Research Article

Kishan Chand Gupta, Sumit Kumar Pandey* and Indranil Ghosh Ray

Applications of design theory for the constructions of MDS matrices for lightweight cryptography

DOI: 10.1515/jmc-2016-0013
Received February 22, 2016; revised November 26, 2016; accepted March 23, 2017

Abstract: In this paper, we observe simple yet subtle interconnections among design theory, coding theory and cryptography. Maximum distance separable (MDS) matrices have applications not only in coding theory but are also of great importance in the design of block ciphers and hash functions. It is nontrivial to find MDS matrices which could be used in lightweight cryptography. In the SAC 2004 paper [12], Junod and Vaudenay considered bi-regular matrices which are useful objects to build MDS matrices. Bi-regular matrices are those matrices all of whose entries are nonzero and all of whose 2×2 submatrices are nonsingular. Therefore MDS matrices are bi-regular matrices, but the converse is not true. They proposed the constructions of efficient MDS matrices by studying the two major aspects of a $d \times d$ bi-regular matrix M, namely $v_1(M)$, i.e. the number of occurrences of 1 in M, and $c_1(M)$, i.e. the number of distinct elements in M other than 1. They calculated the maximum number of ones that can occur in a $d \times d$ bi-regular matrices, i.e. $v_1^{d,d}$ for d up to 8, but with their approach, finding $v_1^{d,d}$ for $d \geq 9$ seems difficult. In this paper, we explore the connection between the maximum number of ones in bi-regular matrices and the incidence matrices of Balanced Incomplete Block Design (BIBD). In this paper, tools are developed to compute $v_1^{d,d}$ for arbitrary d. Using these results, we construct a restrictive version of $d \times d$ bi-regular matrices, introducing by calling almost-bi-regular matrices, having $v_1^{d,d}$ ones for $d \leq 21$. Since, the number of ones in any $d \times d$ MDS matrix cannot exceed the maximum number of ones in a $d \times d$ bi-regular matrix, our results provide an upper bound on the number of ones in any $d \times d$ MDS matrix. We observe an interesting connection between Latin squares and bi-regular matrices and study the conditions under which a Latin square becomes a bi-regular matrix and finally construct MDS matrices from Latin squares. Also a lower bound of $c_1(M)$ is computed for $d \times d$ bi-regular matrices M such that $v_1(M) = v_1^{d,d}$, where $d = q^2 + q + 1$ and q is any prime power. Finally, $d \times d$ efficient MDS matrices are constructed for d up to 8 from bi-regular matrices having maximum number of ones and minimum number of other distinct elements for lightweight applications.

Keywords: BIBD, bi-regular matrix, design, diffusion, Latin square, MDS matrix, mixColumn operation

MSC 2010: 68R05, 94B99

Communicated by: Doug Stinson

1 Introduction

Maximum distance separable (MDS) matrices incorporate diffusion layers in block ciphers and hash functions and are one of the vital constituents of modern age ciphers like Advanced Encryption Standard (AES) [5],

Kishan Chand Gupta, Indranil Ghosh Ray: Applied Statistics Unit, Indian Statistical Institute, 203, B.T. Road, Kolkata 700108, India, e-mail: kishan@isical.ac.in, indranil_r@isical.ac.in
***Corresponding author: Sumit Kumar Pandey:** School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, e-mail: emailpandey@gmail.com

Twofish [19, 20], SHARK [16], Square [4], Khazad [2], Clefia [27] and MDS-AES [15]. The stream cipher MUGI [24] uses MDS matrix in its linear transformations. MDS matrices are also used in the design of hash functions. Hash functions like Maelstrom [6], Grøstl [7] and PHOTON family of light weight hash functions [8] use MDS matrices as main part of their diffusion layers. MDS matrices, in general, have a large description and thus induces costly implementations both in hardware and software. It is nontrivial to find MDS matrices which could be used in lightweight cryptography.

It is difficult to define what an *optimal matrix* is in terms of implementation. In the SAC 2004 paper [12], Junod and Vaudenay studied MDS matrices M under the angle of efficiency and defined two mathematical criteria namely $v_1(M)$, i.e. the number of occurrences of ones and $c_1(M)$, i.e. the number of other distinct elements in the matrix. These lead to two very interesting combinatorial problems:
(1) how to increase the number of occurrences of ones,
(2) how to minimize the number of occurrences of other distinct elements.
They proved some optimality results relative to these two criteria.

Our contribution. The techniques used in [12] to solve these above mentioned combinatorial problems for the construction of $d \times d$ MDS matrices were very specific to the dimension d for d up to 8 and it seems difficult to extend their techniques to solve the same combinatorial problems for higher values of d. In this paper, we further investigate these combinatorial problems in the light of *design theory* and propose more generalized results. In [12], the authors mentioned that maximum number of ones in $d \times d$ MDS matrices is close to $d\sqrt{d}$ but no generalized method is yet known to construct $d \times d$ *bi-regular* matrices having almost $d\sqrt{d}$ ones. A bi-regular matrix is a matrix all of whose entries are nonzero and all of whose 2×2 submatrices are nonsingular. It is evident from the definition that an MDS matrix is a bi-regular matrix, but the converse is not true. For higher values of d, the authors of [12] proposed a construction that can guarantee $3d - 3$ ones (see [12, Lemma 3]) in a $d \times d$ bi-regular matrix.

In a bi-regular matrix, there does not exist any 2×2 submatrix all of whose four entries are the same (otherwise this submatrix would be a singular matrix). If we replace all non-one entries with blank in a bi-regular matrix, we get another matrix, which we call *almost-bi-regular* matrix. An almost-bi-regular matrix is a matrix all of whose entries are either 1 or blank and all of whose 2×2 submatrices contain at most three ones. To get an MDS matrix with maximum possible number of ones, one approach would be to start with an almost-bi-regular matrix with maximum possible number of ones and then replace blanks with suitable non-one values so that the resulting matrix would become MDS. This approach requires two important steps:
(a) the construction of an almost-bi-regular matrix with maximum possible number of ones,
(b) fill the blank entries with non-one entries so that the resulting matrix would become MDS.
To make the resulting MDS matrix an efficient one, we require that the description of the matrix should be very low, i.e.
(i) the number of distinct entries should be as low as possible,
(ii) the number of low hamming weight entries should be as high as possible.
These two criteria were mentioned in [12] by introducing two mathematical notations, $v_1(M)$ which indicates number of ones and $c_1(M)$ which indicates number of distinct entries, for a bi-regular matrix M.

In this paper, we observe an interesting connection between the number of ones in almost-bi-regular matrices and incidence matrices of Balanced Incomplete Block Design (BIBD). Using results on BIBD, we exactly compute the maximum number of ones in $v \times b$ almost-bi-regular matrix whenever there exists $(v, b, r, k, 1)$-BIBD. For arbitrary v and b also, we compute an upper bound on the maximum number of ones in any $v \times b$ almost-bi-regular matrix. Since the number of ones in a $v \times b$ MDS matrix cannot exceed the maximum number of ones in a $v \times b$ almost bi-regular matrix, our result gives an upper bound on the number of ones in any $v \times b$ MDS matrix. Moreover, this paper provides exact upper bounds on the number of ones for $d \times d$ almost-bi-regular matrix for $d \leq 21$.

We propose another simple technique of construction of *bi-regular* matrices and MDS matrices using *Latin squares*. Using the structure of Latin squares, it is shown that bi-regular matrices and MDS matrices can be constructed by judicious selection of elements. This paper shows that if $v_1^{d,d}$ is multiple of d, then

construction of $d \times d$ bi-regular matrices with maximum number of ones starting from Latin squares may be more useful. When $d = q^2 + q + 1$, where q is any prime power, we compute tight lower bound of $c_1(M)$ for $d \times d$ bi-regular matrices M having $v_1^{d,d}$ ones. Finally, $d \times d$ bi-regular matrices are proposed which are having maximum number of ones and minimum number of other elements. Moreover, efficient $d \times d$ MDS matrices are constructed from these bi-regular matrices for d up to 8.

Previous work. Nearly all the ciphers use predefined MDS matrices to incorporate the diffusion property. In some ciphers, however, the possibility of random selection of MDS matrices with some constraints is provided [26]. In this context, we would like to mention that in the papers [1, 8–13, 17, 26], different constructions of MDS matrices are provided. In [8], the authors constructed lightweight MDS matrices from companion matrices by exhaustive search. In [9], new involutory MDS matrices were constructed using properties of Cauchy matrices over additive subgroup of $\mathbb{F}_{2^n}$ and its equivalence with Vandermonde matrices based construction under some constraints was proved. In [10], the authors provably constructed new MDS matrices from companion matrices over $\mathbb{F}_{2^n}$. In [11], the authors constructed new MDS matrices from *circulant matrices* over $\mathbb{F}_{2^n}$. Efficient 4×4 and 8×8 MDS matrices to be used in block ciphers were constructed in [12]. *Involutory* MDS matrices using Vandermonde matrices were constructed in [13, 17]. New involutory MDS matrices using properties of Cauchy matrices were constructed in [26]. Recently in [1], the authors have constructed MDS matrices based on shortened BCH codes.

The organization of the paper is as follows: In Section 2, we provide definitions and preliminaries. In Section 3, we study the construction of almost-bi-regular matrices with maximum number of ones using properties of BIBDs. In Section 4, we study $v_1^{v,b}$ for arbitrary v and b and construct $d \times d$ almost-bi-regular matrices having maximum number of ones for d up to 21. In Section 5, we study the $d \times d$ bi-regular matrix M having maximum number of ones and propose the minimum value of $c_1(M)$, where $d = q^2 + q + 1$ and q is any prime power. In that section, we also study the construction of bi-regular matrices from Latin squares. In Section 6, we propose new and efficient $d \times d$ MDS matrices for d up to 8 having maximum number of ones and minimum number of other distinct elements. We conclude the paper in Section 7.

2 Definition and preliminaries

2.1 MDS code and MDS matrices

An MDS matrix provides diffusion properties that have useful applications in cryptography. The idea comes from coding theory, in particular from maximum distance separable (MDS) code. Let C be an $[n, k, d]$ code. Then $n - k \geq d - 1$. Codes with $n - k = d - 1$ are called maximum distance separable code, or MDS code for short.

Definition 2.1. Let $\mathbb{F}$ be a finite field and let p and q be two integers. Let $x \to M \times x$ be a mapping from $\mathbb{F}^p$ to $\mathbb{F}^q$ defined by the $q \times p$ matrix M. We say that it is an MDS matrix if the set of all pairs $(x, M \times x)$ is an MDS code, i.e. a linear code of dimension p, length $p + q$ and minimal distance $q + 1$.

The following theorem characterizes MDS matrices.

Theorem 2.2 ([14, p. 321]). *An $[n, k, d]$ code C with generator matrix $G = [I|A]$, where A is a $k \times (n - k)$ matrix, is MDS if and only if every square submatrix (formed from any i rows and any i columns, for any $i = 1, 2, \ldots, \min\{k, n - k\}$) of A is nonsingular.*

From the above theorem, it is evident that a square matrix A is an MDS matrix if and only if every square submatrices of A is nonsingular. It is easy to check that the MDS property remains invariant under the two elementary row (or column) operations, namely permutations of rows (or columns) and multiplying a row (or column) of a matrix by a scalar except zero. Also the MDS property is invariant under transpose operation. So we provide the following lemma without proof.

Lemma 2.3. *If A is an MDS matrix over $\mathbb{F}$, then A', obtained by multiplying a row (or column) of A by any $c \in \bar{\mathbb{F}}^*$ (nonzero elements of algebraic closure of $\mathbb{F}$) or by permutations of rows (or columns) is MDS. Also if A is MDS, so is A^T.*

2.2 Bi-regular matrices

In [12], the authors used bi-regular arrays to build MDS matrices. We call it as bi-regular matrix and define it slightly differently but equivalently.

Definition 2.4 (Bi-regular matrix). A matrix is called bi-regular if all entries of the matrix are nonzero and all of its 2×2 submatrices are nonsingular.

Our target is to maximize the number of occurrences of ones in an MDS matrix. One approach may be to construct the *bi-regular* matrix with maximum number of ones and then to check its MDS property. So, we first take a matrix $M = ((m_{i,j}))$, where $m_{i,j}$ is kept blank for all values of i and j. Next, we put the maximum number of ones in this matrix such that in any 2×2 submatrix, not all positions are assigned to 1. We refer to such matrices as *almost-bi-regular* matrices. It may be noted that with judicious choices of other elements in the blank positions of almost-bi-regular matrices, bi-regular matrices may be constructed.

Definition 2.5 (Almost-bi-regular matrix). A matrix with entries either 1 or blank is almost-bi-regular if in any of its 2×2 submatrices, there are at most three ones.

The significance of putting the maximum possible number of ones while constructing almost-bi-regular matrix is that no more 1 can be put in the matrix without violating the almost-bi-regular property. But, it has to be noted that an almost-bi-regular matrix saturated with ones may not guarantee that it contains maximum number of ones (see Remark 3.3). In Section 3 and Section 4, we will develop techniques to construct an almost-bi-regular matrix with maximum number of ones. Next, we replace all blank entries of the almost-bi-regular matrix by judicious choices of elements from $\bar{\mathbb{F}}^*$ other than 1 to make it a bi-regular matrix and then check its MDS property. No algorithm is known to select elements except exhaustive search. It may be noted that, as we construct $d \times d$ MDS matrices M with maximum number (i.e. $v_1^{d,d}$) of ones with low value of $c_1(M)$, search space gets reduced drastically. For example, to construct a 4×4 MDS matrix over $\mathbb{F}_{2^8}$, the size of search space is $2^{8\times 16} = 2^{128}$, but for the 4×4 matrix of Figure 7, the size of search space becomes $2^{8\times 2} = 2^{16}$.

For an efficient implementation of perfect diffusion layer, it is desirable to have the maximum number of ones and the minimum number of different entries in the MDS matrix. In [12], the authors studied these two properties on bi-regular matrices and proposed some bounds.

Definition 2.6 ([12]). Let $M = ((m_{i,j}))$ be a $q \times p$ bi-regular matrix over the field $\mathbb{F}$.

- Let $v_1(M)$ denote the number of pairs (i, j) such that $m_{i,j}$ is equal to 1. We call it the number of occurrences of 1. Also, let $v_1^{q,p}$ be the maximum value of $v_1(M)$ over all $q \times p$ bi-regular matrices M.
- Let $c(M)$ be the cardinality of $\{m_{i,j} : i = 1, \ldots, q, j = 1, \ldots, p\}$. This is called the number of distinct entries. Also let $c^{q,p}$ be the minimum value of $c(M)$ over all $q \times p$ bi-regular matrices M.
- If $v_1(M) > 0$, let $c_1(M) = c(M) - 1$; otherwise $c_1(M) = c(M)$. This is called the number of nontrivial entries.

For example, for the matrix

$$M = \begin{pmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{pmatrix},$$

where α is the root of the generating polynomial $x^8 + x^4 + x^3 + x + 1$ of $\mathbb{F}_{2^8}$, which is used in the *mixColumn* operation in AES [5], we have $v_1(M) = 8$ and $c_1(M) = 2$.

Remark 2.7. The high value of v_1 and the low value of c and c_1 are desirable for constructing efficient MDS matrices.

From [12], we have the following fact.

Fact 1. [12] The following hold:
(a) $v_1^{p,q} = v_1^{q,p}$.
(b) $v_1^{p,q}$ increases with p and q.

In the next lemma, we state some results from [12, Lemma 1].

Lemma 2.8 ([12, Lemma 1]). *The following hold:*
(a) $v_1^{3,p} = p + 3$ *for all* $p \geq 3$.
(b) $v_1^{4,4} = 9$, $v_1^{5,5} = 12$, $v_1^{6,6} = 16$, $v_1^{7,7} = 21$ *and* $v_1^{8,8} = 24$.

2.3 Balanced Incomplete Block Design (BIBD)

In this paper, we show an interesting connection between almost-bi-regular matrices and incidence matrices of BIBDs. Although the notations $v_1(M)$ and $v_1^{q,p}$ were used for bi-regular matrices in [12], we use them (abuse of notations!), from here onwards, for almost-bi-regular matrices also for the same purpose. Thus, in the context of bi-regular matrices, $v_1(M)$ represents the number of ones in the bi-regular matrix M and $v_1^{q,p}$ represents the maximum value of $v_1(M)$ over all $q \times p$ bi-regular matrices M. Similarly, in the context of almost-bi-regular matrices, $v_1(M)$ represents the number of ones in the almost-bi-regular matrix M and $v_1^{q,p}$ represents the maximum value of $v_1(M)$ over all $q \times p$ almost-bi-regular matrices M. It is proved in this paper that for $v \times b$ almost-bi-regular matrices, $v_1^{v,b} = bk$ whenever there exists (v, b, r, k, λ)-BIBD where $\lambda = 1$. We also provide a tight upper bound of $v_1^{d,d}$ for any value of d. Using these techniques, we provide very simple and alternative proof of optimality results of [12] which are given in Lemma 2.8. We propose techniques to construct any $d \times d$ matrix M where $v_1(M)$ is either $v_1^{d,d}$ or very close to it.

Remark 2.9. The existence of an almost-bi-regular matrix with l ones may not guarantee the existence of a bi-regular matrix with the same number of ones, i.e. l ones. But the converse is always true; the existence of a bi-regular matrix with l ones always guarantees the existence of an almost-bi-regular matrix with the same number of ones. Constructing almost-bi-regular matrix from bi-regular matrix is straightforward - replace all non-one elements from the bi-regular matrix with the blank symbol. The new matrix will be almost-bi-regular matrix.

Definition 2.10 ([23]). A design is a pair $(X, \mathcal{A})$ such that the following properties are satisfied:
- X is a set of elements called points,
- $\mathcal{A}$ is a collection (i.e. multiset) of nonempty subsets of X called blocks.

If two blocks in a design are identical, they are said to be *repeated blocks*. This is why $\mathcal{A}$ is referred to as a *multiset* of blocks rather than a set.

Definition 2.11 ([23]). Let v, k and λ be positive integers such that $v > k \geq 2$. A (v, k, λ)- balanced incomplete block design (which we abbreviate (v, k, λ)-BIBD) is a design such that the following properties are satisfied:
(1) $|X| = v$,
(2) each block contains exactly k points,
(3) every pair of distinct points is contained in exactly λ blocks.

In the following two lemmas, we record two important properties of a BIBD.

Lemma 2.12 ([23]). *In a* (v, k, λ)*-BIBD, every element occurs in exactly* $r = \frac{\lambda(v-1)}{(k-1)}$ *blocks. The value* r *is often called the replication number of the BIBD.*

Lemma 2.13 ([23]). *A* (v, k, λ)*-BIBD has exactly* b *blocks, where* $b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{(k^2-k)}$.

Definition 2.14 ([23]). A BIBD in which $b = v$ (or, equivalently, $r = k$ or $\lambda(v-1) = k^2 - k$) is called a symmetric BIBD.

For example, in a $(7, 3, 1)$-BIBD, $X = \{1, 2, 3, 4, 5, 6, 7\}$ and

$$\mathcal{A} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}.$$

Here $v = |X| = 7$ and $b = |\mathcal{A}| = 7$. It is a symmetric BIBD as $v = b$. Also $r = k = 3$.

Lemma 2.15 ([23]). *Suppose that $(X, \mathcal{A})$ is a symmetric (v, k, λ)-BIBD and denote $\mathcal{A} = \{A_0, \ldots, A_{v-1}\}$. Suppose that $0 \le i, j \le v-1$, $i \ne j$. Then $|A_i \cap A_j| = \lambda$.*

In this paper, a special kind of symmetric BIBDs, called *projective planes*, will be used for constructions of almost-bi-regular matrices.

Definition 2.16 (Projective plane, [23]). A $(d^2 + d + 1, d + 1, 1)$-BIBD with $d \ge 2$ is called a projective plane of order d.

It may be noted that although a $(3, 2, 1)$-BIBD exists, this is not regarded as a projective plane of order 1 (also see [23]). Here we mention one very important result on projective plane which is crucial in our work.

Theorem 2.17 ([23]). *For every prime power $q \ge 2$, there exists a (symmetric) $(q^2 + q + 1, q + 1, 1)$-BIBD (i.e. a projective plane of order q).*

In this paper, we will use the notation (v, b, r, k, λ)-BIBD to record the values of all five parameters. Note that for a projective plane, i.e. a $(d^2 + d + 1, d + 1, 1)$-BIBD,

$$r = \frac{v-1}{k-1} = \frac{d^2 + d + 1 - 1}{d} = d + 1$$

and

$$b = \frac{vr}{k} = \frac{(d^2 + d + 1) \times (d + 1)}{(d + 1)} = d^2 + d + 1.$$

So we call it $(d^2 + d + 1, d^2 + d + 1, d + 1, d + 1, 1)$-BIBD.

It is often convenient to represent a BIBD by means of an *incidence matrix*.

Definition 2.18 (Incidence matrix, [23]). Let $(X, \mathcal{A})$ be a design with $X = \{x_0, \ldots, x_{v-1}\}$, $\mathcal{A} = \{A_0, \ldots, A_{b-1}\}$. The incidence matrix of $(X, \mathcal{A})$ is the $v \times b$ matrix $M = ((m_{i,j}))$ defined by the rule

$$m_{i,j} = \begin{cases} 1, & \text{if } x_i \in A_j, \\ 0, & \text{if } x_i \notin A_j, \end{cases} \quad \text{for any } i \in \{0, 1, \ldots, v-1\} \text{ and } j \in \{0, 1, \ldots, b-1\}.$$

For constructions of MDS matrices, we use a slightly modified version of incidence matrix, which we call *derived-incidence matrix*.

Definition 2.19 (Derived-incidence matrix). If all zeros of an incidence matrix are replaced by a special symbol blank, the derived matrix is called derived-incidence matrix.

Fact 2 ([23]). The incidence matrix M of a (v, b, r, k, λ)-BIBD (or the derived-incidence matrix M' obtained from M) satisfies the following properties:

(1) Every column of M (or M') contains exactly k ones.
(2) Every row of M (or M') contains exactly r ones;
(3) Two distinct rows of M (or M') both contain ones in exactly λ columns.

2.4 Jensen's inequality

Theorem 2.20 ([22]). *Suppose that f is a continuous and strictly convex function on the interval I. Suppose further that $\sum_{i=0}^{b-1} t_i = 1$, $0 < t_i$ and $0 \le i \le b-1$. Then $f(\sum_{i=0}^{b-1} t_i k_i) \le \sum_{i=0}^{b-1} t_i f(k_i)$, where $k_i \in I$, $0 \le i \le b-1$. Further, equality occurs if and only if $k_0 = k_1 = \cdots = k_{b-1}$.*

If we take the convex function $f(x) = \frac{x(x-1)}{2}$ and use Jensen's inequality, Lemma 2.21 can be verified easily.

Lemma 2.21. *Let $\sum_{i=0}^{b-1} k_i = n$, where all k_i are positive integers. Then*

$$b \times \frac{\frac{n}{b} \times (\frac{n}{b} - 1)}{2} \leq \sum_{i=0}^{b-1} \binom{k_i}{2}.$$

If $\frac{n}{b} = k$ is an integer, then

$$b \times \binom{k}{2} \leq \sum_{i=0}^{b-1} \binom{k_i}{2}.$$

Proof. Let $f(x) = \frac{x(x-1)}{2}$. Also let $t_i = \frac{1}{b}$ for all $i \in \{0, \ldots, b-1\}$. So,

$$f\left(\sum_{i=0}^{b-1} t_i k_i\right) = f(\frac{n}{b}) = \frac{\frac{n}{b} \times (\frac{n}{b} - 1)}{2}.$$

Also $\sum_{i=0}^{b-1} t_i f(k_i) = \frac{1}{b} \sum_{i=0}^{b-1} \binom{k_i}{2}$. Thus from Theorem 2.20,

$$\frac{\frac{n}{b} \times (\frac{n}{b} - 1)}{2} \leq \frac{1}{b} \sum_{i=0}^{b-1} \binom{k_i}{2}.$$

Hence we have proved the result. □

3 Finding $v_1^{v,b}$ where $(v, b, k, r, 1)$ is a BIBD

One approach for constructing an MDS matrix is to construct first an almost-bi-regular matrix with l ones and then assign nonzero field elements other than 1 to the rest of the positions of the matrix. If the resultant matrix is MDS, return that MDS matrix, else return failure. The above mentioned process can be repeated iteratively

(a) by trying all possible nonzero elements other than 1 for fixed l,
(b) through all choices of l starting from maximum number of ones that matrix can accommodate till 0.

For efficiency, in the resultant MDS matrix M, it is desired to have a high value of v_1 and a low value of c_1 as much as possible. In [12], the authors computed the maximum number of occurrences of 1 in a $d \times d$ matrix, i.e. $v_1^{d,d}$ for d up to 8 and also determined the position of ones in the corresponding bi-regular matrices. With their approach, determining $v_1^{d,d}$ seems difficult for higher values of d.

In this section, we study the connection between the incidence matrix of BIBD and the almost-bi-regular matrix and propose techniques to compute the value of $v_1^{v,b}$ whenever there exists a $(v, b, r, k, 1)$-BIBD. In the following lemma, we show that the derived-incidence matrix of (v, b, r, k, λ)-BIBD is an almost-bi-regular matrix whenever $\lambda = 1$. Not only that, this section furthermore shows that the maximum number of ones which can be put in a $v \times b$ almost-bi-regular matrix is equal to the number of ones in the derived-incidence matrix of $(v, b, r, k, 1)$-BIBD. The equality in the number of ones in both the almost-bi-regular matrix and the derived-incidence matrix of $(v, b, r, k, 1)$-BIBD seems obvious considering the fact that the derived-incidence matrix of (v, b, r, k, λ)-BIBD is an almost-bi-regular matrix whenever $\lambda = 1$. But, this section presents something more: the maximality of ones. To the best of our knowledge, the literature on BIBDs deals only with the existence and constructions, while this section provides a result which proves that those constructions, in fact, yield the maximum number of ones as well.

Lemma 3.1. *The derived-incidence matrix of (v, b, r, k, λ)-BIBD is an almost-bi-regular matrix if and only if $\lambda = 1$.*

Proof. Let us consider the (v, b, r, k, λ)-BIBD, where $\lambda = 1$. Let the set of elements and the set of blocks of this BIBD be $X = \{x_0, \ldots, x_{v-1}\}$ and $\mathcal{A} = \{A_0, \ldots, A_{b-1}\}$, respectively. Let the corresponding $v \times b$ derived-incidence matrix be $M = ((m_{i,j}))$. So, from the definition of the derived-incidence matrix, $m_{i,j} = 1$ if $x_i \in A_j$ for any $i \in \{0, 1, \ldots, v-1\}$ and $j \in \{0, 1, \ldots, b-1\}$; otherwise $m_{i,j}$ is blank.

Let us consider any arbitrary 2×2 submatrix

$$M_1 = \begin{pmatrix} m_{s_1,t_1} & m_{s_1,t_2} \\ m_{s_2,t_1} & m_{s_2,t_2} \end{pmatrix}$$

of M. Note that not all elements of the submatrix are 1 because then we will get $m_{s_i,t_j} = 1$ for $i, j \in \{1, 2\}$. This implies that the elements x_{s_1} and x_{s_2} are contained simultaneously in two blocks A_{t_1} and A_{t_2}, which is a contradiction to the fact that $\lambda = 1$, i.e. a pair of elements can be contained in only one block. So all four elements of any 2×2 submatrix of M are not 1. Thus M is almost-bi-regular.

If $\lambda > 1$, then some pair of elements, say x_{s_1} and x_{s_2}, will occur in at least two blocks, say, A_{t_1} and A_{t_2}. Thus in the 2×2 submatrix M_1 all four entries are 1. So M is not almost-bi-regular. □

Remark 3.2. Let M be the derived-incidence matrix of a BIBD with $\lambda = 1$. We cannot add any more 1 in the matrix M without disturbing the almost-bi-regular property. For example, suppose that the (i, j)-th entry is blank and let us fill the (i, j)-th entry by 1. Also, let us consider any other element of the block A_j, say, x_k. The elements x_i and x_k must be contained in some block, say, A_l. So, $m_{k,l} = m_{k,j} = m_{i,l} = m_{i,j} = 1$. So clearly the 2×2 submatrix formed by taking the k-th row, the i-th row, the l-th column and the j-th column of the matrix M is not almost-bi-regular.

Remark 3.3. Let M be any almost-bi-regular matrix such that no more 1 can be added in the matrix without disturbing the almost-bi-regular property. Note that this condition does not always guarantee that an almost-bi-regular matrix has maximum number of ones.

$$\left(\begin{array}{c|c|c|c} 1 & 1 & 1 & 1 \\ \hline 1 & & & \\ \hline 1 & & & \\ \hline 1 & & & \end{array}\right),$$

no more 1 can be placed without disturbing the bi-regular property. Here the number of occurrences of 1 is 7, but we know $v_1^{4,4} = 9$ and the corresponding matrix may be

$$\left(\begin{array}{c|c|c|c} & 1 & 1 & 1 \\ \hline 1 & 1 & & \\ \hline 1 & & 1 & \\ \hline 1 & & & 1 \end{array}\right).$$

Remark 3.4. Let $M = ((m_{i,j}))$ be any $v \times b$ almost-bi-regular matrix. Let us associate the element x_i corresponding to the i-th row and the block A_j corresponding to the j-th column, where $i \in \{0, \ldots, v-1\}$ and $j \in \{0, \ldots, b-1\}$. Let us consider the design $(X, \mathcal{A})$, where $X = \{x_0, \ldots, x_{v-1}\}$ and $\mathcal{A} = \{A_0, \ldots, A_{b-1}\}$ such that $m_{i,j} = 1$ if and only if $x_i \in A_j$. So M is the derived-incidence matrix of the design $(X, \mathcal{A})$. Note that, since M is almost-bi-regular, any pair of elements will occur in at most one of the blocks of $\mathcal{A}$, i.e. $|A_i \cap A_j| \leq 1$ for all $i, j \in \{0, \ldots, b-1\}$ and $i \neq j$.

In Theorem 3.8, we will show that the derived-incidence matrices of BIBDs with $\lambda = 1$ contain the maximum number of ones maintaining the almost-bi-regular property. But before that, we study some crucial properties of almost-bi-regular matrices and derived-incidence matrices of BIBDs with $\lambda = 1$ in Lemma 3.5, Lemma 3.6 and Lemma 3.7.

Lemma 3.5. *Let M be the derived-incidence matrix of a design $(X, \mathcal{A})$, where $|X| = v$ and $|\mathcal{A}| = b$. Also for an element $x \in X$, let us define the set $\mathcal{S}_x$ as follows: $\mathcal{S}_x = \{(x, y, A) : x, y \in A \text{ and } A \in \mathcal{A},\ y \in X\}$. If M is almost-bi-regular matrix, then $|\mathcal{S}_x| \leq v - 1$.*

Proof. An element x can form maximum $v - 1$ pairs (x, y) with all different $v - 1$ elements. More than $v - 1$ pairs involving x amounts to repetition of some pair in more than one blocks, but since M is almost-bi-regular matrix, any pair of elements (x, y) occurs at most once. Hence we have proved the result. □

Lemma 3.6. *Let M be the derived-incidence matrix of a design $(X, \mathcal{A})$, where $|X| = v$ and $|\mathcal{A}| = b$. Also let us define the set $\mathcal{S}$ as follows: $\mathcal{S} = \{(x, y, A) : x, y \in A \text{ and } A \in \mathcal{A}\}$. If M is an almost-bi-regular matrix, then $|\mathcal{S}| \leq \binom{v}{2}$.*

Proof. Since M is an almost-bi-regular matrix, any pair of elements (x, y) occurs at most in one of the blocks of $\mathcal{A}$. So if $(x, y, A_i) \in \mathcal{S}$, then (x, y) will not be contained in any blocks of $\mathcal{A}$ except A_i. Since there are $\binom{v}{2}$ pairs that can be formed from the elements of X, we have $|\mathcal{S}| \le \binom{v}{2}$. □

Lemma 3.7. *Let the design $(X, \mathcal{A})$ be a $(v, b, r, k, 1)$-BIBD and define $\mathcal{S}$ by $\mathcal{S} = \{(x, y, A) : x, y \in A \text{ and } A \in \mathcal{A}\}$. Then $|\mathcal{S}| = \binom{v}{2}$.*

Proof. Note that in a $(v, b, r, k, 1)$-BIBD, every pair of elements of X occurs exactly in one block. So, $|\mathcal{S}| = \binom{v}{2}$. Alternatively, each block has k elements. Hence, each block contributes $\binom{k}{2}$ elements in $\mathcal{S}$. Since there are b blocks, we have

$$|\mathcal{S}| = \binom{k}{2} \times b = \frac{k(k-1)}{2} \times \frac{vr}{k} = \frac{k(k-1)}{2} \times v \times \frac{(v-1)}{(k-1) \times k} = \frac{v(v-1)}{2} = \binom{v}{2}.$$ □

Theorem 3.8. *Let there exist some $(v, b, r, k, 1)$-BIBD whose derived-incidence matrix is M. Then M has the maximum number of ones, i.e. $v_1^{v,b}$ is the number of ones and $v_1^{v,b} = bk$.*

Proof. Let $(X, \mathcal{A})$ be the $(v, b, r, k, 1)$-BIBD. From Lemma 3.1 and Fact 2, M is almost-bi-regular matrix with bk ones. From Lemma 3.7, $|\mathcal{S}| = \binom{v}{2}$, where $\mathcal{S} = \{(x, y, A) : x, y \in A \text{ for some } A \in \mathcal{A}\}$.

Let, if possible, there be a $v \times b$ almost-bi-regular matrix M' having $(bk + 1)$ ones. For the matrix M', let the corresponding design be $(X, \mathcal{A}')$, where $\mathcal{A}' = \{A'_0, \ldots, A'_{b-1}\}$. Similar to $\mathcal{S}$, let us define the set $\mathcal{S}'$ as follows:

$$\mathcal{S}' = \{(x, y, A) : x, y \in A \text{ for some } A \in \mathcal{A}'\}.$$

Let M'' be the matrix obtained by replacing one occurrence of 1 by blank from, say, the p-th column of M' which has at least two elements. Now M'' has $b \times k$ ones. For the matrix M'', let the corresponding design be $(X, \mathcal{A}'')$, where $\mathcal{A}'' = \{A''_0, \ldots, A''_{b-1}\}$. Let us define the set $\mathcal{S}''$ as follows:

$$\mathcal{S}'' = \{(x, y, A) : x, y \in A \text{ for some } A \in \mathcal{A}''\}.$$

So, $|A'_i| = |A''_i|$ for $i = 0, \ldots, p-1, p+1, \ldots, b-1$ and $|A'_p| = |A''_p| + 1$. Let $|A''_i| = k''_i$ for $i = 0, \ldots, b-1$. Hence, the number of elements in M'' is $b \times k = \sum_{i=0}^{b-1} k''_i$. Also, the block A''_i contributes $\binom{k''_i}{2}$ elements in $\mathcal{S}''$. So,

$$|\mathcal{S}''| = \sum_{i=0}^{b-1} \binom{k''_i}{2}.$$

From Lemma 2.21,

$$\sum_{i=0}^{b-1} \binom{k''_i}{2} \ge b \times \binom{k}{2} = \binom{v}{2} = |\mathcal{S}|.$$

So, $|\mathcal{S}''| \ge |\mathcal{S}|$. Also, $|\mathcal{S}'| = |\mathcal{S}''| + |A''_p|$. So, $|\mathcal{S}'| > |\mathcal{S}| = \binom{v}{2}$, a contradiction to Lemma 3.6. □

Corollary 3.9. *Let $d = q^2 + q + 1$, where q is any prime power. Then $v_1^{d,d} = (q^2 + q + 1) \times (q + 1)$.*

Proof. Let us consider the (v, b, r, k, λ)-BIBD, where $v = b = q^2 + q + 1$, $r = k = q + 1$ and $\lambda = 1$, and let M be its derived-incidence matrix. From Theorem 2.17, such a BIBD exists for any prime power q. From Lemma 3.1, M is almost-bi-regular and from Theorem 3.8, the number of ones in M is $v^{d,d} = (q^2 + q + 1) \times (q + 1)$. □

Remark 3.10. From Corollary 3.9, if $q = 3$, then $d = 3^2 + 3 + 1 = 13$ and thus $v_1^{13,13} = 13 \times (3 + 1) = 52$ and the corresponding matrix is given in Figure 4. Similarly, when $q = 2^2 = 4$, then $d = 4^2 + 4 + 1 = 21$ and thus $v_1^{21,21} = 21 \times (4 + 1) = 105$ and the corresponding matrix is given in Figure 15 of Appendix A.3.

Let M be an almost-bi-regular matrix having maximum number of ones and also let the corresponding design be $(X, \mathcal{A})$. If $(X, \mathcal{A})$ is a BIBD, then for any two elements of X, say x_s and x_t, there always exists a block A of $\mathcal{A}$ such that $x_s, x_t \in A$. If $(X, \mathcal{A})$ is not a BIBD, then such a block may not exist. For example, let us consider the 6×6 matrix of Figure 1. This matrix is an almost-bi-regular matrix with maximum number of ones, but the pair (x_0, x_1) does not occur in any block. Note that Theorem 3.8 can compute the value $v_1^{v,b}$ if there exists a (v, b, r, k, λ)-BIBD, where $\lambda = 1$.

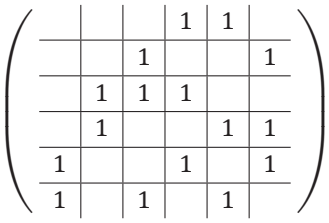


Figure 1. Example of 6×6 almost-bi-regular matrices having sixteend ones which is maximum.

4 Some results on $v_1^{v,b}$ for arbitrary v and b

In this section, we study some upper bounds of $v_1^{v,b}$ for arbitrary v and b. We also determine $v_1^{d,d}$ for d up to 21. In doing so, we first develop tools which are useful. For simplicity and compactness of expression, here we first introduce some notations, definitions and discuss few crucial properties, some of which resemble properties of previous section.

4.1 A few more definitions and notations

Let $M = (m_{ij})$ be a $v \times b$ matrix. Let $R_i = (m_{i0}, m_{i1}, \ldots, m_{i(b-1)})$ and $C_j = (m_{0j}, m_{1j}, \ldots, m_{(v-1)j})$, i.e. the i-th row and the j-th column, respectively. We assume that $0 \le i \le v-1$ and $0 \le j \le b-1$.

We define $R_i \wedge C_j = m_{ij} = C_j \wedge R_i$. If m_{ij} is 1, we say $R_i \wedge C_j = C_j \wedge R_i = 1$, else 0. If $R_i \wedge C_j = C_j \wedge R_i = 1$, we say that the row R_i makes an *intersection* with the column C_j and vice versa.

We define $R_i \wedge R_k = \{j : 0 \le j \le b-1 \text{ and } R_i \wedge C_j = R_k \wedge C_j = 1\}$, i.e. the index set corresponding to these blocks containing both the elements corresponding to R_i and R_k. Similarly, we define

$$C_i \wedge C_k = \{j : 0 \le j \le v-1 \text{ and } C_i \wedge R_j = C_k \wedge R_j = 1\},$$

i.e. the set of elements that are contained in both the blocks corresponding to C_i and C_k.

Let $i \ne j$. If $|R_i \wedge R_j| \ge 1$, then we say that the row R_i makes *pair* with the row R_j. Similarly, if $|C_i \wedge C_j| \ge 1$, then we say that the column C_i makes *pair* with the column C_j. It may be noted that for almost-bi-regular matrices $|R_i \wedge R_j| \le 1$ and $|C_i \wedge C_j| \le 1$ for all distinct indices i, j, which directly follows from the definition of almost-bi-regular matrices. So we have the following lemma.

Lemma 4.1. *Let M be a $v \times b$ matrix. Then M is an almost-bi-regular matrix if and only if $|R_i \wedge R_k| \le 1$ for all $0 \le i < k \le v-1$ and $|C_i \wedge C_k| \le 1$ for all $0 \le i < k \le b-1$.*

Set $|R_i| = |R_i \wedge R_i|$, i.e. the number of columns which *intersect* with the row R_i, and similarly $|C_i| = |C_i \wedge C_i|$ which denotes the number of rows which *intersect* with the column C_i. Let $\max(|C|) = \max\{|C_i|\}_{i=0}^{b-1}$ and $\max(|R|) = \max\{|R_i|\}_{i=0}^{v-1}$. In a similar manner, we define $\min(|C|) = \min\{|C_i|\}_{i=0}^{b-1}$ and $\min(|R|) = \min\{|R_i|\}_{i=0}^{v-1}$. The following two lemmas give interpretations of $|R_i|$ and $|C_j|$, respectively.

Lemma 4.2. *Let M be a $v \times b$ almost-bi-regular matrix. Then the row R_i contains l ones if and only if $|R_i| = l$.*

Proof. Let $J = \{0, 1, \ldots, b-1\}$. Suppose that $|R_i| = |R_i \wedge R_i| = l$. By definition,

$$R_i \wedge R_i = \{j : 0 \le j \le b-1 \text{ and } |R_i \wedge C_j| = 1\}.$$

Let $J_1 = R_i \wedge R_i = \{j_1, j_2, \ldots, j_l\} \subseteq J$. Then we have $R_i \wedge C_j = m_{ij} = 1$ if and only if $j \in J_1$. Hence we obtain that $R_i = (m_{i0}, m_{i1}, \ldots, m_{i(b-1)})$ contains $|J_1| = l$ ones. Conversely, suppose that $R_i = (m_{i0}, m_{i1}, \ldots, m_{i(b-1)})$ contains l ones. Let $J_1 = \{j_1, \ldots, j_n\} \subseteq J$ be the set of indices such that $m_{ij} = 1$ if and only if $j \in J_1$. So, $|J_1| = l$. Moreover, $|R_i \wedge C_j| = 1$ if and only if $j \in J_1$. Therefore, $R_i \wedge R_i = J_1$ and thus $|R_i| = |R_i \wedge R_i| = |J_1| = l$. □

Similarly, we have the following lemma.

Lemma 4.3. *Let M be a $v \times b$ almost-bi-regular matrix. Then the column C_i contains l ones if and only if $|C_i| = l$.*

In the following lemma, we study the correlation between the number of *intersections* and the number of *pairs* that the row R_i makes with different columns and rows, respectively, in an almost-bi-regular matrix.

Lemma 4.4. *Let M be a $v \times b$ almost-bi-regular matrix. Suppose that the row R_i makes intersections with exactly l columns, $C_{j_1}, C_{j_2}, \ldots, C_{j_l}$. If $|C_{j_k}| = c_k$, for $1 \le k \le l$, then the row R_i makes pair with exactly $\sum_{k=1}^{l}(c_k - 1)$ rows.*

Proof. Let $J_1^{(j_k)} = C_{j_k} \wedge C_{j_k}$. Since $|C_{j_k}| = c_k$, it follows that $|J_1^{(j_k)}| = c_k$. Since R_i intersects with column C_{j_k}, we obtain $i \in J_1^{(j_k)}$. Let

$$\overline{J_1}^{(j_k)} = J_1^{(j_k)} \setminus \{i\}.$$

So, $|\overline{J_1}^{(j_k)}| = c_k - 1$.

Now, we show that $\overline{J_1}^{(j_m)} \cap \overline{J_1}^{(j_n)} = \emptyset$ for all $1 \le m < n \le l$. If not, there exists $t \ne i$ for some r, s such that $1 \le r < s \le l$, $0 \le t \le v - 1$ and $t \in \overline{J_1}^{(j_r)} \cap \overline{J_1}^{(j_s)}$. Therefore, $|R_t \wedge C_{j_r}| = |R_t \wedge C_{j_s}| = 1$ which then implies $m_{tj_r} = m_{tj_s} = 1$. Since R_i makes pair with columns C_{j_r} and C_{j_s}, we have $|R_i \wedge C_{j_r}| = |R_i \wedge C_{j_s}| = 1$ which then implies $m_{ij_r} = m_{ij_s} = 1$. Consider a 2×2 submatrix formed by the rows R_i, R_t and columns C_{j_r}, C_{j_s}. The entries of this submatrix will be $m_{ij_r}, m_{ij_s}, m_{tj_r}, m_{tj_s}$ and all are 1, a contradiction. Hence,

$$\overline{J_1}^{(j_m)} \cap \overline{J_1}^{(j_n)} = \emptyset$$

for all $1 \le m < n \le l$.

Choose any $t \in \overline{J_1}^{(j_k)}$. Since $t \in \overline{J_1}^{(j_k)}$, we have $|R_t \wedge C_{j_k}| = 1$. Moreover, $|R_i \wedge C_{j_k}| = 1$ and thus $j_k \in R_i \wedge R_t$. Therefore, $|R_i \wedge R_t| \ge 1$, but from Lemma 4.1, $|R_i \wedge R_t| \le 1$ which then implies $|R_i \wedge R_t| = 1$. Hence, the row R_i makes pair with the row R_t. Conversely, suppose that R_i makes pair with some row R_t. Then $|R_i \wedge R_t| = 1$. Let $z \in R_i \wedge R_t$. Then $|R_i \wedge C_z| = |R_t \wedge C_z| = 1$ and therefore $t \in C_z \wedge C_z$. Since R_i makes pair with C_z, it follows that $z \in \{j_1, j_2, \ldots, j_l\}$. Thus $t \in \overline{J_1}^{(j_k)}$ for some $1 \le k \le l$. Therefore the row R_i makes pair with the row R_t if and only if $t \in \overline{J_1}^{(j_k)}$ for some $1 \le k \le l$.

Let $J_1 = \bigcup_{k=1}^{l} \overline{J_1}^{(j_k)}$. As $\overline{J_1}^{(j_m)} \cap \overline{J_1}^{(j_n)} = \emptyset$ for all $1 \le m < n \le l$, we have

$$|J_1| = \sum_{k=1}^{l} |\overline{J_1}^{(j_k)}| = \sum_{k=1}^{l} (c_k - 1).$$

Therefore, the row R_i makes pair with $\sum_{k=1}^{l}(c_k - 1)$ rows. □

Similarly, by interchanging rows and columns, we have the following lemma.

Lemma 4.5. *Let M be a $v \times b$ almost-bi-regular matrix. Suppose that the column C_i makes intersections with exactly l rows, say $R_{j_1}, R_{j_2}, \ldots, R_{j_l}$. If $|R_{j_k}| = r_k$, then the column C_i makes pair with exactly $\sum_{k=1}^{l}(r_k - 1)$ columns.*

In a $v \times b$ almost-bi-regular matrix, any row can make pair with at most $v - 1$ rows and similarly any column can make pair with at most $b - 1$ columns. So we have the following two lemmas which are similar to Lemma 3.6 but in a different setting.

Lemma 4.6. *Let M be a $v \times b$ almost-bi-regular matrix. Suppose that $|C_i| = k_i$ for $0 \le i \le b - 1$. Then*

$$\sum_{i=0}^{b-1} \binom{k_i}{2} \le \binom{v}{2}.$$

Proof. Let $C_i \wedge C_i = \{j_1, j_2, \ldots, j_{k_i}\}$ and $\mathcal{I}_i = \{(j_r, j_s) : 1 \le r < s \le k_i\}$. We now show that $\mathcal{I}_m \cap \mathcal{I}_n = \emptyset$ for all $0 \le m < n \le b - 1$. If not, then for some $0 \le m < n \le b - 1$ and for some $0 \le p < q \le v - 1$, the tuple (p, q) is an element of $\mathcal{I}_m \cap \mathcal{I}_n$. So, $p, q \in C_m \wedge C_m$ and $p, q \in C_n \wedge C_n$. Thus

$$|R_p \wedge C_m| = |R_q \wedge C_m| = |R_p \wedge C_n| = |R_q \wedge C_n| = 1$$

which then implies there exists a 2×2 submatrix all of whose entries are 1, a contradiction. Hence $\mathcal{I}_m \cap \mathcal{I}_n = \emptyset$ for all $0 \le m < n \le b - 1$.

Let $\mathcal{I} = \{(p, q) : 0 \le p < q \le v-1\}$. It is easy to check that $\bigcup_{i=0}^{b-1} \mathcal{I}_i \subseteq \mathcal{I}$ and therefore $|\bigcup_{i=0}^{b-1} \mathcal{I}_i| \le |\mathcal{I}| = \binom{v}{2}$. Since $\mathcal{I}_m \cap \mathcal{I}_n = \emptyset$, we have

$$\left|\bigcup_{i=0}^{b-1} \mathcal{I}_i\right| = \sum_{i=0}^{b-1} |\mathcal{I}_i| = \sum_{i=0}^{b-1} \binom{k_i}{2} \le |\mathcal{I}| = \binom{v}{2}.$$

Hence the lemma. □

Similarly, by interchanging rows and columns, we have the following lemma.

Lemma 4.7. *Let M be a $v \times b$ almost-bi-regular matrix. Suppose that $|R_i| = k_i$ for $0 \le i \le v-1$. Then*

$$\sum_{i=0}^{v-1} \binom{k_i}{2} \le \binom{b}{2}.$$

Now we define $\mathcal{F}_b(v)$, which is crucial for determining the upper bound of $v_1^{v,b}$.

Definition 4.8. Let b and v be two non-negative integers. We define $\mathcal{F}_b(v) = \lfloor \frac{b+\sqrt{b^2+4bv(v-1)}}{2} \rfloor$.

In Theorem 4.13, we study the upper bound of $v_1^{v,b}$. Before that, we study two important properties of $\mathcal{F}_b(v)$ in Lemma 4.9 and Lemma 4.10, which can be verified by elementary arithmetic.

Lemma 4.9. *If $1 \le v \le b$, then* $\min(\mathcal{F}_v(b), \mathcal{F}_b(v)) = \mathcal{F}_b(v)$.

Lemma 4.10. *If $1 \le v$ and $1 \le b$, then* $\mathcal{F}_b(v+1) - \mathcal{F}_b(v) \ge 1$.

Now we introduce another term, $\mathcal{G}_d(d)$, which helps in determining maximum number of ones in a matrix where some row or column previously contains a fixed number of ones.

Definition 4.11. Let $d \ge 1$. We define $\mathcal{G}_d(d) = 2d-1$ and $\mathcal{G}_d(k) = k + d - 1 + \mathcal{F}_{d-1}(d-k)$ for $0 \le k \le d-1$.

In the next lemma, we show that $\mathcal{G}_d(k)$ is monotone decreasing.

Lemma 4.12. *We have $\mathcal{G}_d(k+1) \le \mathcal{G}_d(k)$ for $d \ge 2$ and $0 \le k \le d-1$.*

Proof. If $0 \le k \le d-2$, then

$$\mathcal{G}_d(k+1) - \mathcal{G}_d(k) = 1 + \mathcal{F}_{d-1}(d-k-1) - \mathcal{F}_{d-1}(d-k).$$

Let $d-1 = b$ and $d-k-1 = a$. Since $d \ge 2$ and $0 \le k \le d-2$, we have $b \ge 1$ and $1 \le d-k-1 = a \le d-1$. Therefore,

$$\mathcal{G}_d(k+1) - \mathcal{G}_d(k) = 1 + \mathcal{F}_b(a) - \mathcal{F}_b(a+1).$$

From Lemma 4.10, $\mathcal{G}_d(k+1) - \mathcal{G}_d(k) \le 1 - 1 = 0$.

If $k = d-1$, then

$$\mathcal{G}_d(k+1) - \mathcal{G}_d(k) = 2d - 1 - (d-1) - d + 1 - \mathcal{F}_{d-1}(1) = 1 - (d-1) = 2 - d \le 0.$$ □

4.2 Some important bounds

In Theorem 4.13 and its corollary, we provide a tight upper bound of $v_1^{v,b}$ and $v_1^{d,d}$ for all values of v, b and d.

Theorem 4.13. *We have* $v_1^{v,b} \le \min(\mathcal{F}_v(b), \mathcal{F}_b(v))$.

Proof. Let $v_1^{v,b} = n$. Also let $|R_i| = r_i$ and $|C_i| = c_i$. Then

$$\sum_{i=0}^{v-1} r_i = n, \quad \sum_{i=0}^{v-1} \binom{r_i}{2} \le \binom{b}{2} \tag{1}$$

from Lemma 4.7, and

$$\sum_{i=0}^{b-1} c_i = n, \quad \sum_{i=0}^{b-1} \binom{c_i}{2} \le \binom{v}{2} \tag{2}$$

from Lemma 4.6. From Jensen's inequality, when (1) holds, we get

$$v \times \binom{\frac{n}{v}}{2} \le \sum_{i=0}^{v-1} \binom{r_i}{2} \le \binom{b}{2}.$$

Solving the above inequality, we get $n^2 - nv - bv(b-1) \le 0$ which then implies

$$n \le \frac{v + \sqrt{v^2 + 4vb(b-1)}}{2}.$$

So,

$$n \le \left\lfloor \frac{v + \sqrt{v^2 + 4vb(b-1)}}{2} \right\rfloor = \mathcal{F}_v(b).$$

Similarly, when (2) holds, we get $n \le \mathcal{F}_b(v)$. Thus, $n \le \min(\mathcal{F}_v(b), \mathcal{F}_b(v))$. □

Corollary 4.14. *We have*

$$v_1^{d,d} \le \left\lfloor d \times \frac{1 + \sqrt{4d-3}}{2} \right\rfloor.$$

Proof. Putting $v = b = d$ in Corollary 4.13, we get

$$v_1^{d,d} \le \mathcal{F}_d(d) = \left\lfloor d \times \frac{1 + \sqrt{4d-3}}{2} \right\rfloor.$$ □

Remark 4.15. For any prime power q, there exists a projective plane which is a symmetric $(q^2+q+1, q^2+q+1, q+1, q+1, 1)$-BIBD. From Corollary 4.14,

$$v_1^{(q^2+q+1, q^2+q+1)} \le \left\lfloor (q^2+q+1) \times \frac{1 + \sqrt{4(q^2+q+1)-3}}{2} \right\rfloor = (q^2+q+1) \times (q+1).$$

Also, note that, from Theorem 3.8, $v_1^{(q^2+q+1, q^2+q+1)} = (q^2+q+1) \times (q+1)$. So, when $d = q^2+q+1$ for some prime power q,

$$v_1^{d,d} = \left\lfloor d \times \frac{1 + \sqrt{4d-3}}{2} \right\rfloor.$$

Similarly, when $(v, b, r, k, 1)$-BIBD exists, $v_1^{v,b} = \mathcal{F}_b(v)$.

In the next theorem, we study the upper bound of $v_1(M)$ for a $d \times d$ matrix M where one of its columns contains k ones.

Theorem 4.16. *Let M be a $d \times d$ almost-bi-regular matrix with one column having k occurrences of 1. Then $v_1(M) \le \mathcal{G}_d(k)$.*

Proof. We consider two cases.

Case $d = 1$. If $k = 0$, then

$$\mathcal{G}_d(k) = k + d - 1 + \mathcal{F}_{d-1}(d-k) = 0 + 1 - 1 + \mathcal{F}_0(1) = 0.$$

If $k = 1$, then

$$\mathcal{G}_d(k) = 2d - 1 = 1.$$

Case $d \ge 2$. If $k = 0$, then the maximum number of ones in M can be at most $\mathcal{F}_d(d-1)$. From Lemma 4.9,

$$\mathcal{F}_d(d-1) \le \mathcal{F}_{d-1}(d) < k + d - 1 + \mathcal{F}_{d-1}(d-k) = \mathcal{G}_d(k).$$

If $k = d$, then the maximum number of ones in M can be at most $d + d - 1 = 2d - 1 = \mathcal{G}_d(k)$.

Let $1 \le k \le d-1$. Without loss of generality, assume that the matrix M contains exactly k ones in column C_0. We further assume that $|R_i \wedge C_0| = 1$ for all $0 \le i \le k-1$ and $|R_j \wedge C_0| = 0$ for all $k \le j \le d-1$. Consider a submatrix of M, say M_1, formed by rows $R_0, R_1, \ldots, R_{k-1}$ and columns $C_0, C_1, C_2, \ldots, C_{d-1}$. Consider another submatrix of M, say M_2, formed by rows $R_k, R_{k+1}, \ldots, R_{d-1}$ and columns $C_0, C_1, \ldots, C_{d-1}$. Since any submatrix of an almost-bi-regular matrix is almost-bi-regular, therefore M_1 and M_2 also will be almost-bi-regular.

In the matrix M_1, the column C_0 makes pair with the rows $R_0, R_1, \ldots, R_{k-1}$, i.e. $|R_i \wedge C_0| = 1$ for all $0 \le i \le k-1$. Therefore, $|C_j| \le 1$ for all $1 \le j \le d-1$. If not, then say $|C_t| \ge 2$ for some $1 \le t \le d-1$. Since $|C_t| \ge 2$, there exists at least two rows R_{j_1}, R_{j_2} for some $0 \le j_1 < j_2 \le k-1$ such that $|R_{j_1} \wedge C_t| = |R_{j_2} \wedge C_t| = 1$. So, $t \in R_{j_1} \wedge R_{j_2}$. But $0 \in R_{j_1} \wedge R_{j_2}$ (as $|R_{j_1} \wedge C_0| = |R_{j_2} \wedge C_0| = 1$). Thus we have $\{0, t\} \subseteq R_{j_1} \wedge R_{j_2}$ which implies $|R_{j_1} \wedge R_{j_2}| \ge 2$, a contradiction (by Lemma 4.1). Hence $|C_j| \le 1$ for all $1 \le j \le d-1$. So the total number of ones in the matrix M_1 will be at most $\sum_{i=0}^{d-1} |C_i| = k + d - 1$.

In the matrix M_2, the column C_0 contains no ones, i.e. $|C_0| = 0$. Consider the $d-k \times d-1$ submatrix $\bar{M}_2$ of the matrix M_2 formed by rows $R_k, \ldots, R_{d-1}$ and columns $C_1, \ldots, C_{d-1}$. Since M_2 is almost-bi-regular, therefore $\bar{M}_2$ also is almost-bi-regular. Hence, the maximum number of ones in $\bar{M}_2$ can be $v_1^{d-k,d-1}$.

Thus, the total number of ones in matrix M can be at most

$$k + d - 1 + v_1^{d-k,d-1} \le k + d - 1 + \mathcal{F}_{d-1}(d-k) = \mathcal{G}_d(k)$$

(from Theorem 4.13). □

In analyzing $v_1^{d,d}$, we often encounter situations where we need to determine the number of columns (rows) needed to accommodate some r rows (columns) of a $v \times b$ almost-bi-regular matrix, each containing, say, k ones. In the next two theorems, we explore lower bound on number of such rows (columns).

Theorem 4.17. *In a $v \times b$ almost-bi-regular matrix, if there are r rows ($r \le v$) each containing k ones, then the number of columns needed to accommodate such r rows should be at least*

$$\max\left(\left\lceil \frac{1 + \sqrt{1 + 4rk(k-1)}}{2} \right\rceil, \left\lceil \frac{rk^2}{r+k-1} \right\rceil\right).$$

Proof. Let the minimum number of columns required to accommodate such r rows be c. Consider the $r \times c$ submatrix M where each row contains exactly k ones. Suppose that, in the matrix M, column C_i contains k_i ones. Then $\sum_{i=0}^{c-1} k_i = rk$. For M to be almost-bi-regular matrix, it is required that
(1) $r\binom{k}{2} \le \binom{c}{2}$ (from Lemma 4.7),
(2) $\sum_{i=0}^{c-1} \binom{k_i}{2} \le \binom{r}{2}$ (from Lemma 4.6).
For (1) to hold, it is required that $rk(k-1) \le c(c-1)$ which then implies $c^2 - c - rk(k-1) \ge 0$. Thus,

$$c \ge \frac{1 + \sqrt{1 + 4rk(k-1)}}{2}$$

and hence

$$c \ge \left\lceil \frac{1 + \sqrt{1 + 4rk(k-1)}}{2} \right\rceil. \tag{a}$$

From Jensen's inequality, when (2) holds, we get

$$\frac{rk(rk-c)}{2c} \le \sum_{i=0}^{c-1} \binom{k_i}{2} \le \binom{r}{2}.$$

From above inequality, we get $c \ge \frac{rk^2}{r+k-1}$ and hence

$$c \ge \left\lceil \frac{rk^2}{r+k-1} \right\rceil. \tag{b}$$

From (a) and (b), we conclude that

$$c \ge \max\left(\left\lceil \frac{1 + \sqrt{1 + 4rk(k-1)}}{2} \right\rceil, \left\lceil \frac{rk^2}{r+k-1} \right\rceil\right),$$

as desired. □

Similarly by interchanging rows and columns, we have the following theorem.

Theorem 4.18. *In a $v \times b$ almost-bi-regular matrix, if there are c columns ($c \le b$) each containing k ones, then the number of rows needed to accommodate such c columns should be at least*

$$\max\left(\left\lceil \frac{1 + \sqrt{1 + 4ck(k-1)}}{2} \right\rceil, \left\lceil \frac{ck^2}{c+k-1} \right\rceil\right).$$

4.3 Finding $v_1^{d,d}$ for d up to 21

For $d = q^2 + q + 1$, where q is any prime power, $v_1^{d,d}$ can be computed using Corollary 3.9. With this technique we handle the case when $d = 3^2 + 3 + 1 = 13$ and $d = 4^2 + 4 + 1 = 21$. For arbitrary d, let q be the lowest prime power such that $d < q^2 + q + 1$. To design the $d \times d$ almost-bi-regular matrices, one approach may be to start by taking the derived-incidence matrix corresponding to the $(q^2+q+1, q^2+q+1, q+1, q+1, 1)$-BIBD and then by reducing $(q^2 + q + 1 - d)$ rows and columns so that minimum number of ones are removed. We show that using this technique, $d \times d$ almost-bi-regular matrices with $v_1^{d,d}$ ones can be constructed for any value of $d < 21$ except for $d = 14$ and 15. The cases when $d \in \{14, 15\}$ are dealt in Lemma 4.23 and Lemma 4.25.

Lemma 4.19 (Alternative proof of some results of part (b) of Lemma 2.8). *We have* $v_1^{2,2} = 3$, $v_1^{3,3} = 6$, $v_1^{4,4} = 9$, $v_1^{5,5} = 12$, $v_1^{6,6} = 16$ *and* $v_1^{7,7} = 21$.

Proof. Since $(3, 3, 2, 2, 1)$-BIBD exists, it follows from Theorem 3.8 that $v_1^{3,3} = 6$ and the corresponding almost-bi-regular matrix is given in Figure 2. From Corollary 3.9, $v_1^{7,7} = 7 \times (2 + 1) = 21$. The derived-incidence matrix of $(7, 7, 3, 3, 1)$-BIBD given in Figure 3.

From Corollary 4.14,

$$v_1^{2,2} \le \left\lfloor 2 \times \frac{1 + \sqrt{4 \times 2 - 3}}{2} \right\rfloor = 3,$$

$$v_1^{6,6} \le \left\lfloor 6 \times \frac{1 + \sqrt{4 \times 6 - 3}}{2} \right\rfloor = 16,$$

$$v_1^{5,5} \le \left\lfloor 5 \times \frac{1 + \sqrt{4 \times 5 - 3}}{2} \right\rfloor = 12,$$

$$v_1^{4,4} \le \left\lfloor 4 \times \frac{1 + \sqrt{4 \times 4 - 3}}{2} \right\rfloor = 9.$$

To complete the proof, we provide the corresponding matrices in Figure 2 and Figure 3. □

$$\left(\begin{array}{c|c|c} 1 & 1 & \\ \hline 1 & & 1 \\ \hline & 1 & 1 \end{array}\right), \quad \left(\begin{array}{c|c} 1 & 1 \\ \hline 1 & \end{array}\right)$$

Figure 2. Examples of $d \times d$ almost-bi-regular matrices having maximum number of ones for $d = 3, 2$.

$$\left(\begin{array}{c|c|c|c|c|c|c} 1 & 1 & 1 & & & & \\ \hline 1 & & & & 1 & 1 & \\ \hline 1 & & & 1 & & & 1 \\ \hline & & 1 & 1 & 1 & & \\ \hline & & 1 & & & 1 & 1 \\ \hline & 1 & & & 1 & & 1 \\ \hline & 1 & & 1 & & 1 & \end{array}\right), \quad \left(\begin{array}{c|c|c|c|c|c} & & & 1 & 1 & \\ \hline & & 1 & & & 1 \\ \hline & 1 & 1 & 1 & & \\ \hline & 1 & & & 1 & 1 \\ \hline 1 & & & 1 & & 1 \\ \hline 1 & & 1 & & 1 & \end{array}\right),$$

$$\left(\begin{array}{c|c|c|c|c} & & 1 & 1 & \\ \hline & 1 & & & 1 \\ \hline 1 & 1 & 1 & & \\ \hline 1 & & & 1 & 1 \\ \hline & & 1 & & 1 \end{array}\right), \quad \left(\begin{array}{c|c|c|c} & 1 & 1 & \\ \hline 1 & 1 & & \\ \hline 1 & & 1 & 1 \\ \hline & 1 & & 1 \end{array}\right)$$

Figure 3. Examples of $d \times d$ almost-bi-regular matrices having maximum number of ones for $d = 7, 6, 5, 4$.

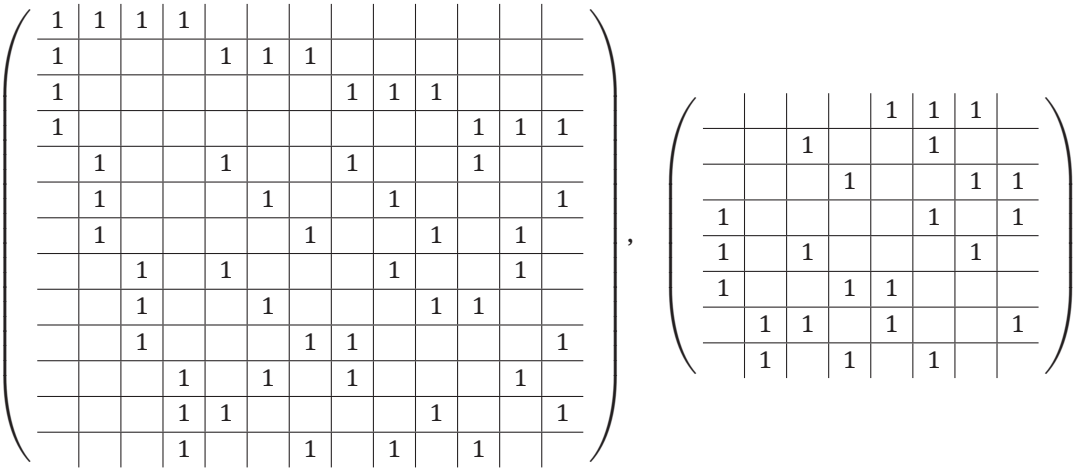


Figure 4. Examples of 13×13 and 8×8 almost-bi-regular matrices having maximum number of ones.

Lemma 4.20 (Alternative proof of one result of part (b) of Lemma 2.8). *We have* $v_1^{8,8} = 24$.

Proof. If $\max(|C|) = 5$, then from Theorem 4.16,

$$\mathcal{G}_8(5) = 5 + 7 + \mathcal{F}_7(3) = 12 + 10 = 22.$$

From Lemma 4.12, $\mathcal{G}_8(j) \le \mathcal{G}_8(5)$ for $j \ge 5$. Hence, any 8×8 almost-bi-regular matrix having $\max(|C|) \ge 5$ can have at most 22 ones.

If $\max(|C|) = 4$, then

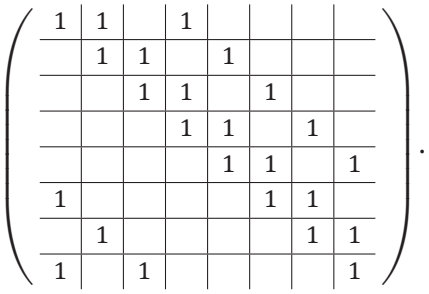
$$\mathcal{G}_8(4) = 4 + 7 + \mathcal{F}_7(4) = 11 + 13 = 24.$$

If $\max(|C|) = 3$, then

$$\mathcal{G}_8(3) = 3 + 7 + \mathcal{F}_7(5) = 10 + 15 = 25,$$

but in this case, the maximum number of ones cannot exceed $3 \times 8 = 24$. So, possible maximum value of ones in almost-bi-regular matrix of size 8 is 24 and it can be achieved when $\max(|C|) = 4$ or $\max(|C|) = 3$. The construction for such a matrix is shown in Figure 4. □

Remark 4.21. Another form of 8×8 almost-bi-regular matrix with $v_1^{8,8}$ ones is



This form corresponds to the circulant matrices and MDS matrices can be constructed from this almost-bi-regular matrix (see [11]). In Section 5, we provide an alternative way to construct MDS matrices using Latin squares, which resemble this form (see Figure 11 and Figure 12). Note that no 8×8 MDS matrix over $\mathbb{F}_{2^8}$ is found which is of the form as given in Figure 4 (see Remark 6.1).

Lemma 4.22. *We have*
(a) $v_1^{9,9} = 29$,
(b) $v_1^{10,10} = 34$ *and* $v_1^{12,12} = 45$,
(c) $v_1^{11,11} = 39$,
(d) $v_1^{13,13} = 52$.

Proof. (a) If $\max(|C|) = 5$, then

$$\mathcal{G}_9(5) = 5 + 8 + \mathcal{F}_8(4) = 13 + 14 = 27$$

(Theorem 4.16). From Lemma 4.12, $\mathcal{G}_9(j) \leq \mathcal{G}_9(5)$ for $j \geq 5$. Hence, any 9×9 almost-bi-regular matrix having $\max(|C|) \geq 5$ can have at most 27 ones. If $\max(|C|) = 4$, then

$$\mathcal{G}_9(4) = 4 + 8 + \mathcal{F}_8(5) = 12 + 17 = 29.$$

If $\max(|C|) = 3$, then

$$\mathcal{G}_9(3) = 3 + 8 + \mathcal{F}_8(6) = 11 + 20 = 31,$$

but in this case, the maximum number of ones cannot exceed $3 \times 9 = 27$. So, the possible maximum value of ones in almost-bi-regular matrix of size 9 is 29 and it can be achieved when $\max(|C|) = 4$. The construction for such matrix is shown in appendix. Such a construction is given in Figure 14 of Appendix A.2.

(b) It can be proved similarly as it was proved for $v_1^{8,8}$ and $v_1^{9,9}$. The constructions for such 10×10 and 12×12 almost-bi-regular matrices with 34 and 45 ones have been shown in Figure 14 of Appendix A.2.

(c) If $\max(|C|) = 5$, then

$$\mathcal{G}_{11}(5) = 5 + 10 + \mathcal{F}_{10}(6) = 15 + 23 = 38.$$

If $\max(|C|) = 4$, then

$$\mathcal{G}_{11}(4) = 4 + 10 + \mathcal{F}_{10}(7) = 14 + 26 = 40.$$

If $\max(|C|) = 3$, then the maximum number of ones cannot exceed $3 \times 11 = 33$. So, $v_1^{11,11} \leq 40$. Now, we show that $v_1^{11,11} \neq 40$. If possible, then there will be at least seven rows (or columns) which contain four ones each. If so, then from Theorem 4.17 (or Theorem 4.18), the minimum number of columns (or rows) required to accommodate such rows (or columns) is 12 which is not possible. Hence $v_1^{11,11} \leq 39$. The construction for an 11×11 almost-bi-regular matrix with 39 ones is shown in Figure 14 of Appendix A.2.

(d) See Remark 3.10. □

We observe that for d up to 20, $d \times d$ almost-bi-regular matrices with maximum number of ones can be constructed starting from a projective plane of order q, where q is the smallest prime such that $d < q^2 + q + 1$ except for $d = 14$ and 15. These two special cases are dealt with in the following lemma. It may be noted that 15×15 and 14×14 matrices formed from the 16×16 matrix of Figure 17 of Appendix A.3 will contain 60 and 53 ones. In Figure 5, we present 15×15 and 14×14 matrices containing 61 and 56 ones, respectively.

Lemma 4.23. *We have* $v_1^{14,14} = 56$.

Proof. If $\max(|C|) = 5$, then

$$\mathcal{G}_{14}(5) = 5 + 13 + \mathcal{F}_{13}(9) = 18 + 37 = 55.$$

If $\max(|C|) = 4$, then the maximum number of ones cannot exceed 56. If $\max(|C|) = 3$, then the maximum number of ones cannot exceed $3 \times 14 = 42$. So, $v_1^{14,14} \leq 56$. The construction for a 14×14 almost-bi-regular matrix with 56 ones is shown in Figure 5. □

Remark 4.24. It may be noted that if a 14×14 matrix contains 56 ones, then from Lemma 4.23, all its rows and columns should contain exactly four ones. Also each row (column) makes twelve pairs with twelve other rows (columns) (from Lemma 4.4 or Lemma 4.5).

Lemma 4.25. *We have* $v_1^{15,15} = 61$.

Proof. If $\max(|C|) = 6$, then

$$\mathcal{G}_{15}(6) = 6 + 14 + \mathcal{F}_{14}(9) = 20 + 39 = 59.$$

If $\max(|C|) = 5$, then

$$\mathcal{G}_{15}(5) = 5 + 14 + \mathcal{F}_{14}(10) = 19 + 43 = 62.$$

If $\max(|C|) = 4$, then the maximum number of ones cannot exceed $4 \times 15 = 60$. So, $v_1^{15,15} \leq 62$. Now, we show that $v_1^{15,15} \neq 62$.

If possible, then there exists a 15×15 almost-bi-regular matrix M which contains 62 ones. Since $\max(|C|) = 5$, there exists a column, say C_i, such that $|C_i| = 5$. If $\min(|R|) \geq 4$, then, from Lemma 4.5, the column C_i makes at least $5 \times (4-1) = 15$ pairs with other columns. Since there are fifteen columns, each column can have at most fourteen pairs with other columns. Thus, a contradiction. So, $\min(|R|) \leq 3$. Similarly, we can show that $\max(|R|) = 5$ and $\min(|C|) \leq 3$.

Let $\min(|C|) \leq 2$. Suppose that the column C_k contains exactly two ones, i.e. $|C_k| = 2$. Let R_l be the row which contains minimum number of ones. Since $\min(|R|) \leq 3$, we have $|R_l| \leq 3$. Consider the 14×14 almost-bi-regular matrix M' obtained by removing the row R_l and the column C_k from M. It is easy to check that M' contains at least $62 - (2+3) = 57$ ones, a contradiction (because $v_1^{14,14} = 56$). Hence, $\min(|C|) \geq 3$, which then implies $\min(|C|) = 3$. Similarly, it can be shown that $\min(|R|) = 3$.

Let the column C_m and the row R_n contain three ones, i.e. $|C_m| = |R_n| = 3$. If $|C_m \wedge R_n| = 1$, then removing C_m and R_n from the matrix M yields a 14×14 almost-bi-regular matrix M' which has $62 - (3+3-1) = 57$ ones, a contradiction. Hence, $|C_m \wedge R_n| = 0$.

Now, construct a matrix $\hat{M}$ after rearranging the columns and rows of the matrix M such that C_{14} and R_{14} in the matrix $\hat{M}$ are C_m and R_n, respectively, of the matrix M. Consider the matrix A constructed by taking the first fourteen rows and the first fourteen columns of the matrix $\hat{M}$. It is easy to check that A is a 14×14 almost-bi-regular matrix having $62 - (3+3) = 56$ ones. In A, each column makes pair with twelve other columns and similarly, each row makes pair with twelve other rows (see Remark 4.24). By the construction of $\hat{M}$, the column C_{14} and the row R_{14} contain three ones with the condition that $|C_{14} \wedge R_{14}| = 0$. Let $C_{14} \wedge C_{14} = \{j_1, j_2, j_3\}$, where $0 \leq j_1 < j_2 < j_3 \leq 13$. In the matrix A, consider the rows R_{j_1}, R_{j_2} and R_{j_3}. From the previous discussion, in the matrix A, either $|R_{j_1} \wedge R_{j_2}| = 0$ or $|R_{j_1} \wedge R_{j_3}| = 0$ but not both (because R_{j_1} makes pair with twelve other rows). Without loss of generality, assume that $|R_{j_1} \wedge R_{j_2}| = 1$. But, in the matrix $\hat{M}$, both $|R_{j_1} \wedge C_{14}| = 1$ and $|R_{j_2} \wedge C_{14}| = 1$. Therefore in the matrix $\hat{M}$, $|R_{j_1} \wedge R_{j_2}| = 2$, a contradiction.

Hence we have $v_1^{15,15} \neq 62$. The construction of a 15×15 almost-bi-regular matrix with 61 ones is shown in Figure 5. □

Lemma 4.26. *We have* $v_1^{16,16} = 67$.

Proof. If $\max(|C|) = 6$, then $\mathcal{G}_{16}(6) = 6 + 15 + \mathcal{F}_{15}(10) = 66$. If $\max(|C|) = 5$, then $\mathcal{G}_{16}(5) = 68$. If $\max(|C|) = 4$, then the maximum number of ones cannot exceed 64. Now, we prove that $v_1^{16,16} \neq 68$.

If possible, then there exists a 16×16 almost-bi-regular matrix M with 68 ones. It is easy to see that $\max(|C|) = \max(|R|) = 5$, $\min(|C|) \neq 5$ and $\min(|R|) \neq 5$ (otherwise M will contain 80 ones). So, $\min(|C|) \leq 4$ and $\min(|R|) \leq 4$.

Let $\min(|C|) \leq 3$ and $\min(|R|) \leq 3$. Suppose that the column C_j and the row R_k has three ones. Construct a matrix M' after removing C_j and R_k from M. It is easy to check that M' is a 15×15 almost-bi-regular matrix with at least $68 - (3+3) = 62$ ones, a contradiction (since $v_1^{15,15} = 61$). Hence, either $\min(|C|) \geq 4$ or $\min(|R|) \geq 4$ which then implies either $\min(|C|) = 4$ or $\min(|R|) = 4$.

Without loss of generality, assume that $\min(|C|) = 4$. Then there will be exactly four columns containing five ones and twelve columns containing four ones. Moreover, there will be at least four rows containing five ones.

Consider the rows which contain five ones. Let these rows be $R_{k_1}, R_{k_2}, R_{k_3}, R_{k_4}$. The number of columns required to accommodate these rows is at least $\max(10, 13) = 13$ (see Theorem 4.17). Let $C_{j_1}, C_{j_2}, \ldots, C_{j_{13}}$ be the columns which accommodate these rows.

Let $|C_{j_i}| = 5$ for some $i \in \{1, \ldots, 13\}$. Then consider the row $R_{k_l} \in \{R_{k_1}, R_{k_2}, R_{k_3}, R_{k_4}\}$ which satisfies $|C_{j_i} \wedge R_{k_l}| = 1$. Since $\min(|C|) = 4$, the row R_{k_l} in the matrix M then makes pairs with at least $4 + 3 \times 4 = 16$ other rows (Lemma 4.4), a contradiction (a row can make pair with at most fifteen other rows). Hence none of $C_{j_1}, C_{j_2}, \ldots, C_{j_{13}}$ can contain five ones. So, there will be at least thirteen columns which contain four ones, but from the above discussion (fourth paragraph of this proof), there are exactly twelve columns containing four ones, a contradiction.

Hence, $v_1^{16,16} \neq 68$. The construction of a 16×16 almost-bi-regular matrix with 67 ones is shown in Figure 17 of Appendix A.3. □

$$M_{15} = \left(\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline 1&1&1&1& & & & & & & & & & & \\ \hline
1& & & &1&1&1& & & & & & & & \\ \hline
1& & & & & & &1&1&1& & & & & \\ \hline
1& & & & & & & & & &1&1&1& & \\ \hline
 &1& & &1& & & 1& & & 1& & & & \\ \hline
 &1& & & &1& & &1& & & & &1& \\ \hline
 &1& & & & &1& & &1& & 1& & &1 \\ \hline
 & &1& &1& & & &1& & & 1& & & \\ \hline
 & &1& & &1& & 1& & & & &1& &1 \\ \hline
 & &1& & & &1& & & &1& & &1& \\ \hline
 & & &1& & & & 1& & & & 1& &1& \\ \hline
 & & &1& & & 1& & 1& & & &1& & \\ \hline
 & & &1& &1& & & & 1&1& & & & \\ \hline
 & & & &1& & & & & 1& & &1&1& \\ \hline
 & & &1&1& & & & & & & & & &1 \\ \hline
\end{array}\right),$$

$$M_{14} = \left(\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline 1&1&1&1& & & & & & & & & & \\ \hline
1& & & &1&1&1& & & & & & & \\ \hline
1& & & & & & &1&1&1& & & & \\ \hline
1& & & & & & & & & &1&1&1& \\ \hline
 &1& & &1& & & 1& & & 1& & & \\ \hline
 &1& & & &1& & &1& & & & &1 \\ \hline
 &1& & & & &1& & & 1& & 1& & \\ \hline
 & &1& &1& & & &1& & & 1& & \\ \hline
 & &1& & &1& & 1& & & & &1& \\ \hline
 & &1& & & &1& & & 1& & & &1 \\ \hline
 & & &1& & & & 1& & & & 1& &1 \\ \hline
 & & &1& & & 1& & 1& & & &1& \\ \hline
 & & &1& &1& & & & 1&1& & & \\ \hline
 & & & &1& & & & & 1& & &1&1 \\ \hline
\end{array}\right)$$

Figure 5. Examples of $d \times d$ almost-bi-regular matrices M_d, $d = 15, 14$, with $v_1(M_{15}) = v_1^{15,15} = 61$ and $v_1(M_{14}) = v_1^{14,14} = 56$.

Lemma 4.27. *We have* $v_1^{17,17} = 74$.

Proof. If $\max(|C|) = 6$, then

$$\mathcal{G}_{17}(6) = 6 + 16 + \mathcal{F}_{16}(11) = 22 + 50 = 72.$$

If $\max(|C|) = 5$, then

$$\mathcal{G}_{17}(5) = 5 + 16 + \mathcal{F}_{16}(12) = 21 + 54 = 75.$$

If $\max(|C|) = 4$, then the maximum number of ones cannot exceed $4 \times 17 = 68$. Now, we show that $v_1^{17,17} \neq 75$.

If possible, then there exists a 17×17 almost-bi-regular matrix M having 75 ones. It is easy to see that $\max(|C|) = \max(|R|) = 5$, $\min(|C|) \neq 5$ and $\min(|R|) \neq 5$ (otherwise M will contain 85 ones). So, $\min(|C|) \leq 4$ and $\min(|R|) \leq 4$.

Suppose that $\min(|C|) \leq 3$ or $\min(|R|) \leq 3$. Without loss of generality, assume that $\min(|C|) = 3$. Suppose that the column C_j contains three ones and the row R_k has four ones. Construct a matrix M' after removing C_j and R_k from M. It is easy to check that M' is a 16×16 almost-bi-regular matrix with at least $75 - (4 + 3) = 68$ ones, a contradiction (since $v_1^{16,16} = 67$). Hence, $\min(|C|) \geq 4$ and $\min(|R|) \geq 4$ which then implies $\min(|C|) = 4$ and $\min(|R|) = 4$.

Since $\min(|C|) = \min(|R|) = 4$, there will be exactly seven columns and rows containing five ones and the remaining ten columns and rows containing four ones.

Let $R_{k_1}, R_{k_2}, \ldots, R_{k_{10}}$ be rows which contain four ones. Let $C_{j_1}, C_{j_2}, \ldots, C_{j_{10}}$ be columns which contain four ones. If $|C_{j_i} \wedge R_{k_l}| = 1$ for some $1 \le i, l \le 10$, then construct a 16×16 matrix M' by removing C_{j_i} and R_{k_l}. It is easy to observe that M' is an almost-bi-regular matrix with $75 - (4 + 4 - 1) = 68$ ones, a contradiction (since $v_1^{16,16} = 67$). Hence $|C_{j_i} \wedge R_{k_l}| = 0$ for all $1 \le i, l \le 10$.

Now, consider a 10×7 matrix $\hat{M}$ formed by rows $R_{k_1}, \ldots, R_{k_{10}}$ and columns different from $C_{j_1}, \ldots, C_{j_{10}}$. Since $|C_{j_i} \wedge R_{k_l}| = 0$, each row in $\hat{M}$ will contain four ones. Hence $\hat{M}$ contains $4 \times 10 = 40$ ones, but from Theorem 4.13, $v_1^{10,7} \le 26$, a contradiction.

Hence we have $v_1^{17,17} \ne 75$. The construction of a 17×17 almost-bi-regular matrix with 74 ones is shown in Figure 17 of Appendix A.3. □

Lemma 4.28. *We have*
(a) $v_1^{18,18} = 81$,
(b) $v_1^{19,19} = 88$,
(c) $v_1^{21,21} = 105$.

Proof. (a) By using a similar argument as used for the case $v_1^{17,17} \ne 75$, it can be shown that $v_1^{18,18} \ne 82$. The construction of a 18×18 almost-bi-regular matrix with 81 ones is shown in Figure 16 of Appendix A.3.

(b) If $\max(|C|) = 6$, then

$$\mathcal{G}_{19}(6) = 6 + 18 + \mathcal{F}_{18}(13) = 24 + 62 = 86.$$

If $\max(|C|) = 5$, then

$$\mathcal{G}_{19}(5) = 5 + 18 + \mathcal{F}_{18}(14) = 23 + 66 = 89.$$

If $\max(|C|) = 4$, then the maximum number of ones cannot exceed $4 \times 19 = 76$. Now, we show that $v_1^{19,19} \ne 89$.

If possible, then there exists a 19×19 almost-bi-regular matrix M with 89 ones. It can be easily shown that then $\max(|C|) = \max(|R|) = 5$ and $\min(|C|) = \min(|R|) = 4$. In the matrix M, there will be exactly thirteen rows and thirteen columns which contain five ones and remaining 6 rows and columns containing four ones. To accommodate thirteen rows having five ones each, at least $\max(17, 20) = 20$ columns (Theorem 4.17) are required, a contradiction.

Hence we have $v_1^{19,19} \ne 89$. The construction of a 19×19 almost-bi-regular matrix with 88 ones is shown in Figure 16 of Appendix A.3.

(c) See Remark 3.10. □

Let $q = 1$ or q be a power of a prime number. Now, we calculate $v_1^{d,d}$ when $d = q^2 + q$. Note than when $d = q^2 + q + 1$, we get a BIBD structure such that $v_1^{d,d} = (q + 1)d$.

Theorem 4.29. *Let $d = q^2 + q$, where $q = 1$ or q is a prime power. Then*

$$v_1^{d,d} = (q^2 + q + 1)(q + 1) - 2(q + 1) + 1 = q^2(q + 2).$$

Proof. Let $q = 1$. Then $v_1^{2,2} = 3$.

Suppose that q is a prime power. If $\max(|C|) = q + 2$, then by elementary arithmetic, it can be proved that $\mathcal{G}_{q^2+q}(q + 2) < (q^2 + q + 1)(q + 1) - 2(q + 1) + 1$. If $\max(|C|) = q$, then the maximum number of ones cannot exceed $q^2(q + 1)$. Hence, to get $v_1^{d,d} \ge q^2(q + 2)$, both $\max(|C|)$ and $\max(|R|)$ should be equal to $q + 1$. Now, we show that if $\max(|C|) = q + 1$, then $v_1^{d,d} \not> q^2(q + 2)$.

If possible, then there exists a $d \times d$ almost-bi-regular matrix M which contains $q^2(q + 2) + 1$ ones. Since $\max(|R|) = q + 1$, there will be at least $q^2 + 1$ rows containing $q + 1$ ones. Then by Theorem 4.17, the number of columns required to accommodate such rows will be at least $q^2 + q + 1$, a contradiction.

Hence we have $v_1^{d,d} \le q^2(q + 2)$. Now, we show that $v_1^{d,d} = q^2(q + 2)$. Since $d + 1 = q^2 + q + 1$, there exists a $(d + 1) \times (d + 1)$ almost-bi-regular matrix $\hat{M}$ containing $q + 1$ ones in each row and in each column. So, $\hat{M}$ contains $(q + 1)(d + 1)$ ones. Remove a column C_j and a row R_k from $\hat{M}$ such that $|C_j \wedge R_k| = 1$ (such a column and row will definitely exist). The remaining matrix will be a $d \times d$ almost-bi-regular matrix with $(d + 1)(q + 1) - (2(q + 1) - 1) = (q^2 + q + 1)(q + 1) - 2(q + 1) + 1$ ones. □

Corollary 4.30. *We have $v_1^{20,20} = 96$.*

Dimension $d \times d$	$v_1^{d,d}$	Upper bound of $v_1^{d,d}$, i.e. $\lfloor d \times \frac{1}{2}(1 + \sqrt{4 \times d - 3}) \rfloor$ (see Corollary 4.14)	Number of ones in the construction using [12, Lemmas 1 and 3]	For illustrations see
3×3	6	6	6	Figure 2
4×4	9	9	9	Figure 3
5×5	12	12	12	Figure 3
6×6	16	16	15	Figure 3
7×7	21	21	21	Figure 3
8×8	24	24	24	Figure 4
9×9	29	30	24	Figure 14
10×10	34	35	27	Figure 14
11×11	39	40	30	Figure 14
12×12	45	46	33	Figure 14
13×13	52	52	36	Figure 4
14×14	56	57	39	Figure 5
15×15	61	64	42	Figure 5
16×16	67	70	45	Figure 17
17×17	74	77	48	Figure 17
18×18	81	83	51	Figure 16
19×19	88	90	54	Figure 16
20×20	96	97	57	Figure 15
21×21	105	105	60	Figure 15

Table 1. Efficient $d \times d$ almost-bi-regular matrices for d up to 21.

Proof. From Theorem 4.29, taking $q = 2^2 = 4$, we get $v_1^{20,20} = 96$. The construction of a 20×20 almost-bi-regular matrix with 96 ones is shown in Figure 15 of Appendix A.3. □

Here, we close this section by summarizing the results of this section in Table 1 for $d \times d$ almost-bi-regular matrices where $d \leq 21$. For $8 < d < 13$, the values of $v_1^{d,d}$ are computed and the corresponding $d \times d$ almost-bi-regular matrices are given in Appendix A.2. For $13 < d \leq 21$, the $d \times d$ almost-bi-regular matrices are given in Appendix A.3. For $d \leq 8$ and $d = 13$ the almost-bi-regular matrices are given in Figure 2, Figure 3 and Figure 4.

5 Some results on $c_1(M)$ where M is a bi-regular matrix having maximum number of ones

In Section 4, we have constructed $d \times d$ almost-bi-regular matrices M with $v_1^{d,d}$ ones. So, next we try to fill the remaining blank positions of these almost-bi-regular matrices M with minimum number of distinct elements other than 1 and 0 (i.e. with minimum $c_1(M)$) in such a way that the bi-regular property is maintained. We denote these $d \times d$ bi-regular matrices by M_d. In Lemma 5.1, we provide a tight lower bound of $c_1(M_d)$ for $d \times d$ bi-regular matrices M_d, where $v_1(M_d) = v_1^{d,d}$ and $d = q^2 + q + 1$, where q is any prime power.

Lemma 5.1. *Let $d = q^2 + q + 1$, where q is any prime power. Also, let M_d be a $d \times d$ bi-regular matrix having $v_1^{d,d}$ ones. Then $c_1(M_d) \geq q^2$.*

Proof. Let $M_d = ((m_{i,j}))$ be the $d \times d$ almost-bi-regular matrix having $v_1^{d,d} = (q + 1) \times (q^2 + q + 1)$ ones and also let the corresponding design be $(X, \mathcal{A})$, where $X = \{x_0, \ldots, x_{q^2+q}\}$ and $\mathcal{A} = \{A_0, \ldots, A_{q^2+q}\}$. So, $(X, \mathcal{A})$ is a $(q^2 + q + 1, q^2 + q + 1, q + 1, q + 1, 1)$-BIBD and let M_d be its derived-incidence matrix.

Each row and column of the matrix M_d contains $(q + 1)$ ones. So in each row and column there are $(q^2 + q + 1) - (q + 1) = q^2$ blank positions. Let, if possible, $c_1(M_d) < q^2$. So, in all rows and columns, some element (apart from 1) will occur more than once.

Let in the j-th column, the i_1-th and i_2-th blank positions be filled by some element a. Let the i_1-th and i_2-th rows correspond to the elements x_{i_1} and x_{i_2}, respectively. Since $(X, \mathcal{A})$ is a BIBD, it follows that x_{i_1} and x_{i_2} must occur simultaneously in any one of the blocks, say A_k. So $m_{i_1,k} = m_{i_2,k} = 1$. Thus the 2×2 submatrix formed by the i_1-th and i_2-th rows and j-th and k-th columns will be of the form $\left(\begin{smallmatrix} 1 & a \\ 1 & a \end{smallmatrix}\right)$ (up to the permutations of columns) which is singular.

Similarly, let in the i-th row, two blank positions, say j_1 and j_2, be filled with a. From Lemma 2.15, any pair of blocks contain exactly one element. So, A_{j_1} and A_{j_2} must contain some element, say x_l. So, $m_{l,j_1} = m_{l,j_2} = 1$. Thus the 2×2 submatrix formed by the i-th and l-th rows and j_1-th and j_2-th columns will be of the form $\left(\begin{smallmatrix} 1 & 1 \\ a & a \end{smallmatrix}\right)$ (up to the permutations of rows) which is singular. Thus, the minimum number of distinct elements cannot be less than q^2. □

In the next lemma, we propose good upper bounds of $c_1(M_d)$ for $d \times d$ matrices M_d for $d = 3, 4, 5, 6, 7, 8, 13$, where $v_1(M_d) = v_1^{d,d}$, and using these matrices, we construct $d \times d$ MDS matrices M_d in Section 6 for d up to 7.

For $d = 8$, 8×8 almost-bi-regular matrices with $v_1^{8,8}$ ones can be constructed starting from a derived-incidence matrix of $(13, 13, 4, 4, 1)$-BIBD as discussed in Lemma 4.20, but bi-regular matrices formed from these almost-bi-regular matrices may not finally become MDS. We tried to construct MDS matrix starting from such a matrix $M_8(e_0, e_1, e_2, e_3, e_4)$ as given in Figure 8, but no such MDS matrices were found for any choices of elements e_i (also see Remark 6.1). At the end of this section, we construct 8×8 MDS matrices with $v_1^{8,8}$ ones using Latin squares.

Lemma 5.2. *For $d \times d$ bi-regular matrices M_d, $d = 2, 3, 4, 5, 6, 7, 8, 13$, having $v_1^{d,d}$ ones, we have $c_1(M_2) = 1$, $c_1(M_3) = 1$, $c_1(M_4) \le 2$, $c_1(M_5) \le 3$, $c_1(M_6) \le 4$, $c_1(M_7) = 4$, $c_1(M_8) \le 5$ and $c_1(M_{13}) = 9$.*

Proof. The matrix M_3 is constructed from the derived-incidence matrix of $(3, 3, 2, 2, 1)$-BIBD, and note that $c_1(M_3) = 1$ and $c_1(M_2) = 1$ is evident from Figure 6. The matrix M_7 corresponds to the derived-incidence matrix of $(7, 7, 3, 3, 1)$-BIBD and from Lemma 5.1, $c_1(M_7) \ge 4$. From the 7×7 bi-regular matrix of Figure 7, it is evident that $c_1(M_7) = 4$. That $c_1(M_6) \le 4$, $c_1(M_5) \le 3$ and $c_1(M_4) \le 2$ is evident from Figure 7. The matrix M_{13} corresponds to the derived-incidence matrix of $(13, 13, 4, 4, 1)$-BIBD and from Lemma 5.1, $c_1(M_{13}) \ge 9$. From the 13×13 bi-regular matrix of Figure 8, it is evident that $c_1(M_{13}) = 9$. From Figure 8, it is clear that $c_1(M_8) \le 5$. □

$$M_3 = \left(\begin{array}{c|c|c} 1 & 1 & e_0 \\ \hline 1 & e_0 & 1 \\ \hline e_0 & 1 & 1 \end{array}\right), \quad M_2 = \left(\begin{array}{c|c} 1 & 1 \\ \hline 1 & e_0 \end{array}\right)$$

Figure 6. Examples of $d \times d$ bi-regular matrices M_d, $d = 3, 2$, having maximum number of ones with $c_1(M_2) = 1$, $c_1(M_3) = 1$.

Construction of bi-regular matrices from Latin squares. We observe an interesting connection between Latin squares and bi-regular matrices, which may give an easy method to construct efficient $d \times d$ MDS matrices whenever $v_1^{d,d}$ is a multiple of d. We construct such efficient MDS matrices for $d = 3$ and 8. It may be noted that in both the cases $v_1^{d,d}$ is multiple of d.

A Latin square of order d with entries from a d-set X is a $d \times d$ matrix L_d in which every cell contains an element of X such that every row of L_d is a permutation of X and every column of L_d is a permutation of X. In our construction, X is a subset of $\mathbb{F}_{2^n}$. In the following lemma, we study an important property of Latin square which is crucial in the construction of bi-regular matrix.

Lemma 5.3. *All Latin squares of order d with entries from a d-set $X \subset \mathbb{F}_{2^n}$ will be bi-regular matrices if and only if $a^2 \ne bc$ and $ab \ne cd$ for any $a, b, c, d \in X$.*

Proof. Let L_d be a $d \times d$ matrix which is some Latin square with entries from a d-set $X \subset \mathbb{F}_{2^n}$ such that $a^2 \ne bc$ and $ab \ne cd$ for all $a, b, c, d \in X$. It may be noted that for any such matrix L_d, the determinants of all 2×2 submatrices are of the form $(a^2 + b^2)$, $(a^2 + bc)$ and $(ab + cd)$, where $a, b, c, d \in X$. Since all elements of X are distinct, $a^2 \ne b^2$ and in characteristic 2, $a^2 + b^2 \ne 0$ for any two $a, b \in X$. Similarly from the given conditions,

$$M_7(e_0,e_1,e_2,e_3)=\left(\begin{array}{c|c|c|c|c|c|c}
1 & 1 & 1 & e_0 & e_1 & e_2 & e_3\\ \hline
1 & e_3 & e_0 & e_1 & 1 & 1 & e_2\\ \hline
1 & e_2 & e_3 & 1 & e_0 & e_1 & 1\\ \hline
e_2 & e_0 & 1 & 1 & 1 & e_3 & e_1\\ \hline
e_0 & e_1 & 1 & e_2 & e_3 & 1 & 1\\ \hline
e_1 & 1 & e_2 & e_3 & 1 & e_0 & 1\\ \hline
e_3 & 1 & e_1 & 1 & e_2 & 1 & e_0
\end{array}\right),$$

$$M_6(e_0,e_1,e_2,e_3)=\left(\begin{array}{c|c|c|c|c|c}
e_3 & e_0 & e_1 & 1 & 1 & e_2\\ \hline
e_2 & e_3 & 1 & e_0 & e_1 & 1\\ \hline
e_0 & 1 & 1 & 1 & e_3 & e_1\\ \hline
e_1 & 1 & e_2 & e_3 & 1 & 1\\ \hline
1 & e_2 & e_3 & 1 & e_0 & 1\\ \hline
1 & e_1 & 1 & e_2 & 1 & e_0
\end{array}\right),$$

$$M_5(e_0,e_1,e_2)=\left(\begin{array}{c|c|c|c|c}
e_0 & e_1 & 1 & 1 & e_2\\ \hline
e_2 & 1 & e_0 & e_1 & 1\\ \hline
1 & 1 & 1 & e_0 & e_1\\ \hline
1 & e_0 & e_2 & 1 & 1\\ \hline
e_1 & e_2 & 1 & e_2 & 1
\end{array}\right),$$

$$M_4(e_0,e_1)=\left(\begin{array}{c|c|c|c}
e_0 & 1 & 1 & e_1\\ \hline
1 & 1 & e_1 & e_0\\ \hline
1 & e_0 & 1 & 1\\ \hline
e_1 & 1 & e_0 & 1
\end{array}\right)$$

Figure 7. Examples of $d \times d$ bi-regular matrices having maximum number of ones for $d = 7, 6, 5, 4$ with $c_1(M_4) = 2$, $c_1(M_5) = 3$, $c_1(M_6) = 4$ and $c_1(M_7) = 4$.

$$M_{13}(e_0,e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8)=\left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c}
1 & 1 & 1 & 1 & e_0 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8\\ \hline
1 & e_6 & e_7 & e_8 & 1 & 1 & 1 & e_0 & e_1 & e_2 & e_3 & e_4 & e_5\\ \hline
1 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & 1 & 1 & 1 & e_0 & e_1 & e_2\\ \hline
1 & e_0 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & 1 & 1 & 1\\ \hline
e_2 & 1 & e_3 & e_4 & 1 & e_5 & e_6 & 1 & e_8 & e_7 & 1 & e_0 & e_1\\ \hline
e_0 & 1 & e_5 & e_6 & e_8 & 1 & e_7 & e_4 & 1 & e_3 & e_1 & e_2 & 1\\ \hline
e_1 & 1 & e_0 & e_3 & e_2 & e_8 & 1 & e_7 & e_5 & 1 & e_4 & 1 & e_6\\ \hline
e_7 & e_1 & 1 & e_0 & 1 & e_2 & e_3 & e_8 & 1 & e_6 & e_5 & 1 & e_4\\ \hline
e_8 & e_4 & 1 & e_7 & e_1 & 1 & e_0 & e_5 & e_2 & 1 & 1 & e_6 & e_3\\ \hline
e_5 & e_2 & 1 & e_1 & e_4 & e_6 & 1 & 1 & e_3 & e_0 & e_7 & e_8 & 1\\ \hline
e_3 & e_5 & e_2 & 1 & e_7 & 1 & e_1 & 1 & e_6 & e_4 & e_8 & 1 & e_0\\ \hline
e_6 & e_7 & e_8 & 1 & 1 & e_3 & e_4 & e_1 & e_0 & 1 & e_2 & e_5 & 1\\ \hline
e_4 & e_8 & e_6 & 1 & e_5 & e_0 & 1 & e_2 & 1 & e_1 & 1 & e_3 & e_7
\end{array}\right),$$

$$M_8(e_0,e_1,e_2,e_3,e_4)=\left(\begin{array}{c|c|c|c|c|c|c|c}
e_0 & e_1 & e_2 & e_3 & 1 & 1 & 1 & e_4\\ \hline
e_4 & e_4 & 1 & e_2 & e_3 & 1 & e_0 & e_1\\ \hline
e_3 & e_4 & e_1 & 1 & e_0 & e_2 & 1 & 1\\ \hline
1 & e_0 & e_4 & e_1 & e_2 & 1 & e_3 & 1\\ \hline
1 & e_3 & 1 & e_0 & e_1 & e_4 & 1 & e_2\\ \hline
1 & e_2 & e_0 & 1 & 1 & e_1 & e_4 & e_3\\ \hline
e_2 & 1 & 1 & e_4 & 1 & e_3 & e_1 & 1\\ \hline
e_1 & 1 & e_3 & 1 & e_4 & 1 & e_2 & e_0
\end{array}\right)$$

Figure 8. Examples of $d \times d$ bi-regular matrices having maximum number of ones for $d = 13$ and 8 with $c_1(M_{13}) = 9$ and $c_1(M_8) \leq 5$.

we have $a^2 + bc \neq 0$ and $ab + cd \neq 0$ for $a, b, c, d \in X$. Thus all 2×2 submatrices are nonsingular. So L_d is bi-regular. The reverse direction of the proof is immediate. □

Let L_d be a Latin square of order d with elements from a d-set $X \subset \mathbb{F}_{2^n}$ satisfying the conditions of Lemma 5.3. So, L_d is a bi-regular matrix. Note that if $1 \in X$, then $v_1(L_d) = d$. Our target is to increase the number of ones and reduce the number of other distinct elements in L_d without disturbing the bi-regular property of L_d. It may be noted that if for some $a, b \in X$, there exists no 2×2 submatrix of L_d having determinant $a^2 + b^2$, then we may replace both a and b by 1 provided determinants of these 2×2 submatrices of L_d involving a or b or both remains nonzero after these replacements. It is easy to observe that if $\lfloor v_1^{d,d}/d \rfloor = t$, then by replacing $t' \leq t$ suitable elements of L_d by 1, we may construct a bi-regular matrix L_d such that $v_1(L_d) = t' \times d \leq t \times d$ provided the determinants of 2×2 submatrices of L_d involving these t' elements remains nonzero after these replacements.

Note that if $v_1^{d,d}$ is not a multiple of d, then the bi-regular matrix with $v_1^{d,d}$ ones cannot be constructed using some Latin square L_d as described above, but in such cases $c_1(L_d)$ may be reduced to the minimum value. For example, let us consider the 4×4 Latin square L_4 of Figure 9.

Also $t = \lfloor v_1^{4,4}/4 \rfloor = \lfloor 9/4 \rfloor = 2$. Now by setting $c = d = 1$ in Figure 9, we construct a 4×4 bi-regular matrix L_4 with $v_1(L_4) = 2 \times 4 = 8$ (see Figure 10). In this case $c_1(L_4) = 2$ which is minimum.

$$\left(\begin{array}{c|c|c|c} a & b & c & d \\ \hline d & a & b & c \\ \hline c & d & a & b \\ \hline b & c & d & a \end{array}\right)$$

Figure 9. A 4×4 Latin square.

$$\left(\begin{array}{c|c|c|c} a & b & 1 & 1 \\ \hline 1 & a & b & 1 \\ \hline 1 & 1 & a & b \\ \hline b & 1 & 1 & a \end{array}\right)$$

Figure 10. A 4×4 bi-regular matrix with eight ones but minimum number of other distinct elements.

Remark 5.4. In the diffusion layer of AES [5], i.e. in the mixcolumn operation, a 4×4 circulant MDS matrix $\mathrm{Circ}(02_x, 03_x, 01_x, 01_x)$ over $\mathbb{F}_{2^8}$ is used. This matrix can be constructed from Figure 10 by setting $a = 02_x$ and $b = 03_x$.

If $v_1^{d,d}$ is a multiple of d, say $t \times d$, then a $d \times d$ bi-regular matrix with $v_1^{d,d}$ ones may be designed by setting t out of d elements to 1. Let us consider the 3×3 and 8×8 Latin squares of Figure 11.

We know that $v_1^{3,3} = 6 = 2 \times 3$. Now by setting $a = b = 1$, we construct a 3×3 bi-regular matrix with maximum number of ones and minimum number of other elements (see Figure 12) and we denote this matrix

$$\left(\begin{array}{c|c|c} a & b & c \\ \hline b & c & a \\ \hline c & a & b \end{array}\right), \quad \left(\begin{array}{c|c|c|c|c|c|c|c} a & b & c & d & e & f & g & h \\ \hline h & a & b & c & d & e & f & g \\ \hline g & h & a & b & c & d & e & f \\ \hline f & g & h & a & b & c & d & e \\ \hline e & f & g & h & a & b & c & d \\ \hline d & e & f & g & h & a & b & c \\ \hline c & d & e & f & g & h & a & b \\ \hline b & c & d & e & f & g & h & a \end{array}\right)$$

Figure 11. A 3×3 and an 8×8 Latin square.

$$L_3(c) = \left(\begin{array}{c|c|c} 1 & 1 & c \\ \hline 1 & c & 1 \\ \hline c & 1 & 1 \end{array}\right), \quad L_8(c,e,f,g,h) = \left(\begin{array}{c|c|c|c|c|c|c|c} 1 & 1 & c & 1 & e & f & g & h \\ \hline h & 1 & 1 & c & 1 & e & f & g \\ \hline g & h & 1 & 1 & c & 1 & e & f \\ \hline f & g & h & 1 & 1 & c & 1 & e \\ \hline e & f & g & h & 1 & 1 & c & 1 \\ \hline 1 & e & f & g & h & 1 & 1 & c \\ \hline c & 1 & e & f & g & h & 1 & 1 \\ \hline 1 & c & 1 & e & f & g & h & 1 \end{array}\right)$$

Figure 12. A 3×3 and an 8×8 bi-regular matrix with maximum number of ones.

$$\left(\begin{array}{c|c|c|c|c|c|c|c} a & b & c & d & e & f & g & h \\ \hline e & c & b & f & a & d & h & g \\ \hline g & d & f & b & h & c & a & e \\ \hline c & e & a & h & b & g & f & d \\ \hline h & f & d & c & g & b & e & a \\ \hline d & g & h & a & f & e & b & c \\ \hline b & a & e & g & c & h & d & f \\ \hline f & h & g & e & d & a & c & b \end{array}\right)$$

Figure 13. An 8×8 Latin square where one element can be set to be 1 without disturbing the bi-regular property.

by $L_3(c)$. It is easy to verify that in $\mathbb{F}_{2^n}$ $(n > 2)$, the matrix $L_3(c)$ of Figure 12 becomes MDS for all values of c other that 0 and 1.

Similarly by setting $a = b = d = 1$ in the 8×8 matrix, we can construct an 8×8 bi-regular matrix with $v_1^{8,8} = 3 \times 8 = 24$ ones and five other elements (see Figure 12) and we denote this matrix by $L_8(c, e, f, g, h)$. In $\mathbb{F}_{2^8}$, represented by the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$, if we take $c = 02_x$, $e = 04_x$, $f = 06_x$ and $g = h = 03_x$, then the 8×8 matrix $L_8(02_x, 04_x, 06_x, 03_x, 03_x)$ of Figure 12 becomes MDS.

Remark 5.5. The 8×8 matrix of Figure 12 is a circulant matrix. With judicious choices of elements, the 8×8 bi-regular matrix of Figure 12 can be converted to a circulant MDS matrix. Note that, using techniques of [3, 11, 21], a similar kind of circulant MDS matrices can be constructed.

Note that, using this technique, it may not be possible to convert any $d \times d$ Latin square into a $d \times d$ bi-regular matrix with maximum number of ones (see Figure 13). It is easy to observe that in the 8×8 Latin square of Figure 13, if more than one element is set to 1, then the bi-regular property will be disturbed. So, in this case, this Latin square can be converted into a bi-regular matrix with maximum eight number of ones.

6 Efficient MDS matrices

In this section, we propose $d \times d$ MDS matrices for d up to 8 from bi-regular matrices designed in Section 5. In Table 2, we present some $d \times d$ MDS matrices over $\mathbb{F}_{2^8}$ for d up to 8 having $v_1^{d,d}$ ones. Also, any matrix of Table 2 can be implemented with less number of multiplication tables which may be advantageous for a system where constraints on processor are more than that on memory. Although all matrices M_d of Table 2 are efficient, their inverses may not be efficient. So implementing these matrices for Lai–Massey networks or hash functions may be suitable.

Remark 6.1. We exhaustively searched for 8×8 MDS matrices of the form $M_8(e_0, e_1, e_2, e_3, e_4)$ (see Figure 8) over $\mathbb{F}_{2^8}$, but no MDS matrix of this form is found. It may be noted that in [12], an 8×8 almost-bi-regular matrix with maximum number of ones similar to the 8×8 matrix of Figure 4 was proposed, but no MDS matrix based on that form was reported. In Figure 12 of Section 5, we have constructed 8×8 bi-regular

Dimension $d \times d$	MDS matrices	Cost of implementations	For illustrations see
3×3	$M_3(02_x)$	6 XORs, 3 table lookups and 4 temp	Figure 6
4×4	$M_4(03_x, 04_x)$	12 XORs, 7 table lookups and 4 temps	Figure 7
	$M_4(02_x, 05_x)$	12 XORs, 7 table lookups and 6 temps	Figure 7
5×5	$M_5(02_x, 03_x, 09_x)$	20 XORs, 13 table lookups and 8 temps	Figure 7
	$M_5(02_x, 03_x, 08_x)$	20 XORs, 13 table lookups and 8 temps	Figure 7
6×6	$M_6(03_x, 09_x, 0a_x, 0e_x)$	30 XORs, 20 table lookups and 10 temps	Figure 7
	$M_6(05_x, 06_x, 0e_x, 0f_x)$	30 XORs, 20 table lookups and 10 temps	Figure 7
7×7	$M_7(03_x, 09_x, 0a_x, 0e_x)$	42 XORs, 28 table lookups and 11 temps	Figure 7
	$M_7(05_x, 06_x, 0e_x, 0f_x)$	42 XORs, 28 table lookups and 11 temps	Figure 7
8×8	$L_8(02_x, 04_x, 06_x, 03_x, 03_x)$	56 XORs, 40 table lookups and 11 temps	Figure 12

Table 2. The $d \times d$ *circulant MDS matrices* over $\mathbb{F}_{2^8}$ with generating polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$ for $d = 3, 4, 5, 6, 7$ and with generating polynomial $x^8 + x^4 + x^3 + x^2 + 1$ for $d = 8$.

matrices with maximum number of ones and five distinct elements from the 8×8 Latin square of Figure 11. With this construction, MDS matrices can be formed (see Remark 5.5). For similar kind of constructions also, see [11].

Remark 6.2. The matrix $M_7(03_x, 09_x, 0a_x, 0e_x)$ of Table 2 is implemented in Appendix A.1. The idea of this implementation is taken from [5]. The other matrices of Table 2 and Table 3 can be implemented similarly.

6.1 Comparison with other existing matrices

In the following table (Table 3), we compare the cost of implementations of few of our proposed matrices and some existing matrices which are used in several ciphers and hash functions.

			Cost of implementation				
Dimension	Type	Matrix	#XOR	#table	#table-lookup	#temp	Comments
4×4	M_4	$M_4(03_x, 04_x)$	12	2	7	6	Table 2
	circulant	$\mathrm{Circ}(02_x, 03_x, 01_x, 01_x)$	12	2	8	6	see [5]
	recursive	$\mathrm{Serial}(1, \alpha, 1, \alpha^2)^4$	12	2	8	6	see [8]
	companion	$\mathrm{Serial}(1, \alpha, 1, 1 + \alpha)^4$	12	2	8	6	see [10, 18]
		$\mathrm{Serial}(\alpha, 1, 1, \alpha^2)^4$	12	2	8	6	see [10, 25]
5×5	M_5	$M_5(02_x, 03_x, 09_x)$	20	3	13	8	Table 2
	circulant	$\mathrm{Circ}(01_x, 01_x, 02_x, 03_x, 02_x)$	20	2	15	8	see [11]
6×6	M_6	$M_6(03_x, 09_x, 0a_x, 0e_x)$	30	4	20	10	Table 2
	circulant	$\mathrm{Circ}(01_x, 01_x, 02_x, 03_x, 05_x, 07_x)$	30	4	24	10	see [11]
7×7	M_7	$M_7(03_x, 09_x, 0a_x, 0e_x)$	42	4	28	11	Table 2
	circulant	$\mathrm{Circ}(01_x, 01_x, 02_x, 01_x, 05_x, 04_x, 06_x)$	42	4	28	11	see [11]
8×8	L_8	$L_8(02_x, 04_x, 06_x, 03_x, 03_x)$	56	4	40	11	Figure 12
	circulant	$\mathrm{Circ}(01_x, 01_x, 02_x^{-1}, 01_x, 04_x^{-1}, 06_x^{-1}, 03_x^{-1}, 03_x^{-1})$	56	4	40	11	see [11]

Table 3. Comparison between some good matrices of this paper and some other matrices.

7 Conclusion

MDS matrices provide optimal diffusion components which can be used as building blocks of cryptographic primitives, like block ciphers and hash functions. Multiplication by 1 over the finite field is trivial and so matrices with more occurrences of ones may have more compact and improved footprint which is desirable for lightweight applications. Also, matrices with less number of other distinct elements may be imple-

mented efficiently using table lookup. Towards this, two combinatorial problems were studied by Junod and Vaudenay in [12], namely, how to maximize the number of ones and how to minimize other distinct elements in a bi-regular matrix. They calculated the maximum number of ones that can occur in $d \times d$ MDS matrices for d up to 8. They also computed some important bounds on the number of distinct elements in $d \times d$ MDS matrices. But for higher values of d, using their techniques seems difficult.

We have observed simple yet subtle interconnections between the number of ones in MDS matrices and the incidence matrices of Balanced Incomplete Block Design (BIBD). This observation gives a generalize technique to solve these combinatorial problems for any values of d for all practical purpose. We have exactly computed the maximum number of ones in a $v \times b$ MDS matrix whenever there exists $(v, b, r, k, 1)$-BIBD. We have computed the upper bound of $v_1^{v,b}$ for any value of v and b. Using these results, in this paper we have provided $d \times d$ almost-bi-regular matrices M for d up to 21 having maximum number of ones. Techniques used in this paper can be extended for higher values of d. We also compute the minimum number of distinct elements for these $d \times d$ bi-regular matrices having $v_1^{d,d}$ ones, where $d = q^2 + q + 1$ and q is any prime power.

We have proposed another technique to construct bi-regular matrices and MDS matrices using Latin squares. We have shown that using the structure of Latin squares, bi-regular matrices and MDS matrices can be constructed by judicial selection of elements. Although this is a very easy method, yet this method does not guarantee the maximum occurrences of ones in all cases. We have shown that if $v_1^{d,d}$ is a multiple of d, then our method may be useful to construct $d \times d$ bi-regular matrices with maximum number of ones. From bi-regular matrices, finally we have constructed efficient $d \times d$ MDS matrices for d up to 8.

A Apendix

A.1. We provide an implementation of the matrix $M_7(03_x, 09_x, 0a_x, 0e_x)$ proposed in Table 2. This implementation requires 42 XORs, 11 temporary variables and 28 table lookups in four multiplication tables, say, `tab_03`, `tab_09`, `tab_0a`, and `tab_0e` corresponding to the multiplication by 03_x, 09_x, $0a_x$ and $0e_x$, respectively.

```
u0 = a[0]; u1 = a[1]; u2 = a[2]; u3 = a[3]; u4 = a[4]; u5 = a[5]; u6 = a[6];
/* a is the input vector */
u = tab_03[a[3]]; v = tab_09[a[4]], w = tab_0a[a[5]]; x = tab_0e[a[6]];
a[0] = u0 ⊕ u1 ⊕ u2 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[2]]; v = tab_09[a[3]], w = tab_0a[a[6]]; x = tab_0e[a[1]];
a[1] = u0 ⊕ u4 ⊕ u5 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[4]]; v = tab_09[a[5]], w = tab_0a[a[1]]; x = tab_0e[a[2]];
a[2] = u0 ⊕ u3 ⊕ u6 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[1]]; v = tab_09[a[6]], w = tab_0a[a[0]]; x = tab_0e[a[5]];
a[3] = u2 ⊕ u3 ⊕ u4 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[0]]; v = tab_09[a[1]], w = tab_0a[a[3]]; x = tab_0e[a[4]];
a[4] = u2 ⊕ u5 ⊕ u6 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[5]]; v = tab_09[a[0]], w = tab_0a[a[2]]; x = tab_0e[a[3]];
a[5] = u1 ⊕ u4 ⊕ u6 ⊕ u ⊕ v ⊕ w ⊕ x;
u = tab_03[a[6]]; v = tab_09[a[2]], w = tab_0a[a[4]]; x = tab_0e[a[0]];
a[6] = u1 ⊕ u3 ⊕ u5 ⊕ u ⊕ v ⊕ w ⊕ x;
```

A.2. From Corollary 3.9, $v_1^{13,13} = 52$. Let us consider the derived-incidence matrix of $(13, 13, 4, 4, 1)$-BIBD in Figure 4 having $v_1^{13,13}$ ones. By elimination of suitable rows and columns from this matrix so that the minimum number of occurrences of 1 is canceled, we form $d \times d$ matrices for $d = 12, 11, 10$ and 9. For $d = 8$ the corresponding matrix is given in Figure 4.

$$M_{12} = \begin{pmatrix}
 & & & 1 & 1 & 1 & & & & & & \\
 & & & & & & 1 & 1 & 1 & & & \\
 & & & & & & & & & 1 & 1 & 1 \\
1 & & & 1 & & & 1 & & & 1 & & \\
1 & & & & 1 & & & 1 & & & & 1 \\
1 & & & & & 1 & & & 1 & & 1 & \\
 & 1 & & 1 & & & & 1 & & & 1 & \\
 & 1 & & & 1 & & & & 1 & 1 & & \\
 & 1 & & & & 1 & 1 & & & & & 1 \\
 & & 1 & & 1 & & 1 & & & & 1 & \\
 & & 1 & 1 & & & & & 1 & & & 1 \\
 & & 1 & & & 1 & & 1 & & 1 & &
\end{pmatrix},$$

$$M_{11} = \begin{pmatrix}
 & & & & & 1 & 1 & 1 & & & \\
 & & & & & & & & 1 & 1 & 1 \\
1 & & & & & 1 & & & 1 & & \\
1 & & & 1 & & & 1 & & & & 1 \\
1 & & & & 1 & & & 1 & & 1 & \\
 & 1 & & & & & 1 & & & 1 & \\
 & 1 & & 1 & & & & 1 & 1 & & \\
 & 1 & & & 1 & 1 & & & & & 1 \\
 & & 1 & 1 & & 1 & & & & 1 & \\
 & & 1 & & & & & 1 & & & 1 \\
 & & 1 & & 1 & & 1 & & 1 & &
\end{pmatrix},$$

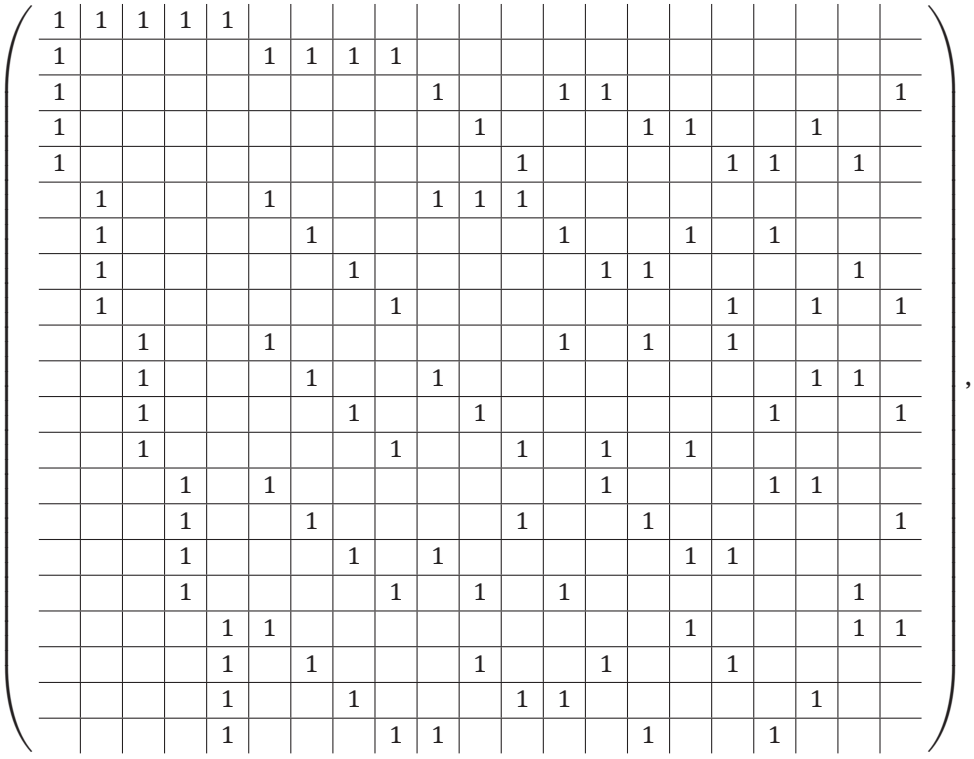
$$M_{10} = \begin{pmatrix}
 & & & & 1 & 1 & 1 & & & \\
 & & & & & & & 1 & 1 & 1 \\
 & & 1 & & & 1 & & & & 1 \\
 & & & 1 & & & 1 & & 1 & \\
1 & & & & & 1 & & & 1 & \\
1 & & 1 & & & & 1 & 1 & & \\
1 & & & 1 & 1 & & & & & 1 \\
 & 1 & 1 & & 1 & & & & 1 & \\
 & 1 & & & & & 1 & & & 1 \\
 & 1 & & 1 & & 1 & & 1 & &
\end{pmatrix},$$

$$M_9 = \begin{pmatrix}
 & & & & 1 & 1 & 1 & & \\
 & & 1 & & & 1 & & & 1 \\
 & & & 1 & & & 1 & 1 & \\
1 & & & & & 1 & & 1 & \\
1 & & 1 & & & & 1 & & \\
1 & & & 1 & 1 & & & & 1 \\
 & 1 & 1 & & 1 & & & 1 & \\
 & 1 & & & & & 1 & & 1 \\
 & 1 & & 1 & & 1 & & &
\end{pmatrix}.$$

Figure 14. Examples of $d \times d$ almost-bi-regular matrices M_d, $d = 12, 11, 10, 9$, with $v_1(M_d) = v_1^{d,d} = \lfloor d \times \frac{1+\sqrt{4d-3}}{2} \rfloor - 1$.

A.3. From Corollary 3.9, we have $v_1^{21,21} = 105$. Let us consider the derived-incidence matrix of projective plane $(2^{2^2} + 2^2 + 1, 2^2 + 1, 1)$ i.e. $(21, 21, 5, 5, 1)$-BIBD in Figure 15 having $v_1^{21,21}$ ones. By elimination of suitable rows and columns from this matrix so that the minimum number of occurrences of 1 is cancelled, we form $d \times d$ matrices for $d = 20, 19, 18, 17, 16$.

$M_{21} =$



,

$M_{20} =$

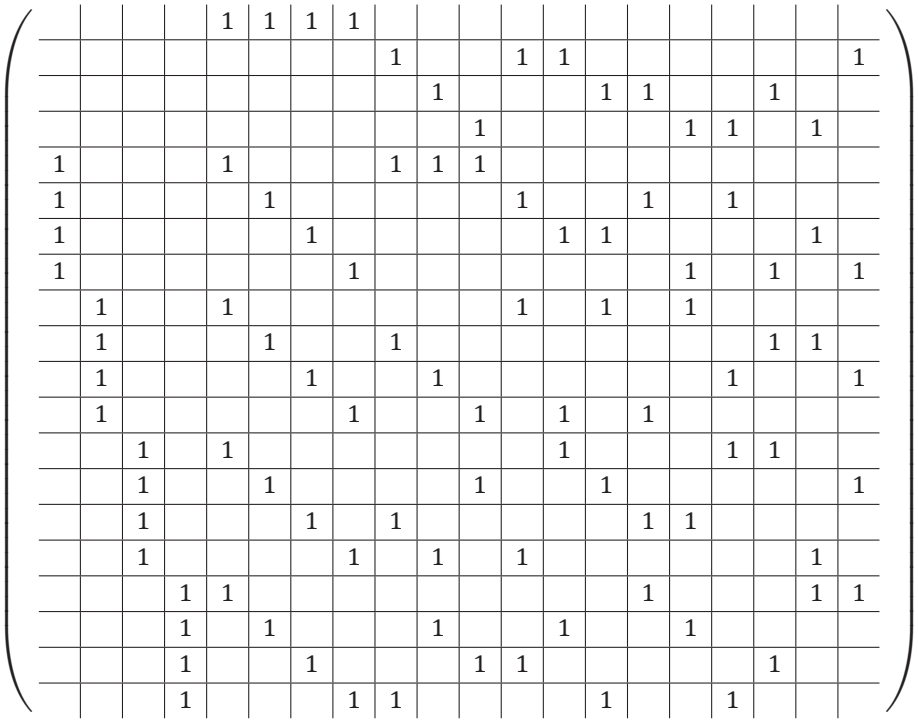


Figure 15. Examples of $d \times d$ almost-bi-regular matrices M_d, $d = 21, 20$, with $v_1(M_{21}) = v_1^{21,21} = 105$ and $v_1(M_{20}) = v_1^{20,20} = 96$.

$$M_{19} = \begin{pmatrix}
 & & & & & & & 1 & & & 1 & 1 & & & & & & & 1 \\
 & & & & & & & & 1 & & & & 1 & 1 & & & 1 & & \\
 & & & & & & & & & 1 & & & & & 1 & 1 & & 1 & \\
1 & & & & & & & 1 & 1 & 1 & & & & & & & & & \\
1 & & & & 1 & & & & & & 1 & & & 1 & & 1 & & & \\
1 & & & & & 1 & & & & & & 1 & 1 & & & & & 1 & \\
1 & & & & & & 1 & & & & & & & & 1 & & 1 & & 1 \\
 & 1 & & & & & & & & & 1 & & 1 & & 1 & & & & \\
 & 1 & & & 1 & & & 1 & & & & & & & & & 1 & 1 & \\
 & 1 & & & & 1 & & & 1 & & & & & & & 1 & & & 1 \\
 & 1 & & & & & 1 & & & 1 & & 1 & & 1 & & & & & \\
 & & 1 & & & & & & & & 1 & & & & 1 & 1 & & & \\
 & & 1 & & 1 & & & & & 1 & & & 1 & & & & & & 1 \\
 & & 1 & & & 1 & & 1 & & & & & & 1 & 1 & & & & \\
 & & 1 & & & & 1 & & 1 & & 1 & & & & & & & 1 & \\
 & & & 1 & & & & & & & & & & 1 & & & & 1 & 1 \\
 & & & 1 & 1 & & & & 1 & & & 1 & & & 1 & & & & \\
 & & & 1 & & 1 & & & & 1 & 1 & & & & & & 1 & & \\
 & & & 1 & & & 1 & 1 & & & & & 1 & & & 1 & & &
\end{pmatrix},$$

$$M_{18} = \begin{pmatrix}
 & & & & & & 1 & & & 1 & 1 & & & & & & & 1 \\
 & & & & & & & 1 & & & & 1 & 1 & & & 1 & & \\
 & & & & & & & & 1 & & & & & 1 & 1 & & 1 & \\
 & & & 1 & & & & & & 1 & & & 1 & & 1 & & & \\
 & & & & 1 & & & & & & 1 & 1 & & & & & 1 & \\
 & & & & & 1 & & & & & & & & 1 & & 1 & & 1 \\
1 & & & & & & & & & 1 & & 1 & & 1 & & & & \\
1 & & & 1 & & & 1 & & & & & & & & & 1 & 1 & \\
1 & & & & 1 & & & 1 & & & & & & & 1 & & & 1 \\
1 & & & & & 1 & & & 1 & & 1 & & 1 & & & & & \\
 & 1 & & & & & & & & & 1 & & & & 1 & 1 & & \\
 & 1 & & 1 & & & & & 1 & & & 1 & & & & & & 1 \\
 & 1 & & & 1 & & 1 & & & & & & 1 & 1 & & & & \\
 & 1 & & & & 1 & & 1 & & 1 & & & & & & & 1 & \\
 & & 1 & & & & & & & & & & 1 & & & & 1 & 1 \\
 & & 1 & 1 & & & & 1 & & & 1 & & & 1 & & & & \\
 & & 1 & & 1 & & & & 1 & 1 & & & & & & 1 & & \\
 & & 1 & & & 1 & 1 & & & & & 1 & & & 1 & & &
\end{pmatrix}.$$

Figure 16. Examples of $d \times d$ almost-bi-regular matrices M_d, $d = 19, 18$, with $v_1(M_{19}) = v_1^{19,19} = 88$ and $v_1(M_{18}) = v_1^{18,18} = 81$.

$$M_{17} = \begin{pmatrix}
 & & & & & 1 & & & 1 & 1 & & & & & & & 1 \\
 & & & & & & 1 & & & & 1 & 1 & & & 1 & & \\
 & & & & & & & 1 & & & & & 1 & 1 & & 1 & \\
 & & 1 & & & & & & 1 & & & 1 & & 1 & & & \\
 & & & 1 & & & & & & 1 & 1 & & & & & 1 & \\
 & & & & 1 & & & & & & & & 1 & & 1 & & 1 \\
 & & 1 & & & 1 & & & & & & & & & 1 & 1 & \\
 & & & 1 & & & 1 & & & & & & & 1 & & & 1 \\
 & & & & 1 & & & 1 & & 1 & & 1 & & & & & \\
1 & & & & & & & & & 1 & & & & 1 & 1 & & \\
1 & & 1 & & & & & 1 & & & 1 & & & & & & 1 \\
1 & & & 1 & & 1 & & & & & & 1 & 1 & & & & \\
1 & & & & 1 & & 1 & & 1 & & & & & & & 1 & \\
 & 1 & & & & & & & & & & 1 & & & & 1 & 1 \\
 & 1 & 1 & & & & 1 & & & 1 & & & 1 & & & & \\
 & 1 & & 1 & & & & 1 & 1 & & & & & & 1 & & \\
 & 1 & & & 1 & 1 & & & & & 1 & & & 1 & & &
\end{pmatrix},$$

$$M_{16} = \begin{pmatrix}
 & & & & 1 & & & 1 & 1 & & & & & & & 1 \\
 & & & & & 1 & & & & 1 & 1 & & & 1 & & \\
 & & & & & & 1 & & & & & 1 & 1 & & 1 & \\
 & 1 & & & & & & 1 & & & 1 & & 1 & & & \\
 & & 1 & & & & & & 1 & 1 & & & & & 1 & \\
 & & & 1 & & & & & & & & 1 & & 1 & & 1 \\
 & 1 & & & 1 & & & & & & & & & 1 & 1 & \\
 & & 1 & & & 1 & & & & & & & 1 & & & 1 \\
 & & & 1 & & & 1 & & 1 & & 1 & & & & & \\
 & 1 & & & & & 1 & & & 1 & & & & & & 1 \\
 & & 1 & & 1 & & & & & & 1 & 1 & & & & \\
 & & & 1 & & 1 & & 1 & & & & & & & 1 & \\
1 & & & & & & & & & & 1 & & & & 1 & 1 \\
1 & 1 & & & & 1 & & & 1 & & & 1 & & & & \\
1 & & 1 & & & & 1 & 1 & & & & & & 1 & & \\
1 & & & 1 & 1 & & & & & 1 & & & 1 & & &
\end{pmatrix}.$$

Figure 17. Examples of $d \times d$ almost-bi-regular matrices M_d, $d = 17, 16$, with $v_1(M_{17}) = v_1^{17,17} = 74$ and $v_1(M_{16}) = v_1^{16,16} = 67$.

Acknowledgment: Major part of the work was done when the second author was at R. C. Bose Centre for Cryptology & Security, Indian Statistical Institute, 203, B.T. Road, Kolkata-700108, India.

References

[1] D. Augot and M. Finiasz, Direct construction of recursive MDS diffusion layers using shortened BCH codes, in: *Fast Software Encryption* (FSE 2014), Lecture Notes in Comput. Sci. 8540, Springer, Berlin (2015), 3–17.

[2] P. Barreto and V. Rijmen, The Khazad legacy-level block cipher, submission to the NESSIE Project (2000), http://cryptonessie.org.

[3] P. S. L. M. Barreto and V. Rijmen, Whirlpool, in: *Encyclopedia of Cryptography and Security. Second Edition*, Springer, New York (2011), 1384–1385.

[4] J. Daemen, L. R. Knudsen and V. Rijmen, The block cipher square, in: *Fast Software Encryption* (FSE 1997), Lecture Notes in Comput. Sci. 1267, Springer, Berlin (1997), 149–165.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer, Berlin, 2002.
[6] G. D. Filho, P. Barreto and V. Rijmen, The Maelstrom-0 hash function, in: *Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security (2006)*; available at http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2006/0017.pdf.
[7] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schlaffer and S. Thomsen, Grøstl – A SHA-3 candidate, submission to NIST (2008), http://www.groestl.info.
[8] J. Guo, T. Peyrin and A. Poschmann, The PHOTON family of lightweight hash functions, in: *Advances in Cryptology* (CRYPTO 2011), Lecture Notes in Comput. Sci. 6841, Springer, Berlin (2011), 222–239.
[9] K. C. Gupta and I. G. Ray, On constructions of involutory MDS matrices, in: *Progress in Cryptology* (AFRICACRYPT 2013), Lecture Notes in Comput. Sci. 7918, Springer, Berlin (2013), 43–60.
[10] K. C. Gupta and I. G. Ray, On constructions of MDS matrices from companion matrices for lightweight cryptography, in: *Security Engineering and Intelligence Informatics* (CD-ARES 2013), Lecture Notes in Comput. Sci. 8128, Springer, Berlin (2013), 29–43.
[11] K. C. Gupta and I. G. Ray, On constructions of circulant MDS matrices for lightweight cryptography, in: *Information Security Practice and Experience* (ISPEC 2014), Lecture Notes in Comput. Sci. 8434, Springer, Berlin (2014), 564–576.
[12] P. Junod and S. Vaudenay, Perfect diffusion primitives for block ciphers building efficient MDS matrices, in: *Selected Areas in Cryptography* (Waterloo 2004), Lecture Notes in Comput. Sci. 3357, Springer, Berlin (2005), 84–99.
[13] J. Lacan and J. Fimes, Systematic MDS erasure codes based on Vandermonde matrices, *IEEE Commun. Lett.* **8** (2004), no. 9, 570–572.
[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, 1986.
[15] J. Nakahara, Jr. and E. Abrahao, A new involutory MDS matrix for the AES, *Int. J. Netw. Secur.* **9** (2009), no. 2, 109–116.
[16] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers and E. D. Win, The cipher SHARK, in: *Fast Software Encryption* (FSE 1996), Lecture Notes in Comput. Sci. 1039, Springer, Berlin (1996), 99–112.
[17] M. Sajadieh, M. Dakhilalian, H. Mala and B. Omoomi, On construction of involutory MDS matrices from Vandermonde matrices in GF(2^q), *Des. Codes Cryptogr.* **64** (2012), no. 3, 287–308.
[18] M. Sajadieh, M. Dakhilalian, H. Mala and P. Sepehrdad, Recursive diffusion layers for block ciphers and hash functions, in: *Fast Software Encryption* (FSE 2012), Lecture Notes in Comput. Sci. 7549, Springer, Berlin (2012), 385–401.
[19] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, Twofish: A 128-bit block cipher, in: *First Advanced Encryption Standard (AES) Candidate Conference*, National Institute for Standards and Technology, Gaithersburg (1998); available at https://www.schneier.com/academic/paperfiles/paper-twofish-paper.pdf.
[20] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, *The Twofish Encryption Algorithm*, John Wiley & Sons, New York, 1999.
[21] T. Shiraj and K. Shibutani, On the diffusion matrix employed in the Whirlpool hashing function, preprint (2003), https://www.cosic.esat.kuleuven.be/nessie/reports/phase2/whirlpool-20030311.pdf.
[22] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, 1995.
[23] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer, New York, 2003.
[24] D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi and B. Preneel, A new keystream generator MUGI, in: *Fast Software Encryption* (FSE 2002), Lecture Notes in Comput. Sci. 2365, Springer, Berlin (2002), 179–194.
[25] S. Wu, M. Wang and W. Wu, Recursive diffusion layers for (lightweight) block ciphers and hash functions, in: *Selected Areas in Cryptography* (SAC 2012), Lecture Notes in Comput. Sci. 7707, Springer, Berlin (2013), 355–371.
[26] A. M. Youssef, S. Mister and S. E. Tavares, On the design of linear transformations for substitution permutation encryption networks, in: *Workshop on Selected Areas in Cryptography* (SAC 1997), Carleton University, Ottawa (1997), 40–48.
[27] Sony Corporation, *The 128-bit block cipher CLEFIA* Algorithm Specification (2007), http://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf.