=1}^{p+1} \big(\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1}\big).$$

It suffices to show that $\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \le p - k + 1$, for then

$$\tfrac{1}{2}p(p+1) = \sum_{k=1}^{p+1} \big(\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1}\big) \le \sum_{k=1}^{p+1} (p - k + 1) = \tfrac{1}{2}p(p+1),$$

which forces $\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} = p-k+1$ for all k.

We may represent $\mathcal{N}_{p+1}$ on the point set $\mathcal{P} = \mathbb{F}_p^2 = \mathbb{F}_p \times \mathbb{F}_p$, with lines

$$\ell_{rs} = \{(x, rx+s) : x \in \mathbb{F}_p\}, \quad \ell_{\infty s} = \{(s,y) : y \in \mathbb{F}_p\}, \qquad r,s \in \mathbb{F}_p,$$

or by the corresponding characteristic functions $\chi_{rs}, \chi_{\infty s} \in \mathbb{F}_p^{\mathcal{P}}$. (We deviate slightly from the convention of Section 2 by using subscripts from $\mathbb{F}_p = \{0,1,2,\ldots,p{-}1\}$ rather than from $\{1,2,3,\ldots,p\}$.) Let $\mathcal{N}_{k-1} \subset \mathcal{N}_k$ be $(k{-}1)$- and k-subnets of $\mathcal{N}_{p+1}$. Since $\operatorname{Aut}\mathcal{N}_{p+1}$ acts transitively on the $p+1$ parallel classes, we may suppose that the lines of $\mathcal{N}_{k-1}$ are

$$\{\ell_{rs} : r \in E,\ s \in \mathbb{F}_p\}, \quad E \subseteq \mathbb{F}_p,\ |E| = k-1$$

and that $\mathcal{N}_k$ has the additional parallel class $\{\ell_{\infty s} : s \in \mathbb{F}_p\}$. Define

$$\mathcal{V}_k = \left\{ (a_0, a_1, a_2, \ldots, a_{p-1}) \in \mathbb{F}_p^p \ :\ \sum_{s=0}^{p-1} a_s \chi_{\infty s} \in \mathcal{C}_p(\mathcal{N}_{k-1}) = \sum_{r\in E}\sum_{s=0}^{p-1} \mathbb{F}_p \chi_{rs} \right\}.$$

Then $\dim_p \mathcal{V}_k = p - \operatorname{rank}_p \mathcal{N}_k + \operatorname{rank}_p \mathcal{N}_{k-1}$, and so it suffices to show that $\dim_p \mathcal{V}_k \geq k-1$. We may suppose that $k \geq 2$.

We first show that $\big(0^{k-2}, 1^{k-2}, 2^{k-2}, \ldots, (p{-}1)^{k-2}\big) \in \mathcal{V}_k$. (For $k=2$ we must define $0^0 = 1$.) Consider the unique solution $\big(b_r : r \in E\big)$ to the linear system

$$\sum_{r\in E} r^e b_r = \begin{cases} 0, & 0 \leq e \leq k-3; \\ 1, & e = k-2. \end{cases}$$

(The coefficient matrix of this system is a $(k{-}1) \times (k{-}1)$ Vandermonde matrix, whence the existence and uniqueness of the solution $(b_r : r \in E)$.) Then

$$\text{(6.2)} \qquad \sum_{s=0}^{p-1} s^{k-2} \chi_{\infty s} = \sum_{r\in E}\sum_{s=0}^{p-1} (-s)^{k-2} b_r \chi_{rs}.$$

To verify the latter, the right side of (6.2), evaluated at an arbitrary point $(x,y) \in \mathcal{P}$, yields

$$\sum_{r\in E} (rx-y)^{k-2} b_r = \sum_{e=0}^{k-2} \Big(\sum_{r\in E} r^e b_r \Big) \binom{k-2}{e} x^e (-y)^{k-2-e} = x^{k-2},$$

which agrees with the value of the left side of (6.2) at (x,y). Thus $\big(0^{k-2}, 1^{k-2}, \ldots, (p{-}1)^{k-2}\big)$ $\in \mathcal{V}_k$ as claimed.

For $1 \le t \le k-1$, choose a subset $E_t \subseteq E$ of size t corresponding to a t-subnet $\mathcal{N}_t \subseteq \mathcal{N}_{k-1}$. Replacing E by E_t in the above argument gives $\bigl(0^{t-1}, 1^{t-1}, 2^{t-1}, \ldots, (p-1)^{t-1}\bigr) \in \mathcal{V}_k$. Thus

$$\mathcal{V}_k \supseteq \bigl\{\bigl(f(0), f(1), f(2), \ldots, f(p-1)\bigr) \,:\, f(X) \in \mathbb{F}_p[X],\ \deg f \le k-2\bigr\},$$

and so $\dim_p \mathcal{V}_k \ge k-1$ as required. □

Observe by the argument of the above proof that we must have

$$\mathcal{V}_k = \bigl\{\bigl(f(0), f(1), f(2), \ldots, f(p-1)\bigr) \,:\, f(X) \in \mathbb{F}_p[X],\ \deg f \le k-2\bigr\},$$

and since any nonzero $f(X) \in \mathbb{F}_p[X]$ has at most $\deg f$ roots, $\mathcal{V}_k$ has minimum weight $p-k+2$ for $k \ge 2$. Thus $\mathcal{V}_k$ is an MDS code (maximum distance separable; see [14]). This means that *any* $p-k+1$ of $\{\chi_{\infty s} : s \in \mathbb{F}_p\}$ suffice to extend a basis of $\mathcal{C}_p(\mathcal{N}_{k-1})$ to a basis of $\mathcal{C}_p(\mathcal{N}_k)$, which justifies the recipe given in Section 1 for producing an explicit basis of $\mathcal{C}_p(\mathcal{N}_{p+1})$. The dual code $\mathcal{V}_k^{\perp}$ is also MDS, of length p, dimension $p-k+1$, and minimum weight k; in fact $\mathcal{V}_k^{\perp}$ is an extended Reed-Solomon code.

REFERENCES

[1] R. Baer, "Nets and groups", *Trans. Amer. Math. Soc.* **46** pp. 110–141, 1939.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory,* Bibliographisches Institut: Zürich, 1985.

[3] R. H. Bruck, "Finite nets I. Numerical invariants", *Can. J. Math.* **3** pp. 94–107, 1951.

[4] ——————, *A Survey of Binary Systems,* Springer-Verlag: Berlin, 1958.

[5] ——————, "Finite nets II. Uniqueness and embedding", *Pacific J. Math.* **13** pp. 421–457, 1963.

[6] R. H. Bruck and H. J. Ryser, "The non-existence of certain finite projective planes", *Can. J. Math.* **1** pp. 88–93, 1949.

[7] P. Dembowski, *Finite Geometries,* Springer-Verlag, 1968.

[8] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications,* Academic Press: New York, 1974.

[9] D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn,, "Orthomorphisms of groups and orthogonal Latin squares. I", *Can. J. Math.* **13** No.13 pp. 356–372, 1961.

[10] D. Jungnickel, “On difference matrices and regular Latin squares”, *Abh. Math. Sem. Hamburg* **50** pp. 219–231, 1980.

[11] ——————, “Latin Squares, their geometries and their groups. A survey”, in *Coding Theory and Design Theory Part II: Design Theory* (ed. D. Ray-Chaudhuri), Springer-Verlag, 1990, pp. 166–225.

[12] D. Jungnickel and G. Grams, “Maximal difference matrices of order ≤ 10”, *Disc. Math.* **58** pp. 199–203, 1986.

[13] E. S. Lander, *Symmetric Designs: an Algebraic Approach,* Lond. Math. Soc. Lecture Notes #74, Cambridge Univ. Press, 1983.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland: Amsterdam, 1977.

[15] E. T. Parker, “Orthogonal Latin squares”, *Proc. Nat. Acad. Sci. U.S.A.* **45** pp. 859–862, 1959.

[16] G. Pickert, *Projektive Ebenen,* 2nd edition, Springer-Verlag: Berlin, 1975.

[17] R. Roth and M. Peters, “Four pairwise orthogonal Latin squares of order 24”, *J. Comb. Theory Ser. A* **44** pp. 152–155, 1987.

[18] P. J. Schellenberg, G. H. J. van Rees and S. A. Vanstone, “Four pairwise orthogonal Latin squares of order 15”, *Ars Comb.* **6** pp. 141–150, 1978.

[19] D. T. Todorov, “Three mutually orthogonal Latin squares of order 14”, *Ars. Comb.* **20** pp. 45–47, 1985.

[20] ——————, privately communicated to D. Jungnickel and forwarded to the author, April, 1990.

[21] W. D. Wallis and L. Zhu, Four pairwise orthogonal diagonal Latin squares of side 12”, *Utilitas Mathematica* **12C** pp. 205–207, 1982.

[22] S. P. Wang, “On self-orthogonal Latin squares and partial transversals of Latin squares”, Ph. D. thesis, Ohio State University, 1978.

[23] L. Zhu, “Orthogonal diagonal Latin squares of order 14”, *J. Austral. Math. Soc. Ser. A* **36** pp. 1–3, 1984.