

Ordinary Graphs and Subplane Partitions

Marc Fossorier ^a, Jaroslav Ježek ^{b,1}, J. B. Nation ^c and
Alex Pogel ^d

^a*Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA*

^b*Charles University, Sokolovska 83, 18600 Praha 8, Czech Republic*

^c*Department of Mathematics, University of Hawaii, Honolulu, HI 96822, USA*

^d*Physical Science Laboratory, New Mexico State University, Las Cruces, NM 88003, USA*

Abstract

We introduce a generalization of symmetric (v, k, λ) block designs, and show how these could potentially be used to construct projective planes of non-prime-power order.

Key words: projective plane, nondesarguesian plane, subplane partition, block design, directed graph

If q is a prime power and $n^2 + n + 1 = N(q^2 + q + 1)$, then conceivably we could construct a projective plane of order n by gluing together N planes of order q . For example, $18^2 + 18 + 1 = 343 = 49 \cdot 7$. Can we make a projective plane of order 18 by gluing 49 planes of order 7?

With this in mind, we will discuss a class of directed graphs which arises when we attempt such a construction. The existence of a graph with the necessary parameters is the first problem we face. Then we will describe how the graphs may be used to build the putative plane of order n . The gluing maps are an even more serious obstacle. Nonetheless, it is an intriguing program, which just possibly could work.

Email addresses: marc@aravis.eng.hawaii.edu (Marc Fossorier), jezek@csmat.karlin.mff.cuni.cz (Jaroslav Ježek), jb@math.hawaii.edu (J. B. Nation), apogel@psl.nmsu.edu (Alex Pogel).

¹ Supported in part by the grants GAČR 201/99/0263 and MSM 113200007.

1 Ordinary Graphs and their Associated Matrices

Let \mathbf{G} be a loopless directed graph. For a vertex i of \mathbf{G} , let

$$\begin{aligned}\uparrow i &= \{j : i \rightarrow j\} \\ \downarrow i &= \{k : k \rightarrow i\}.\end{aligned}$$

Define binary relations A, B, C on the vertices of \mathbf{G} by

- (1) $i A j$ if $i \neq j$ and there is no edge between i and j ,
- (2) $i B j$ if $i \rightarrow j$ or $j \rightarrow i$ but not both,
- (3) $i C j$ if $i \rightarrow j$ and $j \rightarrow i$.

We say that \mathbf{G} is an *ordinary graph* of type $\langle n, r, a, b, c \rangle$ if

- (1) \mathbf{G} has n vertices,
- (2) $|\uparrow i| = |\downarrow i| = r$ for each vertex i of \mathbf{G} ,
- (3) if $i A j$ then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = a$,
- (4) if $i B j$ then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = b$,
- (5) if $i C j$ then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = c$.

We allow a, b or c to be the special symbol \times to indicate that in \mathbf{G} the corresponding relation A, B or C is empty.

This definition is easily interpreted in terms of the adjacency matrix \mathbf{M} of \mathbf{G} . An $n \times n$ 0-1 matrix $\mathbf{M} = (m_{ij})$ is the adjacency matrix of an ordinary graph of type $\langle n, r, a, b, c \rangle$ if it has a zero diagonal and

$$(\mathbf{M}\mathbf{M}^t)_{ij} = (\mathbf{M}^t\mathbf{M})_{ij} = \begin{cases} r & \text{if } i = j, \\ a & \text{if } i \neq j \text{ and } m_{ij} + m_{ji} = 0, \\ b & \text{if } m_{ij} + m_{ji} = 1, \\ c & \text{if } m_{ij} + m_{ji} = 2. \end{cases}$$

We will also refer to the adjacency matrix of an ordinary graph as an *ordinary matrix*.

Recall, for example, that the incidence matrix of a symmetric (v, k, λ) block design is a $v \times v$ 0-1 matrix satisfying $\mathbf{M}\mathbf{M}^t = \mathbf{M}^t\mathbf{M} = (k - \lambda)\mathbf{I} + \lambda\mathbf{J}$. Thus the corresponding graph is ordinary of type $\langle v, k, \lambda, \lambda, \lambda \rangle$, with possibly one or more of the λ 's replaced by an \times . We will produce other types of examples in the next section.

Question. In the examples we have found so far, if a 0-1 matrix \mathbf{M} has constant row and column sums, and satisfies the conditions above for $(\mathbf{M}\mathbf{M}^t)_{ij}$,

then $\mathbf{M}^t\mathbf{M} = \mathbf{M}\mathbf{M}^t$ (so \mathbf{M} is normal). Is this always the case? If so, it would generalize a well-known result of Ryser [15] for symmetric block designs.

Let us begin with a basic counting lemma.

Lemma 1 *Let \mathbf{G} be an ordinary graph of type $\langle n, r, a, b, c \rangle$. Let α be the number of (unordered) pairs in the A relation, and similarly β is the number of pairs in B , γ the number of pairs in C . Then*

- (1) $\alpha + \beta + \gamma = \binom{n}{2}$,
- (2) $\beta + 2\gamma = nr$,
- (3) $a\alpha + b\beta + c\gamma = n\binom{r}{2}$.

An ordinary graph is *symmetric* if $i \rightarrow j$ implies $j \rightarrow i$ (equivalently, $\mathbf{M}^t = \mathbf{M}$ or $\beta = 0$). Likewise, a graph is *antisymmetric* if $i \rightarrow j$ implies $j \not\rightarrow i$ (equivalently, $\mathbf{M} + \mathbf{M}^t + \mathbf{I} \leq \mathbf{J}$ or $\gamma = 0$).

Note: the conflict of terminology is unfortunate, but a symmetric (v, k, λ) block design need not be symmetric in this sense.

Given an ordinary graph \mathbf{G} , we define the *complement* \mathbf{G}^* to be the loopless graph such that, for vertices $i \neq j$, $i \rightarrow_{\mathbf{G}^*} j$ if and only if $i \not\rightarrow_{\mathbf{G}} j$. In matrix terms, if \mathbf{M} is the adjacency matrix for \mathbf{G} , then $\mathbf{J} - \mathbf{I} - \mathbf{M}$ is the adjacency matrix for \mathbf{G}^* . The following calculation is easy.

Lemma 2 *Let \mathbf{G} be an ordinary graph of type $\langle n, r, a, b, c \rangle$. If $A \neq \emptyset$, $B \neq \emptyset$ and $C \neq \emptyset$, then \mathbf{G}^* is an ordinary graph of type $\langle n, n - 1 - r, n + c - 2r, n + b - 2r - 1, n + a - 2r - 2 \rangle$.*

The modifications for when $A = \emptyset$ or $B = \emptyset$ or $C = \emptyset$ are straightforward. For example, if $A = \emptyset$ and $B, C \neq \emptyset$, so that \mathbf{G} has type $\langle n, r, \times, b, c \rangle$, then \mathbf{G}^* has type $\langle n, n - 1 - r, n + c - 2r, n + b - 2r - 1, \times \rangle$.

Corollary 3 *Let \mathbf{G} be an ordinary graph of type $\langle n, r, a, b, c \rangle$.*

- (1) *If $A \neq \emptyset$, then $n + a \geq 2r + 2$.*
- (2) *If $B \neq \emptyset$, then $n + b \geq 2r + 1$.*
- (3) *If $C \neq \emptyset$, then $n + c \geq 2r$.*

2 Examples

We have several methods for constructing ordinary graphs and matrices, sometimes overlapping.

Symmetric (v, k, λ) block designs.

These are ordinary graphs of type $\langle v, k, a, b, c \rangle$ with a, b and c either λ or \times . This class includes complete loopless graphs (with adjacency matrix $\mathbf{J} - \mathbf{I}$), graphs whose adjacency matrix is a permutation matrix, and graphs whose adjacency matrix is the incidence matrix of a finite projective plane. It also includes ordinary tournaments, discussed below.

Circulant ordinary matrices.

A matrix $\mathbf{M} = (m_{ij})$ for $0 \leq i, j < n$ is said to be *circulant* if there is a sequence $\mathbf{e} = \langle e_0, \dots, e_{n-1} \rangle$ such that $m_{ij} = e_{(j-i) \bmod n}$. Given a sequence \mathbf{e} of 0's and 1's, let us denote the corresponding circulant matrix by $\mathbf{C}(\mathbf{e})$. This familiar construction allows us to build many examples of ordinary matrices. Indeed, it is simple to write a program which will generate the circulant matrices of a given size, and check which ones are ordinary. Table 1 lists a few examples found in this way.

Note that circulant matrices are normal: $\mathbf{C}(\mathbf{e})^t \mathbf{C}(\mathbf{e}) = \mathbf{C}(\mathbf{e}) \mathbf{C}(\mathbf{e})^t$.

Of crucial importance to us later is the following well-known theorem of J. Singer [16]; see [6], Theorem 11.3.1.

Theorem 4 *For each prime power q , there is a circulant ordinary matrix representing the incidence matrix of a desarguesian projective plane of order q .*

Ordinary graphs with $a = 0$

Jon Kalk [10] has classified all ordinary graphs of type $\langle n, r, 0, b, c \rangle$. Note that an easy application of Lemma 1 shows that $a = 0$ whenever $n > r^2 + r + 1$. By duality, he obtains a characterization of ordinary graphs whose type satisfies $n + c = 2r$, which includes the case when $r > (n - r - 1)^2$.

Other ordinary graphs

It is also not hard to generate small ordinary graphs that are symmetric or antisymmetric. One can also write a program that attempts to construct an ordinary graph of a fixed type. These programs show that some apparently

Table 1
Some examples of circulant ordinary matrices

$\langle \mathbf{e} \rangle$	type
01001	$\langle 5, 2, 1, \times, 0 \rangle$
01110	$\langle 5, 3, \times, 2, 1 \rangle$
001010	$\langle 6, 2, 0, \times, 1 \rangle$
011010	$\langle 6, 3, 2, 1, 1 \rangle$
0101000	$\langle 7, 2, 1, 0, \times \rangle$
0110100	$\langle 7, 3, \times, 1, \times \rangle$
0110010	$\langle 7, 3, 2, 1, 0 \rangle$
0110001	$\langle 7, 3, 1, 1, 1 \rangle$
01101000	$\langle 8, 3, 1, 1, 0 \rangle$
000100100	$\langle 9, 2, 0, \times, 1 \rangle$
0100011000	$\langle 10, 3, 0, 1, 2 \rangle$
0010101000	$\langle 10, 3, 0, 2, 1 \rangle$
01110100100	$\langle 11, 5, 2, 2, 2 \rangle$
01101101000	$\langle 11, 5, 3, 2, 1 \rangle$
01011100010	$\langle 11, 5, \times, 2, \times \rangle$
0110100000100	$\langle 13, 4, 1, 1, \times \rangle$
0110001000001	$\langle 13, 4, 1, 1, 1 \rangle$
0101100001101	$\langle 13, 6, 3, \times, 2 \rangle$
011101100101000	$\langle 15, 7, 3, 3, 3 \rangle$
0100101101010000000	$\langle 19, 6, 3, 1, \times \rangle$
0111101010000110010	$\langle 19, 9, 4, 4, 4 \rangle$
0100111101010000110	$\langle 19, 9, \times, 4, \times \rangle$
011001000000000101000	$\langle 21, 5, 1, 1, \times \rangle$
011000010100000000010	$\langle 21, 5, 1, 1, 1 \rangle$
000100100100100100000	$\langle 21, 5, 0, 4, 3 \rangle$
011011011001000011001	$\langle 21, 10, 7, 3, 4 \rangle$

plausible types may fail to exist. For example, there is no $\langle 13, 7, a, b, c \rangle$ ordinary graph with $a = 7$ or \times , $b = 4$ or \times , and $c = 1$ or \times . (This also follows from Kalk's results for the case $n + c = 2r$, as $c = \times$ does not occur by Lemma 1.)

Ordinary Tournaments

A *tournament* is a loopless, directed graph such that for each pair i, j of distinct vertices, exactly one of the relations $i \rightarrow j$ or $j \rightarrow i$ holds. Thus a square 0-1 matrix \mathbf{M} is the adjacency matrix of a tournament if and only if $\mathbf{M} + \mathbf{M}^t + \mathbf{I} = \mathbf{J}$.

An ordinary tournament has type $\langle n, r, \times, b, \times \rangle$. A straightforward application of Lemma 1 yields $r = 2b + 1$ and $n = 2r + 1 = 4b + 3$. Thus we have the following result.

Lemma 5 *An ordinary tournament has type $\langle 4k + 3, 2k + 1, \times, k, \times \rangle$ for some integer $k \geq 0$. Its adjacency matrix satisfies*

$$\begin{aligned}\mathbf{M} + \mathbf{M}^t + \mathbf{I} &= \mathbf{J} \\ \mathbf{M}\mathbf{M}^t &= \mathbf{M}^t\mathbf{M} = k\mathbf{J} + (k + 1)\mathbf{I}.\end{aligned}$$

In this case, we say that \mathbf{M} is an ordinary tournament of *order* k . Ordinary tournaments are also known as *doubly regular* tournaments, and were studied in Reid and Brown [13]. Because they are one of the building blocks which can be used in the construction of the next section, let us review some of their properties.

By a theorem of H. Ryser, if a square 0-1 matrix of size $4k + 3$ satisfies $\mathbf{M} + \mathbf{M}^t + \mathbf{I} = \mathbf{J}$ and $\mathbf{M}\mathbf{M}^t = k\mathbf{J} + (k + 1)\mathbf{I}$, then $\mathbf{M}^t\mathbf{M} = \mathbf{M}\mathbf{M}^t$, and hence \mathbf{M} is the adjacency matrix of an ordinary tournament of order k (see e.g. [6], Theorem 10.2.3).

It was shown in [13] that the existence of an ordinary tournament of order k is equivalent to the existence of a skew Hadamard matrix of order $n + 1$. Thus we have a number of constructions for ordinary tournaments (see [6], Chapter 14, [13] and [14]), but we do not know whether there exists a tournament of order k for every $k \geq 0$.

We recall a classic construction due to R. Paley [12] that yields an ordinary tournament of order k whenever $4k + 3$ is a prime power. Let $q = p^\alpha = 4k + 3$, and define a sequence $\mathbf{e} = \langle e_i : i \in \text{GF}(q) \rangle$ by

$$e_i = \begin{cases} 1 & \text{if } i \text{ is a nonzero quadratic residue in } \text{GF}(q), \\ 0 & \text{otherwise.} \end{cases}$$

Then the matrix \mathbf{M} with $m_{ij} = e_{(j-i)}$ is the adjacency matrix of an ordinary tournament of order k . If $\alpha = 1$ then \mathbf{M} will be circulant, while if $\alpha > 1$ then \mathbf{M} is represented as a difference set on a non-cyclic abelian group.

When the Paley construction is done using a field $\text{GF}(q)$ with $q = 4k + 1$, it yields an ordinary matrix of type $\langle 4k + 1, 2k, k, \times, k - 1 \rangle$. The difference is due to the fact that, for an odd prime power q , -1 is a quadratic residue in $\text{GF}(q)$ if and only if $q \equiv 1 \pmod{4}$.

The complement of a tournament is usually referred to as its *dual*. The dual is represented by the matrix \mathbf{M}^t , and a tournament is said to be *self-dual* if there is a permutation matrix \mathbf{P} such that $\mathbf{M}^t = \mathbf{P}^t \mathbf{M} \mathbf{P}$. Ordinary tournaments obtained from quadratic residues are self-dual, with the map $i \rightarrow -i$ inducing the isomorphism.

It is reasonable to ask how many different ordinary tournaments of order k there are. For k small, this is amenable to computer searches.

Theorem 6 *The following list gives isomorphism types of ordinary tournaments of order k .*

0. For $k = 0$ there is 1 isomorphism type.
1. For $k = 1$ there is 1 isomorphism type.
2. For $k = 2$ there is 1 isomorphism type.
3. For $k = 3$ there are 2 isomorphism types (dual to each other).
4. For $k = 4$ there are at least 2 isomorphism types.
5. For $k = 5$ there are at least 28 isomorphism types.
6. For $k = 6$ there are at least 20 isomorphism types.

Let \mathbf{T} be a tournament. A subset $C \subseteq \mathbf{T}$ is a *subchain* if the relation \rightarrow is transitive on C , i.e., if the elements of C can be indexed as c_i for $1 \leq i \leq k$ so that $c_i \rightarrow c_j$ if and only if $i < j$. The following technical result is useful in constructing ordinary tournaments.

Lemma 7 *Let \mathbf{T} be an ordinary tournament of order $k \geq 3$. Then \mathbf{T} contains a 5-element subchain.*

Denote by M the maximal cardinality of a subchain of an ordinary tournament of order k . Using a computer, we were able to find the number M in these cases:

For $k = 0$, $M = 2$.

For $k = 1$, $M = 3$.

For $k = 2$, $M = 4$.

For $k = 3$, $M = 5$ (for both isomorphism types).

For $k = 4$, $M = 5$ (for both known isomorphism types).

For $k = 5$, $M = 6$ for all the 28 known isomorphism types.

For $k = 6$, for 3 isomorphism types we have $M = 7$ while for the remaining 17 known isomorphism types we have $M = 6$.

Every tournament can be considered as a groupoid, with respect to the multiplication defined as follows: $aa = a$ for all a ; if $a \rightarrow b$ then $ab = ba = a$.

Theorem 8 *Every ordinary tournament is a simple groupoid.*

PROOF. Let \mathbf{T} be an ordinary tournament of order k , and let r be a non-identical congruence of \mathbf{T} . There is at least one non-singleton block B of r . Take two different elements $a, b \in B$. Without loss of generality, $a \rightarrow b$. Clearly, if x is an element such that either $b \rightarrow x \rightarrow a$ or $a \rightarrow x \rightarrow b$, then $x \in B$. There are $(k + 1) + k = 2k + 1$ such elements x , and hence $|B| \geq 2k + 3$. So, every non-singleton block of r contains more than a half of the elements of T . It follows that for any $c \in T - B$, $\{c\}$ is a block of r . But for any such c , either $c \rightarrow x$ for all $x \in B$ or $x \rightarrow c$ for all $x \in B$, and either the out- or the in-degree of c is too large. Hence $B = T$. \square

3 Subplane partitions and ordinary graphs

Let $\Pi = \langle P, L, \leq \rangle$ be a projective plane of order n (so that $|P| = |L| = n^2 + n + 1$, each line contains $n + 1$ points and each point lies on $n + 1$ lines). Suppose there is a partition of Π into equal sized subplanes $\Pi_i = \langle P_i, L_i, \leq_i \rangle$ ($0 \leq i < N$) of order q . Since $n^2 + n + 1 = N(q^2 + q + 1)$, it is necessary that $n^2 + n + 1$ is divisible by $q^2 + q + 1$. For example, we could have $n = 18$ and $q = 2$; in this case, $N = 49$ as $343 = 49 \cdot 7$. Such a partition is called a *subplane partition* of Π .

We will write $i \rightarrow j$ if $i \neq j$ and there exist $p \in P_i$ and $\ell \in L_j$ with $p \leq \ell$. A subplane partition of Π will be called *ordinary* if $i \rightarrow j$ implies that for every $p \in P_i$ there exists an $\ell \in L_j$ with $p \leq \ell$. In that case, for each pair (i, j) with $i \rightarrow j$, we obtain a bijection λ_{ij} of P_i onto L_j by defining $\lambda_{ij}(p) = \ell$ where $\ell \in L_j$ and $p \leq \ell$. In other words, $\lambda_{ij} =_{\leq} |_{P_i \times L_j}$.

We want to show that $\langle N, \rightarrow \rangle$, with the arrow relation defined in the preceding paragraph, is an ordinary graph whenever $\Pi = \bigcup_{0 \leq i < N} \Pi_i$ is an ordinary partition.

Theorem 9 *Let $\Pi_i = \langle P_i, L_i, \leq_i \rangle$ ($0 \leq i < N$) be an ordinary partition of a projective plane Π of order n into subplanes of order q . The following are true:*

- (1) For each $i = 0, \dots, N - 1$, $|\uparrow i| = |\downarrow i| = n - q$.
- (2) If $i A j$, then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = q^2 + q + 1$.
- (3) If $i B j$, then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = q^2$.
- (4) If $i C j$, then $|\uparrow i \cap \uparrow j| = |\downarrow i \cap \downarrow j| = q^2 - q - 1$.

Thus $\langle N, \rightarrow \rangle$ is an ordinary graph of type $\langle N, n - q, a, b, c \rangle$ with $a = q^2 + q + 1$ or \times , $b = q^2$ or \times , and $c = q^2 - q - 1$ or \times .

PROOF. By duality, it is sufficient to find the cardinality of the first set in each case.

(1) Every point of P_i lies on $n + 1$ lines, where $k + 1$ of them belong to L_i ; clearly, the remaining $n - k$ ones belong to pairwise different L_j 's.

(2) Denote by p_1, \dots, p_{q^2+q+1} the points of P_i and by r_1, \dots, r_{q^2+q+1} the points of P_j . For every $u \in \{1, \dots, q^2+q+1\}$ define k_u by $p_1 \vee r_u \in L_{k_u}$. It follows from the assumptions that these numbers k_u are pairwise distinct, and different from i and j ; their number is $q^2 + q + 1$, and each has the property $i \rightarrow k_u \& j \rightarrow k_u$. Now every line from $L_{k_1} \cup \dots \cup L_{k_{q^2+q+1}}$ (there are $(q^2 + q + 1)^2$ such lines) contains a point from P_i and a point from P_j , and hence can be expressed as $p_u \vee r_v$ for some $u \in P_i$ and $v \in P_j$. The number of lines that can be expressed in this form is, of course, at most $(q^2 + q + 1)^2$. So, every line $p_u \vee r_v$ with $u \in P_i$ and $v \in P_j$ belongs to $L_{k_1} \cup \dots \cup L_{k_{q^2+q+1}}$. Consequently, if k is such that $i \rightarrow k \& j \rightarrow k$, then $k \in \{k_1, \dots, k_{q^2+q+1}\}$.

(3) Let $i \rightarrow j$ and $j \not\rightarrow i$. Take a point $p \in P_i$. There is precisely one line in L_j containing p ; this line contains precisely $q + 1$ points of P_j ; denote the remaining points of P_j by r_1, \dots, r_{q^2} . Define k_1, \dots, k_{q^2} by $p \vee r_u \in L_{k_u}$. We can proceed similarly as in the previous case to show that these numbers k_1, \dots, k_{q^2} are the only numbers k with the property that $i \rightarrow k$ and $j \rightarrow k$.

(4) Let $i \rightarrow j$ and $j \rightarrow i$. Take a point $p \in P_i$. There is precisely one line $A \in L_j$ containing p . This line contains precisely $q + 1$ points of P_j . Also, p belongs to $q + 1$ lines of L_i , each of which contains precisely one point of P_j , and this point does not belong to A . So, there are precisely $q^2 + q + 1 - (q + 1) - (q + 1) = q^2 - q - 1$ points r of P_j such that the line $p \vee r$ does not belong to either L_i or L_j . Denote these points by r_1, \dots, r_{q^2-q-1} and define k_1, \dots, k_{q^2-q-1} by $p \vee r_u \in L_{k_u}$. As in the proof of property (2), one can show that these are the only numbers k with $i \rightarrow k$ and $j \rightarrow k$. \square

We also need to describe a basic property of the maps λ_{ij} .

Lemma 10 Let $\Pi_i = \langle P_i, L_i, \leq_i \rangle$ for $0 \leq i < N$ be an ordinary partition of a projective plane Π of order n into subplanes of order q . If $i \neq j$ and $p \in P_i$

and $r \in P_j$, then exactly one of the following holds:

- (1) $r \leq_j \lambda_{ij}(p)$, or
- (2) $p \leq_i \lambda_{ji}(r)$, or
- (3) there exists k such that $\lambda_{ik}(p) = \lambda_{jk}(r)$.

The condition of this lemma just makes each pair of points join to a unique line. It follows from general principles that this also makes each pair of lines meet in a unique point; see e.g. [5], Theorem 20.8.1.

Conversely, if the conditions of Theorem 9 and Lemma 10 are satisfied, we can construct a projective plane of order n . We formulate this as follows.

Theorem 11 *Assume that $n^2 + n + 1 = N(q^2 + q + 1)$, and that there exists a projective plane Ψ of order q . Let $\Pi_i = \langle P_i, L_i, \leq_i \rangle$ for $0 \leq i < N$ be disjoint copies of Ψ . Suppose*

- (1) *there exists an ordinary graph $\langle N, \rightarrow \rangle$ of type $\langle N, n - q, a, b, c \rangle$ with $a = q^2 + q + 1$ or \times , $b = q^2$ or \times , and $c = q^2 - q - 1$ or \times , and*
- (2) *there exist bijections $\lambda_{ij} : P_i \rightarrow L_j$ for each pair with $i \rightarrow j$ such that if $i \neq j$ and $p \in P_i$ and $r \in P_j$, then exactly one of the following holds:*
 - (a) $r \leq_j \lambda_{ij}(p)$, or
 - (b) $p \leq_i \lambda_{ji}(r)$, or
 - (c) there exists k such that $\lambda_{ik}(p) = \lambda_{jk}(r)$.

Then there exists a projective plane of order n with an ordinary subplane partition into subplanes of order q .

The construction and proof are entirely straightforward in view of the previous discussion, *viz.*, if $p \in P_i$ and $\ell \in L_j$, then $p \leq \ell$ if and only if $i = j$ and $p \leq_i \ell$, or $i \rightarrow j$ and $\ell = \lambda_{ij}(p)$. In the next section we will give a matrix version of the construction.

Now we have several tasks to address. The first is to identify pairs n, q which are candidates. If $n \equiv q \pmod{q^2 + q + 1}$ or $n \equiv q^2 \pmod{q^2 + q + 1}$ then $q^2 + q + 1$ divides $n^2 + n + 1$. In the first case it is evident, and in the second case $n^2 + n + 1 \equiv q^4 + q^2 + 1 = (q^2 + q + 1)(q^2 - q + 1) \equiv 0 \pmod{q^2 + q + 1}$. If $q^2 + q + 1$ is prime, then the converse is true: $q^2 + q + 1$ divides $n^2 + n + 1$ only if $n \equiv q$ or $q^2 \pmod{q^2 + q + 1}$.

Table 2 gives a list of candidates for $n \leq 60$. We have omitted those n for which no plane of order n exists by the Bruck-Ryser Theorem [3]. The nonexistence of several types with $n+c = 2r$ follows from J. Kalk's classification [10]. On the other hand, he has constructed an ordinary graph of type $\langle 43, 31, 31, 25, 19 \rangle$.

The second task, given n and q , is to find an ordinary graph of the required

type. Two natural cases immediately present themselves.

The first natural case is when q is a prime power and $n = q^2$. R. H. Bruck proved that the desarguesian plane of order q^2 always has a subplane partition into subplanes of order q , based on J. Singer's result that any finite desarguesian plane may be derived from a difference set [2]. Peter Yff showed that these planes may have other partitions into subplanes of order q ; see [17], [18]. In each case, $N = q^2 - q + 1$ and the corresponding graph is complete of type $\langle N, N - 1, \times, \times, N - 2 \rangle$. This still leaves open the possibility that nondesarguesian planes of order q^2 may have a subplane partition.

The second natural case is when q is a prime power and $n = 2q^2 + q + 1$. In this case we could use an ordinary tournament of order q^2 , which has type $\langle 4q^2 + 3, 2q^2 + 1, \times, q^2, \times \rangle$. For $q = 2$ we have $n = 11$, an intriguing possibility. However, any attempt to construct a nondesarguesian plane of order 11 must bear in mind the known constraints; see, e.g., [7] or [8], and Theorem 16 below. For $q = 3$ we have $n = 22$, which is eliminated by the Bruck-Ryser theorem. The cases $q = 4$, $n = 37$ and $q = 5$, $n = 56$ seem *a priori* promising. The methods we have used to attempt these constructions will be described in the next section.

The third, and most difficult task, given candidates n , q and an appropriate ordinary graph, is to find bijections λ_{ij} satisfying the required property. One method for attempting this will also be given in the next section.

4 Matrix interpretation

Now suppose that n and q are given, and that we can find an ordinary matrix \mathbf{M} of type $\langle N, n - q, a, b, c \rangle$, where as usual $N = \frac{n^2+n+1}{q^2+q+1}$, $a = q^2 + q + 1$ or \times , $b = q^2$ or \times , and $c = q^2 - q - 1$ or \times . Thus \mathbf{M} is an $N \times N$ 0-1 matrix satisfying certain conditions on $\mathbf{M}\mathbf{M}^t = \mathbf{M}^t\mathbf{M}$ involving $n - q$, a , b and c . Let \mathbf{P} be the incidence matrix of a projective plane of order q , i.e., \mathbf{P} is a square 0-1 matrix of size $q^2 + q + 1$ satisfying $\mathbf{P}\mathbf{P}^t = \mathbf{P}^t\mathbf{P} = q\mathbf{I} + \mathbf{J}$.

Our goal is to construct the incidence matrix of a projective plane of order n , i.e., a square 0-1 matrix \mathbf{H} of size $n^2 + n + 1$ satisfying $\mathbf{H}\mathbf{H}^t = n\mathbf{I} + \mathbf{J}$. (This implies that $\mathbf{H}^t\mathbf{H} = \mathbf{H}\mathbf{H}^t$.) The construction requires that we find suitable permutation matrices \mathbf{E}_{ij} for each pair (i, j) with $i \rightarrow j$, which must satisfy some matrix equations given below. The matrices \mathbf{E}_{ij} will be square of size $q^2 + q + 1$.

Table 2
Possible combinations for special subplane partitions

n	$n^2 + n + 1$	q	N	comments
4	$21 = 7 \cdot 3$	2	3	works
9	$91 = 13 \cdot 7$	3	7	works
9	$91 = 7 \cdot 13$	2	13	no, type $\langle 13, 7, 7, 4, 1 \rangle$ DNE
11	$133 = 7 \cdot 19$	2	19	need type $\langle 19, 9, 7, 4, 1 \rangle$
16	$273 = 21 \cdot 13$	4	13	works
16	$273 = 13 \cdot 21$	3	21	no, type $\langle 21, 13, 13, 9, 5 \rangle$ DNE
18	$343 = 7 \cdot 49$	2	49	need type $\langle 49, 16, 7, 4, 1 \rangle$
23	$553 = 7 \cdot 79$	2	79	need type $\langle 79, 21, 7, 4, 1 \rangle$
25	$651 = 31 \cdot 21$	5	21	works
25	$651 = 21 \cdot 31$	4	31	no, type $\langle 31, 21, 21, 16, 11 \rangle$ DNE
25	$651 = 7 \cdot 93$	2	93	need type $\langle 93, 23, 7, 4, 1 \rangle$
29	$871 = 13 \cdot 67$	3	67	need type $\langle 67, 26, 13, 9, 5 \rangle$
32	$1057 = 7 \cdot 151$	2	151	need type $\langle 151, 30, 7, 4, 1 \rangle$
35	$1261 = 13 \cdot 97$	3	97	need type $\langle 97, 32, 13, 9, 5 \rangle$
36	$1333 = 31 \cdot 43$	5	43	need type $\langle 43, 31, 31, 25, 19 \rangle$
37	$1407 = 21 \cdot 67$	4	67	need type $\langle 67, 33, 21, 16, 11 \rangle$
37	$1407 = 7 \cdot 201$	2	201	need type $\langle 201, 35, 7, 4, 1 \rangle$
39	$1561 = 7 \cdot 223$	2	223	need type $\langle 223, 37, 7, 4, 1 \rangle$
42	$1807 = 13 \cdot 139$	3	139	need type $\langle 139, 39, 13, 9, 5 \rangle$
48	$2353 = 13 \cdot 181$	3	181	need type $\langle 181, 45, 13, 9, 5 \rangle$
49	$2451 = 57 \cdot 43$	7	43	works
51	$2653 = 7 \cdot 379$	2	379	need type $\langle 379, 49, 7, 4, 1 \rangle$
53	$2863 = 7 \cdot 409$	2	409	need type $\langle 409, 51, 7, 4, 1 \rangle$
55	$3081 = 13 \cdot 237$	3	237	need type $\langle 237, 52, 13, 9, 5 \rangle$
56	$3193 = 31 \cdot 103$	5	103	need type $\langle 103, 51, 31, 25, 19 \rangle$
58	$3423 = 21 \cdot 163$	4	163	need type $\langle 163, 54, 21, 16, 11 \rangle$
58	$3423 = 7 \cdot 489$	2	489	need type $\langle 489, 56, 7, 4, 1 \rangle$
60	$3661 = 7 \cdot 523$	2	523	need type $\langle 523, 58, 7, 4, 1 \rangle$

Define \mathbf{H} to be a block matrix $\mathbf{H} = (\mathbf{H}_{ij})$ for $0 \leq i, j < N$ where

$$\mathbf{H}_{ij} = \begin{cases} \mathbf{P} & \text{if } i = j, \\ \mathbf{E}_{ij} & \text{if } m_{ij} = 1, \\ \mathbf{O} & \text{if } i \neq j \text{ and } m_{ij} = 0. \end{cases}$$

In terms of this block construction, $(\mathbf{H}\mathbf{H}^t)_{ij} = \sum_k \mathbf{H}_{ik}\mathbf{H}_{jk}^t$. Our objective is to have $\mathbf{H}\mathbf{H}^t = n\mathbf{I} + \mathbf{J}$, and hence

$$\sum_{0 \leq k < N} \mathbf{H}_{ik}\mathbf{H}_{jk}^t = \begin{cases} n\mathbf{I} + \mathbf{J} & \text{if } i = j, \\ \mathbf{J} & \text{if } i \neq j. \end{cases}$$

Since the matrices \mathbf{E}_{ik} are chosen to be permutation matrices, $\mathbf{E}_{ik}\mathbf{E}_{ik}^t = \mathbf{I}$. There are $n - q$ permutation matrices in each “row” of \mathbf{H} , while $\mathbf{P}\mathbf{P}^t = q\mathbf{I} + \mathbf{J}$. Thus any choice of the matrices \mathbf{E}_{ij} will satisfy the equations for $i = j$, and the difficulty lies with the off-diagonal block positions. We record this as follows.

Theorem 12 *The construction above will yield the incidence matrix of a projective plane of order n precisely when we can find permutation matrices \mathbf{E}_{st} for $s \rightarrow t$ such that, for all pairs $(i, j) \in N^2$ with $i \neq j$, we have $\sum_k \mathbf{H}_{ik}\mathbf{H}_{jk}^t = \mathbf{J}$.*

Now the equations $\sum_k \mathbf{H}_{ik}\mathbf{H}_{jk}^t = \mathbf{J}$, with each \mathbf{H}_{ik} either \mathbf{P} , \mathbf{O} , or an unknown permutation matrix \mathbf{E}_{ik} , are too unwieldy to handle. Therefore we will consider a sequence of simplifying assumptions, in hopes that we do not lose all the solutions in the process.

Assumption A. Assume that \mathbf{P} is a circulant matrix, $\mathbf{P} = \mathbf{C}(\mathbf{p})$. As long as our plane of order q is desarguesian, there is no loss of generality in this. Moreover, it allows us to handle \mathbf{P}^t effectively.

Lemma 13 *If $\mathbf{P} = \mathbf{C}(p_0, \dots, p_{m-1})$, then $\mathbf{P}^t = \mathbf{C}(p_0, p_{m-1}, p_{m-2}, \dots, p_1)$, where $m = q^2 + q + 1$.*

Assumption B. Assume that \mathbf{M} is a circulant matrix, $\mathbf{M} = \mathbf{C}(\mathbf{f})$. This of course carries some loss of generality. Nonetheless, this class provides enough examples to keep us busy.

Assumption C. If \mathbf{M} is circulant, then we may take \mathbf{H} to be block-circulant:

$$\mathbf{H}_{ij} = \begin{cases} \mathbf{P} & \text{if } i = j, \\ \mathbf{F}_k & \text{if } j - i \equiv k \pmod{N} \text{ and } f_k = 1, \\ \mathbf{O} & \text{if } j - i \equiv k \pmod{N} \text{ and } f_k = 0, \end{cases}$$

where the matrices \mathbf{F}_k are unknown permutation matrices.

This tactic greatly reduces the number of equations to be considered: we may

fix $i = 0$ and just solve the equations $\sum_k \mathbf{H}_{0k} \mathbf{H}_{jk}^t = \mathbf{J}$ for $1 \leq j < N$. But there is an added benefit: the equations for j and $N - j$ are transposes of each other. (This is a straightforward calculation.) Thus, if we take \mathbf{H} to be block circulant as above, it suffices to solve the $\lceil \frac{N-1}{2} \rceil = \lfloor \frac{N}{2} \rfloor$ equations $\sum_k \mathbf{H}_{0k} \mathbf{H}_{jk}^t = \mathbf{J}$ for $1 \leq j \leq \lfloor \frac{N}{2} \rfloor$.

The cost is that we have introduced a lot of symmetry: the map $\varphi : h_{ij} \mapsto h_{i+m, j+m}$ where $m = q^2 + q + 1$ is an automorphism of the matrix \mathbf{H} , and hence of the corresponding projective plane. An automorphism of order N is not necessarily fatal to our attempt to construct a non-desarguesian plane of order n , but it is certainly a significant restriction.

If we want to construct a projective plane of non-prime-power order, then we should stop with (at most) the first three assumptions, and allow the permutation matrices \mathbf{F}_k to be arbitrary. However, in order to illustrate the general method, let us proceed and consider systems with an additional property.

Assumption D. Let $\mathbf{S} = \mathbf{C}(0100 \dots 0)$, corresponding to the cyclic permutation on $m = q^2 + q + 1$. Assume that $\mathbf{F}_k = \mathbf{S}^{x_k}$ when $f_k = 1$, where each x_k is an unknown with $0 \leq x_k < m$, and of course $\mathbf{F}_k = \mathbf{O}$ when $f_k = 0$.

Since desarguesian planes are also cyclic, with Assumption A this introduces additional symmetries, *viz.*, a cyclic automorphism ψ of order m which permutes the indices within the blocks of \mathbf{H} simultaneously. Moreover, ψ commutes with φ . The restrictions imposed by this assumption are significant, and will be discussed in the final section.

With Assumption D, the problem reduces to solving at least one member of a set of (possibly inconsistent) linear equations in \mathbb{Z}_{q^2+q+1} . The following lemma is crucial to our calculations.

Lemma 14 *Let $\mathbf{S} = \mathbf{C}(0100 \dots 0)$.*

- (1) $(\mathbf{S}^x)^t = \mathbf{S}^{-x}$.
- (2) \mathbf{S} commutes with circulant matrices:

$$\mathbf{S}\mathbf{C}(\mathbf{e}) = \mathbf{C}(\mathbf{e})\mathbf{S} = \mathbf{C}(e_{m-1}, e_0, e_1, \dots, e_{m-2}).$$

Now let us illustrate how these constructions work with several examples. We begin by reversing Bruck's decomposition of a desarguesian plane of order q^2 into subplanes of order q . For small values of q , at least, it is feasible to build a plane of order q^2 as a union of planes of order q , using the complete graph of type $\langle N, N - 1, \times, \times, N - 2 \rangle$. The construction of a plane of order 4 is perhaps too straightforward to be instructive, so we skip the case $q = 2$.

Example 1: Constructing planes of order 9 and 16. For $q = 3$, we

have $N = 7$. Thus $\mathbf{M} = \mathbf{C}(0111111)$, we may take $\mathbf{P} = \mathbf{C}(0110100000100)$, and $\mathbf{S} = \mathbf{C}(0100000000000)$. The matrix \mathbf{H} then has the block form $\mathbf{H} = \mathbf{C}(\mathbf{P}, \mathbf{S}^{x_1}, \mathbf{S}^{x_2}, \mathbf{S}^{x_3}, \mathbf{S}^{x_4}, \mathbf{S}^{x_5}, \mathbf{S}^{x_6})$. The equations we obtain from $\mathbf{H}\mathbf{H}^t = \mathbf{J}$ simplify to the requirement that the following three combinations all be equal to \mathbf{J} :

$$\begin{aligned} & \mathbf{P} + \mathbf{P}^t \mathbf{S}^{x_1+x_6} + \mathbf{S}^{2x_1-x_2} + \mathbf{S}^{x_1+x_2-x_3} + \mathbf{S}^{x_1+x_3-x_4} + \mathbf{S}^{x_1+x_4-x_5} + \mathbf{S}^{x_1+x_5-x_6} \\ & \mathbf{P} + \mathbf{P}^t \mathbf{S}^{x_2+x_5} + \mathbf{S}^{x_1+x_2-x_3} + \mathbf{S}^{2x_2-x_4} + \mathbf{S}^{x_2+x_3-x_5} + \mathbf{S}^{x_2+x_4-x_6} + \mathbf{S}^{x_2+x_6-x_1} \\ & \mathbf{P} + \mathbf{P}^t \mathbf{S}^{x_3+x_4} + \mathbf{S}^{x_3+x_1-x_4} + \mathbf{S}^{x_3+x_2-x_5} + \mathbf{S}^{2x_3-x_6} + \mathbf{S}^{x_3+x_5-x_1} + \mathbf{S}^{x_3+x_6-x_2}. \end{aligned}$$

Now, for $\mathbf{P} = \mathbf{C}(\mathbf{f})$, let $F = \{i : \mathbf{f}_i = 1\} = \{1, 2, 4, 10\}$. Likewise, for $\mathbf{P}^t = \mathbf{C}(\mathbf{g})$, let $G = \{i : \mathbf{g}_i = 1\} = \{3, 9, 11, 12\}$. Note that $F \cap G = \emptyset$, and let $R_0 = \mathbb{Z}_{13} - (F \cup G) = \{0, 5, 6, 7, 8\}$. Moreover, two translates of \mathbf{P}^t share this property: $\mathbf{P}^t \mathbf{S}^9$ and $\mathbf{P}^t \mathbf{S}^{10}$ have 1's in places disjoint from \mathbf{P} . If $\mathbf{P}^t \mathbf{S}^9 = \mathbf{C}(\mathbf{h})$, let $H = \{i : \mathbf{h}_i = 1\} = \{5, 7, 8, 12\}$, so that $R_9 = \mathbb{Z}_{13} - (F \cup H) = \{0, 3, 6, 9, 11\}$. Similarly, we obtain $R_{10} = \{3, 5, 7, 11, 12\}$.

To solve the first matrix equation, it is necessary and sufficient that $x_1 + x_6 \in \{0, 9, 10\}$ and $\{2x_1 - x_2, x_1 + x_2 - x_3, x_1 + x_3 - x_4, x_1 + x_4 - x_5, x_1 + x_5 - x_6\} = R_{x_1+x_6}$, with all calculations done modulo 13. To solve the second equation, we need $x_2 + x_5 \in \{0, 9, 10\}$ and $\{x_1 + x_2 - x_3, 2x_2 - x_4, x_2 + x_3 - x_5, x_2 + x_4 - x_6, x_2 + x_6 - x_1\} = R_{x_2+x_5}$. The third equation requires $x_3 + x_4 \in \{0, 9, 10\}$ and $\{x_3 + x_1 - x_4, x_3 + x_2 - x_5, 2x_3 - x_6, x_3 + x_5 - x_1, x_3 + x_6 - x_2\} = R_{x_3+x_4}$. There are three solution sets satisfying all three conditions, one of which is $x_1 = x_6 = 0$, $x_2 = x_5 = 5$, and $x_3 = x_4 = 11$. (The other solutions are similar).

The case $q = 4$ is also doable. We have $N = 13$, and we may take say $\mathbf{P} = \mathbf{C}(\mathbf{f})$ where $F = \{i : \mathbf{f}_i = 1\} = \{1, 4, 5, 10, 12\}$. Proceeding as above, we obtain six sets of equations modulo 21, one solution of which is $x_1 = x_{12} = 0$, $x_2 = x_{11} = 2$, and $x_3 = x_{10} = 9$, $x_4 = x_9 = 6$, $x_5 = x_8 = 14$, and $x_6 = x_7 = 20$.

For q larger, the computations become quite slow.

Example 3: Constructing planes of order 4, 7, 13, 16, 19 and 31 as unions of triangles. We may regard the triangle, with its adjacency matrix $\mathbf{P} = \mathbf{C}(011)$ satisfying $\mathbf{P}\mathbf{P}^t = \mathbf{I} + \mathbf{J}$, as a (degenerate) projective plane of order $q = 1$. If $n \equiv 1 \pmod{3}$, then 3 divides $n^2 + n + 1$. In that case, we can try to construct a projective plane of order n by gluing triangles over an ordinary graph of type $\langle N, n-1, a, b, \times \rangle$ where $N = \frac{n^2+n+1}{3}$, $a = 3$ or \times , and $b = 1$ or \times .

For $n = 4$, we can use $\mathbf{M} = \mathbf{C}(0110100)$ as an ordinary graph of type $\langle 7, 3, \times, 1, \times \rangle$. Of course, $\mathbf{S} = \mathbf{C}(010)$. The matrix \mathbf{H} then has the block form

$\mathbf{H} = \mathbf{C}(\mathbf{P}, \mathbf{S}^{x_1}, \mathbf{S}^{x_2}, \mathbf{O}, \mathbf{S}^{x_4}, \mathbf{O}, \mathbf{O})$. The equations we obtain from $\mathbf{H}\mathbf{H}^t = \mathbf{J}$ are

$$\begin{aligned}\mathbf{P} + \mathbf{S}^{2x_1-x_2} &= \mathbf{J} \\ \mathbf{P} + \mathbf{S}^{2x_2-x_4} &= \mathbf{J} \\ \mathbf{P} + \mathbf{S}^{2x_4-x_1} &= \mathbf{J}\end{aligned}$$

Thus we need $2x_1 - x_2 \equiv 2x_2 - x_4 \equiv 2x_4 - x_1 \equiv 0 \pmod{3}$, with the obvious solution $x_1 = x_2 = x_4 = 0$.

To construct a plane of order 7 as a union of triangles, we need an ordinary graph of type $\langle 19, 6, 3, 1, \times \rangle$. From Table 1, $\mathbf{M} = \mathbf{C}(010010110101000000)$ works. The matrix equations are

$$\begin{aligned}\mathbf{P} + \mathbf{S}^{x_1+x_6-x_7} &= \mathbf{J} \\ \mathbf{P} + \mathbf{S}^{x_4+x_7-x_{11}} &= \mathbf{J} \\ \mathbf{P} + \mathbf{S}^{x_9+x_{11}-x_1} &= \mathbf{J} \\ \mathbf{S}^{x_4-x_6} + \mathbf{S}^{x_7-x_9} + \mathbf{S}^{x_9-x_{11}} &= \mathbf{J} \\ \mathbf{S}^{x_1-x_4} + \mathbf{S}^{x_4-x_7} + \mathbf{S}^{x_6-x_9} &= \mathbf{J} \\ \mathbf{S}^{x_1-x_6} + \mathbf{S}^{x_4-x_9} + \mathbf{S}^{x_6-x_{11}} &= \mathbf{J}.\end{aligned}$$

Thus we need $x_1 + x_6 - x_7 \equiv x_4 + x_7 - x_{11} \equiv x_9 + x_{11} - x_1 \equiv 0 \pmod{3}$, and we need that each of the sets $\{x_4 - x_6, x_7 - x_9, x_9 - x_{11}\}$, $\{x_1 - x_4, x_4 - x_7, x_6 - x_9\}$, $\{x_1 - x_6, x_4 - x_9, x_6 - x_{11}\}$ is equivalent to $\{0, 1, 2\}$ modulo 3. There are two solutions, one of which is $x_4 = x_6 = x_9 = 0$ and $x_1 = x_7 = x_{11} = 1$.

Interestingly, for $n = 10$, we could not find an ordinary graph of the type $\langle 37, 9, 3, 1, \times \rangle$, which might still exist even though a plane of order 10 does not. (Neither have we proved that such a graph does not exist.) There is, however, a circulant ordinary graph of type $\langle 37, 9, 2, 2, \times \rangle$.

We were able to construct planes of orders 13, 16, 19 and 31 as unions of triangles; the results of the calculations are omitted. For $n \geq 19$, we searched for the ordinary graphs using a method which is not exhaustive and depends on $N = \frac{n^2+n+1}{3}$ being prime. This does not apply when $n = 25$, and produced no results for $n = 22$ and $n = 28$.

On the basis of this evidence, it seems reasonable to conjecture that if q is a prime power and $n \equiv 1 \pmod{3}$, then the desarguesian plane of order q has a decomposition into triangles. So far, we have been unable to prove this, either.

Example 3: Attempts to construct a plane of order $2q^2 + q + 1$. If q and $N = 4q^2 + 3$ are prime powers, then we can try to construct a plane of order $n = 2q^2 + q + 1$ using the quadratic residue tournament of order q^2 . The systems of equations we obtain in this case are again tractable. We will show that there is no solution when $q = 2^k$ ($k \geq 1$) and N is prime.

Assume that $N = 4q^2 + 3$ is prime. The quadratic residue tournament has a circulant matrix $\mathbf{M} = \mathbf{C}(\mathbf{f})$ with $f_i = 1$ if i is a nonzero quadratic residue in \mathbb{Z}_N . Let QR_N denote the set of nonzero quadratic residues modulo N . The matrix \mathbf{H} to be constructed is block-circulant of the form $\mathbf{C}(\mathbf{P}, \mathbf{F}_1, \dots, \mathbf{F}_{N-1})$ with $\mathbf{F}_i = \mathbf{S}^{x_i}$ when $i \in \text{QR}_N$, and \mathbf{O} when $i \notin \text{QR}_N$. Since $N \equiv 3 \pmod{4}$, we know that -1 is not a quadratic residue modulo N . Hence for each i , exactly one of \mathbf{F}_i and \mathbf{F}_{N-i} is nonzero.

If we consider the $\frac{N-1}{2} = 2q^2 + 1$ equations

$$\mathbf{P}\mathbf{F}_i^t + \mathbf{F}_1\mathbf{F}_{i+1}^t + \dots + \mathbf{F}_{N-1}\mathbf{F}_{N-1+i}^t = \mathbf{J}$$

where i is a nonzero quadratic residue, then we will have one of each pair of equivalent matrix equations, with no term \mathbf{P}^t involved. These equations simplify to

$$\mathbf{P} + \sum_{\substack{i+k \equiv j \pmod{N} \\ j, k \in \text{QR}_N}} \mathbf{S}^{x_i - x_j + x_k} = \mathbf{J}$$

for each fixed $i \in \text{QR}_N$.

Suppose the matrix $\mathbf{P} = \mathbf{C}(\mathbf{p})$ has 1's in positions b_1, \dots, b_{q+1} . Let $R = \mathbb{Z}_{q^2+q+1} - \{b_1, \dots, b_{q+1}\}$, and note that $|R| = q^2$. It suffices to find values in \mathbb{Z}_{q^2+q+1} for the $2q^2 + 1$ variables x_j so that, for each nonzero quadratic residue i , the q^2 expressions $x_i - x_j + x_k$ with $i + k \equiv j \pmod{N}$ and $j, k \in \text{QR}_N$ take on each of the values of R exactly once.

Let us formalize this. Let X_N denote the set of variables x_i where i is a nonzero quadratic residue modulo N , and for each such i let T_i be the corresponding set of expressions $x_i - x_j + x_k$ with $i + k \equiv j \pmod{N}$. We seek a map $\varphi : X_N \rightarrow \mathbb{Z}_{q^2+q+1}$ such that $\varphi(T_i) = R$ for every $i \in \text{QR}_N$.

If $i \neq k$, then the expression $x_i - x_j + x_k$ occurs twice, once in T_i and once in T_k . However, when 2 is a quadratic residue modulo N , then the expression $2x_i - x_j$ occurs only once (in T_i), while if 2 is a not quadratic residue the expression $2x_i - x_j$ does not occur at all. Recall that, for p prime, 2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $7 \pmod{8}$. Now $N = 4q^2 + 3 \equiv 3 \pmod{8}$ when q is even, i.e., $q = 2^k$, and $N \equiv 7 \pmod{8}$ when q is odd. Let us show that no solution exists in the former case.

Lemma 15 *If $q = 2^k$ and N is prime, then there is no map $\varphi : X_N \rightarrow \mathbb{Z}_{q^2+q+1}$ such that $\varphi(T_i) = R$ for every $i \in \text{QR}_N$.*

PROOF. There are $2q^2 + 1$ nonzero quadratic residues modulo N . Since each T_i contains q^2 expressions and each expression occurs twice, $\bigcup_i T_i$ contains $\frac{1}{2}(2q^2 + 1)q^2$ expressions. Now $\bigcup_i \varphi(T_i)$ takes on the q^2 values of R . By the pigeonhole principle, there exists an $r \in R$ such that $|\varphi^{-1}(r)| > q^2$, and hence

$|\varphi^{-1}(r)| \geq q^2 + 1$. The expressions in $\varphi^{-1}(r)$ occur in two T_i 's each, for a total of at least $2q^2 + 2$ times. Hence there is an i_0 such that T_{i_0} contains at least two expressions in $\varphi^{-1}(r)$, so that $\varphi(T_{i_0}) \neq R$. \square

We conclude that the special construction we have described does not work in these cases.

Theorem 16 *Let $q = 2^k$ with $k \geq 1$, and let $n = 2q^2 + q + 1$. Assume that $N = 4q^2 + 3$ is prime. Then there is no choice of integers $x_i \in \mathbb{Z}_{q^2+q+1}$ for $i \in \text{QR}_N$ such that the block-circulant matrix $\mathbf{C}(\mathbf{P}, \mathbf{F}_1, \dots, \mathbf{F}_{N-1})$ is the incidence matrix of a projective plane, where \mathbf{P} is a circulant incidence matrix for a plane of order q , and $\mathbf{F}_i = \mathbf{S}^{x_i}$ when $i \in \text{QR}_N$, and $\mathbf{F}_i = \mathbf{O}$ when $i \notin \text{QR}_N$.*

In particular, this applies when $q = 2$, $n = 11$, $N = 19$ and when $q = 4$, $n = 37$, $N = 67$. It also applies for $q = 2^k$ with $k = 5, 7, 8, 13$ and 14 . The proof can be modified to include the case where N is a prime power, but we do not know whether that ever actually occurs.

For q odd, we have no general theorem. However, the considerations in the next section show that the above construction fails when N is a prime power, $n < 2,000,000$ and n is not a prime power.

5 Modifications required to construct nondesarguesian planes

The examples we have constructed so far are all desarguesian. In fact, Assumptions A, B, C and D together virtually ensure that this will be the case. The authors would like to thank Dean Crnković and Mario-Osvin Pavčević for pointing out to us the nature of these difficulties, which are due to the following elementary result.

Theorem 17 *Let $\mathbf{H} = (\mathbf{H}_{ij})$ for $0 \leq i, j < N$ be a block-circulant matrix which is the incidence matrix of a symmetric block design. If each \mathbf{H}_{ij} is a circulant $m \times m$ matrix, then \mathbf{H} can be represented as a difference set on the abelian group $\mathbb{Z}_N \times \mathbb{Z}_m$.*

PROOF. The hypotheses mean that there is an array $\mathbf{e} = (e_{rs} : r < N, s < m)$ such that $h_{mi+k, mj+\ell} = e_{(j-i) \bmod N, (\ell-k) \bmod m}$. Then $\mathbb{Z}_N \times \mathbb{Z}_m$ acts on the index set $0, \dots, mN - 1$ via

$$\alpha_{(a,b)}(mi + k) = m((a + i) \bmod N) + ((b + k) \bmod m).$$

It is straightforward to check that the action is regular and each $\alpha_{(a,b)}$ is an automorphism. \square

Section 8 of D. Jungnickel's survey [9] gives a good summary of the difficulties of constructing nondesarguesian planar abelian difference sets. Following Jungnickel, we note that there are three main conjectures about how these things work.

Conjecture 18 *Any finite projective plane admitting a Singer group is desarguesian. (A Singer group is a group of automorphisms which is regular on the points and lines of a plane.)*

Conjecture 19 *If there is an abelian planar difference set of order n , then n is a prime power.*

Conjecture 20 *Any abelian planar difference set is cyclic.*

Note that the latter two conjectures would be a consequence of the first. There is substantial evidence supporting these conjectures. The following results are especially relevant.

Theorem 21 *Let \mathbf{P} be a finite projective plane with a Singer group G . Then either \mathbf{P} is desarguesian or G is a normal subgroup of $\text{Aut } \mathbf{P}$.*

Theorem 22 *All cyclic planes of order m or m^2 with $m \leq 9$ are desarguesian.*

Theorem 23 *Every abelian difference set of order $n < 2,000,000$ has prime power order.*

Theorem 21 is due to U. Ott [11], Theorem 22 is due to R. Bruck [2], and Theorem 23 is a result of D. Gordon [4] extending earlier work of Keiser, Evans and Mann.

With respect to the more general conjecture that the order of any finite projective plane must be a prime power, we have the following recent result of A. Blokhuis, D. Jungnickel and B. Schmidt [1].

Theorem 24 *If a projective plane of order n has an abelian collineation group of order n^2 , then n is a prime power.*

Clearly, our future investigations should eliminate some of the Assumptions from Section 4. Also, much work remains to be done on the existence of ordinary matrices of various types.

References

- [1] A. Blokhuis, D. Jungnickel and B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2 , *Proc. Amer. Math. Soc.* 130 (2002), 1473–1476.
- [2] R. H. Bruck, Quadratic extensions of cyclic planes, in: *Proc. Symp. Appl. Math.*, Vol. 10 (Amer. Math. Soc., Providence, R.I., 1960), 15–44.
- [3] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. J. Math.* 1 (1949), 88–93.
- [4] D. Gordon, The prime power conjecture is true for $n < 2,000,000$, *Electron. J. Combin.* 1 (1994), Research Paper 6.
- [5] M. Hall, Jr., *Theory of Groups* (Macmillan, New York, 1959).
- [6] M. Hall, Jr., *Combinatorial Theory* (Blaisdell Publishing Co., Waltham MA, 1967).
- [7] C. Y. Ho, Characterization of projective planes of small prime orders, *J. Combin. Theory Ser. A* 41 (1986), 189–220.
- [8] K. Horvatić-Baldasar, E. Kramer and I. Matulić-Bedenić, On a projective plane of order 11 with Frobenius group of order 21, *Rad. Mat.* 6 (1990), 71–76.
- [9] D. Jungnickel, Difference Sets, in: *Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. Stinson, eds. (Wiley, New York, 1992), 241–324.
- [10] J. Kalk, Ordinary graphs with $a = 0$, manuscript, 2002.
- [11] U. Ott, Endliche zyklische Ebenen, *Math. Z.* 144 (1975), 195–215.
- [12] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* 12 (1933), 311–320.
- [13] K. B. Reid and E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices, *J. Combin. Theory Ser. A* 12 (1972), 431–560.
- [14] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, in: *Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. Stinson, eds. (Wiley, New York, 1992), 241–324.
- [15] H. J. Ryser, A note on a combinatorial problem, *Proc. Amer. Math. Soc.* 1 (1950), 422–424.
- [16] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* 43 (1938), 377–385.
- [17] P. Yff, On subplane partitions of a finite projective plane, *J. Combin. Theory Ser. A* 22 (1977), 118–122.
- [18] P. Yff, A subplane partition of the cyclic plane of order 81, *Arab J. Math.* 1 (1980), 32–37.