Binary matrices

Autor(en):   **Marrero, Osvaldo / Pasles, Paul C.**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr):   **57 (2002)**

PDF erstellt am: **26.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-7613

❙Elemente der Mathematik

Binary matrices

Osvaldo Marrero and Paul C. Pasles

Osvaldo Marrero studied mathematics at the University of Miami, and biometry and statistics at Yale University. After holding various positions in academia and in industry, he is now a professor at Villanova University. He has published papers in epidemiology, mathematics, medicine, and statistics.

Paul C. Pasles received a B.A. degree from the University of Pennsylvania, followed by M.A. and Ph.D. degrees from Temple University. He is now Assistant Professor of Mathematical Sciences at Villanova University. Presently, he is writing a book on Benjamin Franklin's magic squares.

1 Introduction and mathematical applications

Soon in their college courses students learn about some number systems and other mathematical settings that may seem strange at first. This can occur in courses in linear algebra or in abstract algebra. For example, one has binary matrices, whose entries are restricted to the set $\{0, 1\}$. Such matrices are useful in the following problem. Given a set of $v := 7$ elements, is it possible to find 7 subsets each having $k := 3$ elements and such that any two of these subsets have $\lambda := 1$ element in common? After a little experimentation one can find a solution. Explicitly, if the set is $X := \{x_1, \ldots, x_7\}$, then a solution is given by the subsets $X_1 := \{x_1, x_2, x_3\}$, $X_2 := \{x_1, x_4, x_5\}$, $X_3 := \{x_1, x_6, x_7\}$,

In dieser Arbeit werden verschiedene Aspekte von binären Matrizen vorgestellt. Beispiele demonstrieren, wie diese Matrizen in der Mathematik und in statistischen Anwendungen sinnvoll eingesetzt werden. Innermathematisch tauchen binäre Matrizen als Inzidenzmatrizen auf, die bei der Lösung kombinatorischer Probleme nützlich sind. In der statistischen Versuchsplanung und -auswertung und beim Arbeiten mit linearen Modellen der Datenanalyse sind binäre Matrizen geeignete Beschreibungsmittel. In der vorliegenden Arbeit beweisen die Autoren einige neue Ergebnisse über algebraische Eigenschaften von binären Matrizen. Diese Ergebnisse ermöglichen interessante, aber unvollständige Einsichten in die algebraische Natur binärer Matrizen; es bleibt Raum für weitere Untersuchungen. Da der mathematische Hintergrund der Darlegungen eher elementar ist, eignet sich das Material auch zum Einsatz in der Lehre.

$X_4 := \{x_2, x_4, x_6\}$, $X_5 := \{x_2, x_5, x_7\}$, $X_6 := \{x_3, x_4, x_7\}$, and $X_7 := \{x_3, x_5, x_6\}$. This is an example of a (v, k, λ)-*design*. Such a design can be represented by a binary matrix, the *incidence matrix* $A := [a_{ij}]$, defined by

$$a_{ij} := \begin{cases} 1, & \text{if } x_j \in X_i, \\ 0, & \text{if } x_j \notin X_i. \end{cases}$$

Thus, a (v, k, λ)-design exists if and only if there exists a $v \times v$ binary matrix A such that

$$AA' = \begin{bmatrix} k & \lambda & \cdots & \lambda \\ \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & k \end{bmatrix},$$

where A' is the transpose of A. To avoid uninteresting situations, it is usually assumed that $0 < \lambda < k < v - 1$. Thus, in terms of the corresponding incidence matrix, a solution to the problem above for $v := 7$, $k := 3$, and $\lambda := 1$ is given by

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

The (v, k, λ)-designs are of interest to both mathematicians (see, e.g., [3], [4], [7]) and statisticians, who tend to use the terms (*symmetric*) *balanced incomplete block designs* (see, e.g., [1]). The existence problem for (v, k, λ)-designs remains unsolved after many years; that is, it is not known what are the conditions on the parameters v, k, and λ that ensure the existence of a (v, k, λ)-design. Some partial results are known, however. For instance, a necessary condition for the existence of a (v, k, λ)-design is that $k(k - 1) = \lambda(v - 1)$ (see, e.g., [3], [4], [7]); the proof is based on a counting argument.

Incidence matrices have been the principal tool for the study of (v, k, λ)-designs and other combinatorial designs (see, e.g., [3], [4], [7]). In fact many results about these designs have been obtained by using matrix or linear algebra. For example, after some experimentation, one is likely to believe that a $(v := 8, k := 4, \lambda := 2)$-design cannot exist. But how does one prove such nonexistence? It turns out that, when v is even, a necessary condition for the existence of a (v, k, λ)-design is that $k - \lambda$ be a perfect square. The proof is accessible to anyone who has had a first course in linear algebra. Indeed, suppose a (v, k, λ)-design exists, and let A be its incidence matrix. One computes the determinant of AA' by performing the following operations on AA'. Subtract the first column from each of the other columns, and then add each row except the first row to the first row; finally, expand along the main diagonal. Thus, $\det(AA') = (k +$

$\lambda(v-1))(k-\lambda)^{v-1}$, which is not zero, since $0 < \lambda < k < v-1$. Now, using both the condition $k(k-1) = \lambda(v-1)$ and properties of the determinant function, one has $(\det A)^2 = k^2(k-\lambda)^{v-1}$. Therefore, if v is even, then $k-\lambda$ must be a square. Thus, in particular, a $(v := 8, k := 4, \lambda := 2)$-design cannot exist.

Binary matrices and vectors are of interest in combinatorics as well as in related fields such as coding and information theory and cryptology. *Complementation* – interchanging 0's and 1's – is often used on binary matrices and vectors. In particular, this operation is useful in the construction of combinatorial designs. For instance, there is the following classical result: the complement of the incidence matrix of a (v, k, λ)-design is the incidence matrix of a $(v, k-\lambda, v-2k+\lambda)$-design (see, e.g., [7, p. 98]).

Several results about designs have been obtained by arguments that involve the nonsingularity of a binary matrix. As examples one can cite:

1. Fisher's inequality (see, e.g., [3, p. 129]; [4, Theorem 19.6, p. 194]; [7, Theorem 1.1, p. 99]);

2. the fact that if A is the incidence matrix of a (v, k, λ)-design and A' is the transpose of A, then $AA' = A'A$ (see, e.g., [3, Theorems 10.2.2 and 10.2.3, p. 130]; [4, Theorem 19.10, p. 201]; [7, Theorem 2.1, p. 103]); and

3. some results concerning designs that are related to modular Hadamard matrices (see, e.g., [5, Theorem 2.3, p. 199 and Theorem 5.1, p. 209]).

Such considerations led us to study the relationship between complementation, linear independence, and nonsingularity for binary matrices and vectors.

The proofs given for the examples cited in the preceding paragraph assume characteristic zero; specifically, one considers the binary matrices as having entries from $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, respectively the fields of rational, real, or complex numbers. However, unless otherwise specified, in the present paper we regard binary matrices and vectors as having entries from any field $\mathbf{F}$ whatever, whose characteristic is denoted by $\mathrm{char}\,\mathbf{F}$. The superscript c will denote the result of complementation; for instance, A^c and u^c will be, respectively, the complements of the binary matrix A and of the binary vector u.

In Section 2 we present concrete statistical applications of binary matrices. Section 3 is concerned with complementation and linear independence, and Section 4 deals with complementation and nonsingularity. Section 5 presents some results about algebraic properties of sets related to the material in Sections 3 and 4.

2 Statistical applications

We give two concrete examples that show how binary matrices are used in statistics. The first example is concerned with the design of experiments, and the second deals with the use of linear models in statistical data analysis.

The first example comes from agriculture. Suppose it is desired to compare the yield of seven varieties of wheat when planted in a large square field. Of course, differences in soil fertility can influence the wheat yield. To minimize the effect of such influences on the statistical comparisons, one can plan the experiment as follows. Divide the field into seven parallel blocks (or rows) and seven parallel columns, all of the same width.

Further, suppose it is desired to plant three wheat varieties in each block, so as to ensure that each pair of distinct blocks have one variety in common. Naturally, the first question is whether such a plan is possible. The answer is "yes", and a solution is given by the incidence matrix for a $(v := 7, k := 3, \lambda := 1)$-design shown in the previous section. The rows in the matrix correspond to the blocks in the field, and the columns in the matrix correspond to the varieties of wheat. Thus, the field is divided into forty-nine square plots, each such plot corresponding to an entry in the matrix. Moreover, in that matrix, the entry "1" means "plant", and the entry "0" means "do not plant". For instance, varieties 1, 2, and 3 are planted as indicated in the first block, and varieties 2, 5, and 7 are planted as indicated in the fifth block. In the statistical design of experiments, such a plan is called a *symmetric balanced incomplete block design* for $v := 7$ varieties, having $k := 3$ varieties in each block, and such that each pair of distinct blocks have $\lambda := 1$ variety in common. "Symmetric" means that the number of blocks is the same as the number of varieties. It was shown in the previous section that a similar plan for the parameters $v := 8$, $k := 4$, and $\lambda := 2$ cannot be realized.

Taken from medicine, the second example illustrates the linear-models approach to the statistical data analysis in the one-way analysis of variance. Suppose we want to compare three treatments for one disease with respect to the length of stay (days) in the hospital. Thus, twelve patients with that disease are randomized to receive one of the three treatments. Suppose that the lengths of stay resulting from these treatments are, respectively, $(4, 6, 5, 6)$, $(5, 4, 4)$, and $(6, 5, 6, 5, 5)$. The statistical preference would be to have the same sample size in each of the treatment groups, but this is not necessary, and in practice it does not always happen because, for instance, some patients may drop out of the study. The null hypothesis in the analysis of variance is that the treatment effects are equal, and the alternative hypothesis is that the null hypothesis is false. The linear model we consider for the analysis of variance is $Y_{ij} = \beta_i + \varepsilon_{ij}$, where Y_{ij} is the observed value for the jth patient on the ith treatment, β_i is the ith treatment effect, and ε_{ij} is the random error associated with the observed value Y_{ij}. It is customary to assume that the errors are independent and identically distributed normal random variables with mean zero. In matrix form we can write

$$
\begin{bmatrix} 4 \\ 6 \\ 5 \\ 6 \\ \hline 5 \\ 4 \\ 4 \\ \hline 6 \\ 5 \\ 6 \\ 5 \\ 5 \end{bmatrix}
=
\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}
\begin{bmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix}
+
\begin{bmatrix} \varepsilon_{11} \\ \varepsilon_{12} \\ \varepsilon_{13} \\ \varepsilon_{14} \\ \hline \varepsilon_{21} \\ \varepsilon_{22} \\ \varepsilon_{23} \\ \hline \varepsilon_{31} \\ \varepsilon_{32} \\ \varepsilon_{33} \\ \varepsilon_{34} \\ \varepsilon_{35} \end{bmatrix},
$$

or, more compactly, $Y = X\beta + \varepsilon$. The binary matrix X is known as the *design matrix* or the *X-matrix*. This matrix approach to the analysis of variance is useful because it helps

to identify clearly the model that is being assumed, and it helps to simplify the pertinent mathematics. For instance, it can be shown that the vector $\widehat{\beta}$ of least-squares estimates for the parameter vector β is given by the solution to the so-called *normal equations* $X'X\widehat{\beta} = X'Y$. Additional information is available, for example, in [2].

3 Complementation and linear independence

For each $i \in \{1, \ldots, n\}$, the $n \times n$ binary matrix A is said to be *i-row independent* if each set of i distinct rows in A is linearly independent. The negation of i-row independence is *i-row dependence*. Analogous definitions apply to columns. Our results will be concerned mainly with rows, but it is clear that, in general, there are corresponding results for columns. We begin this section with some observations about i-row independence. Then, in Proposition 4, we provide a best possible characterization involving complementation and i-row independence.

Proposition 1. *An $n \times n$ binary i-row independent matrix need not be i-column independent, and conversely.*

Proof. The proof is accomplished by providing an example for the case $i = 2$. The matrix

$$A := \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

is 2-row independent but 2-column dependent.

The converse follows by considering the transpose A' of A. $\square$

Subsets of linearly independent sets are linearly independent. However, a set containing a linearly independent subset need not be linearly independent. Similar facts are recorded in the next two propositions in terms of i-row independence. The next result says, for example, that in a singular matrix it is possible for each pair of distinct rows to be linearly independent.

Proposition 2. *For all $n \geq 3$, there exists an $n \times n$ binary 2-row independent matrix that is i-row dependent for all $i \geq 3$.*

Proof. Let $n \geq 3$, and let

$$A := \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Then A is 2-row independent. However, the first, second, and last rows of A are linearly dependent. Therefore, A is i-row dependent for all $i \geq 3$. $\square$

Proposition 3. *Let $i \in \{2, \ldots, n\}$. If the $n \times n$ binary matrix A is i-row independent, then A is j-row independent for each $j \in \{1, \ldots, i-1\}$. The converse is false.*

Proof. We prove the contrapositive. Let $i \in \{2, \ldots, n\}$, $j \in \{1, \ldots, i-1\}$, and suppose the $n \times n$ binary matrix A is j-row dependent. Then there exist j rows $u_1, \ldots, u_j$ in A and j scalars $\alpha_1, \ldots, \alpha_j$, not all zero, such that $\alpha_1 u_1 + \cdots + \alpha_j u_j = 0$. Now select from A additional rows $u_{j+1}, \ldots, u_i \notin \{u_1, \ldots, u_j\}$. Then $\alpha_1 u_1 + \cdots + \alpha_j u_j + 0 u_{j+1} + \cdots + 0 u_i = 0$, and hence A is i-row dependent.

That the converse is false follows from Proposition 2. □

To obtain a characterization relating complementation to i-row independence, we need the following concept. A binary matrix A is said to have *no row of equal entries* if A has no row of all 0's and no row of all 1's. Clearly, A has no row of equal entries if and only if A^c has no row of equal entries.

Proposition 4. *Let A be a square binary matrix having no row of equal entries. Then A is 2-row independent if and only if A^c is 2-row independent.*

Proof. Let A be a square binary matrix having no row of equal entries. If u and v are rows in A, then the corresponding rows u^c and v^c in A^c may be obtained by computing $u^c = 1 - u$ and $v^c = 1 - v$, where 1 is the vector of all 1's.

Suppose A is 2-row independent. Then each pair of distinct row vectors u and v in A are linearly independent. Let $\alpha, \beta \in \mathbf{F}$, and suppose $\alpha u^c + \beta v^c = 0$. Then $\alpha(1-u) + \beta(1-v) = 0$, which implies $(\alpha + \beta, \ldots, \alpha + \beta) = \alpha u + \beta v$; that is, each entry in $\alpha u + \beta v$ is equal to $\alpha + \beta$. Because u and v are binary and linearly independent, and because A has no row of equal entries, one must then have $\alpha = \beta = 0$. Therefore u^c and v^c are linearly independent. Thus, A^c is 2-row independent.

The proof of the converse is similar. □

The preceding proposition is best possible with respect to i-row independence in that the result need not be valid when A is i-row independent for $i > 2$. Indeed, if A is the 3×3 identity matrix, then A is a binary matrix having no row of equal entries and A is 3-row independent over any field whatever; however, A^c is not 3-row independent whenever char $\mathbf{F} = 2$. This example also serves to point out that Proposition 4 is false if one replaces "2-row independent" with "nonsingular"; see Proposition 5 and its proof below.

4 Complementation and nonsingularity

Complementation does not preserve nonsingularity, as the next proposition shows.

Proposition 5. *The complement of a nonsingular binary matrix need not be nonsingular. In fact, for each $n \geq 3$ and any field $\mathbf{F}$ whatever, there exists a nonsingular $n \times n$ binary matrix A over $\mathbf{F}$ such that the complement A^c is singular whenever char $\mathbf{F}$ divides $n-1$. When $n = 2$, there exists a nonsingular binary matrix whose complement is singular over any field whatever.*

Proof. For $n \geq 3$, we exhibit a family of matrices that meets our requirements. The $n \times n$ identity matrix I_n is a nonsingular binary matrix over any field $\mathbf{F}$ whatever. However, (see, e.g., [6, Lemma, p. 219]), one has $\det I_n^c = (-1)^{n-1}(n-1)$, so that I_n^c is singular whenever $\operatorname{char} \mathbf{F}$ divides $n-1$.

For $n = 2$, the binary matrix

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

is nonsingular but its complement is singular over any field whatever. $\square$

5 Algebraic properties

From an algebraic viewpoint, we study certain sets of $n \times n$ binary matrices over $\mathbf{F}$. For each $i \in \{1, \ldots, n\}$, let $RI_n[i]$ and NS_n denote the sets of such matrices that are, respectively, i-row independent and nonsingular. Note that $RI_n[n] = NS_n$. We begin with some observations about these sets.

Proposition 6. *Each of the following statements is valid:*

1. *The sets $RI_n[1], \ldots, RI_n[n-1]$, and NS_n satisfy $NS_n \subseteq RI_n[n-1] \subseteq \cdots \subseteq RI_n[2] \subseteq RI_n[1]$.*

2. *An $n \times n$ binary matrix $A \in RI_n[1]$ if and only if A has no row of all 0's.*

3. *If $n \geq 3$, then $RI_n[3] \subsetneqq RI_n[2]$ and, therefore, $NS_n \subsetneqq RI_n[2]$.*

4. *$NS_n = RI_n[2]$ if and only if $n = 2$.*

Proof. The first statement follows from the fact that subsets of linearly independent sets are also linearly independent. The second statement is true because a vector is linearly independent if and only if that vector is not the zero vector. The third statement follows from Proposition 2.

The fourth statement can be proved as follows. If $n = 2$, then 2-row independence is equivalent to nonsingularity; thus, $NS_n = RI_n[2]$. Conversely, if $NS_n = RI_n[2]$, then the matrices in question must have at least two rows; hence, we have $n \geq 2$. Moreover, from the first statement in this proposition, it follows that $NS_n = RI_n[n-1] = \cdots = RI_n[2]$. Thus, if $n \geq 3$, one has a contradiction with Proposition 2. Therefore, we must have $n = 2$. $\square$

In Proposition 6 we have characterized $RI_n[1]$, and we have shown that, if $n \geq 3$, then $NS_n \subsetneqq RI_n[2]$. Thus, ignoring $RI_n[1]$, we see that the sets $RI_n[2]$ and NS_n are at the extremes of the chain $NS_n \subseteq RI_n[n-1] \subseteq \cdots \subseteq RI_n[2]$. Therefore we study further $RI_n[2]$ and NS_n.

The subsets of $RI_n[2]$ and NS_n made up of the matrices that have no row of equal entries will be $RI_n^*[2]$ and NS_n^*, respectively. Some algebraic properties of these four sets will be noted. These remarks provide an intriguing but as yet incomplete understanding of the algebraic nature of these sets.

Proposition 7. *Viewed as a map, complementation satisfies the following properties:*

1. *Complementation is a permutation of $RI_n^*[2]$, but it need not be a permutation of NS_n^*. Moreover, as an element in the group of permutations of $RI_n^*[2]$, complementation has order two.*

2. *With respect to matrix multiplication in each of $RI_n^*[2]$ and NS_n^*, complementation is neither homomorphic nor anti-homomorphic. That is, in general, if $A, B \in RI_n^*[2]$ or $A, B \in NS_n^*$, then $(AB)^c$ need not equal either of $A^c B^c$ or $B^c A^c$.*

Proof. Consider complementation as a map so that $A \mapsto A^c$.

It follows from Proposition 4 that complementation is a permutation of $RI_n^*[2]$. Of course, complementation followed by complementation is the identity map of $RI_n^*[2] \to RI_n^*[2]$. Therefore, as an element in the group of permutations of $RI_n^*[2]$, complementation has order two.

The family of matrices given in the proof of Proposition 5 shows that complementation need not be a permutation of NS_n^*. This completes the proof of the first property.

It is easy to find examples to show that the second property is valid. For instance, for $n := 2$, let

$$A := B := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

so that $A, B \in RI_2^*[2] = NS_2^*$. Then $(AB)^c \neq A^c B^c$ and $(AB)^c \neq B^c A^c$. $\square$

Proposition 8. *For all $n \geq 2$, neither $RI_n[2]$ nor NS_n is closed under complementation.*

Proof. Let $n \geq 2$, and let the $n \times n$ binary matrix A be defined by

$$A := \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & 1 & 0 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}.$$

The determinant of A can be computed as follows. First, expand by the entry in position $(1,1)$ in A. Next, in the resulting array, subtract every row but the last from the last row. Then it is clear that $\det A = 1$, regardless of the characteristic of $\mathbf{F}$. Therefore A is nonsingular, and thus $A \in NS_n$ and $A \in RI_n[2]$. However, A^c has one row and one column of all 0's. Therefore $A^c \notin NS_n$ and $A^c \notin RI_n[2]$. $\square$

Proposition 9. *For all $n \geq 3$, neither $RI_n^*[2]$ nor NS_n^* is closed under matrix multiplication and, therefore, neither $RI_n^*[2]$ nor NS_n^* can be a group under matrix multiplication.*

Proof. Let $n \geq 3$, and let the $n \times n$ binary matrices A and B be defined by

$$
A := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \quad \text{and} \quad B := \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.
$$

Clearly, each of A and B has no row of equal entries. Expanding up along the main diagonal, beginning with the entry in position (n, n), one sees that $\det A = \det B = 1$, regardless of the characteristic of $\mathbf{F}$. Therefore A and B are nonsingular, and thus $A, B \in NS_n^* \subseteq RI_n^*[2]$.

However, the matrix AB has one row of equal entries. Hence, $AB \notin RI_n^*[2]$ and $AB \notin NS_n^*$. This implies that neither $RI_n^*[2]$ nor NS_n^* can be a group under matrix multiplication. $\square$

Proposition 10. *If $n \geq 4$, $k \in \{0, \ldots, n-4\}$, $\operatorname{char} \mathbf{F} \not\equiv 0 (\operatorname{mod} n-2-k)$, and $\operatorname{char} \mathbf{F} \neq 2$, then neither $RI_n[2]$ nor NS_n is closed under matrix multiplication. Therefore, under these conditions, neither $RI_n[2]$ nor NS_n can be a group under matrix multiplication.*

Proof. Let $n \geq 4$ and $k \in \{0, \ldots, n-4\}$, and assume that $\operatorname{char} \mathbf{F} \not\equiv 0 (\operatorname{mod} n-2-k)$ and that $\operatorname{char} \mathbf{F} \neq 2$.

For notation, I_a is the $a \times a$ identity matrix, $J_{a,b}$ is the $a \times b$ matrix of all 1's, and $Z_{a,b}$ is the $a \times b$ matrix of all 0's.

For the said n and k, let the $n \times n$ matrix $A(k)$ be defined by

$$
A(k) := \left[\begin{array}{c|c} J_{1,1} & J_{1,n-1} \\ \hline \begin{array}{c} J_{n-1-k,1} \\ \\ Z_{k,1} \end{array} & I_{n-1} \end{array} \right].
$$

The determinant of $A(k)$ can be computed by performing on $A(k)$ the following operations: subtract every row but the first from the first row, and then expand along the main diagonal. The result is $\det A(k) = 2 + k - n$, which is not zero because $\operatorname{char} \mathbf{F} \not\equiv 0$ $(\operatorname{mod} n - 2 - k)$. Thus, $A(k)$ is nonsingular and, therefore, $A(k) \in NS_n \subseteq RI_n[2]$.

Because $\operatorname{char} \mathbf{F} \neq 2$, the matrix $(A(k))^2$ is not binary. Hence, $(A(k))^2 \notin RI_n[2]$ and $(A(k))^2 \notin NS_n$. Therefore neither $RI_n[2]$ nor NS_n is closed under matrix multiplication. This implies that neither $RI_n[2]$ nor NS_n can be a group under matrix multiplication. $\square$

Proposition 11. *If $\operatorname{char} \mathbf{F} = 2$, then it is possible for NS_n to be a group under matrix multiplication; in this case, it is also possible for NS_n^* to be a subgroup of NS_n.*

Proof. Let char $\mathbf{F} = 2$, and let $n := 2$. The proof is accomplished by exhibiting the elements that make up the group NS_2 and the subgroup NS_2^*.

There are sixteen 2×2 binary matrices, of which six are nonsingular, regardless of the field characteristic. These six matrices are

$$A_1 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ A_2 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ A_3 := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

$$A_4 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \ A_5 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \ \text{and} \ A_6 := \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix};$$

thus, $NS_2 = \{A_1, A_2, A_3, A_4, A_5, A_6\}$ and $NS_2^* = \{A_1, A_2\}$.

When char $\mathbf{F} = 2$, NS_2 is a group under matrix multiplication, as can be verified, for example, by constructing the group-multiplication table. Moreover, NS_2 is not isomorphic to the cyclic group of order six because A_2, A_4 and A_5 have order two. Therefore NS_2 must be isomorphic to the symmetric group S_3. Also, NS_2^* is a subgroup of NS_2, and NS_2^* is isomorphic to the cyclic group of order two. $\qquad\square$

References

[1] Box, G.E.P.; Hunter, W.G. and Hunter, J.S.: *Statistics for Experimenters: An Introduction to Design, Data Analysis, and Model Building*, Wiley, New York, 1978.

[2] Draper, N.R. and Smith, H.: *Applied Regression Analysis*, second edition, Wiley, New York, 1981.

[3] Hall, M., Jr.: *Combinatorial Theory*, second edition, Wiley, New York, 1986.

[4] van Lint, J.H. and Wilson, R.M.: *A Course in Combinatorics*, Cambridge Univ. Press, Cambridge, UK, 1992.

[5] Marrero, O.: A survey of pseudo (v, k, λ)-designs, *Aequationes Math.* 16 (1977), 195–220.

[6] Marrero, O. and Pasles, P.C.: Row coincidences in nonsingular binary matrices, *European J. Combin.* 22 (2001), 217–224.

[7] Ryser, H.J.: *Combinatorial Mathematics*, Wiley, New York, 1963.

Osvaldo Marrero
Department of Mathematical Sciences
Villanova University
800 Lancaster Avenue
Villanova, Pennsylvania 19085-1699, USA
e-mail: `Osvaldo.Marrero@villanova.edu`

Paul C. Pasles
Department of Mathematical Sciences
Villanova University
800 Lancaster Avenue
Villanova, Pennsylvania 19085-1699, USA
e-mail: `Paul.Pasles@villanova.edu`