On describing the incidence matrix of a finite projective plane via orthogonal latin squares and via a digraph complete set of latin squares

Claude Levesque

Département de Mathématiques et de Statistique
Université Laval, Québec, Canada G1K 7P4
cl@mat.ulaval.ca

Dedicated to professor Mirka Miller on the occasion of her birthday

Abstract. A fast direct method for obtaining the incidence matrix of a finite projective plane of order n via $n-1$ mutually orthogonal $n \times n$ latin squares is described. Conversely, $n-1$ mutually orthogonal $n \times n$ latin squares are directly exhibited from the incidence matrix of a projective plane of order n. A projective plane of order n can also be described via a digraph complete set of latin squares and a new procedure for doing it will also be described.

1. Introduction

A **projective plane** Π **of order** n consists of a collection $\{\wp_1, \wp_2, \ldots, \wp_{n^2+n+1}\}$ of *points* together with a collection $\{\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_{n^2+n+1}\}$ of *lines* subject to the following three axioms (see p. 89 of [R]):

(A1) *Any two distinct points of Π are on one and only one common line of Π.*

(A2) *Any two distinct lines of Π pass through one and only one common point of Π.*

(A3) *There exist four distinct points of Π, no three of which are on the same line.*

The third axiom garantees that one does not deal with a degenerating projective plane with only one line, and allows to define a projective plane of order n without specifying that in practice there are n^2+n+1 points and n^2+n+1 lines.

The **incidence matrix** of Π will be a $(n^2+n+1) \times (n^2+n+1)$ matrix $\mathbf{F}$ where the (i,j) element of $\mathbf{F}$ is defined by

$$\mathbf{F}(i,j) = \begin{cases} 1 \text{ if } \wp_i \text{ is on } \mathcal{L}_j \text{ (namely, } \mathcal{L}_j \text{ is incident with } \wp_i), \\ 0 \text{ if } \wp_i \text{ is not on } \mathcal{L}_j \text{ (namely, } \mathcal{L}_j \text{ is not incident with } \wp_i). \end{cases}$$

This matrix reflects the facts that on each line there are exactly $n+1$ points and through each point pass exactly $n+1$ lines. Our definition of $\mathbf{F}$ corresponds to the definition of $\mathbf{F}^t$ (the transpose of $\mathbf{F}$) given on page 286 of [D-K].

Before describing the content of the next sections, let us recall some definitions.

A **latin square of order** n, also called a $n \times n$ *latin square*, is a matrix A whose entries come from a set S of n elements no two of which appear on the same row nor on the same column. In this paper, we will take $S = \{1, 2, \ldots, n\}$.

Two $n \times n$ latin squares A, B are said to be **mutually orthogonal** if the cardinality of the set of couples $\{(A(i,j), B(i,j)) : 1 \leq i,j \leq n\}$ is exactly n^2.

A **digraph complete set** of $n \times n$ latin squares is a set of $n-1$ latin squares $D_1, D_2, \ldots, D_{n-1}$ having the following property: *For all* $r, s \in \{1, 2, \ldots, n\}$ *with* $r \neq s$, *the set of couples*

$$\{(\overline{\mathbf{D}}(i,r),\, \overline{\mathbf{D}}(i,s)) : 1 \leq i \leq n-1\}$$

obtained from the r-th and the s-th columns of the $(n^2-n) \times n$ *matrix*

$$\overline{\mathbf{D}} = \begin{pmatrix} D_1 \\ D_2 \\ \vdots \\ D_{n-1} \end{pmatrix}$$

is of cardinality $n^2 - n$ *(and excludes the set* $\{(j,j) : 1 \leq j \leq n\}$ *).*

It is known that out of a set of $n-1$ mutually orthogonal latin squares one can construct a digraph complete set of latin squares. Vice-versa, from a digraph complete set of latin squares, one can construct a set of $n-1$ mutually orthogonal latin squares. See page 289 of [D-K].

The first purpose of this paper is to exhibit a mechanical way of obtaining directly the *incidence matrix* of a finite projective plane of order n from $n-1$ mutually orthogonal $n \times n$ latin squares. As a matter of fact, given the incidence matrix of a finite projective plane of order n, we can reverse the above procedure and exhibit directly $n-1$ mutually orthogonal $n \times n$ latin squares. This is the content of Chapter 2.

The second purpose of this paper is to describe (in Chapter 3) a new direct method for exhibiting a digraph complete set of latin squares from the incidence matrix of a projective plane, and to give a procedure for doing the converse. The method is slightly different from the one described in pages 286-291 of [D-K], the latter method involving computations of permutation matrices.

Note in passing that the lines of a finite projective plane of order n can be used to form an error correcting code $\mathcal{C}$; see Section 10.1 of [D-K]. Unfortunately, it is an open problem to describe the integers n for which finite projective planes of order n do exist, though some mathematicians conjecture that they exist if and only if n is a power of a prime.

In this paper, different matrices come into play:

- I_m is the $m \times m$ identity matrix;
- $A_1, A_2, \ldots, A_{n-1}$ are $n \times n$ matrices;
- $D_1, D_2, \ldots, D_{n-1}$ are $n \times n$ matrices;
- $\mathcal{C}_j$ is a $n \times n$ matrix with 1's in its j-th column and 0 elsewhere (for $1 \leq j \leq n$);
- D_0 is the $n \times n$ matrix whose i-th row, for $i = 1, \ldots, n$, is $(i\ i\ \ldots\ i)$;
- $\mathcal{P}_{ij}$ is a $n \times n$ permutation matrix (for $1 \leq i, j \leq n$);
- $\mathbf{M}, \mathbf{M}^{(1)}, \mathbf{M}^{(2)}, \ldots, \mathbf{M}^{(n)}$ are $n^2 \times (n+1)$ matrices;
- $\widetilde{\mathbf{M}}, \widetilde{\mathbf{M}}^{(1)}, \widetilde{\mathbf{M}}^{(2)}, \ldots, \widetilde{\mathbf{M}}^{(n)}$ are $n^2 \times (n+1)$ matrices;
- $\mathbf{D}, \mathbf{D}^{(1)}, \mathbf{D}^{(2)}, \ldots, \mathbf{D}^{(n)}$ are $n^2 \times n$ matrices;
- $\widetilde{\mathbf{D}}, \widetilde{\mathbf{D}}^{(1)}, \widetilde{\mathbf{D}}^{(2)}, \ldots, \widetilde{\mathbf{D}}^{(n)}$ are $n^2 \times n$ matrices;
- $\overline{\mathbf{D}}$ is a $(n^2 - n) \times n$ matrix;
- $\mathbf{F}$, $\mathbf{G}$, $\mathbf{H}$ are $(n^2+n+1) \times (n^2+n+1)$ matrices;
- $\overline{\mathbf{F}}$ is a $n^2 \times (n^2+n)$ matrix.

Moreover, the (i,j) element of a matrix N is denoted $N(i,j)$. It will not be denoted N_{ij} to avoid some conflicts with the n^2 permutation matrices $\mathcal{P}_{ij}$ involving a double set of indices (and coming into play out of $n!$ possible permutations).

§2. Incidence matrix via orthogonal latin squares

Let us define the notion of **matriarchal matrix.**

Definition. Let $n \geq 2$ and $s \geq 1$. A $n^2 \times s$ matrix $\mathbf{M}$ is called a *matriarchal matrix* if the entries in the rows of the first two columns form n^2 different couples in lexicographic order, and if the rows of each $n^2 \times 2$ submatrix of $\mathbf{M}$ are the n^2 couples of $\{(i,j) : 1 \leq i, j \leq n\}$.

We shall say that the $n^2 \times s$ matriarchal matrix $\mathbf{M}$ is *attached to s mutually orthogonal latin squares $A_1, \ldots, A_s$ of order n* (with $1 \leq s \leq n-1$), if the entries in the rows of the first two columns of $\mathbf{M}$ are in lexicographic order and if for $j = 1, \ldots, s$, the $(j+2)$-th column of $\mathbf{M}$ is the concatenation of the rows of A_j. In other words, the row of $\mathbf{M}$ containing the couple (i,j) in the first two columns will then contain the (i,j) element of respectively $A_1, \ldots, A_s$ in that row. This matrix $\mathbf{M}$ can be found on page 82 of [R].

Example. Let $n = 4$. To the orthogonal latin squares

$$A_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

is attached the *matriarchal matrix*

$$
\mathbf{M} = \left(\begin{array}{cc||c||c||c}
1 & 1 & 1 & 1 & 1 \\
1 & 2 & 2 & 2 & 2 \\
1 & 3 & 3 & 3 & 3 \\
1 & 4 & 4 & 4 & 4 \\
\cline{3-5}
2 & 1 & 2 & 3 & 4 \\
2 & 2 & 1 & 4 & 3 \\
2 & 3 & 4 & 1 & 2 \\
2 & 4 & 3 & 2 & 1 \\
\cline{3-5}
3 & 1 & 3 & 4 & 2 \\
3 & 2 & 4 & 3 & 1 \\
3 & 3 & 1 & 2 & 4 \\
3 & 4 & 2 & 1 & 3 \\
\cline{3-5}
4 & 1 & 4 & 2 & 3 \\
4 & 2 & 3 & 1 & 4 \\
4 & 3 & 2 & 4 & 1 \\
4 & 4 & 1 & 3 & 2
\end{array}\right).
$$

Remark. Let $\mathbf{F}$ be the incidence matrix of a finite projective plane. Suppose that $\mathbf{F}'$ is the matrix obtained from $\mathbf{F}$ by interchanging two rows or two columns. Then $\mathbf{F}'$ is still the incidence matrix of some finite projective plane of order n. A series of such exchanges of rows and columns on $\mathbf{F}$ will be called a reordering of the rows and columns of $\mathbf{F}$.

The first main result of this paper is the following one.

Theorem 2.1. **(1)** *Suppose there exist $n-1$ mutually orthogonal latin squares $A_1, A_2, \dots, A_{n-1}$, of order n, and let $\mathbf{M}$ be the matriarchal matrix attached to $A_1, \dots, A_{n-1}$. For $j = 1, \dots, n$, let $\mathbf{M}^{(j)}$ be the matrix obtained from $\mathbf{M}$ by writing 1 in place of j and 0 elsewhere. Suppose that $\mathbf{0}$ is a column of 0's, $\mathbf{1}$ is a column of 1's, and I_{n+1} is the $(n+1)\times(n+1)$ identity matrix. Then the $(n^2+n+1)\times(n^2+n+1)$ matrix*

$$
\mathbf{F} = \left(\begin{array}{cccc|c}
\mathbf{M}^{(1)} & \mathbf{M}^{(2)} & \dots & \mathbf{M}^{(n)} & \mathbf{0} \\
\hline
I_{n+1} & I_{n+1} & \cdots & I_{n+1} & \mathbf{1}
\end{array}\right)
$$

is the incidence matrix of a finite projective plane Π of order n.

(2) *Conversely, let $\mathbf{F}$ be the incidence matrix of a finite projective plane Π of order n and without loss of generality suppose that (after some eventual interchanges of rows and columns) there exist blocks $\mathbf{M}^{(1)}$, $\mathbf{M}^{(2)}, \dots$, $\mathbf{M}^{(n)}$ such that $\mathbf{F}$ is defined by*

$$
\mathbf{F} = \left(\begin{array}{cccc|c}
\mathbf{M}^{(1)} & \mathbf{M}^{(2)} & \dots & \mathbf{M}^{(n)} & \mathbf{0} \\
\hline
I_{n+1} & I_{n+1} & \cdots & I_{n+1} & \mathbf{1}
\end{array}\right)
$$

For $j = 1, \dots, n$, let $\widetilde{\mathbf{M}}^{(j)}$ be the matrix obtained from $\mathbf{M}^{(j)}$ by writing j in place of 1. Then an eventual reordering of the rows of

$$
\widetilde{\mathbf{M}} = \widetilde{\mathbf{M}}^{(1)} + \widetilde{\mathbf{M}}^{(2)} + \dots + \widetilde{\mathbf{M}}^{(n)}
$$

gives a matriarchal matrix **M** *attached to* $n-1$ *mutually orthogonal latin squares of order* n. **Example.** Let $n = 4$. Consider the three mutually

orthogonal latin squares A_1, A_2, A_3 of the preceding example, and the matriarchal matrix **M** attached to them. Then the matrices $\mathbf{M}^{(1)}$, $\mathbf{M}^{(2)}$, $\mathbf{M}^{(3)}$, $\mathbf{M}^{(4)}$ are defined by

$$\mathbf{M}^{(1)} = \begin{pmatrix} 1&1&1&1&1\\ 1&0&0&0&0\\ 1&0&0&0&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&1&0&0&0\\ 0&0&0&0&1\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&0&1&0&0 \end{pmatrix}, \mathbf{M}^{(2)} = \begin{pmatrix} 0&0&0&0&0\\ 0&1&1&1&1\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 1&0&1&0&0\\ 1&1&0&0&0\\ 1&0&0&0&1\\ 1&0&0&1&0\\ 0&0&0&0&1\\ 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&1 \end{pmatrix}, \mathbf{M}^{(3)} = \begin{pmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&1&1&1&1\\ 0&0&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 1&0&1&0&0\\ 1&0&0&1&0\\ 1&1&0&0&0\\ 1&0&0&0&1\\ 0&0&0&0&1\\ 0&0&1&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0 \end{pmatrix}$$

$$\mathbf{M}^{(4)} = \begin{pmatrix} 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&1&1&1&1\\ 0&0&0&0&1\\ 0&0&0&1&0\\ 0&0&1&0&0\\ 0&1&0&0&0\\ 0&0&0&1&0\\ 0&0&1&0&0\\ 0&0&1&0&1\\ 0&1&0&0&0\\ 1&0&1&0&0\\ 1&0&0&0&1\\ 1&0&0&1&0\\ 1&1&0&0&0 \end{pmatrix},$$

whereupon one can build the incidence matrix

$$\mathbf{F} = \left(\begin{array}{cccc|c} \mathbf{M}^{(1)} & \mathbf{M}^{(2)} & \mathbf{M}^{(3)} & \mathbf{M}^{(4)} & \mathbf{0} \\ \hline I_5 & I_5 & I_5 & I_5 & \mathbf{1} \end{array} \right),$$

namely

$$
\mathbf{F} = \left(\begin{array}{ccccc|ccccc|ccccc|ccccc||c}
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0\\
0&1&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&1&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&0&1&0&1&0&0&0&1&0&1&0&0&0&0&0&1&0&0&0\\
0&0&0&0&1&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&1&0&1&0&0&0&1&0&0&1&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&1&0&0&0&1&0&1&0&0&0&0\\
0&1&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&1&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&1&0\\
0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&1&1&0&0&0&0\\
\hline\hline
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&1\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1
\end{array}\right).
$$

The procedure can be reversed: from $\mathbf{F}$ extract $\mathbf{M}^{(1)}$, $\mathbf{M}^{(2)}$, $\mathbf{M}^{(3)}$, $\mathbf{M}^{(4)}$; consider $\widetilde{\mathbf{M}}^{(1)}$, $\widetilde{\mathbf{M}}^{(2)}$, $\widetilde{\mathbf{M}}^{(3)}$, $\widetilde{\mathbf{M}}^{(4)}$; build $\widetilde{\mathbf{M}} = \widetilde{\mathbf{M}}^{(1)} + \widetilde{\mathbf{M}}^{(2)} + \widetilde{\mathbf{M}}^{(3)} + \widetilde{\mathbf{M}}^{(4)}$ and an eventual reordering of the rows of $\widetilde{\mathbf{M}}$ leads to a matriarchal matrix $\mathbf{M}$ out of which one can extract 3 mutually orthogonal 4×4 latin squares.

Proof of Theorem 2.1. Part (1). Let us consider a set of points $\{\wp_1,\ \wp_2, \dots,\ \wp_{n^2+n+1}\}$ and a set of lines $\{\mathcal{L}_1,\ \mathcal{L}_2, \dots, \mathcal{L}_{n^2+n+1}\}$ containing some points according to the rule that for $1 \le i, j \le n^2 + n + 1$ we have

$$\wp_i \in \mathcal{L}_j \iff \mathbf{F}(i,j) = 1.$$

We want to prove that these $n^2 + n + 1$ points and these $n^2 + n + 1$ lines will form a projective plane of order n.

Consider first the $n^2 \times (n^2 + n)$ submatrix

$$\overline{\mathbf{F}} = \left(\mathbf{M}^{(1)}\,\mathbf{M}^{(2)}\,\dots\,\mathbf{M}^{(n)}\right)$$

of $\mathbf{F}$. The integer 1 will appear exactly n times in each column of $\overline{\mathbf{F}}$ (since each integer of $\{1, 2, \dots, n\}$ occurs n times in any column of $\mathbf{M}$) and $n + 1$ times in each row of $\mathbf{F}$ (since each row of $\mathbf{M}$ has $n + 1$ entries). Therefore 1 appears $n + 1$ times in each row of $\mathbf{F}$ and $n + 1$ times in each column of $\mathbf{F}$. To prove that $\mathbf{F}$ is the incidence matrix of a finite projective plane, there are three axioms to verify. It will prove useful to use the disjoint sets $\mathcal{S}$ and $\mathcal{T}$ of points defined by

$$\mathcal{S} = \{\wp_1, \wp_2, \ldots, \wp_{n^2}\}, \qquad \mathcal{T} = \{\wp_{n^2+1}, \wp_{n^2+2}, \ldots, \wp_{n^2+n+1}\}.$$

First axiom. In order to verify the first axiom, we must prove that two distinct points of Π are on one and only one line of Π.

It is clear that any pair of points of $\mathcal{T}$ are on $\mathcal{L}_{n^2+n+1}$ and only on $\mathcal{L}_{n^2+n+1}$. It is also clear that a point $\wp_i$ of $\mathcal{S}$ and a point $\wp_{n^2+j}$ of $\mathcal{T}$ are on and only on the line $\mathcal{L}_{j+(t-1)(n+1)}$ whose index is determined by the unique value of t verifying $\mathbf{M}(i,j) = t$, i.e., $\mathbf{M}^{(t)}(i,j) = \mathbf{F}(i, j+(t-1)(n+1)) = 1$.

Finally, consider a pair $\wp_i$ and $\wp_j$ of points of $\mathcal{S}$ with, say, $i < j$. If there exists $s \in \{1, 2, \ldots, n\}$ such that $i, j \in \{(s-1)n+1, (s-1)n+2, \ldots, (s-1)n+n\}$, then it is clear that $\wp_i$ and $\wp_j$ are on and only on the line $\mathcal{L}_{(s-1)(n+1)+1}$. Moreover, if $i \equiv j \pmod n$, then $\wp_i$ and $\wp_j$ are on and only on the line $\mathcal{L}_{(s-1)(n+1)+2}$ where $s \in \{1, 2, \ldots, n\}$ verifies $s \equiv i \equiv j \pmod n$.

Let us consider now the case when the indices i of $\wp_i$ and j of $\wp_j$ satisfy none of the last two properties. We want to prove that there exists a line $\mathcal{L}_t$ with $t \not\equiv 1, 2 \pmod{n+1}$ which has the property that $\wp_i$ and $\wp_j$ are on $\mathcal{L}_t$. Suppose that there is no such line. This means that for $s = 1, \ldots, n-1$, the elements $(i, s+2)$ and $(j, s+2)$ of the matrix $\mathbf{M}$ are different from k for all $k \in \{1, 2, \ldots, n\}$. Since for $s = 1, 2, \ldots, n-1$, the $(2+s)$-th column of $\mathbf{M}$ is made up with the concatenation of the rows of the latin square A_s and since $|i-j| > n$ with $i \not\equiv j \pmod n$, we get a contradiction. In other words, there exists $k \in \{1, 2, \ldots, n\}$ such that for some $s \in \{1, 2, \ldots, n-1\}$, we have $\mathbf{M}(i, 2+s) = \mathbf{M}(j, 2+s) = k$, i.e.,

$$\begin{aligned} \mathbf{M}^{(k)}(i, 2+s) &= \mathbf{M}^{(k)}(j, 2+s) = \mathbf{F}(i, 2+s+(k-1)(n+1)) \\ &= \mathbf{F}(j, 2+s+(k-1)(n+1)) = 1, \end{aligned}$$

whereupon $\wp_i$ and $\wp_j$ are on the line $\mathcal{L}_{2+s+(k-1)(n+1)}$.

Let us prove now that two distinct points of $\mathcal{S}$ cannot be on two different lines of Π. Suppose the contrary, i.e., suppose that there exist i, j, r, s with $i < j$, $r < s$, such that $\mathbf{F}(i,r) = \mathbf{F}(i,s) = \mathbf{F}(j,r) = \mathbf{F}(j,s) = 1$:

	...	$\mathcal{L}_r$	...	$\mathcal{L}_s$	...
$\wp_i$	...	1	...	1	...
$\vdots$		$\vdots$		$\vdots$	
$\wp_j$	...	1	...	1	...

Table

It means that there are two different columns of $\mathbf{M}$ in which for some u, $v \in \{1, 2, \ldots, n\}$ (not necessarily distinct) the couple (u, v) appears in row

i and in row j; this is a contradiction to either the property of having latin squares (when $u = v$) or to the orthogonality hypothesis (when $u \neq v$). In conclusion, two distinct points of S are on one and only one line of Π. This secures the first axiom.

Second axiom. In order to verify the second axiom, we must prove that two distinct lines of Π pass through one and only one point of Π.

It is clear that the line $\mathcal{L}_{t+(s-1)(n+1)}$ of Π, with $1 \leq t \leq n+1$, $1 \leq s \leq n-1$, and the line $\mathcal{L}_{n^2+n+1}$ have only the point $\wp_{n^2+t}$ in common.

Let us prove now that the lines $\mathcal{L}_{i+(s-1)(n+1)}$ and $\mathcal{L}_{j+(s-1)(n+1)}$ with $1 \leq i < j \leq n+1$ have at least one point in common. Those two lines, which are connected to the matrix $\mathbf{M}^{(s)}$, have in common the point $\wp_u$ where u is the index of the row in which the couple (s, s) appears in the i-th and the j-th columns. This is in fact the only point in common. Suppose that on the contrary there is another point. Then for some u and v with $1 \leq u < v \leq n^2$, we have in the matrix $\mathbf{M}^{(s)}$ the following:

	$\cdots$	$\mathcal{L}_{i+(s-1)(n+1)}$	$\cdots$	$\mathcal{L}_{j+(s-1)(n+1)}$	$\cdots$
$\wp_u$	$\cdots$	1	$\cdots$	1	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
$\wp_v$	$\cdots$	1	$\cdots$	1	$\cdots$

Table

This contradicts the first axiom.

Let us prove now that for $i \neq j$ the lines $\mathcal{L}_{i+(s-1)(n+1)}$ and $\mathcal{L}_{j+(t-1)(n+1)}$, with $s \neq t$, have at least one point in common. Those two lines come respectively from the blocks $\mathbf{M}^{(s)}$ and $\mathbf{M}^{(t)}$ and the point is $\wp_u$ where u is the index of the row in which the couple (s, t) appears in the i-th column and the j-th column of $\mathbf{M}^{(s)}$ and $\mathbf{M}^{(t)}$ respectively. As a matter of fact, it is the only point in common, since otherwise for some u and v with $1 \leq u < v \leq n^2$, we have in the blocks $\mathbf{M}^{(s)}$ and $\mathbf{M}^{(t)}$ the following contradiction:

	$\cdots$	$\mathcal{L}_{i+(s-1)(n+1)}$	$\cdots$	$\mathcal{L}_{j+(t-1)(n+1)}$	$\cdots$
$\wp_u$	$\cdots$	1	$\cdots$	1	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
$\wp_v$	$\cdots$	1	$\cdots$	1	$\cdots$

Table

Third axiom. Consider the four distinct lines

$$\begin{aligned}
\mathcal{L}_1 &= \{\wp_1,\ \wp_2,\ \wp_3, \dots,\ \wp_{n-1},\ \wp_n,\ \wp_{n^2+1}\},\\
\mathcal{L}_2 &= \{\wp_1,\ \wp_{n+1},\ \wp_{2n+1}, \dots,\ \wp_{n^2-2n+1},\ \wp_{n^2-n+1},\ \wp_{n^2+2}\},\\
\mathcal{L}_{n+2} &= \{\wp_{n+1},\ \wp_{n+2},\ \wp_{n+3}, \dots,\ \wp_{2n-1},\ \wp_{2n},\ \wp_{n^2+1}\},\\
\mathcal{L}_{n+3} &= \{\wp_2,\ \wp_{n+2},\ \wp_{2n+2}, \dots,\ \wp_{n^2-2n+2},\ \wp_{n^2-n+2},\ \wp_{n^2+2}\},
\end{aligned}$$

whose description is prescribed by the lexicographic order of the couples of each row of the first two columns of $\mathbf{M}$ and the definition of $\mathbf{M}^{(1)}$ and $\mathbf{M}^{(2)}$. We will show that the four points

$$\wp_1,\ \wp_2,\ \wp_{n+1},\ \wp_{n+2}$$

satisfy the third axiom. ¿From the matrix $\mathbf{F}$, one can extract the following pertinent information:

	$\mathcal{L}_1$	$\mathcal{L}_2$	$\dots$	$\mathcal{L}_{n+2}$	$\mathcal{L}_{n+3}$	$\dots$
$\wp_1$	1	1	$\dots$	0	0	$\dots$
$\wp_2$	1	0	$\dots$	0	1	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$	
$\wp_{n+1}$	0	1	$\dots$	1	0	$\dots$
$\wp_{n+2}$	0	0	$\dots$	1	1	$\dots$

Table

We will show that among the four points $\wp_1,\ \wp_2,\ \wp_{n+1},\ \wp_{n+2}$, no three of them belong to the same line. Suppose the contrary. Then there exists $r \neq 1, 2, n+1, n+2$, such that the line $\mathcal{L}_r$ contains

$$\begin{cases}
\text{either } \wp_1,\ \wp_2,\ \wp_{n+1}, & \text{whereupon } \wp_1,\ \wp_2 \text{ are on } \mathcal{L}_1 \text{ and } \mathcal{L}_r,\\
\text{or } \wp_1,\ \wp_2,\ \wp_{n+2}, & \text{whereupon } \wp_1,\ \wp_2 \text{ are on } \mathcal{L}_1 \text{ and } \mathcal{L}_r,\\
\text{or } \wp_1,\ \wp_{n+1},\ \wp_{n+2}, & \text{whereupon } \wp_{n+1},\ \wp_{n+2} \text{ are on } \mathcal{L}_{n+2} \text{ and } \mathcal{L}_r,\\
\text{or } \wp_2,\ \wp_{n+1},\ \wp_{n+2}, & \text{whereupon } \wp_{n+1},\ \wp_{n+2} \text{ are on } \mathcal{L}_{n+2} \text{ and } \mathcal{L}_r.
\end{cases}$$

In each of the four possibilities, we have a contradiction to the second axiom. The third axiom is now secured.

Part (2). This part simply reverses the process of Part (1). □.

3. Incidence matrix via a digraph complete set of latin squares

us first recall how J. Dénes and A.D. Keedwell [D-K] defined the canonical incidence matrix $\mathbf{G}$** of a projective plane Π of order hat Π has the following properties:

(A) *For $i = 1, \ldots, n+1$, $\wp_i$ is a point of $\mathcal{L}_1$ and $\mathcal{L}_i$ is a line through $\wp_1$.*
(B) *For all $k, j \in \{1, \ldots, n\}$, $\wp_{nk+j+1}$ is a point of $\mathcal{L}_{k+1}$ and $\mathcal{L}_{nk+j+1}$ passes through $\wp_{k+1}$.*

These two properties imply (see Section 8.5 of [D-K]) that the incidence matrix **G** can be written as

$$\mathbf{G} = \left(\begin{array}{c|c|cccc} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \hline \mathcal{C}_1 & \mathbf{0} & \mathcal{C}_1^t & \mathcal{C}_2^t & \ldots & \mathcal{C}_n^t \\ \hline \mathcal{C}_2 & \mathbf{0} & \mathcal{P}_{11} & \mathcal{P}_{12} & \ldots & \mathcal{P}_{1n} \\ \mathcal{C}_3 & \mathbf{0} & \mathcal{P}_{21} & \mathcal{P}_{22} & \ldots & \mathcal{P}_{2n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \mathcal{C}_n & \mathbf{0} & \mathcal{P}_{n-1,1} & \mathcal{P}_{n-1,2} & \ldots & \mathcal{P}_{n-1,n} \\ \mathbf{0} & \mathbf{1} & \mathcal{P}_{n1} & \mathcal{P}_{n2} & \ldots & \mathcal{P}_{nn} \end{array}\right) \qquad (1)$$

where **0** and **1** are respectively appropriate blocks of 0's and 1's, and where the following properties are satisfied:

(1) *For $i = 1, \ldots, n$, $\mathcal{C}_i$ is a $n \times n$ matrix with $1's$ in its i-th column and 0 elsewhere; moreover, $\mathcal{C}_i^t$ is the transpose of $\mathcal{C}_i$.*
(2) *For all $i, j \in \{1, \ldots, n\}$, the $n \times n$ matrix $\mathcal{P}_{ij}$ turns out to be some permutation matrix (i.e., $\mathcal{P}_{ij}$ has exactly one entry 1 in each row and in each column and has 0 elsewhere).*

Suppose now that we require that

(3) *for all $i, j \in \{1, \ldots, n\}$, $\mathcal{P}_{i1} = \mathcal{P}_{1j} = I_n$.*

Then **G** is called the **canonical incidence matrix** of a finite projective plane Π and we have the following:

(a) *For all $i, j \in \{2, \ldots, n\}$, $\mathcal{P}_{ij}$ has no entry 1 on its main diagonal.*
(b) *For all $i, r, s, k \in \{1, \ldots, n\}$ with $r \neq s$ and $i \geq 2$, the k-th rows (resp. columns) of $\mathcal{P}_{ir}$ and $\mathcal{P}_{is}$ are distinct.*
(c) *For all $i, r, s, m, k, t \in \{1, \ldots, n\}$ with $r \neq s$, $m \geq 2$ and $i \geq 2$, the k-th rows (resp. columns) of $\mathcal{P}_{ir}$ and $\mathcal{P}_{is}$ cannot be simultaneously identical to the t-th rows of $\mathcal{P}_{mr}$ and $\mathcal{P}_{ms}$ in that order.*

As explained in [D-K], the construction of a *digraph complete set* of latin squares is very simple and elegant: for $i = 2, \ldots, n$, take

$$D_{i-1} = (\mathcal{P}_{i1}T \quad \mathcal{P}_{i2}T \quad \ldots \quad \mathcal{P}_{in}T) \quad \text{with} \quad T = \begin{pmatrix} 1 \\ 2 \\ \vdots \\ n \end{pmatrix}.$$

In general, these latin squares $D_1, D_2, \ldots, D_{n-1}$ need not to be mutually orthogonal.

Examples. The 3×3 matrices

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

form a set of mutually orthogonal latin squares which is not a digraph complete set of latin squares. The 3×3 matrices

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

form a digraph complete set of latin squares which is not a set of mutually orthogonal latin squares.

In the rest of this section, we would like to describe another way of exhibiting a digraph complete set of latin squares from an incidence matrix of a projective plane.

Before proceeding, we need to define the notion of **basic incidence matrix H** of a projective plane Π of order n. First, suppose that Π verifies the following properties:

(a) *For $i = 1, \ldots, n$, $\mathcal{P}_i$ is a point of $\mathcal{L}_1$, and $\mathcal{L}_i$ is a line through $\mathcal{P}_1$; moreover, $\mathcal{P}_{n^2+n+1}$ is a point of $\mathcal{L}_1$ and $\mathcal{L}_{n+1}$ is a line through $\mathcal{P}_1$.*

(b) *For all $k, j \in \{1, \ldots, n\}$, $\mathcal{P}_{nk+j}$ is a point of $\mathcal{L}_{k+1}$ and $\mathcal{L}_{nk+j+1}$ passes through $\mathcal{P}_{k+1}$, except for $k = n$, where $\mathcal{L}_{n^2+j+1}$ passes through $\mathcal{P}_{n^2+n+1}$.*

This implies that **H** can be written as

$$\mathbf{H} = \left(\begin{array}{c||cccc||c} \mathbf{1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{1} \\ \hline \mathcal{C}_1 & \mathcal{C}_1^t & \mathcal{C}_2^t & \cdots & \mathcal{C}_n^t & \mathbf{0} \\ \hline \mathcal{C}_2 & \mathcal{P}_{11} & \mathcal{P}_{12} & \cdots & \mathcal{P}_{1n} & \mathbf{0} \\ \mathcal{C}_3 & \mathcal{P}_{21} & \mathcal{P}_{22} & \cdots & \mathcal{P}_{2n} & \mathbf{0} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \mathcal{C}_n & \mathcal{P}_{n-1,1} & \mathcal{P}_{n-1,2} & \cdots & \mathcal{P}_{n-1,n} & \mathbf{0} \\ \mathbf{0} & \mathcal{P}_{n1} & \mathcal{P}_{n2} & \cdots & \mathcal{P}_{nn} & \mathbf{1} \end{array}\right), \qquad (2)$$

where **1** is some judicious block of 1's, **0** is some judicious block of 0's, and where we have:

(1) *for* $i = 1, \ldots, n$, C_i *is a* $n \times n$ *matrix having only* 1*'s in its* i*-th column and* 0*'s elsewhere,* C_i^t *being the transpose of* C_i;

(2) *for all* $i, j \in \{1, \ldots, n\}$, $\mathcal{P}_{ij}$ *is a* $n \times n$ *permutation matrix (i.e.,* $\mathcal{P}_{ij}$ *has exactly one entry* 1 *in each row and in each column and* 0 *elsewhere).*

If we require that

(3) *for all* $i, j \in \{1, \ldots, n\}$, $\mathcal{P}_{i1} = \mathcal{P}_{nj} = I_n$,

then **H** is called a **basic incidence matrix.** If the weaker condition

(3′) *for all* $j \in \{1, \ldots, n\}$, $\mathcal{P}_{nj} = I_n$,

is satisfied, then **H** is called a **semi-basic incidence matrix.**

When **H** is a *basic incidence matrix of a projective plane of order* n, the following properties are satisfied:

(a) *For all* $i, r, s, k \in \{1, \ldots, n\}$, *with* $r \neq s$ *and* $i < n$, *the* k*-th rows of* $\mathcal{P}_{ir}$ *and* $\mathcal{P}_{is}$ *are distinct.*

(b) *For all* $i, r, s, m, k, t \in \{1, \ldots, n\}$, *with* $r \neq s$, $i \neq m$, $m < n$ *and* $i < n$, *the* k*-th rows of* $\mathcal{P}_{ir}$ *and* B_{is} *cannot be simultaneously identical to the* t*-th rows of* $\mathcal{P}_{mr}$ *and* $\mathcal{P}_{ms}$ *in that order.*

(c) *For all* $i \in \{1, \ldots, n-1\}$ *and for any* $j \in \{2, \ldots, n\}$, $\mathcal{P}_{ij}$ *has no entry* 1 *on its main diagonal.*

When **H** is semi-basic, the last properties (a) and (b) are satisfied. The matrix **G** in (1) and the matrix **H** in (2) are almost the same: the $(1+n)$-th column of **G** has been relocated to become the last column in **H**; eventually, some identity matrices have also been relocated. The nice feature of **H**, when we ignore its first row and its last column, is that we deal with $n \times n$ blocks.

Let us state now the second result of this paper.

Theorem 3.1. **(i)** *Suppose there exists a digraph complete set* $D_1, \ldots, D_{n-1}$ *of* $n \times n$ *latin squares. Let*

$$\mathbf{D} = \begin{pmatrix} D_0 \\ \hline D_1 \\ D_2 \\ \vdots \\ D_{n-1} \end{pmatrix}, \quad \textit{with} \quad D_0 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ \vdots & \vdots & & \vdots \\ n & n & \cdots & n \end{pmatrix},$$

and for $j = 1, \ldots, n$, *denote*

$$\mathbf{D}^{(j)} = \begin{pmatrix} D_0^{(j)} \\ \hline D_1^{(j)} \\ \vdots \\ D_{n-1}^{(j)} \end{pmatrix}$$

the matrix obtained from $\mathbf{D}$ *by writing* 1 *in place of* j *and* 0 *elsewhere, with the blocks* $\mathbf{D}^{(j)}$ *having a naturally inherited meaning. Define the* $n^2 \times n$ *matrix* $\mathbf{C}$ *by*

$$\mathbf{C} = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix},$$

where for $i = 1, \ldots, n$, C_i *is a* $n \times n$ *matrix having only* 1*'s in its* i*-th column and* 0*'s elsewhere. Then for some judiciously chosen blocks of* 0*'s and blocks of* 1*'s*

$$\mathbf{H} = \left(\begin{array}{c|cccc|c} 1 & 0 & 0 & \cdots & 0 & 1 \\ \hline \mathbf{C} & \mathbf{D}^{(1)} & \mathbf{D}^{(2)} & \cdots & \mathbf{D}^{(n)} & \mathbf{0} \\ \hline \mathbf{0} & I_n & I_n & \cdots & I_n & \mathbf{1} \end{array}\right)$$

is the semi-basic incidence matrix of a finite projective plane Π *of order* n. *If there are only entries* 1 *on the main diagonal of* D_i *for* $i = 1, \ldots, n-1$, *then* $\mathbf{H}$ *is basic.*

(ii) *Conversely, let* $\mathbf{H}$ *be the incidence matrix of a finite projective plane* Π *of order* n *and (without loss of generality) assume that there exist* $n^2 \times n$ *blocks* $\mathbf{D}^{(1)}, \mathbf{D}^{(2)}, \ldots, \mathbf{D}^{(n)}$ *such that for some judiciously chosen blocks of* 0*'s and blocks of* 1*'s, the* $(n^2+n+1) \times (n^2+n+1)$ *matrix*

$$\mathbf{H} = \left(\begin{array}{c|cccc|c} 1 & 0 & 0 & \cdots & 0 & 1 \\ \hline \mathbf{C} & \mathbf{D}^{(1)} & \mathbf{D}^{(2)} & \cdots & \mathbf{D}^{(n)} & \mathbf{0} \\ \hline \mathbf{0} & I_n & I_n & \cdots & I_n & \mathbf{1} \end{array}\right)$$

is semi-basic. For $j = 1, \ldots, n$, *let* $\widetilde{\mathbf{D}}^{(j)}$ *be the matrix obtained from the block* $\mathbf{D}^{(j)}$ *by writing* j *in place of* 1. *Then the last* $(n-1)n$ *rows of the* $n^2 \times (n+1)$ *matrix*

$$\mathbf{D} = \widetilde{\mathbf{D}}^{(1)} + \widetilde{\mathbf{D}}^{(2)} + \cdots + \widetilde{\mathbf{D}}^{(n)} = \begin{pmatrix} D_0 \\ \hline D_1 \\ \vdots \\ D_{n-1} \end{pmatrix}, \quad \text{where } D_0 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ \vdots & \vdots & & \vdots \\ n & n & \cdots & n \end{pmatrix},$$

give birth to a digraph complete set $D_1, \ldots, D_{n-1}$ *of latin squares. If* $\mathbf{H}$ *is basic, then there are only* 1*'s on the main diagonal of* D_i *for* $i = 1, \ldots, n-1$.

Example. Let $n = 4$. Consider the digraph complete set of latin squares

$$D_1 = \begin{pmatrix} 1 & 4 & 2 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

(which by the way happen to be mutually orthogonal). Then from

$$\mathbf{D} = \begin{pmatrix} D_0 \\ \hline\hline D_1 \\ \hline D_2 \\ \hline D_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \\ \hline\hline 1 & 4 & 2 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ \hline 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ \hline 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

one can build

$$\mathbf{D}^{(1)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline\hline 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathbf{D}^{(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline\hline 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{D}^{(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ \hline\hline 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$
\mathbf{D}^{(4)} = \left(\begin{array}{cccc}
0&0&0&0\\
0&0&0&0\\
0&0&0&0\\
1&1&1&1\\
\hline\hline
0&1&0&0\\
0&0&0&1\\
0&0&1&0\\
1&0&0&0\\
\hline
0&0&1&0\\
0&1&0&0\\
0&0&0&1\\
1&0&0&0\\
\hline
0&0&0&1\\
0&0&1&0\\
0&1&0&0\\
1&0&0&0
\end{array}\right) .
$$

This leads to the *semi-basic* incidence matrix

$$
\mathbf{H} = \left(\begin{array}{c|cccc|c}
\mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1\\
\hline
\mathbf{C} & \mathbf{D}^{(1)} & \mathbf{D}^{(2)} & \mathbf{D}^{(3)} & \mathbf{D}^{(4)} & \mathbf{0}\\
\hline
\mathbf{0} & I_4 & I_4 & I_4 & I_4 & \mathbf{1}
\end{array}\right) = \left(\begin{array}{c|cccc|c}
\mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1\\
\hline
C_1 & D_0^{(1)} & D_0^{(2)} & D_0^{(3)} & D_0^{(4)} & \mathbf{0}\\
\hline
C_2 & D_1^{(1)} & D_1^{(2)} & D_1^{(3)} & D_1^{(4)} & \mathbf{0}\\
C_3 & D_2^{(1)} & D_2^{(2)} & D_2^{(3)} & D_2^{(4)} & \mathbf{0}\\
C_4 & D_3^{(1)} & D_3^{(2)} & D_3^{(3)} & D_3^{(4)} & \mathbf{0}\\
\hline
\mathbf{0} & I_4 & I_4 & I_4 & I_4 & \mathbf{1}
\end{array}\right) ,
$$

namely to

$$
\mathbf{H} = \left(\begin{array}{cccc||cccc|cccc|cccc|cccc||c}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\hline\hline
1&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0\\
\hline
0&1&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0\\
0&1&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0&0\\
0&1&0&0&0&1&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0\\
\hline
0&0&1&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&1&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0\\
0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
\hline
0&0&0&1&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&1&0&0&1&0&0&0&0&1&1&0&0&0&0&1&0&0&0\\
0&0&0&1&0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0&0\\
\hline\hline
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&1\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&1
\end{array}\right).
$$

Proof of Theorem 3.1. Part (1). Notice that 1 appears $n+1$ times in each row of $\mathbf{H}$ and $n+1$ times in each column of $\mathbf{H}$. We want to prove that the three axioms for a projective plane Π of order n are verified.

First axiom. We want to prove that two distinct points $\wp_i$, $\wp_j$ of Π are on one and only one line of Π.

Let $i = 1$. When j corresponds to a row of C_u, then $\wp_1$ and $\wp_j$ are on and only on $\mathcal{L}_u$. When $j \in \{n^2+2, n^2+3, \ldots, n^2+n+1\}$, then $\wp_1$ and $\wp_j$ are on and only on $\mathcal{L}_{n^2+n+1}$.

Suppose that i corresponds to a row of $D_0^{(u)}$ for some $u \in \{1, 2, \ldots, n\}$ and that j corresponds to a row of $D_s^{(u)}$ ($s \in \{1, 2, \ldots, n-1\}$) or to a row of I_n. Then on that row of $D_s^{(u)}$ or of I_n, we can find 1 exactly once in, say, column t of $D_s^{(u)}$. As a matter of fact, the absence of such a 1 in $D_s^{(u)}$ translates into the absence of u in column t of D_s, a contradiction to the latin square property of D_s. Therefore $\wp_i$ and $\wp_j$ are on $\mathcal{L}_{t+(u-1)n}$. The value of t is unique; otherwise, $D_s^{(u)}$ would not be a permutation matrix.

Suppose that i corresponds to the row a of D_r and that j corresponds to the row b of D_s ($s \neq r$) or to the row b of I_n. Here $r, s \in \{1, 2, \ldots, n-1\}$. Let us now provide a proof of the following claim and the proof of the first axiom will be finished.

CLAIM: There exist unique integers u and $t \in \{1, 2, \ldots, n\}$ such that one can find 1 as the (a, t) element of $D_r^{(u)}$ and as the (b, t) element of $D_s^{(u)}$.

This is clear when $a = b$ since the first column of each D_i is $\begin{pmatrix} 1 \\ 2 \\ \vdots \\ n \end{pmatrix}$.

Therefore, when $a = b$, we have $t = 1$ and $\wp_i$ and $\wp_j$ are on $\mathcal{L}_{an+1}$. Suppose $a \neq b$ and suppose that the row a of of D_r is $(a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_n)$. Now the elements $a_2, a_3, \ldots, a_n$ appear in columns $2, 3, \ldots, n$ respectively of D_s. Moreover, the elements $a_2, a_3, \ldots, a_n$ appear in rows $r_2, r_3, \ldots, r_n$ of D_s. where $\{r_2, r_3, \ldots, r_n\} = \{1, 2, \ldots, n\} \backslash \{b\}$. Therefore in the row b of D_s, we are sure to find an integer u which has also the property that u appears in the row a of D_r and also the property that u appears in the same column of D_r and D_s. Let us prove that t and u are unique. Otherwise, suppose there exist u', t', with $u' \neq u$, $t' \neq t$, with also the property that one can find 1 as the (a, t') element of $D_r^{(u)}$ and as the (b, t') element of $D_r^{(v)}$. Then we get a contradiction with the property (b) of a semi-basic incidence matrix. This secures the above claim.

Second axiom. In order to verify the second axiom, we must prove that two distinct lines of Π pass through one and only one point of Π.

This is clear for the line $\mathcal{L}_i$ $(1 \leq i \leq n^2 + n)$ and the line $\mathcal{L}_{n^2+n+1}$. This is also clear for the line $\mathcal{L}_i$ and the line $\mathcal{L}_j$ when $sn + 1 \leq i < j \leq (s + 1)n$ for any $s \in \{1, 2, \ldots, n\}$.

This is obvious for the lines $\mathcal{L}_i$ and the line $\mathcal{L}_j$ when $1 \leq i \leq n$ and $n + 1 \leq j \leq n^2 + n$, and also when $n + 1 \leq i < j \leq n^2 + n$. At each step, it is important to remember that the matrices $\mathbf{D}^{(i)}$ are made of blocks which are $n \times n$ permutation matrices.

Third axiom. Consider the four distinct lines

$$\begin{aligned}
\mathcal{L}_1 &= \{\wp_1, \wp_2, \wp_3, \ldots, \wp_{n-1}, \wp_n, \wp_{n+1}\}, \\
\mathcal{L}_2 &= \{\wp_1, \wp_{n+2}, \wp_{n+3}, \ldots, \wp_{2n-1}, \wp_{2n}, \wp_{2n+1}\}, \\
\mathcal{L}_{n+1} &= \{\wp_2, \wp_{n+2}, \wp_{2n+2}, \ldots, \wp_{(n-2)n+2}, \wp_{(n-1)n+2}, \wp_{n^2+2}\}, \\
\mathcal{L}_{2n+1} &= \{\wp_3, \wp_{n+3}, \wp_{2n+3}, \ldots, \wp_{(n-2)n+3}, \wp_{(n-1)n+3}, \wp_{n^2+2}\},
\end{aligned}$$

the four distinct points

$$\wp_1, \quad \wp_2, \quad \wp_{n+3}, \quad \wp_{n^2+2},$$

and the following pertinent information:

	$\mathcal{L}_1$	$\mathcal{L}_2$	$\dots$	$\mathcal{L}_{n+1}$	$\dots$	$\mathcal{L}_{2n+1}$	$\dots$
$\wp_1$	1	1	$\dots$	0	$\dots$	0	$\dots$
$\wp_2$	1	0	$\dots$	1	$\dots$	0	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$	
$\wp_{n+3}$	0	1	$\dots$	0	$\dots$	1	$\dots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$	
$\wp_{n^2+2}$	0	0	$\dots$	1	$\dots$	1	$\dots$

Table

Then we can show as above that among the four points $\wp_1$, $\wp_2$, $\wp_{n+3}$, $\wp_{n^2+2}$, no three of them belong to the same line. Suppose the contrary. Then there exists $r \neq 1, 2, n+3, n^2+2$, such that the line $\mathcal{L}_r$ contains

$$\begin{cases} \text{either } \wp_1,\ \wp_2,\ \wp_{n+3}, & \text{whereupon } \wp_1,\ \wp_2 \text{ are on } \mathcal{L}_1 \text{ and } \mathcal{L}_r, \\ \text{or } \wp_1,\ \wp_2,\ \wp_{n^2+2}, & \text{whereupon } \wp_2,\ \wp_{n^2+2} \text{ are on } \mathcal{L}_{n+1} \text{ and } \mathcal{L}_r, \\ \text{or } \wp_1,\ \wp_{n+3},\ \wp_{n^2+2}, & \text{whereupon } \wp_1,\ \wp_{n+3} \text{ are on } \mathcal{L}_2 \text{ and } \mathcal{L}_r, \\ \text{or } \wp_2,\ \wp_{n+3},\ \wp_{n^2+2}, & \text{whereupon } \wp_{n+3},\ \wp_{n^2+2} \text{ are on } \mathcal{L}_{2n+1} \text{ and } \mathcal{L}_r. \end{cases}$$

In each of the four possibilities, we have a contradiction to the second axiom. The third axiom is now secured.

Part (2) This part simply reverses the process of Part (1). □

Acknowledgements. I wish to express my deepest gratitude to the members of the mathematics department of the University of Hawai'i at Mānoa for the facilities provided during my academic visits, with a special "Mahalo" to professor JB Nation and to professor Adolf Mader for their support. I am also grateful to the organizers of the *International Conference on Graph Theory and Information Security* (ICGTIS 2007, Bandung, Indonesia), for being given the opportunity of contributing this paper.

References

[D-K] J. Dénes and A.D. Keedwell, *Latin Squares and Their Applications*, Academic Press, (1974), 547 pages.

[R] H.J. Ryser, *Combinatorial Mathematics*, The Carus Math. Monographs of MAA, No. **14**, (1963), xiv+154 pages.