# On the p-ranks of net graphs

Peeters, M.J.P.

*Published in:*
Designs Codes and Cryptography

*Publication date:*
1995

Designs, Codes and Cryptography, 5, 139–153 (1995)


# On the $p$-Ranks of Net Graphs

RENÉ PEETERS* m.j.p.peeters@kub.nl
*Department of Economics, Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands*

**Communicated by:** D. Jungnickel

*Received August 13, 1992; Revised October 4, 1993*

**Abstract.** Let $\Pi$ be a $k$-net of order $n$ with line-point incidence matrix $N$ and let $A$ be the adjacency matrix of its collinearity graph. In this paper we study the $p$-ranks (that is, the rank over $\mathbb{F}_p$) of the matrix $A + kI$ with $p$ a prime dividing $n$. Since $A + kI = N^T N$ these $p$-ranks are closely related to the $p$-ranks of $N$. Using results of Moorhouse on the $p$-ranks of $N$, we can determine $r_p(A + kI)$ if $\Pi$ is a 3-net (latin square) or a desarguesian net of prime order. On the other hand we show how results for the $p$-ranks of $A + kI$ can be used to get results for the $p$-ranks of $N$, especially in connection with the Moorhouse conjecture. Finally we generalize the result of Moorhouse on the $p$-rank of $N$ for desarguesian nets of order $p$ a bit to special subnets of the desarguesian affine plane of order $p^e$.

## 1. Introduction

A graph is called *strongly regular* (See for instance [4]) if there exist integers $\rho$, $\lambda$ and $\mu$ such that

1. the graph is regular with valency $\rho$,
2. the number of vertices adjacent to two adjacent vertices is $\lambda$,
3. the number of vertices adjacent to two non-adjacent vertices is $\mu$.

If $\Gamma$ is a strongly regular graph with parameters $(v, \rho, \lambda, \mu)$, then its complement $\overline{\Gamma}$ is also strongly regular with parameters $(\overline{v}, \overline{\rho}, \overline{\lambda}, \overline{\mu}) = (v, v - \rho - 1, v - 2\rho + \mu - 2, v - 2\rho + \lambda)$. A strongly regular graph has 3 eigenvalues $\rho, r$ and $s$ with multiplicities 1, $f$ and $g$ respectively, satisfying

$$\lambda - \mu = r + s, \ \mu - \rho = rs$$

$$f + g = v - 1, \ \rho + fr + gs = 0$$

Let $A$ be the adjacency matrix of a strongly regular graph $\Gamma$ and let $p$ be a prime number. The $p$-ranks of the matrices $A + cI$ for integral $c$ (notation: $r_p(A + cI)$) were studied in [1]. It turns out that if $\Gamma$ has integral eigenvalues $r_p(A + cI)$ is completely determined by the parameters of $\Gamma$, except maybe for $r_p(A - sI)$ with $p$ dividing $r - s$ in which case $\min\{f + 1, g + 1\}$ is an upper bound. We will refer to these $p$-ranks as the relevant $p$-ranks

* The author is financially supported by the Cooperation Centre Tilburg and Eindhoven Universities.

of $\Gamma$. In this paper we will study these $p$-ranks for a special class of strongly regular graphs: net graphs, i.e., the collinearity graphs of nets.

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

1. every line has exactly $n$ points,
2. parallelism (the property of being either equal or disjoint) is an equivalence relation on the lines,
3. there are $k$ parallel classes, each consisting of $n$ lines,
4. any two non-parallel lines meet exactly once.

Thus an $(n+1)$-net of order $n$ is an affine plane of order $n$ and a $k$-net of order $n$ is equivalent to $k-2$ *Mutually Orthogonal Latin Squares* (MOLS), that is a set of $k-2$ latin squares every pair being orthogonal (cf. [5]).

Given a $k$-net of order $n$, its *net graph* is defined as the graph with the points of the net as its vertices, two vertices being adjacent if there is a line through the two corresponding points. Net graphs are strongly regular with parameters

$$\begin{array}{llll} v = n^2 & \lambda = (n-2)+(k-1)(k-2) & r = n-k & f = k(n-1) \\ \rho = k(n-1) & \mu = k(k-1) & s = -k & g = (n-k+1)(n-1) \end{array}$$

In case of a 3-net (so we have only one latin square), these are called *latin square graphs*. Strongly regular graphs with the same parameters as net graphs (latin square graphs) are called *pseudo net graphs* (*pseudo latin square graphs*). The complement of a net graph has parameters

$$\begin{array}{llll} \overline{v} = n^2 & \overline{\lambda} = (n-2)+(n-k)(n-k-1) & \overline{r} = k-1 & \overline{f} = g \\ \overline{\rho} = (n-k+1)(n-1) & \overline{\mu} = (n-k+1)(n-k) & \overline{s} = -(n-k+1) & \overline{g} = f \end{array}$$

which are the same as those of the net graph of an $(n-k+1)$-net, so it is a pseudo net graph. If for a $k$-net of order $n$ the complement of its net graph is again a net graph, so it is the collinearity graph of an $(n-k+1)$-net of order $n$, then these two nets together form an affine plane of order $n$. The graphs with the same parameters as a net graph of a 2-net are unique (These are the *lattice graphs* $L_2(n)$), except for the case $n=4$, where the Shrikhande graph is the only exception (see for instance [4]). This means that an $(n-1)$-net can always be completed to an affine plane unless we have the 3-net of order 4 corresponding with the multiplication table of the cyclic group of order 4, whose latin square graph is the complement of the Shrikhande graph. See [3] for more details about the completion of nets.

We denote the row space of a matrix $A$ over $\mathbb{F}_p$ by $\langle A \rangle_p$. Vectors will be row vectors and $\mathbf{1}$ and $\mathbf{0}$ denote the all-one vector and the zero vector respectively. We denote the all-one matrix by $J$. For a matrix $A$ we denote by $\ker_p(A)$ the vector space over $\mathbb{F}_p$ consisting of all vectors $\underline{x}$ satisfying $\underline{x}A = \mathbf{0}$.

From the (integral) eigenvalues of a (pseudo) net graph we derive that the only $p$-ranks of $A + cI$, where $A$ is the adjacency matrix of the graph and $c$ is integral, that are not

determined by the parameters of the graph are the $p$-ranks of $A+kI$ with $p$ dividing $n$. Let $N$ be the line-point incidence matrix of a $k$-net, then we have for the adjacency matrix of its collinearity graph $A+kI = N^T N$. So in case of a net graph we have $r_p(A+kI) \leq r_p(N)$ for all prime numbers $p$. More precisely we have that $r_p(A+kI) = kn - \dim \ker_p(N) - \dim(\ker_p(N) \cap \langle N^T \rangle_p)$, so using some elementary linear algebra we get:

$$r_p(A+kI) = kn - \dim \ker_p(N) - \dim(\ker_p(N) \cap \ker_p(N)^{\perp}) \tag{1}$$

If $G$ is the Gram matrix of a basis of $\ker_p(N)$, that is the matrix with entries the inner products of the basis vectors, then an equivalent formula is:

$$r_p(A+kI) = kn - 2\dim \ker_p(N) + r_p(G) \tag{2}$$

These relations turn out to be very useful because in some cases we can find an explicit basis for $\ker_p(N)$ and can compute the $p$-rank of its Gram matrix or can prove that $\ker_p(N) \subseteq \ker_p(N)^{\perp}$.

It is easy to see that the relevant $p$-ranks for (pseudo) net graphs with the same parameters as the collinearity graph of a 0-net, 1-net or 2-net of order $n$ are 0, $n$ and $2n-2$ respectively. So the first interesting case is that of a (pseudo) latin square graph. In the following section we determine the relevant $p$-ranks for latin square graphs, that is $r_p(A+3I)$ for $p$ dividing $n$, where $A$ is the adjacency matrix of the collinearity graph of a 3-net of order $n$. In the last section we study the relevant $p$-ranks of net graphs in general. By equations (1) and (2) these ranks are closely related to the ranks of the incidence matrices of the nets which were studied by Moorhouse [14] and Dougherty [6]. Moorhouse completely determined the $p$-ranks of the incidence matrices of latin squares (3-nets) of order $n$ for $p$ dividing $n$. Using his results we can determine the relevant $p$-ranks of latin square graphs. In the last section we show that the relevant $p$-ranks of net graphs can be used to get results for the $p$-rank of the incidence matrix of the net.

## 2. Latin Square Graphs

Let $L$ be a latin square of order $n$. Its latin square graph has as vertex set the $n^2$ cells of the latin square, two cells being adjacent if they appear in the same row or column or have the same symbol. Because permuting rows and columns of a latin square does not influence its latin square graph, we may assume that the latin square is in standard form, which means that the elements of its first row and column are in the same order. In this case the latin square can be seen as the multiplication table of a loop. Moorhouse [14] determined all $p$-ranks of the incidence matrix $N$ for 3-nets using loop theory. We will use his results to determine the relevant $p$-ranks of latin square graphs. First we will discuss some loop theory. For more details we refer to [2].

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

1. for all $a, c \in G$ the equation $a * x = c$ has a unique solution $x \in G$,
2. for all $b, c \in G$ the equation $x * b = c$ has a unique solution $x \in G$,

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

A loop is a group if and only if it obeys the associative law $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$. Subloops and homomorphisms of a loop upon an other loop are defined in the obvious way. A subloop $H$ of $G$ is called a *normal subloop* of $G$ if for all $x, y \in G$

$$xH = Hx,$$
$$(Hx)y = H(xy),$$
$$y(xH) = (yx)H.$$

So also $x(Hy) = (xH)y$. If we define $(Hx)(Hy) := H(xy)$, it follows in a straightforward manner that $G/H$ is a loop: the *quotient loop of $G$ modulo $H$*.

LEMMA 1 *(cf. [2]) If $\theta$ is a homomorphism from a loop $G$ upon a loop $H$, then* $\ker\theta$ *is a normal subloop of $G$ and*

$$G/\ker\theta \cong H.$$

A loop homomorphism $\theta : G \to \mathbb{F}_p$, i.e. a map $\theta : G \to \mathbb{F}_p$, such that $\theta(g * h) = \theta(g) + \theta(h)$ for all $g, h \in G$ is called a *p-character* of $G$. These $p$-characters form a vector space over $\mathbb{F}_p$ which will be denoted with $\mathrm{Hom}(G, \mathbb{F}_p)$. Clearly $G/\ker\theta \cong C_p$ if $\theta \not\equiv 0$, which means that the multiplication table of $G$ as a latin square can be obtained from the multplication table of the cyclic group of order $p$ by replacing its entries by latin squares of order $|G|/p$. Such a latin square is called a non-uniform product of the multiplication table of the cyclic group of order $p$ and latin squares of order $|G|/p$ (cf. [5]) (The reviewer suggested to mention at this point the extensive work done by K. W. Johnson and J. D. H. Smith on characters of finite quasigroups ([7], [8], [9], [10], [11], [12]). The $p$-characters used here are just additive versions of the ordinary characters of loops. Actually, they lie only in the largest elementary abelian $p$-quotient of the ordinary linear characters (written additively).)

THEOREM 2 *(cf. Moorhouse [14]) Let $G$ be a loop of order $n$ and let $p$ be a prime such that $p^e$ divides $n$ but $p^{e+1}$ does not. Then*

$$\dim \mathrm{Hom}(G, \mathbb{F}_p) = s \leq e$$

*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.*

Let $L$ be a latin square that is in standard form and let $G$ be the loop with the latin square as multiplication table. As in Moorhouse [14], we use $G \times G = \{(x, y) | x, y \in G\}$ as point set of the corresponding 3-net. The $3n$ lines of the net are denoted with $l_{ig}$, $i = 1, 2, 3$; $g \in G$.

The characteristic functions $\chi_{1g}$, $\chi_{2g}$, $\chi_{3g}$ of these lines are the rows of the incidence matrix $N$. So

$$\left.\begin{aligned}\chi_{1g}(x, y) &= \delta_{g,x}\\ \chi_{2g}(x, y) &= \delta_{g,y}\\ \chi_{3g}(x, y) &= \delta_{g,x*y}\end{aligned}\right\} \text{for all } x, y, g \in G.$$

THEOREM 3 *(cf. Moorhouse [14]) Let $p$ be any prime number and $N$ and $G$ as above. If $\phi_1, \phi_2, \ldots, \phi_s$ form a basis of* $\mathrm{Hom}(G, \mathbb{F}_p)$, *then*

$$\begin{aligned}\ker_p(N) = \langle &(1, \ldots, 1|0, \ldots, 0| -1, \ldots, -1), (0, \ldots, 0|1, \ldots, 1| -1, \ldots, -1),\\ &(\phi_1(g)|\phi_1(g)| - \phi_1(g)), \ldots, (\phi_s(g)|\phi_s(g)| - \phi_s(g))\rangle,\end{aligned}$$

*where the 3 parts of the vectors correspond with the 3 parallel classes and thus*

$$r_p(N) = 3n - 2 - \dim \mathrm{Hom}(G, \mathbb{F}_p)$$

This explicit description of the kernel of $N$ enables us to determine all $p$-ranks of the matrix $A + 3I = N^T N$ (where $A$ is the adjacency matrix of a latin square graph), but we will restrict ourselves to the case where $p$ divides $n$.

THEOREM 4 *Let $G$ be a loop and $A$ the adjacency matrix of the latin square graph corresponding to the multiplication table of $G$, then for $p$ dividing $n$:*

$$\begin{aligned}r_p(A + 3I) &= 3n - 5\\ &\quad \textit{if } p = 2, \dim \mathrm{Hom}(G, \mathbb{F}_p) = 1, \textit{ and 4 does not divide } n,\\ &= 3n - 6\\ &\quad \textit{if } p = 2, \dim \mathrm{Hom}(G, \mathbb{F}_p) = 2, \textit{ and 8 does not divide } n,\\ &= 3n - 4 - 2\dim \mathrm{Hom}(G, \mathbb{F}_p)\\ &\quad \textit{otherwise.}\end{aligned}$$

*Proof.* Let $N$ be the line-point incidence matrix of the corresponding 3-net, then by (1) we still have to determine $\dim(\ker_p(N) \cap \ker_p(N)^{\perp})$. If $\theta(\neq 0) \in \mathrm{Hom}(G, \mathbb{F}_p)$, then $G/\ker\theta \cong C_p$, so

$$2\sum_{g\in G}\theta(g) = 2\frac{n}{p}\sum_{i=0}^{p-1} i = n(p-1) \equiv 0 \pmod{p}$$

and

$$3\sum_{g\in G}\theta(g)^2 = 3\frac{n}{p}\sum_{i=0}^{p-1} i^2 = \frac{1}{2}n(p-1)(2p-1) \equiv 0 \pmod{p},$$

unless $p = 2$ and 4 does not divide $n$.

If $\phi, \theta \in \mathrm{Hom}(G, \mathbb{F}_p)$ are linearly independent, then $G/(\ker\theta \cap \ker\phi) \cong C_p \times C_p$, so

$$3\sum_{g\in G}\phi(g)\theta(g) = 3\frac{n}{p^2}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1} ij = \frac{3}{4}n(p-1)^2 \equiv 0 \pmod{p},$$

unless $p = 2$ and 8 does not divide $n$.

Theorem 3 and the three relations above imply that $\ker_p(N) \subseteq \ker_p(N)^\perp$ except for the two special cases mentioned in the theorem for which $\dim(\ker_p(N) \cap \ker_p(N)^\perp) = 2$. □

So in general we have for the adjacency matrix $A$ of any latin square graph:

$$r_p(A + 3I) \leq 3n - 4,$$

which, for $n > 4$, is a better bound than the one we get from the eigenvalues:

$$r_p(A + 3I) \leq \min\{3n - 2, n^2 - 3n + 3\}.$$

We can generalize this result to net graphs using the following lemma (see also [6]):

LEMMA 5 *Let $N_k$ be the incidence matrix of a $k$-net $\Pi_k$ of order $n$, let $p$ be a prime dividing $n$ and let $(x_{11}, \ldots, x_{1n}|x_{21}, \ldots, x_{2n}|\ldots\ldots|x_{k1}, \ldots, x_{kn}) \in \ker_p(N_k)$. Then for some $s \in \mathbb{F}_p$:*

$$\sum_{j=1}^{n} x_{ij} = s\ , i = 1, 2, \ldots, k$$

*with $s = 0$ if $k \not\equiv 1 \pmod{p}$ or if $\Pi_k$ can be extended by at least one more line (that means there exists a set of $n$ points that meets every line in precisely one point).*

*Proof.* Let $\underline{x} = (x_{11}, \ldots, x_{1n}|x_{21}, \ldots, x_{2n}|\ldots\ldots|x_{k1}, \ldots, x_{kn}) \in \ker_p(N_k)$ and define $s_i := \sum_{j=1}^{n} x_{ij}$ for $i = 1, 2, \ldots, k$, then we will prove first that $s_1 = s_2 = \cdots = s_k$ (in $\mathbb{F}_p$). Since $\underline{x}N_k = \mathbf{0}$, also $\underline{x}N_kN_k^T = \mathbf{0}$; but $N_kN_k^T = (J_k - I_k) \otimes J_n \pmod{p}$, so $(s_1, s_2, \ldots, s_k)(J - I) = \mathbf{0}$, so $s_i = \sum_{j=1}^{k} s_j$ for $i = 1, 2, \ldots, k$ and thus $s_i = s$ $(i = 1, 2, \ldots, k)$ for some $s \in \mathbb{F}_p$ with $(k-1)s \equiv 0 \pmod{p}$. Hence $s = 0$ if $k \not\equiv 1 \pmod{p}$. Now suppose $\Pi_k$ can be extended by a single additional line with characteristic vector $\underline{\chi}$, then $N_k\underline{\chi}^T = \mathbf{1}^T$, so $s = \sum_{i=1}^{k}\sum_{j=1}^{n} x_{ij} = \underline{x}\mathbf{1}^T = \underline{x}N_k\underline{\chi}^T = \mathbf{0}\underline{\chi}^T = 0$. □

COROLLARY 6 *Let $A$ be the adjacency matrix of a net graph corresponding to a $k$-net of order $n$ with incidence matrix $N_k$ and let $p$ be a prime number dividing $n$, then:*

$$r_p(A + kI) \leq r_p(N_k) - (k-1) \leq kn - 2(k-1)$$

*Proof.* The result follows by relation (1) and the fact that the $k-1$ vectors $(\mathbf{1}|-\mathbf{1}|\mathbf{0}|\ldots|\mathbf{0})$, $(\mathbf{1}|\mathbf{0}|-\mathbf{1}|\mathbf{0}|\ldots|\mathbf{0})\ldots\ldots(\mathbf{1}|\mathbf{0}|\ldots|\mathbf{0}|-\mathbf{1})$ (The vectors are divided in $k$ parts of $n$ coefficients

corresponding to the $k$ parallel classes of $n$ lines.) are in $\ker_p(N_k) \cap \ker_p(N_k)^\perp$. Trivially they are in $\ker_p(N_k)$, since for each parallel class the sum of the characteristic functions of their lines is the all-one vector and by Lemma 5 they are in $\ker_p(N_k)^\perp$. □

COROLLARY 7 *(cf. Dougherty [6]) Let $N_k$ be the incidence matrix of a $k$-net $\Pi_k$ of order $n$, let $N_{k-1}$ be the incidence matrix of some $(k-1)$-subnet thereof and let $p$ be a prime dividing $n$, then*

$$r_p(N_k) \geq r_p(N_{k-1}) + 1$$

*unless $k \equiv 1 \pmod{p}$ and $\Pi_k$ cannot be extended by an additional line.*

In fact if $N_{n+1}$, $N_n$ and $N_{n-1}$ are the incidence matrices of an affine plane of order $n$ and some $n$- and $(n-1)$-subnet thereof then for $p$ dividing $n$

$$r_p(N_{n+1}) = r_p(N_n) = r_p(N_{n-1}) + 1.$$

These equalities follow from the observation that for the affine plane the sum (mod $p$) of the characteristic vectors of all $n+1$ lines incident with some fixed point is the all-one vector.

## 3. Net Graphs

In this section we give some results for the relevant $p$-ranks of (pseudo) net graphs. In general it turns out to be hard to find an expression for these ranks, but for the special case of the collinearity graph of a desarguesian net of prime order the relevant $p$-rank can be determined.

### *3.1. General Results*

We start with some relations between the relevant $p$-ranks of a (pseudo) net graph and its complement.

LEMMA 8 *Let $\Gamma$ be a (pseudo) net graph with the same parameters as the collinearity graph of a $k$-net of order $n$ and let $A$ be its adjacency matrix. Let $\overline{\Gamma}$ be its complement with adjacency matrix $\overline{A} = J - A - I$ and let $p$ be a prime dividing $n$, then:*

*(i)* $$|r_p(A + kI) - r_p(\overline{A} + (n+1-k)I)| \leq 1$$

*(ii) If $\Gamma$ is the collinearity graph of some $k$-net of order $n$ with $k \neq 0$, then we have*

$$r_p(A + kI) = r_p(\overline{A} + (n+1-k)I)$$

*unless $p$ divides $k-1$ and $\Gamma$ has no coclique (independent set) of size $n$, so the net cannot be extended by a single additional line.*

*Proof.* The first result follows directly from the identity $\overline{A}+(n+1-k)I \equiv J-(A+kI)$ (mod $p$). Let $\Gamma$ be the collinearity graph of a $k$-net of order $n$ with $k \neq 0$. Adding up the $n$ rows of $A+kI$ corresponding to the points of some line of the net yields $(k-1)\mathbf{1}$, so $\mathbf{1} \in \langle A+kI\rangle_p$ if $p$ does not divide $k-1$. If we add up the corresponding rows of $J-(A+kI)$ we get $(n+1-k)\mathbf{1}$, so if $p$ does not divide $k-1$ also $\mathbf{1} \in \langle \overline{A}+(n+1-k)I\rangle_p$.
If furthermore $\Gamma$ has a coclique of size $n$, this coclique corresponds to $n$ points of the net, no two collinear. This means that for each parallel class the $n$ lines of this class contain one point of the coclique each. Adding up the $n$ rows of $A+kI$ and its complement corresponding to the points of a coclique of size $n$ yields $k\mathbf{1}$ and $(n-k)\mathbf{1}$ respectively. Hence $k\mathbf{1}-(k-1)\mathbf{1}=\mathbf{1} \in \langle A+kI\rangle_p$ and similar $\mathbf{1} \in \langle \overline{A}+(n+1-k)I\rangle_p$. □

This lemma implies for instance that the relevant $p$-ranks of the collinearity graphs of a $k$-net of order $n$ and a $(n+1-k)$-net of order $n$ that together form an affine plane of order $n$ are the same unless $k=0$ or $k=n+1$.

LEMMA 9 *Let $\Pi_{n+1}$ be an affine plane of order $n$ with incidence matrix $N_{n+1}$ and let $p$ be a prime dividing $n$ precisely once. Let $\Pi_k$ be a $k$-subnet of $\Pi_{n+1}$ with incidence matrix $N_k$, then*

$$\ker_p(N_k) \subseteq \ker_p(N_k)^{\perp} \qquad \text{if } 1 \leq k \leq n$$

$$\dim(\ker_p(N_{n+1}) \cap \ker_p(N_{n+1})^{\perp}) = \dim \ker_p(N_{n+1}) - 1$$

*Proof.* For an incidence matrix $N_k$ of a $k$-net of order $n$ we denote the Gram matrix of a basis of $\ker_p(N_k)$ by $G_k$. Let $\Pi_l$ and $\Pi_k$ be an $l$-net and a $k$-net of the same order respectively with $\Pi_l$ a subnet of $\Pi_k$ and let $N_l$ and $N_k$ be their incidence matrices. Now $\ker_p(N_l)$ can be identified with the subspace of $\ker_p(N_k)$ consisting of all vectors that have zero entries for all positions corresponding with the lines of $\Pi_k$ that are not contained in $\Pi_l$. So, by taking an appropriate basis for $\ker_p(N_k)$ –such that a subset of the basis vectors can be identified with a basis of $\ker_p(N_l)$– the Gram matrix of this basis of $\ker_p(N_l)$ appears as a submatrix of the Gram matrix of the basis of $\ker_p(N_k)$ and thus it cannot have a bigger rank. So $r_p(G_l) \leq r_p(G_k)$.
It is well known (see for instance Lander [13], p. 57) that $r_p(N_{n+1}) = \frac{1}{2}n(n+1)$, so $\dim \ker_p(N_{n+1}) = \frac{1}{2}n(n+1)$. Since $N_{n+1}^T N_{n+1} = J$ we get by relation (2) that $r_p(G_{n+1}) = 1$ which is equivalent to the second result. Now by the observation above $r_p(G_n)$ is equal to either 0 or 1. By Lemma 8(ii) we have $r_p(N_n^T N_n) = r_p(A_1 + I) = r_p(J_n \otimes I_n) = n$, where $A_1$ is the adjacency matrix of the collinearity graph of a 1-net, so by (2): $n^2 - 2\dim \ker_p(N_n) + r_p(G_n) = n$. So $r_p(G_n)$ is even and thus it must be zero which means that $\ker_p(N_n) \subseteq \ker_p(N_n)^{\perp}$. Since $r_p(G_k) \leq r_p(G_n) = 0$ and hence $\ker_p(N_k) \subseteq \ker_p(N_k)^{\perp}$ for the incidence matrix $N_k$ of any $k$-subnet of the affine plane with $1 \leq k \leq n$ the result follows. □

Lemma 8 and Lemma 9 together imply the following:

THEOREM 10 *Given an affine plane of order $n$ and a prime $p$ dividing $n$ precisely once. Let $1 \leq k \leq n$. Partition the affine plane into a $k$-net and a $(n+1-k)$-net with incidence matrices $N_k$ and $N_{n+1-k}$ respectively, then:*

$$r_p(N_{n+1-k}) - r_p(N_k) = \frac{1}{2}n(n+1-2k)$$

*Proof.* By Lemma 8(ii) we have that

$$r_p(N_k^T N_k) = r_p(N_{n+1-k}^T N_{n+1-k}),$$

so by Lemma 9 and (1)

$$nk - 2\dim\ker_p(N_k) = n(n+1-k) - 2\dim\ker_p(N_{n+1-k})$$

which yields

$$nk - \dim\ker_p(N_k) = n(n+1-k) - \dim\ker_p(N_{n+1-k}) - \frac{1}{2}n(n+1-2k)$$

from which the result follows. □

The main conjecture of the paper by Moorhouse [14] is as follows:

*Conjecture (Moorhouse).* Given a $k$-net of order $n$ and a $(k-1)$-subnet thereof with incidence matrices $N_k$ and $N_{k-1}$ respectively. If $p$ is a prime that divides $n$ precisely once, then

$$r_p(N_k) - r_p(N_{k-1}) \geq n - k + 1.$$

In connection with this conjecture we mention the following corollary of Theorem 10:

COROLLARY 11 *Let $\Pi_{n-1}$ be an $(n-1)$-net of order $n$ with an $(n-2)$-subnet $\Pi_{n-2}$ and let $N_{n-1}$ and $N_{n-2}$ be their incidence matrices. If $p$ is a prime dividing $n$ precisely once, then*

$$r_p(N_{n-1}) - r_p(N_{n-2}) = 1 + \dim\mathrm{Hom}(G, \mathbb{F}_p),$$

*where $G$ is a loop corresponding with the 3-net with parallel classes the class that is in $\Pi_{n-1}$ but not in $\Pi_{n-2}$ and the two parallel classes that complete $\Pi_{n-1}$ to an affine plane of order $n$.*

### 3.2. *Desarguesian Nets*

In his paper [14] Moorhouse determined the $p$-rank of the line-point incidence matrices of desarguesian nets of (prime) order $p$. (A desarguesian net is by definition a subnet

of a desarguesian affine plane.) He proved that for a desarguesian $k$-net of order $p$ with incidence matrix $N_k$:

$$r_p(N_k) = pk - \frac{1}{2}(k-1)k. \tag{3}$$

Using this result we can prove that:

THEOREM 12 *Let $A_k$ be the adjacency matrix of the collinearity graph of a desarguesian $k$-net of order $p$, then*

$$r_p(A_k + kI) = \begin{cases} k(p+1-k) & \text{for } 0 \leq k < p+1, \\ 1 & \text{for } k = p+1. \end{cases}$$

*Proof.* The statement follows straightforward from (1), (3) and Lemma 9. □

By (3) and Theorem 12 we see that if $N_k$ is a desarguesian $k$-net of prime order $p$ then $r_p(N_k)$ and $r_p(N_k^T N_k)$ depend only on $p$ and $k$ and not on which $k$-subset of the $p+1$ parallel classes of the affine plane is chosen. This is in general not the case for desarguesian nets of order $q = p^e$ with $e > 1$. Table 1 gives all possible $p$-ranks for desarguesian nets of order $q$ with $q \in \{4, 8, 9, 16\}$ and $p$ dividing $q$ obtained by computer. For larger values of $q$, the variety in the occuring values for the $p$-ranks increases which suggests there is no simple general formula for these $p$-ranks. However, if we regard some special subnets we might get some results, such as:

THEOREM 13 *Let $N_k$ be the incidence matrix of a desarguesian $k$-net $\Pi_k$ of order $p^e$ for which the $k$ points at infinity corresponding with the $k$ parallel classes lie in the same (projective) subplane of order $p$ (So $k \leq p+1$). Then*

$$r_p(N_k) \leq kp^e - \binom{e+k-1}{e+1}. \tag{4}$$

*If equality holds then:*

$$r_p(N_k^T N_k) = kp^e - 2\binom{e+k-1}{e+1} + \epsilon \tag{5}$$

*where*

$$\begin{aligned} \epsilon &= 1 \quad \text{if } e = 1 \text{ and } k = p+1 \\ &= p \quad \text{if } e = 2 \text{ and } k = p+1 \\ &= 0 \quad \text{otherwise.} \end{aligned}$$

*Remark.* By Moorhouse's result ((3)), (4) holds with equality if $e = 1$ and by Theorem's 3 and 4 also if $k \leq 3$. Computer results suggest that that (4) holds with equality in general,

*Table 1.* All possible $p$-ranks of desarguesian nets of order 4,8,9 or 16.

| | $q=4, p=2$ | | $q=8, p=2$ | | $q=9, p=3$ | | $q=16, p=2$ | |
|---|---|---|---|---|---|---|---|---|
| $k$ | $r_pN_k$ | $r_pN_k^TN_k$ | $r_pN_k$ | $r_pN_k^TN_k$ | $r_pN_k$ | $r_pN_k^TN_k$ | $r_pN_k$ | $r_pN_k^TN_k$ |
| 17 | | | | | | | 81 | 1 |
| 16 | | | | | | | 81 | 16 |
| 15 | | | | | | | 80 | 30 |
| 14 | | | | | | | 79 | 36 |
| 13 | | | | | | | 78 | 38, 42 |
| 12 | | | | | | | 77 | 36, 40, 42 |
| 11 | | | | | | | 76 | 34, 36, 38, 42 |
| 10 | | | | | 36 | 1 | 75 | 30, 36, 40, 42 |
| 9 | | | 27 | 1 | 36 | 9 | 74 | 30, 36, 40, 42 |
| 8 | | | 27 | 8 | 35 | 16 | 73 | 30, 36, 40, 42 |
| 7 | | | 26 | 14 | 34 | 19 | 68 | 30, 36, 40, 42 |
| 6 | | | 25 | 14 | 33 | 18, 19 | 63 | 34, 36, 38, 42 |
| 5 | 9 | 1 | 24 | 14 | 30 | 16, 20 | 56; 58 | 36; 40, 42 |
| 4 | 9 | 4 | 23 | 14 | 26; 27 | 19; 18 | 51; 53 | 38; 42 |
| 3 | 8 | 6 | 19 | 14 | 23 | 19 | 42 | 36 |
| 2 | 7 | 6 | 15 | 14 | 17 | 16 | 31 | 30 |
| 1 | 4 | 4 | 8 | 8 | 9 | 9 | 16 | 16 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

but we couldn't prove this. As the theorem states, we can only prove that $\dim \ker_p(N_k) \geq \binom{e+k-1}{e+1}$ and that if equality holds also the second statement holds. The first part of the proof is a generalization of the method used by Moorhouse [14] to derive relation (3).

*Proof.* Let $q = p^e$ and take as point set $\mathcal{P} = \mathbb{F}_q \times \mathbb{F}_q$. Let $\Pi_{p+1}$ be the $(p+1)$-net with lines:

$$l_{rs} = \{(x, rx + s) \mid x \in \mathbb{F}_q\}, l_{\infty s} = \{(s, y) \mid y \in \mathbb{F}_q\}, s \in \mathbb{F}_q, r \in \mathbb{F}_p$$

Let $\chi_{rs}$, $\chi_{\infty s}$ $(r \in \mathbb{F}_p, s \in \mathbb{F}_q)$ be the characteristic functions of these lines. Without loss of generality we may assume that $\Pi_k$ is a subnet of $\Pi_{p+1}$. Now let $\Pi_{k-1} \subset \Pi_k$ be (any) $(k-1)$- and $k$-subnets of $\Pi_{p+1}$. Since the automorphism group of $\Pi_{p+1}$ acts transitively on the $p+1$ parallel classes, we may suppose that the lines of $\Pi_{k-1}$ are

$$\{l_{rs} \mid r \in E, s \in \mathbb{F}_q\}, E \subseteq \mathbb{F}_p, |E| = k-1$$

and that $\Pi_k$ has the additional parallel class $\{l_{\infty s} \mid s \in \mathbb{F}_q\}$. Define

$$\mathcal{V}_k = \{(a_s : s \in \mathbb{F}_q) \in \mathbb{F}_p^q \mid \sum_{s \in \mathbb{F}_q} a_s \chi_{\infty s} \in \mathcal{C}_p(\Pi_{k-1}) = \sum_{r \in E} \sum_{s \in \mathbb{F}_q} \mathbb{F}_p \chi_{rs}\}$$

We will show that $\dim \mathcal{V}_k \geq \binom{e+k-2}{e}$.

Let $k \geq 2$. Since $\mathbb{F}_q$ is a vector space of dimension $e$ over $\mathbb{F}_p$ we may represent every element $x \in \mathbb{F}_q$ by a vector $(x_0, x_1, \ldots, x_{e-1}) \in \mathbb{F}_p^e$. We will first show that the vector

$(a_s : s \in \mathbb{F}_q)$ where $a_s = \prod_{i=0}^{e-1} s_i^{\alpha_i}$, with $\alpha_i \in \mathbb{N}$ and $\sum_{i=0}^{e-1} \alpha_i = k-2$ is in $\mathcal{V}_k$. Note that there are $\binom{e+k-3}{e-1}$ of these vectors.

Consider the unique solution $(\beta_r : r \in E)$ to the linear system

$$\sum_{r \in E} r^j \beta_r = \begin{cases} 0 & , 0 \le j \le k-3 \\ 1 & , j = k-2 \end{cases}$$

(There exists precisely one solution since the coefficient matrix of this system is a $(k-1) \times (k-1)$ Vandermonde matrix) and let $\alpha_0, \alpha_1, \ldots, \alpha_{e-1}$ be non-negative integers satisfying $\sum_{i=0}^{e-1} \alpha_i = k-2$. Define

$$\begin{aligned} a_s &:= \prod_{i=0}^{e-1} s_i^{\alpha_i} \qquad s = (s_0, \ldots, s_{e-1}) \in \mathbb{F}_q \\ b_{rs} &:= \beta_r \prod_{i=0}^{e-1} (-s_i)^{\alpha_i} \quad r \in E, s = (s_0, \ldots, s_{e-1}) \in \mathbb{F}_q \end{aligned}$$

then

$$\sum_{s \in \mathbb{F}_q} a_s \chi_{\infty s} = \sum_{r \in E} \sum_{s \in \mathbb{F}_q} b_{rs} \chi_{rs} \tag{6}$$

For verification evaluate this relation at an arbitrary point $(x, y) \in \mathcal{P}$. If $x = (x_0, \ldots, x_{e-1})$ and $y = (y_0, \ldots, y_{e-1})$ the left side of (6) yields

$$\prod_{i=0}^{e-1} x_i^{\alpha_i}$$

and the right side yields

$$\begin{aligned} &\sum_{r \in E} \beta_r \prod_{i=0}^{e-1} (r x_i - y_i)^{\alpha_i} \\ &= \sum_{r \in E} \beta_r \prod_{i=0}^{e-1} \left( \sum_{j=0}^{\alpha_i} \binom{\alpha_i}{j} r^j x_i^j (-y_i)^{\alpha_i - j} \right) \\ &= \sum_{r \in E} \beta_r \left( \sum_{j=0}^{k-2} \sum_{\substack{j_0, \ldots, j_{e-1} \\ j_0 + \cdots + j_{e-1} = j \\ j_i \le \alpha_i}} \binom{\alpha_0}{j_0} \cdots \binom{\alpha_{e-1}}{j_{e-1}} r^j x_0^{j_0} \cdots x_{e-1}^{j_{e-1}} (-y_0)^{\alpha_0 - j_0} \cdots (-y_{e-1})^{\alpha_{e-1} - j_{e-1}} \right) \\ &= \sum_{j=0}^{k-2} \sum_{\substack{j_0, \ldots, j_{e-1} \\ j_0 + \cdots + j_{e-1} = j \\ j_i \le \alpha_i}} \left( \sum_{r \in E} r^j \beta_r \right) \binom{\alpha_0}{j_0} \cdots \binom{\alpha_{e-1}}{j_{e-1}} x_0^{j_0} \cdots x_{e-1}^{j_{e-1}} (-y_0)^{\alpha_0 - j_0} \cdots (-y_{e-1})^{\alpha_{e-1} - j_{e-1}} \\ &= \prod_{i=0}^{e-1} x_i^{\alpha_i} \end{aligned}$$

Thus $(a_s : s \in \mathbb{F}_q) \in \mathcal{V}_k$ with $a_s = \prod_{i=0}^{e-1} s_i^{\alpha_i}$, $\alpha_i \in \mathbb{N}$ and $\sum_{i=0}^{e-1} \alpha_i = k-2$.

For $0 \leq t \leq k-2$, choose a subset $E_t \subseteq E$ of size $t+1$ corresponding to a $(t+1)$-subnet $\Pi_{t+1} \subseteq \Pi_{k-1}$. Replacing $E$ by $E_t$ in the above argument gives

$$(a_s : s \in \mathbb{F}_q) \in \mathcal{V}_k \text{ with } a_s = \prod_{i=0}^{e-1} s_i^{\alpha_i}, \alpha_i \in \mathbb{N} \text{ and } \sum_{i=0}^{e-1} \alpha_i = t$$

Thus

$$\begin{aligned} \mathcal{V}_k \supseteq & \{(f(s_0, \ldots, s_{e-1}) : s \in \mathbb{F}_q) \mid f(X_0, \ldots, X_{e-1}) \\ & \in \mathbb{F}_p[X_0, \ldots, X_{e-1}], \deg f \leq k-2\} \end{aligned}$$

and since for each $f(X_0, \ldots, X_{e-1}) \in \mathbb{F}_q[X_0, \ldots, X_{e-1}]$ with $\deg f \leq k-2 (\leq p-1)$ we have $f(x_0, \ldots, x_{e-1}) = 0$ for all $(x_0, \ldots, x_{e-1}) \in \mathbb{F}_p^e$ if and only if $f = 0$, the dimension of $\mathcal{V}_k$ is at least the dimension of the vector space of polynomials $f \in [X_0, \ldots, X_{e-1}]$ with $\deg f \leq k-2$, so $\dim_p \mathcal{V}_k \geq \sum_{t=0}^{k-2} \binom{t+e-1}{e-1} = \binom{e+k-2}{e}$. Hence if $N_k$ is an incidence matrix of a $k$-subnet of $\Pi_{p+1}$ then

$$\dim \ker_p(N_k) \geq \sum_{l=2}^{k} \binom{e+l-2}{e} = \binom{e+k-1}{e+1}. \tag{7}$$

If $e = 1$ then $\Pi_{p+1}$ is a desarguesian affine plane of (prime) order $p$ and hence $\dim \ker_p(N_{p+1}) = \binom{p+1}{2}$, so we found all vectors in $\ker_p(N_{p+1})$ and hence (7) holds with equality for all $k \in \{0, 1, \ldots, p+1\}$ which yields (3). If however $e > 1$ a similar argument is still missing.

Now suppose that indeed (7) holds with equality so we have an explicit basis for $\ker_p(N_k)$ for every $k$-subnet of $\Pi_{p+1}$. We prove that in this case the Gram matrix of a basis of $\ker_p(N_k)$ has $p$-rank equal to 1 if $e = 1 \wedge k = p+1$, equal to $p$ if $e = 2 \wedge k = p+1$ and equal to 0 otherwise.

The case $e = 1$ is already proved, so we may assume that $e > 1$. Let $\Pi_k$ consist of the lines $\{l_{\infty s} \mid s \in \mathbb{F}_q\}$ and $\{l_{rs} \mid r \in E, s \in \mathbb{F}_q\}$ for some $E \subseteq \mathbb{F}_p$, $|E| = k-1$. Let $\emptyset \neq E_1, E_2 \subseteq E$, let $\alpha_i, \gamma_i \in \mathbb{N}$ $(i = 0, 1, \ldots, e-1)$ such that $\sum_{i=0}^{e-1} \alpha_i = |E_1| - 1$ and $\sum_{i=0}^{e-1} \gamma_i = |E_2| - 1$, and let $\beta_r, \delta_r \in \mathbb{F}_p$, $(r \in \mathbb{F}_p)$ be defined by $\beta_r = 0$ if $r \notin E_1$, $\delta_r = 0$ if $r \notin E_2$, and $(\beta_r : r \in E_1)$ and $(\delta_r : r \in E_2)$ are the unique solutions of the linear systems

$$\sum_{r \in E_1} r^j \beta_r = \begin{cases} 0 & 0 \leq j \leq |E_1| - 2 \\ 1 & j = |E_1| - 1 \end{cases}$$

and

$$\sum_{r \in E_2} r^j \delta_r = \begin{cases} 0 & 0 \leq j \leq |E_2| - 2 \\ 1 & j = |E_2| - 1 \end{cases}$$

respectively. Now calculate the inner product of the vectors

$$\underline{v}_1 := \left( -\prod_{i=0}^{e-1} s_i^{\alpha_i} \mid \prod_{i=0}^{e-1} (-s_i)^{\alpha_i} \beta_0 \mid \ldots \mid \prod_{i=0}^{e-1} (-s_i)^{\alpha_i} \beta_{p-1} \right)$$

and

$$\underline{v}_2 := \left( -\prod_{i=0}^{e-1} s_i^{\gamma_i} | \prod_{i=0}^{e-1} (-s_i)^{\gamma_i} \delta_0 | \ldots | \prod_{i=0}^{e-1} (-s_i)^{\gamma_i} \delta_{p-1} \right)$$

where for every component $(s_0, s_1, \ldots, s_{e-1})$ runs through $\mathbb{F}_p^e$. This yields

$$\underline{v}_1 \underline{v}_2^T = \prod_{i=0}^{e-1} \left( \sum_{s_i \in \mathbb{F}_p} s_i^{\alpha_i + \gamma_i} \right) \left( 1 + \sum_{i \in \mathbb{F}_p} \beta_i \delta_i \right).$$

Since

$$\sum_{x \in \mathbb{F}_p} x^\alpha = \begin{cases} -1 & \text{if } \alpha = i(p-1) \text{ with } i \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

$\underline{v}_1 \underline{v}_2^T = 0$ unless for all $i \in \{0, 1, \ldots, e-1\}$: $\alpha_i + \gamma_i \in \{p-1, 2(p-1)\}$. (Notice that $\sum_{i=0}^{e-1} \alpha_i \leq p-1$ and $\sum_{i=0}^{e-1} \gamma_i \leq p-1$.) So the only cases in which the inner product could be non-zero are:

(ia) $e = 1$ and $\alpha_0 = \gamma_0 = p-1$ (so $k = p+1$),

(ib) $e = 1$ and $\alpha_0 + \gamma_0 = p-1$,

(ii) $e = 2$ and $\alpha_0 = \gamma_1 = \alpha$; $\alpha_1 = \gamma_0 = p-1-\alpha$ for some $\alpha \in \{0, 1, \ldots, p-1\}$ (so $k = p-1$).

Since we wouldn't consider the case $e = 1$ here we just mention that the inner product is -1 in case (ia) and 0 in case (ib). Now suppose we are in case (ii) and let $(\beta_0, \beta_1, \ldots, \beta_{p-1}) = (\delta_0, \delta_1, \ldots, \delta_{p-1}) =: \underline{\beta}$ and let $S$ be the coefficient matrix of the system defining $\underline{\beta}$, so $S_{j,r} = r^j$ $(r \in \mathbb{F}_p, j = 0, 1, \ldots, p-1)$ and $S\underline{\beta}^T = (0, 0, \ldots, 0, 1)^T$. Then $\underline{v}_1 \underline{v}_2^T = (-1)^2(1 + \underline{\beta}\underline{\beta}^T) = 1 + (0, \ldots, 0, 1)(SS^T)^{-1}(0, \ldots, 0, 1)^T = 1$. (Indeed, $(SS^T)_{ij} = \sum_{r \in \mathbb{F}_p} r^{i+j}$ which is equal to $-1$ if $i + j = p-1$ or $i = j = p-1$ and equal to 0 otherwise. So the $(i, j)$-entry of $(SS^T)^{-1}$ is equal to $-1$ if $i + j = p-1$, equal to 1 if $i = j = 0$ and equal to 0 otherwise, so in particular the $(p-1, p-1)$-entry is equal to 0.)

If we take vectors of the same type as $\underline{v}_1$ and $\underline{v}_2$ as basis vectors for $\ker_p(N_{p+1})$ all except for $p$ entries of the corresponding Gram matrix are zero and no two of these non-zero entries occur in the same row or column. □

## Note Added in Proof

The author recently proved that in Theorem 13, (4) holds with equality if $1 \leq k \leq p$.

## References


1. A. E. Brouwer and C. A. van Eijl, On the $p$-rank of the adjacency matrices of strongly regular graphs, *Journal of Alg. Comb.* Vol. 1 (1992) pp. 329–346.
2. R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, Berlin (1958).
3. R. H. Bruck, Finite nets II, Uniqueness and embedding, *Pacific J. Math.* Vol. 13 (1963) pp. 421–457.
4. P. J. Cameron, Strongly Regular Graphs, in: *Selected topics in graph theory*, L. W. Beineke and R. J. Wilson (eds.), Academic Press, London, (1978) pp. 337–360.
5. J. Dénes and A. D. Keedwell, *Latin Squares, New Developments in the Theory and Applications*, Annals of Discrete Mathematics 46, North-Holland, Amsterdam (1991).
6. S. Dougherty, Nets and their codes, *Designs, Codes and Cryptography*, Vol. 3 (1993) pp. 315–331.
7. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups, *European J. Combin.* Vol. 5 (1984) pp. 43–50.
8. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups II: induced characters, *European J. Combin.* Vol. 7 (1986) pp. 131–137.
9. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups III: quotients and fusion, *European J. Combin.* Vol. 10 (1989) pp. 47–56.
10. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups IV: products and superschemes, *European J. Combin.* Vol. 10 (1989) pp. 257–263.
11. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups V: linear characters, *European J. Combin.* Vol. 10 (1989) pp. 449–456.
12. K. W. Johnson and J. D. H. Smith, Characters of finite quasigroups VI: critical examples and doubletons, *European J. Combin.* Vol. 11 (1990) pp. 267–275.
13. E. S. Lander, *Symmetric Designs: An Algebraic Approach*, Lond. Math. Soc. Lecture Notes, 74, Cambridge Univ. Press (1983).
14. G. E. Moorhouse, Bruck nets, codes, and characters of loops, *Designs, Codes and Cryptography*, Vol. 1 (1991) pp. 7–29.