IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2022, No. 4, pp. 266–290. DOI:10.46586/tosc.v2022.i4.266-290

On the Lower Bound of Cost of MDS Matrices

Ayineedi Venkateswarlu[1] and Abhishek Kesarwani[2] and Sumanta Sarkar[3]

[1] Indian Statistical Institute, Chennai Centre, Chennai, India
venku@isichennai.res.in
[2] IHUB NTIHAC FOUNDATION, IIT Kanpur, Kanpur, India
abhishekkmath@gmail.com
[3] University of Warwick, Coventry, United Kingdom
sumanta.sarkar@warwick.ac.uk

Abstract. Ever since lightweight cryptography emerged as one of the trending topics in symmetric key cryptography, optimizing the implementation cost of MDS matrices has been in the center of attention. In this direction, various metrics like d-XOR, s-XOR and g-XOR have been proposed to mimic the hardware cost. Consequently, efforts also have been made to search for the optimal MDS matrices for dimensions relevant to cryptographic applications according to these metrics. However, finding the optimal MDS matrix in terms of hardware cost still remains an unsolved problem. In this paper, we settle the question of the optimal 4×4 MDS matrices over $GL(n, \mathbb{F}_2)$ under the recently proposed metric *sequential XOR count based on words* (sw-XOR). We prove that the sw-XOR of such matrices is at least $8n + 3$, and the bound is tight as matrices with sw-XOR cost 35 and 67 for the values of $n = 4$ and 8, respectively, were already known. Moreover, the lower bound for these values of n matches with the known lower bounds according to s-XOR and g-XOR metrics.

Keywords: Lightweight cryptography · Diffusion layer · MDS matrix · Hardware implementation · XOR cost

1 Introduction

Catering to the need of securing the IoT networks that comprise of small embedded devices, the so called lightweight cryptography has emerged. Research on lightweight cryptography received further boost when NIST announced the call for standardization of lightweight authenticated encryption with associated data [LWC18]. Lightweight cryptography is based on symmetric key, and such a design basically targets to optimize one of the following performance metrics: hardware cost, software efficiency, latency and energy.

One of the classical models for designing a block cipher is the Substitution Permutation Network (SPN), and notably the Advanced Encryption Standard (AES) [DR02] was also based on this design principle. SPN has a nonlinear component and a linear component. The nonlinear component is built by S-boxes that basically provides the confusion property, that is, making the relation between the key and the ciphertext very much complex. On the other hand, the linear component can be represented as a matrix that is called diffusion matrix; it basically diffuses the plaintext throughout the ciphertext.

One approach to design lightweight SPNs would be to apply lightweight S-boxes and lightweight diffusion matrices. There have been different approaches for constructing lightweight S-boxes, for instance, GIFT [BPP+17] has an extremely lightweight 4×4 S-box, Sycon[MSST22] has a lightweight 5×5 S-box, and [CDL15] showed a way to construct lightweight S-boxes using Feistel and MISTY structures.

When it comes to choosing diffusion matrices, it is often preferred to choose MDS matrices as these matrices provide the optimal diffusion. For example, the `MixColumns`

Received: 2022-09-01 Accepted: 2022-11-01 Published: 2022-12-07

operation in AES uses a 4×4 MDS matrix over $\mathbb{F}_{2^8}$. However, in MIDORI [BBI+15], a non-MDS matrix was chosen as the designers aimed to make an energy efficient block cipher. The construction of MDS matrices with low hardware footprint is an active area of research and many such constructions can be found in [SKOP15, BKL16, SS16a, LS16, LW16, SS16b, LW17, JPST17, SS17, DL18]

Even after so many years of effort, the key question of finding the MDS matrices for dimensions relevant to cryptographic designs with the minimal implementation cost is still unsolved. The general problem which is to minimize the number of linear operations necessary to compute a set of linear functions is termed as Shortest Linear Program (SLP) problem, and it is known to be NP-hard [BMP08]. However, heuristic algorithms have been proposed to optimize the implementation of binary matrices [Paa97, BMP08, Ber09, BP10]. There have also been many other notions proposed to capture the hardware cost of a matrix, and according to those cost metrics MDS matrices have been analyzed.

There are generally three metrics discussed in the literature: d-XOR, s-XOR, and g-XOR. The direct XOR or d-XOR count is basically the number of 1's in the binary matrix (see [KPPY14, LW16]). In [ZWZZ16], the authors proposed an approach to find efficient implementation of MDS matrices using graph-theoretical model and transfer the main problem to the shortest path problem in graph theory. It was also shown that the optimal implementation of an MDS matrix depends upon the minimum number of additive elementary matrices (known as Type III) that appear in its decomposition. It was then reformulated in [JPST17, BKL16] as sequential XOR or s-XOR to estimate the implementation cost. Also, a graph-based meet-in-the-middle (MITM) search algorithm to find efficient implementation of MDS matrices called LIGHTER was developed in [JPST17]. However, the problem with these graph-theoretical tools is that they do not scale well. Note that, s-XOR uses in-place replace operations without using any extra registers. Then it was observed in [KLSW17] that by allowing extra registers to save intermediate values, one may get a better estimate for the XOR cost. This is known as g-XOR and it is linked with the Shortest Linear Program (SLP). A series of works have considered the problem of finding efficient implementations of MDS matrices with respect to either s-XOR or g-XOR [KLSW17, DL18, XZL+20, YZW21].

In designing lightweight MDS matrices, most of the early works concentrated on constructing MDS matrices with entries in a finite field $\mathbb{F}_{2^n}$ or $GL(n, \mathbb{F}_2)$ such that the entries are efficiently implemented. Most practical purposes, the entries considered are binary matrices of small orders like 4 or 8. Due to the smaller size of the entries, many ad-hoc techniques were used to search for efficient MDS matrices. This is often called local optimization. In another direction, to reduce the hardware area requirements, considering serial implementations, specially structured MDS matrices such as circulant (e.g., [LW16]), Toeplitz (e.g., [SS16b]) or recursive MDS matrices (e.g., [GPP11, KPSV21]) were studied extensively. Many of those ad-hoc search techniques locally optimize the entries of some specially structured MDS matrices.

In [KSV19], a method was presented to exhaustively search for various types of MDS matrices over $GL(4, \mathbb{F}_2)$, and they provided MDS matrices locally optimized with respect to d-XOR and s-XOR metrics. Similarly, there have been many works such as [LW16, LWL18, ZWS18, DL18, XZL+20, YZW21] that considered MDS matrices over the general linear group $GL(n, \mathbb{F}_2)$, and many such works considered global optimization.

In [DL18], a direct construction of lightweight MDS matrix was shown. The construction starts with an identity matrix over $\mathbb{F}_2[\alpha]$ and in every step a linear operation is applied. They considered linear operations which are `XOR` : $x \leftarrow x + y$, `COPY` : $x \leftarrow y$ and `Multiplication` : $x \leftarrow \alpha x$, where $x, y, \in \mathbb{F}_2^n$ and α is a non-singular matrix of order n. After each of these operations, the newly obtained matrix is checked for MDS property. This way, the authors were able to produce 4×4 MDS matrices over the ring $\mathbb{F}_2[\alpha]$. When they instantiated α with the 4×4 binary matrix A_4 which is the companion matrix of

$X^4 + X + 1$, they obtained an MDS matrix with XOR cost 35, and with the 8×8 matrix A_8 which is the companion matrix of $X^8 + X + 1$, they obtained an MDS matrix XOR cost 67. These matrices still hold the record for their respective dimensions. In [XZL$^+$20], the authors reduced the problem of optimizing implementations of matrices to the problem of optimizing matrix decomposition. As a result, they were able to find the implementation of the MDS matrix of AES with s-XOR cost 92, which performs equally well as the previous best result under g-XOR metric [Max19]. Later, [YZW21] improved the efficiency of the heuristic algorithm of [XZL$^+$20] which enables them to search for lightweight involutory MDS matrices in a larger space with the computation remains in a reasonable range.

Our Contributions

The construction of lightweight MDS matrices proposed in [DL18] showed a minimal approach, that can ensure achieving MDS matrices which are of low cost. This approach was taken up by [WLTZ21] that extended it by treating the linear operations as the multiplications by the three types of elementary matrices. It is well-known that any non-singular matrix over $\mathbb{F}_{2^n}$ can be decomposed as a product of elementary matrices. Analogously, elementary block matrices can be considered for the case of block matrices. Considering such block-wise decompositions, a new metric called *sequential XOR count based on words* (sw-XOR) was introduced in [WLTZ21] to estimate the hardware cost. This can be viewed as a restricted version of the sequential XOR count (s-XOR) which is defined considering elementary matrix decomposition over $\mathbb{F}_2$. In [DL18], the authors obtained 3×3 and 4×4 MDS matrices over $GL(n, \mathbb{F}_2)$ with XOR cost $5n + 1$ and $8n + 3$ respectively. However, establishing the lower bounds seems to be a hard problem. The g-XOR metric gives the optimal implementation in terms of XOR gate count, but it does not have a nice mathematical structure as compared to sw-XOR or s-XOR metrics. In [WLTZ21], the authors introduced the concept of *path*. The path of a matrix is an ordered list of elementary (block) matrices of Type III that appear in a special form of the matrix decomposition. As we see later, the sw-XOR of a matrix mainly depends on the number of Type III elementary (block) matrices, i.e., the number of elements in a path of the matrix. The authors then considered short paths to search for MDS matrices over $\mathbb{F}_{2^n}$. Due to the commutativity of multiplication over finite fields, the authors identified potential paths that can give MDS matrices treating entries as elements of a boolean polynomial ring. After a huge search effort, the best 4×4 MDS matrix over $\mathbb{F}_{2^n}$ they obtained was with sw-XOR cost $8n + 3$ over $\mathbb{F}_{2^n}$ for $n = 4, 8$, which did not improve the state of the art. Then the authors extended the search techniques to the case of general linear group $GL(n, \mathbb{F}_2)$. However, the complexity of their search techniques for finding an MDS matrix with sw-XOR cost equal to $8n + 2$ is prohibitively high. In fact, as reported in [WLTZ21], the size of the search space is $\geq 2^{43}$ even for the case of $n = 4$. Apparently, the search problem in the domain of block matrices over $GL(n, \mathbb{F}_2)$ looks huge and appears difficult to exhaust.

In this process, the authors of [WLTZ21] also made some initial observations on the equivalence of paths. In this paper, we first rephrase some of the basic results presented in [WLTZ21] by including Type I elementary block matrices. This brings more clarity on the connection between matrices and their path. We then formalize the notion of equivalence of paths in a much broader sense of preserving MDS property. As a result, we are able to group the paths into (extended) equivalence classes. This significantly reduces the effort required to search for potential paths. In fact, we will show that it is enough to verify a set of representative paths whether they can generate MDS matrices or not. By symbolic computation, treating the entries of matrices as elements in a free algebra, we show that there are exactly two paths that can generate MDS matrices. We then analyze the sw-XOR cost of the matrices generated by these two paths by applying suitable transformations. Finally, we show that there is no 4×4 MDS matrix over $GL(n, \mathbb{F}_2)$ with

sw-XOR cost equal to $8n+2$. We also show that, to find 4×4 MDS matrices with sw-XOR cost equal to $8n+3$, it is enough to consider the two paths that are given in this paper. We have also verified that the lower bound for the sw-XOR cost of 3×3 MDS matrices over $GL(n,\mathbb{F}_2)$ is $5n+1$.

The rest of paper is organized as follows. In Section 2, we present some basic results on block matrix decomposition as a product of elementary block matrices. Then we discuss some properties of MDS matrices. Next, we discuss various XOR count metrics used to estimate the cost of hardware implementations. In Section 2.4, we first present a framework that simplifies the search for low cost MDS matrices. We then present our main result establishing the lower bound. Section 4 concludes the paper.

2 Background

2.1 Notation

Firstly, we introduce some basic notations used throughout the paper.

$\mathbb{F}_2$	the finite field with two elements 0 and 1.
$\mathbb{F}_q$	the finite field containing q elements with $char(\mathbb{F}_q)=2$.
$\mathcal{M}_n=\mathcal{M}(n,\mathbb{F}_2)$	the ring of $n\times n$ matrices over $\mathbb{F}_2$.
$\mathcal{M}(n,\mathbb{F}_q)$	the ring of $n\times n$ matrices over $\mathbb{F}_q$.
$GL(n,\mathbb{F}_q)$	the group of non-singular $n\times n$ matrices over $\mathbb{F}_q$.
$\mathcal{P}_n$	the group of $n\times n$ permutation matrices over $\mathbb{F}_2$.
$\mathcal{M}(n,m)$	the ring of $m\times m$ block matrices over $\mathcal{M}_n=\mathcal{M}(n,\mathbb{F}_2)$.
$\mathcal{D}(n,m)$	the group of $m\times m$ block diagonal matrices over $GL(n,\mathbb{F}_2)$.
$\mathcal{P}(n,m)$	the group of $m\times m$ block permutation matrices in $\mathcal{M}(n,m)$.
$I_{n,m}$	the identity matrix in $\mathcal{M}(n,m)$.
$\mathtt{I}_n$	the identity matrix in $\mathcal{M}_n$.

Observe that the elements of $\mathcal{M}(n,m)$, $\mathcal{D}(n,m)$ and $\mathcal{P}(n,m)$ can be viewed as $mn\times mn$ binary matrices. Note also that the matrices in $\mathcal{D}(n,m)$ and $\mathcal{P}(n,m)$ are non-singular. For $M\in\mathcal{M}(n,m)$, the (i,j)-th entry of the block matrix M is denoted by $M[i,j]$ for $1\le i,j\le m$. We denote a matrix $D\in\mathcal{D}(n,m)$ with $Diag(\mathtt{A}_1,\ldots,\mathtt{A}_m)$, where $\mathtt{A}_i\in GL(n,\mathbb{F}_2)$, $1\le i\le m$, are the diagonal entries of D, i.e., $D[i,i]=\mathtt{A}_i$. The zero matrix/vector is denoted by $\mathbf{0}$ with suitable size. Note that the transpose of a block matrix $M\in\mathcal{M}(n,m)$ denoted by M^T is the usual transpose considering M as an $mn\times mn$ binary matrix, i.e., $M^T[i,j]=M[j,i]^T$.

Since matrix multiplication is not commutative in general, we would like to stress that the product notation represents the following:

$$\prod_{i=1}^{l} M_i = M_l\cdots M_2M_1.$$

2.2 Elementary Block Matrices

There are three types of elementary row or column operations. An elementary matrix is a square matrix that has been obtained by performing an elementary row or column operation on an identity matrix. Left multiplication (pre-multiplication) by an elementary matrix represents elementary row operation, while right multiplication (post-multiplication) represents elementary column operation. We consider block-wise elementary row or column operations, and so the corresponding matrices are called elementary block matrices.

Definition 1. There are three types of elementary block matrices.

Type I: $E(i,j)$ is the matrix obtained by interchanging the i-th and the j-th rows of $I_{n,m}$;

Type II: $E_i(\mathtt{A})$ is the matrix obtained by multiplying the i-th row of $I_{n,m}$ with $\mathtt{A}$, where $\mathtt{A} \in GL(n, \mathbb{F}_2)$.

Type III: $E_{i,j}(\mathtt{B})$ is the matrix obtained by replacing the i-th row of $I_{n,m}$ with the sum of its i-th row and $\mathtt{B}$ times its j-th row, where $\mathtt{B} \in \mathcal{M}_n$.

Similarly, one can easily see the definition of elementary matrices over any field. Note that we often call the matrices $\mathtt{A}, \mathtt{B}$ in the above definition as *coefficients* and $i, j \in \mathbb{N}$ as *indices*. We first discuss some basic results on the decomposition of block matrices as a product of elementary block matrices. It is to be noted that, though the definition of Type III elementary block matrices allow the coefficient matrix $\mathtt{B} \in \mathcal{M}_n$, our interest is in the decompositions of the form in which the coefficient matrices of Type III elementary block matrices are restricted to non-singular matrices, i.e., $\mathtt{B} \in GL(n, \mathbb{F}_2)$. Observe that the product of two Type III elementary block matrices in $\mathcal{M}(n,m)$ satisfies

$$E_{i,j}(\mathtt{B}_1)E_{i,j}(\mathtt{B}_2) = E_{i,j}(\mathtt{B}_1 + \mathtt{B}_2), \tag{1}$$

where $\mathtt{B}_1, \mathtt{B}_2 \in \mathcal{M}_n$. The sum $\mathtt{B}_1 + \mathtt{B}_2$ can be a singular matrix for some $\mathtt{B}_1, \mathtt{B}_2 \in GL(n, \mathbb{F}_2)$. It is well-known that any non-singular matrix can be decomposed as a product of elementary matrices [Mey00, Theorem 3.9.3]. It is in fact valid for the case of elementary block matrices as well.

Lemma 1. *[WLTZ21, Corollary 1] Any non-singular block matrix in $\mathcal{M}(n,m)$ can be decomposed as a product of elementary block matrices of Type I, Type II and Type III with non-singular coefficient matrices.*

The proof given in [WLTZ21, Appendix A.1] misses a case and so we present a complete proof in Appendix A. It is easy to see the following result.

Lemma 2. *A block permutation matrix $P \in \mathcal{P}(n,m)$ can be expressed as a product of elementary block matrices of Type I and vice versa. A block diagonal matrix $D \in \mathcal{D}(n,m)$ can be expressed as a product of elementary block matrices of Type II and vice versa.*

The following result is useful in reordering the elementary block matrices in a decomposition.

Lemma 3. *Let* $f_{i,j}(x) = \begin{cases} i & x = j \\ j & x = i \\ x & x \neq i,j \end{cases}$ *, where $x, i, j \in \mathbb{N}$. Then we have*

1. *$E(i,j)E_k(\mathtt{A}) = E_{k'}(\mathtt{A})E(i,j)$, where $k' = f_{i,j}(k)$.*
2. *$E(i,j)E_{k,l}(\mathtt{B}) = E_{k',l'}(\mathtt{B})E(i,j)$, where $k' = f_{i,j}(k)$ and $l' = f_{i,j}(l)$*

By Lemma 2, we can see that a block permutation matrix can be decomposed as a product of Type I elementary block matrices and so we get the following result. Let σ be a permutation over $\{1, 2, \ldots, m\}$. Let $M \in \mathcal{M}(n,m)$ be a block matrix with rows $\mathbf{r}_1, \ldots, \mathbf{r}_m$. Let $P_\sigma \in \mathcal{P}(n,m)$ denote the block permutation matrix which permutes the rows of M when it is left-multiplied by P_σ, i.e, the rows of the matrix $P_\sigma M$ are $\mathbf{r}_{\sigma(1)}, \ldots, \mathbf{r}_{\sigma(m)}$.

Corollary 1. *Let $P_\sigma \in \mathcal{P}(n,m)$ be a block permutation matrix corresponding to a permutation σ over $\{1, 2, \ldots, m\}$. Then we have*

1. *$P_\sigma Diag(\mathtt{A}_1, \ldots, \mathtt{A}_m)P_\sigma^{-1} = Diag(\mathtt{A}_{\sigma(1)}, \ldots, \mathtt{A}_{\sigma(m)})$.*

2. $P_\sigma E_{k,l}(\mathtt{B})P_\sigma^{-1} = E_{\sigma(k),\sigma(l)}(\mathtt{B})$.

Remark 1. Observe that the group of block permutation matrices $\mathcal{P}(n,m)$ acts by conjugation on the set of block diagonal matrices $\mathcal{D}(n,m)$ and also on the set of elementary block matrices of Type III in $\mathcal{M}(n,m)$. Observe that for any $i,j \in \{1,2,\ldots,m\}$ such that $i \neq j$, by choosing σ such that $\sigma(k) = i$ and $\sigma(l) = j$, the conjugation by P_σ on $E_{k,l}(\mathtt{B})$ gives $E_{i,j}(\mathtt{B}) = P_\sigma E_{k,l}(\mathtt{B})P_\sigma^{-1}$.

Note that, given a decomposition, by applying Lemma 3, one can move the Type I elementary block matrices to the left/right, and in this rearrangement, only the indices of Type II and Type III elementary block matrices are appropriately modified but the coefficients remain the same. Thus we get the following result.

Lemma 4. *[WLTZ21, Corollary 2] Any non-singular block matrix $M \in \mathcal{M}(n,m)$ can be decomposed as a product of a block permutation matrix and elementary block matrices of Type II and Type III with non-singular coefficient matrices.*

Therefore, for any non-singular block matrix $M \in \mathcal{M}(n,m)$, it can be decomposed as

$$M = P\big(\prod_{k=1}^{m} E_k(\mathtt{A}_{k,l})\big)E_{i_l,j_l}(\mathtt{B}_l)\cdots\big(\prod_{k=1}^{m} E_k(\mathtt{A}_{k,1})\big)E_{i_1,j_1}(\mathtt{B}_1)\big(\prod_{k=1}^{m} E_k(\mathtt{A}_{k,0})\big), \tag{2}$$

where $P \in \mathcal{P}(n,m)$ and $\mathtt{A}_{k,t}$'s and $\mathtt{B}_t$'s are in $GL(n,\mathbb{F}_2)$.

Remark 2. Block permutation matrix is not part of the decomposition in [WLTZ21, Corollary 2] as it can be replaced with a product of appropriate Type III elementary block matrices by applying $E(i,j) = E_{i,j}(\mathtt{I}_n)E_{j,i}(\mathtt{I}_n)E_{i,j}(\mathtt{I}_n)$.

Observe that the product of elementary block matrices of Type II is a non-singular block diagonal matrix, and therefore the identity (2) can be rewritten in the following form.

Lemma 5. *[WLTZ21, Proposition 2] Any non-singular block matrix $M \in \mathcal{M}(n,m)$ can be decomposed as a product of a block permutation matrix, block diagonal matrices and elementary block matrices of Type III with non-singular coefficient matrices. Specifically,*

$$M = PD_lE_{i_l,j_l}(\mathtt{B}_l)\cdots D_1E_{i_1,j_1}(\mathtt{B}_1)D_0, \tag{3}$$

where $P \in \mathcal{P}(n,m)$, $D_t = \prod_{k=1}^{m} E_k(\mathtt{A}_{k,t}) \in \mathcal{D}(n,m)$ with $\mathtt{A}_{k,t} \in Gl(n,\mathbb{F}_2)$ for $0 \leq t \leq l$, and $E_{i_t,j_t}(\mathtt{B}_t)$ is an elementary block matrix of Type III with $\mathtt{B}_t \in GL(n,\mathbb{F}_2)$ for $1 \leq t \leq l$.

It is easy to see the following result on the inverse of elementary block matrices.

Lemma 6. *Let $\mathtt{A} \in GL(n,\mathbb{F}_2)$ and $\mathtt{B} \in \mathcal{M}_n$. The Type I and Type III elementary block matrices are involutory, i.e., $E(i,j)^{-1} = E(i,j)$ and $E_{i,j}(\mathtt{B})^{-1} = E_{i,j}(\mathtt{B})$. In the case of Type II elementary block matrices, we have $E_i(\mathtt{A})^{-1} = E_i(\mathtt{A}^{-1})$.*

As a consequence of the above result, the inverse of the matrix M in (3) can be given by

$$M^{-1} = D_0^{-1}E_{i_1,j_1}(\mathtt{B}_1)\cdots D_{l-1}^{-1}E_{i_l,j_l}(\mathtt{B}_l)D_l^{-1}P^{-1}. \tag{4}$$

Also, the transpose of the matrix M in (3) can be given by

$$M^T = D_0^TE_{j_1,i_1}(\mathtt{B}_1^T)\cdots D_{l-1}^TE_{j_l,i_l}(\mathtt{B}_l^T)D_l^TP^T. \tag{5}$$

We can use the following result to move the Type II matrices to the left/right in a given decomposition.

Lemma 7. *Let* $\mathtt{A} \in GL(n, \mathbb{F}_2)$ *and* $\mathtt{B} \in \mathcal{M}_n$*. Then, the multiplication of Type II and Type III elementary block matrices satisfies the following.*

$$E_k(\mathtt{A})E_{i,j}(\mathtt{B}) = \begin{cases} E_{i,j}(\mathtt{B})E_k(\mathtt{A}), & k \neq i, j; \\ E_{i,j}(\mathtt{AB})E_k(\mathtt{A}), & k = i; \\ E_{i,j}(\mathtt{BA}^{-1})E_k(\mathtt{A}), & k = j. \end{cases} \tag{6}$$

Remark 3. Note that, given a decomposition as in (3), in reordering (moving to the left/right) the diagonal matrices, the coefficients of the Type III matrices are modified appropriately, but there is no change in the row/column indices of the Type III elementary block matrices.

As a consequence of the above lemma, we get the following result.

Lemma 8. *[WLTZ21, Proposition 2](Split elementary form) Any non-singular block matrix* $M \in \mathcal{M}(n, m)$ *can be decomposed as a product of a block permutation matrix, a block diagonal matrix and elementary block matrices of Type III with non-singular coefficient matrices. Specifically,*

$$M = PDE_{i_l,j_l}(\mathtt{B}'_l) \cdots E_{i_1,j_1}(\mathtt{B}'_1), \tag{7}$$

where $P \in \mathcal{P}(n, m)$*,* $D \in \mathcal{D}(n, m)$ *and* $E_{i_t,j_t}(\mathtt{B}'_t)$ *is an elementary block matrix of Type III with* $\mathtt{B}'_t \in GL(n, \mathbb{F}_2)$ *for* $1 \leq t \leq l$*.*

2.3 MDS Matrices and the Cost of their Hardware Implementation

In early studies, mainly MDS matrices over a finite field $\mathbb{F}_q$ were considered. In hardware implementation, one has to implement field element multiplication considering its corresponding binary matrix by choosing a basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. As a generalization and also hoping to get efficient matrices, many of the later works considered block matrices.

Definition 2. An $m \times m$ block matrix $M \in \mathcal{M}(n, m)$ is MDS if and only if all its square block submatrices are non-singular.

Given an MDS block matrix, the following transformations preserve the MDS property.

Fact 2.1. *Let* $M \in \mathcal{M}(n, m)$*,* $P_1, P_2 \in \mathcal{P}(n, m)$ *and* $D_1, D_2 \in \mathcal{D}(n, m)$*. If* M *is MDS then* M^{-1}*,* M^T*,* P_1MP_2 *and* D_1MD_2 *are also MDS.*

The hardware cost or simply cost of any binary matrix is the number of (2-input) XOR gates required in its implementation. There are mainly three metrics introduced in the literature to estimate the hardware cost of a binary matrix: Direct XOR count (d-XOR), Sequential XOR count(s-XOR) and generalized XOR or slp-XOR count (g-XOR).

Definition 3. [KPPY14] [Direct XOR count (d-XOR)] Let $M \in \mathcal{M}_n$ be a matrix over $\mathbb{F}_2$ of order n. The Hamming weight of M, denoted by $\omega_H(M)$, is the number of 1's in the matrix M. The direct XOR count or d-XOR of M, denoted by $\mathcal{C}_d(M)$, is $\omega_H(M) - n$.

Definition 4. [JPST17] [Sequential XOR count (s-XOR)] Given a non-singular matrix $M \in GL(n, \mathbb{F}_2)$ of order n over $\mathbb{F}_2$, the sequential XOR count or s-XOR of M, denoted by $\mathcal{C}_s(M)$, is the smallest integer t such that the matrix M can be decomposed as

$$M = P \prod_{k=1}^{t} C_k,$$

where P is a permutation matrix over $\mathbb{F}_2$ and C_k is an elementary matrix of Type III over $\mathbb{F}_2$ for $1 \leq k \leq t$.

Given an input vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, $M\mathbf{x}$ can be obtained by iteratively computing $\mathbf{x}_k = C_k\mathbf{x}_{k-1}$ and finally $P\mathbf{x}_t$, where $\mathbf{x}_0 = \mathbf{x}$. Since C_k is an elementary matrix of Type III over $\mathbb{F}_2$, we can interpret $C_k\mathbf{x}$ as $x_i \leftarrow x_i \oplus x_j$ for some i, j such that $1 \leq i \neq j \leq n$. This can be viewed as an in-place replacement operation. So the sequential xor count is the number of bit-wise XORs in a sequential program limited to in-place operations without extra registers. Then the generalized XOR count is proposed by allowing additional registers (to trade-off some XOR operations). This is linked with a Shortest Linear straight-line Program (SLP). For this reason, the generalized XOR count is often called slp XOR count (see also [BMP08, KLSW17])

Definition 5. [XZL$^+$20] [Generalized XOR count (g-XOR)] Let $M \in \mathcal{M}_n$ be a matrix over $\mathbb{F}_2$ of order n and $\mathbf{x} = (x_1, \ldots, x_n)$ be an input vector over $\mathbb{F}_2$. Each element of $M\mathbf{x}$ is a linear expression on the n inputs $x_1, \ldots, x_n$, and so it can be obtained by a sequence of XOR operations. If required, new variables can also be added by considering $x_k = x_i \oplus x_j$ for $1 \leq i, j < k$ and $k = n+1, \ldots, n+t$. The n outputs (entries of $M\mathbf{x}$) are a subset of x_i's. The generalized XOR count or g-XOR of M, denoted by $\mathcal{C}_g(M)$, is defined as the minimum number of XOR operations required to completely compute the n outputs.

One can define d-XOR or g-XOR for rectangular binary matrices in a similar manner, where as the s-XOR is defined only for non-singular binary matrices. Also, observe that the d-XOR or the s-XOR of a matrix is always greater than or equal to its g-XOR. But the additional registers used to store the intermediate values in g-XOR is not accounted for in the comparison.

Now we present some transformations of an MDS matrix which preserve XOR costs. These can easily be seen from the above definitions (see also [BKL16, Lemma 1]).

Proposition 1. *Let $M \in GL(n, \mathbb{F}_2)$ and $P, Q \in \mathcal{P}_n$. Then*

$$(i)\ \mathcal{C}_d(M) = \mathcal{C}_d(PMQ); \quad (ii)\ \mathcal{C}_s(M) = \mathcal{C}_s(PMQ); \quad (iii)\ \mathcal{C}_g(M) = \mathcal{C}_g(PMQ).$$

As mentioned earlier any non-singular binary matrix $M \in GL(n, \mathbb{F}_2)$ can be decomposed as a product of elementary matrices over $\mathbb{F}_2$. Then similar to the identities (4) and (5), given a decomposition of M, one can get decompositions of M^{-1} and M^T and they consist of the same number of Type III elementary matrices as the given one. Therefore we get the following result (see also [BKL16, Corollary 1]).

Proposition 2. *Let $M \in GL(n, \mathbb{F}_2)$. Then*

$$\mathcal{C}_s(M) = \mathcal{C}_s(M^{-1}) = \mathcal{C}_s(M^T).$$

In general, the matrices M and M^T are not permutation equivalent, but as discussed above, their s-XOR costs are equal, i.e., $\mathcal{C}_s(M) = \mathcal{C}_s(M^T)$. This answers the question posed in [YZW21, Section 6].

2.4 Sequential XOR Count Based on Words

Recently, considering matrix decomposition as a product of elementary block matrices, a new XOR count metric called sequential XOR count based on words was proposed in [WLTZ21]. Let $M \in \mathcal{M}(n, m)$ be a non-singular block matrix of order m over $\mathcal{M}_n$. By Lemma 1, the matrix M can be decomposed as a product of elementary block matrices Type I, Type II and Type III with non-singular coefficient matrices. Suppose that

$$M = \prod_{k=1}^{t} G_k,$$

where G_k is an elementary block matrix for $1 \leq k \leq t$. As discussed in the definition of s-XOR, the matrix M can be implemented by iteratively applying G_k on the input vector for $1 \leq k \leq t$. In this way, the sequential XOR count based on words (sw-XOR) is defined as the sum of s-XOR costs of the elementary block matrices in a decomposition of the matrix M which gives the minimum. Note that we consider elementary block matrix decompositions where the coefficient matrices of Type III elementary block matrices are non-singular only, otherwise the minimum will be the same as the s-XOR cost. With this restriction, we first discuss s-XOR costs of elementary block matrices.

Proposition 3. *[WLTZ21, Proposition 7] Let G be an elementary block matrix in $\mathcal{M}(n, m)$. Then the s-XOR cost of G (considering it as an $mn \times mn$ binary matrix) is as given below.*

1. *If $G = E(i, j)$ is an elementary block matrix of Type I, then $\mathcal{C}_s(G) = 0$;*
2. *If $G = E_i(\mathtt{A})$ is an elementary block matrix of Type II for some $\mathtt{A} \in GL(n, \mathbb{F}_2)$, then $\mathcal{C}_s(G) = \mathcal{C}_s(\mathtt{A})$;*
3. *If $G = E_{i,j}(\mathtt{B})$ is an elementary block matrix of Type III for some $\mathtt{B} \in GL(n, \mathbb{F}_2)$, then*

$$\begin{cases} \mathcal{C}_s(G) = n + \mathcal{C}_s(\mathtt{B}) & \textit{if } \mathcal{C}_s(\mathtt{B}) \textit{ is either } 0 \textit{ or } 1; \\ n + 1 \leq \mathcal{C}_s(G) \leq \omega_H(\mathtt{B}) & \textit{otherwise.} \end{cases} \tag{8}$$

Remark 4. Clearly, for any block permutation matrix $P \in \mathcal{P}(n, m)$, we have $\mathcal{C}_s(P) = 0$. By the above proposition, it is clear that the s-XOR cost of a Type II elementary block matrix depends only on the coefficient. Also, the s-XOR of a block diagonal matrix $D = Diag(\mathtt{A}_1, \ldots, \mathtt{A}_m) \in \mathcal{D}(n, m)$ is given by $\mathcal{C}_s(D) = \sum_{k=1}^{m} \mathcal{C}_s(\mathtt{A}_k)$. By Corollary 1, we can see that there exists a permutation matrix $P \in \mathcal{P}(n, m)$ such that $E_{i',j'}(\mathtt{B}) = PE_{i,j}(\mathtt{B})P^{-1}$ for two Type III matrices $E_{i,j}(\mathtt{B}), E_{i',j'}(\mathtt{B})$ in $\mathcal{M}(n, m)$. So by Proposition 1, the s-XOR of both the Type III matrices must be the same. Therefore the s-XOR cost of an elementary block matrix depends only on the coefficient but not on the indices.

By the above proposition we have

$$n \leq \mathcal{C}_s(E_{i,j}(\mathtt{B})) \leq \omega_H(\mathtt{B}) = n + \mathcal{C}_d(\mathtt{B}), \tag{9}$$

where $\mathtt{B} \in GL(n, \mathbb{F}_2)$.

Definition 6 (Sequential XOR count based on words)**.** Let $M \in \mathcal{M}(n, m)$ be a non-singular block matrix of order m over $\mathcal{M}_n$. The sequential XOR count based on words or sw-XOR of M, denoted by $\mathcal{C}_{sw}(M)$, is given by

$$\mathcal{C}_{sw}(M) = \min \ \{\sum_{k=1}^{t} \mathcal{C}_s(G_k) : M = \prod_{k=1}^{t} G_k\},$$

where the coefficient matrices of Type III elementary block matrices are non-singular.

Since the s-XOR of Type I elementary block matrices is 0, for any decomposition of the matrix M, the contribution of such matrices is 0 in the sum above. As noted in Remark 4, the s-XOR of Type II or Type III matrices does not depend on the indices. Then by the discussion leading to Lemma 4, we can also express the sw-XOR of a block matrix $M \in \mathcal{M}(n, m)$ as follows:

$$\mathcal{C}_{sw}(M) = \min \ \{\sum_{k=1}^{t'} \mathcal{C}_s(G'_k) : M = P \prod_{k=1}^{t'} G'_k\},$$

where G'_k, $1 \leq k \leq t'$, is an elementary block matrix of either Type II or Type III with non-singular coefficient matrix. So it is the minimum over all the decompositions of the block matrix M of the form given in (2). It may be possible to get a better estimate of the XOR cost of the matrix M by replacing $\mathcal{C}_s(G'_k)$ with $\mathcal{C}_g(G'_k)$ in the above sum. Observe that $\mathcal{C}_s(E_i(\mathtt{P})) = \mathcal{C}_s(\mathtt{P}) = 0$ for $\mathtt{P} \in \mathcal{P}_n$. Therefore we get the following result.

Corollary 2. *Let $P \in \mathcal{P}(n,m)$ and $D \in \mathcal{D}(n,m)$ be a block diagonal matrix such that the diagonal blocks are permutation matrices in $\mathcal{P}_n$. Then $\mathcal{C}_{sw}(P) = \mathcal{C}_{sw}(D) = \mathcal{C}_{sw}(PD) = 0$.*

We now present some transformations of a block matrix which preserve sw-XOR cost similar to Propositions 1 and 2.

Proposition 4. *Let $M \in \mathcal{M}(n,m)$ be a non-singular block matrix. Let $P_1, P_2 \in \mathcal{P}(n,m)$ and $D_1, D_2 \in \mathcal{D}(n,m)$ be block diagonal matrices such that the diagonal blocks of D_1, D_2 are permutation matrices in $\mathcal{P}_n$. Then $\mathcal{C}_{sw}(M) = \mathcal{C}_{sw}(P_1MP_2) = \mathcal{C}_{sw}(D_1MD_2)$.*

Proposition 5. *Let $M \in \mathcal{M}(n,m)$ be a non-singular block matrix. Then*

$$\mathcal{C}_{sw}(M) = \mathcal{C}_{sw}(M^{-1}) = \mathcal{C}_{sw}(M^T).$$

As mentioned in Proposition 8, a non-singular block matrix can be decomposed as a product of a block permutation matrix, a block diagonal matrix and elementary block matrices of Type III with non-singular coefficient matrices. Considering the part of a decomposition which consists of only elementary block matrices of Type III with non-singular coefficient matrices, the authors in [WLTZ21] introduced the concept of a path. Using this, the authors established that any 4×4 matrix with a path consisting of less than 8 Type III matrices cannot be MDS. By symbolic computation, they analyze paths of length 8 to identify potential paths that can generate MDS matrices. They first analyzed paths considering matrices over finite fields. It was shown that there cannot be an MDS matrix of order 4 over a finite field $\mathbb{F}_{2^n}$ with sw-XOR cost less than $8n+3$. In the case of finite fields, they have also shown that the lower bound is tight by exhibiting matrices for $n = 4$ and 8. Then they analyzed paths considering the block matrices over $GL(n, \mathbb{F}_2)$. As the search space is huge, they could not verify this case even for $n = 4$. The authors also made some initial observations on the equivalence of paths. In the next section, we formalize the notion of equivalence of paths in a broader sense. Using this notion, we form (extended) equivalence classes. The main advantage of our approach is that the search for low cost MDS matrices can be restricted to a smaller domain of paths. We also discuss suitable tools to manage the symbolic expressions in a free algebra over $\mathbb{F}_2$. We have also considered the case of 3×3 matrices over $GL(n, \mathbb{F}_2)$. The lower bound on the sw-XOR cost of 3×3 MDS matrices over $GL(n, \mathbb{F}_2)$ is $5n+1$.

3 Settling the Lower Bound of sw-XOR

In this section, we first define a path which is an ordered list of elementary block matrices of Type III (ignoring the coefficients). We say a block matrix belongs to some path if it has a decomposition in which the Type III matrices appear in the same order (from the right) as in the path. We then define an equivalence of paths. We join together a few equivalence classes and define extended equivalence classes (loosely speaking, which preserve MDS property). Next we search for potential paths that generate MDS matrices in the case of 4×4 block matrices. Finally, we show that the lower bound on the sw-XOR cost of MDS matrices in $\mathcal{M}(n, 4)$ is $8n+3$.

Definition 7. A path of length l over $\mathcal{M}(n,m)$ is an ordered list $\mathcal{B} = (E_{i_1,j_1}(\cdot), \ldots, E_{i_l,j_l}(\cdot))$ of l elementary block matrices of Type III ignoring the coefficients. Let $\mathbf{M}_{\mathcal{B}}$ denote the set of matrices that can be generated by a path $\mathcal{B} = (E_{i_1,j_1}(\cdot), \ldots, E_{i_l,j_l}(\cdot))$, and they are given by

$$M = PDE_{i_l,j_l}(\mathtt{B}_l) \cdots E_{i_2,j_2}(\mathtt{B}_2)E_{i_1,j_1}(\mathtt{B}_1)Q, \tag{10}$$

where $P, Q \in \mathcal{P}(n,m)$, $D \in \mathcal{D}(n,m)$ and $\mathtt{B}_k \in \mathcal{M}_n$ for $1 \le k \le l$. For simplicity, we omit $(\cdot)$ and write $\mathcal{B} = (E_{i_1,j_1}, \ldots, E_{i_l,j_l})$. For this reason, the path $\mathcal{B}$ can be viewed as an ordered list of tuples $[(i_1, j_1), (i_2, j_2), \ldots, (i_l, j_l)]$ such that $1 \le i_k \ne j_k \le m$ for $1 \le k \le l$.

From the discussion leading to Lemma 8, considering the other direction, we can see that the matrix $M \in \mathbf{M}_{\mathcal{B}}$ given in (10) can also be expressed as

$$M = PD_lE_{i_l,j_l}(\mathtt{B}'_l)D_{l-1}\cdots D_1E_{i_1,j_1}(\mathtt{B}'_1)D_0Q \in \mathbf{M}_{\mathcal{B}}, \tag{11}$$

for $D_k \in \mathcal{D}(n,m)$, $0 \le k \le l$, such that $D = \prod_{k=0}^{l} D_k$ and suitable $\mathtt{B}'_k \in \mathcal{M}_n$ for $1 \le k \le l$. Note that the matrix decomposition form given in the identity (11) is used to analyze the sw-XOR cost of $M \in \mathbf{M}_{\mathcal{B}}$ considering $\mathtt{B}'_k \in GL(n, \mathbb{F}_2)$. For other purposes, we use the matrix decomposition form given in the identity (10). Note also that for a matrix $M \in \mathbf{M}_{\mathcal{B}}$, the path corresponding to a decomposition of M with optimal sw-XOR implementation may be different from $\mathcal{B}$.

Next we see that there are many paths that generate the same set of matrices. We illustrate these ideas through examples. Let $\mathcal{B} = (E_{i_1,j_1}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$ and suppose that $i_s = i_{s+1}$ and $j_s = j_{s+1}$ for some $1 \le s < l$, i.e., the adjacent pair of s-th and $(s+1)$-th elements of the path $\mathcal{B}$ are the same. Then these two elements can be merged into one by using the identity (1). We can then see by (10) that the path $\mathcal{B}' = (E_{i_1,j_1}, \ldots, E_{i_{s-1},j_{s-1}}, E_{i_{s+1},j_{s+1}}, \ldots, E_{i_l,j_l})$ of length $(l-1)$ also generates the same set of matrices.

Example 1. Let $\mathcal{B}_1 = (E_{2,1}, E_{1,2}, E_{1,2}, E_{3,4}, E_{1,3}, E_{1,2}, E_{2,1})$ be a path of length 7 over $\mathcal{M}(n,4)$. Then by the identity (10), a matrix $M \in \mathbf{M}_{\mathcal{B}_1}$ is of the form

$$M = PDE_{2,1}(\mathtt{B}_7)E_{1,2}(\mathtt{B}_6)E_{1,3}(\mathtt{B}_5)E_{3,4}(\mathtt{B}_4)E_{1,2}(\mathtt{B}_3)E_{1,2}(\mathtt{B}_2)E_{2,1}(\mathtt{B}_1)Q,$$

where $P, Q \in \mathcal{P}(n,4)$, $D \in \mathcal{D}(n,4)$ and $\mathtt{B}_t \in \mathcal{M}_n$ for $1 \le t \le 7$. By the identity (1), we have $E_{1,2}(\mathtt{B}_3)E_{1,2}(\mathtt{B}_2) = E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2)$. So we get

$$M = PDE_{2,1}(\mathtt{B}_7)E_{1,2}(\mathtt{B}_6)E_{1,3}(\mathtt{B}_5)E_{3,4}(\mathtt{B}_4)E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2)E_{2,1}(\mathtt{B}_1)Q.$$

Let $\mathcal{B}_2 = (E_{2,1}, E_{1,2}, E_{3,4}, E_{1,3}, E_{1,2}, E_{2,1})$ be the path of length 6 obtained by removing the second element from $\mathcal{B}_1$. Clearly, we can see that if $M \in \mathbf{M}_{\mathcal{B}_1}$ then $M \in \mathbf{M}_{\mathcal{B}_2}$ and vice versa.

It is easy to see the following result on the commutativity of elementary block matrices of Type III. The proof is given in Appendix B.

Lemma 9. *Let $\mathtt{B}, \mathtt{B}' \in \mathcal{M}_n$. We have $E_{i,j}(\mathtt{B})E_{i',j'}(\mathtt{B}') = E_{i',j'}(\mathtt{B}')E_{i,j}(\mathtt{B})$ if $i \ne j'$ and $j \ne i'$ holds true.*

Let $\mathcal{B} = (E_{i_1,j_1}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$ and suppose that $i_s \ne j_{s+1}$ and $j_s \ne i_{s+1}$ for some $1 \le s < l$, i.e., the adjacent pair of s-th and $(s+1)$-th elements of the path $\mathcal{B}$ commute. Then by Definition 7 we can see that the path $\hat{\mathcal{B}} = (E_{i_1,j_1}, \ldots, E_{i_{s-1},j_{s-1}}, E_{i_{s+1},j_{s+1}}, E_{i_s,j_s}, E_{i_{s+2},j_{s+2}}, \ldots, E_{i_l,j_l})$ obtained by altering the order of that adjacent pair in $\mathcal{B}$ also generates the same set of matrices. We call such an exchange of elements in the path $\mathcal{B}$ a *valid exchange* on the path $\mathcal{B}$.

Example 2. Let us consider the path $\mathcal{B}_2$ given in Example 1. By Lemma 9, we have $E_{3,4}(\mathtt{B}_4)E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2) = E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2)E_{3,4}(\mathtt{B}_4)$. So we get

$$M = PDE_{2,1}(\mathtt{B}_7)E_{1,2}(\mathtt{B}_6)E_{1,3}(\mathtt{B}_5)E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2)E_{3,4}(\mathtt{B}_4)E_{2,1}(\mathtt{B}_1)Q.$$

Let $\mathcal{B}_3 = (E_{2,1}, E_{3,4}, E_{1,2}, E_{1,3}, E_{1,2}, E_{2,1})$ be the path of length 6 obtained by reordering the second and third elements of $\mathcal{B}_2$. Clearly, we can see that if $M \in \mathbf{M}_{\mathcal{B}_2}$ then $M \in \mathbf{M}_{\mathcal{B}_3}$ and vice versa.

There can be several adjacent pairs of elements in a path $\mathcal{B}$ where the elements in each pair commute with each other. Thus there can be many valid exchanges possible on a path. Also, after applying a valid exchange on a path $\mathcal{B}$, this in turn can give rise to a new valid exchange(s) on the path obtained. So one can iteratively apply a sequence of valid exchanges on a path $\mathcal{B}$, and the paths obtained after each iteration/valid exchange generate the same set of matrices as the path $\mathcal{B}$ generates. It may happen that, after a sequence of valid exchanges, the same element appears at adjacent positions. In that case, these two positions can be merged as discussed earlier. Thus we get the following result.

Proposition 6. *Let $\mathcal{B} = (E_{i_1,j_1}, \dots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$. Suppose that $i_s = i_t$ and $j_s = j_t$ for some $1 \le s < t \le l$. Also, suppose that $i_k \neq j_s$ and $j_k \neq i_s$ for all k, $s < k < t$. Then the path $\mathcal{B}' = (E_{i_1,j_1}, \dots, E_{i_{s-1},j_{s-1}}, E_{i_{s+1},j_{s+1}}, \dots, E_{i_l,j_l})$ generates the same set of matrices as the path $\mathcal{B}$ generates, and it is of length $(l-1)$. Similarly, a path $\mathcal{B}''$ obtained by placing E_{i_t,j_t} at any position from s-th to $(t-1)$-th positions and without changing the order of the other elements in $\mathcal{B}'$ also generates the same set of matrices.*

Proof. We have $i_s = i_t$ and $j_s = j_t$. Also, by Lemma 9, we have $E_{i_s,j_s}(\mathtt{B})E_{i_k,j_k}(\mathtt{B}') = E_{i_k,j_k}(\mathtt{B}')E_{i_s,j_s}(\mathtt{B})$ for any $\mathtt{B}, \mathtt{B}' \in \mathcal{M}_n$ and $s < k < t$. Therefore, E_{i_s,j_s} can be moved right by a sequence of valid exchanges and similarly E_{i_s,j_s} can be moved left. From the above discussion, E_{i_s,j_s} and E_{i_t,j_t} can be merged since they are the same. Hence the result. □

If the path $\mathcal{B}$ of length l satisfies the condition given in the above proposition, then we get a path $\mathcal{B}'$ of length $(l-1)$ and it also generates the same set of matrices. In such a case, we say that the path $\mathcal{B}$ can be *shortened*, and the shortened paths also generate the set of matrices.

Example 3. Let us consider the path $\mathcal{B}_3$ given in Example 2. By Lemma 9, we have $E_{1,2}(\mathtt{B}_6)E_{1,3}(\mathtt{B}_5) = E_{1,3}(\mathtt{B}_5)E_{1,2}(\mathtt{B}_6)$. Also $E_{1,2}(\mathtt{B}_6)E_{1,2}(\mathtt{B}_3 + \mathtt{B}_2) = E_{1,2}(\mathtt{B}_6 + \mathtt{B}_3 + \mathtt{B}_2)$. So we get

$$M = PDE_{2,1}(\mathtt{B}_7)E_{1,3}(\mathtt{B}_5)E_{1,2}(\mathtt{B}_6 + \mathtt{B}_3 + \mathtt{B}_2)E_{3,4}(\mathtt{B}_4)E_{2,1}(\mathtt{B}_1)Q.$$

Let $\mathcal{B}_4 = (E_{2,1}, E_{3,4}, E_{1,2}, E_{1,3}, E_{2,1})$ be the path of length 5 obtained by shortening $\mathcal{B}_3$. Clearly, we can see that if $M \in \mathbf{M}_{\mathcal{B}_3}$ then $M \in \mathbf{M}_{\mathcal{B}_4}$ and vice versa. Moreover, based on the commutativity of Type III matrices as stated in Lemma 9, we can also see that the following four paths can be obtained by iteratively applying valid exchanges on $\mathcal{B}_4$, and they also generate the same set of matrices as the path $\mathcal{B}_4$ generates.

$$\mathcal{B}_5 = (E_{3,4}, E_{2,1}, E_{1,2}, E_{1,3}, E_{2,1}) \qquad \mathcal{B}_6 = (E_{2,1}, E_{1,2}, E_{3,4}, E_{1,3}, E_{2,1})$$
$$\mathcal{B}_7 = (E_{2,1}, E_{3,4}, E_{1,3}, E_{1,2}, E_{2,1}) \qquad \mathcal{B}_8 = (E_{3,4}, E_{2,1}, E_{1,3}, E_{1,2}, E_{2,1})$$

Next we extend the action of the group of block permutation matrices $\mathcal{P}(n,m)$ on the set of elementary block matrices of Type III (see Remark 1) to the set of paths of length l over $\mathcal{M}(n,m)$. In this way, we can get some more paths which generate the same set of matrices. Let $\mathcal{B} = (E_{i_1,j_1}, \dots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$. Let $P_\sigma \in \mathcal{P}(n,m)$ be a block permutation matrix corresponding to a permutation σ over $\{1, 2, \dots, m\}$. Then by Corollary 1 we have $E_{\sigma(i_t),\sigma(j_t)}(\mathtt{B}) = P_\sigma E_{i_t,j_t}(\mathtt{B})P_\sigma^{-1}$ for $1 \le t \le l$. Now consider

$$\mathcal{B}_\sigma = P_\sigma \mathcal{B} P_\sigma^{-1} = (E_{\sigma(i_1),\sigma(j_1)}, \dots, E_{\sigma(i_l),\sigma(j_l)}).$$

It is easy to verify that $\mathcal{P}(n,m)$ acts by conjugation on the set of paths of length l. We say that the path $\mathcal{B}_\sigma$ is a *conjugate* of the path $\mathcal{B}$. Then by the identity (10) and Corollary 1, we can see that the path $\mathcal{B}_\sigma$ also generates the same set of matrices as the path $\mathcal{B}$ generates.

Example 4. Let us consider the paths $\mathcal{B}_t$, $4 \le t \le 8$, of length 5 over $\mathcal{M}(n,4)$ mentioned in Example 3. Any conjugate of the path $\mathcal{B}_t$ also generates the same set of matrices as the path $\mathcal{B}_t$ generates. Observe that there are $4! = 24$ conjugates for each path $\mathcal{B}_t$, and any such path generates the same set of matrices. In this way, we see that there are 120 distinct paths which are of length 5 and generate the same set of matrices as the path $\mathcal{B}_4$ generates.

Let $R \in \mathcal{P}(n,m)$. Observe that if two Type III elementary block matrices $E_{i,j}(\mathtt{B})$ and $E_{i',j'}(\mathtt{B}')$ commute then their conjugates $RE_{i,j}(\mathtt{B})R^{-1}$ and $RE_{i',j'}(\mathtt{B}')R^{-1}$ also commute. If $\hat{\mathcal{B}}$ is the path obtained by applying a valid exchange on a path $\mathcal{B}$. Then the conjugate $R\hat{\mathcal{B}}R^{-1}$ of $\hat{\mathcal{B}}$ is the same as the path obtained by applying the corresponding valid exchange on the conjugate path $R\mathcal{B}R^{-1}$ of $\mathcal{B}$. In other words, these two transformations can be applied on a path in any order. Based on the discussion above, next we define an equivalence of two paths.

Definition 8. Suppose that $\mathcal{B}$ and $\mathcal{B}'$ are two paths of the same length over $\mathcal{M}(n,m)$. Then the path $\mathcal{B}$ is said to be equivalent to the path $\mathcal{B}'$ if it is a conjugate of a path obtained by iteratively applying valid exchanges (altering the order of an adjacent and commuting pair of elements) on the path $\mathcal{B}'$.

Remark 5. Consider the path $\mathcal{B}_4 = (E_{2,1}, E_{3,4}, E_{1,2}, E_{1,3}, E_{2,1})$ given in Example 3. As discussed in Example 4, there are 120 paths in the equivalence class of $\mathcal{B}_4$. Note that though $\mathbf{M}_{\mathcal{B}_i} = \mathbf{M}_{\mathcal{B}_4}$ for $i = 1,2,3$ as discussed in Examples 1-3, but they are not equivalent to $\mathcal{B}_4$ as the lengths are different.

Remark 6. Suppose that the paths $\mathcal{B}$ and $\mathcal{B}'$ are equivalent. From the discussion prior to Definition 8, we can see that if $\mathcal{B}$ can be shortened by applying Proposition 6, then the path $\mathcal{B}'$ can also be shortened accordingly.

Based on the discussion in this section, we can get the following result.

Theorem 1. *Let $\mathcal{B}$ and $\mathcal{B}'$ be two paths of the same length over $\mathcal{M}(n,m)$. If $\mathcal{B}$ is equivalent to $\mathcal{B}'$ then $\mathbf{M}_{\mathcal{B}} = \mathbf{M}_{\mathcal{B}'}$.*

We denote the set of all paths in the equivalence class of a path $\mathcal{B}$ over $\mathcal{M}(n,m)$ by $\mathbf{EC}_{\mathcal{B}}$. Now, we present an algorithm to generate $\mathbf{EC}_{\mathcal{B}}$ given a path $\mathcal{B}$ of length l over $\mathcal{M}(n,m)$.

Algorithm 1 Generating Paths in an Equivalence Class

```
Input : A path $\mathcal{B}$ of length $l$ over $\mathcal{M}(n,m)$
Output : The set of all paths in the equivalence class $\mathbf{EC}_{\mathcal{B}}$ of $\mathcal{B}$
Generate all possible paths by applying valid exchanges on the path $\mathcal{B}$; Iteratively apply this process on the paths obtained until no new path can be obtained; Let $\mathbf{E}$ be set of all such paths.
$\mathbf{EC}_{\mathcal{B}} = \{R\mathcal{B}'R^{-1} : \mathcal{B}' \in \mathbf{E}, R \in \mathcal{P}(n,m)\}$.
```

By Fact 2.1, if $M \in \mathcal{M}(n,m)$ is MDS then M^{-1}, M^T and $(M^{-1})^T$ are also MDS. Next we see paths that generate either M^{-1} or M^T or $(M^{-1})^T$ if $M \in \mathbf{M}_{\mathcal{B}}$ for some path $\mathcal{B} = (E_{i_1,j_1}, E_{i_2,j_2}, \ldots, E_{i_l,j_l})$ of length l over $\mathcal{M}(n,m)$. We define

$$Rev(\mathcal{B}) = (E_{i_l,j_l}, \ldots, E_{i_2,j_2}, E_{i_1,j_1})$$

as the path obtained by reversing the order of the elements in $\mathcal{B}$. Similarly, we define

$$Irc(\mathcal{B}) = (E_{j_1,i_1}, E_{j_2,i_2}, \ldots, E_{j_l,i_l})$$

as the path obtained by interchanging the row and column indices of the elements in $\mathcal{B}$ (without changing the order of the elements in $\mathcal{B}$). From the discussion above and Definition 8, we have the following observations.

1. $\mathcal{B}' \in \mathbf{EC}_{\mathcal{B}}$ if and only if $Rev(\mathcal{B}') \in \mathbf{EC}_{Rev(\mathcal{B})}$;
2. $\mathcal{B}' \in \mathbf{EC}_{\mathcal{B}}$ if and only if $Irc(\mathcal{B}') \in \mathbf{EC}_{Irc(\mathcal{B})}$;
3. $Irc(Rev(\mathcal{B})) = Rev(Irc(\mathcal{B})) = (E_{j_l,i_l}, \ldots, E_{j_2,i_2}, E_{j_1,i_1})$.

According to the identity (10), a matrix $M \in \mathbf{M}_{\mathcal{B}}$ generated by the path $\mathcal{B}$ is of the form

$$M = PDE_{i_l,j_l}(\mathtt{B}_l) \cdots E_{i_1,j_1}(\mathtt{B}_1)Q,$$

where $P, Q \in \mathcal{P}(n,m),\ D \in \mathcal{D}(n,m)$ and $\mathtt{B}_t \in \mathcal{M}_n$ for $1 \le t \le l$. Then we have

1. $M^{-1} = Q^{-1}E_{i_1,j_1}(\mathtt{B}_1) \cdots E_{i_l,j_l}(\mathtt{B}_l)D^{-1}P^{-1}$;
2. $M^T = Q^T E_{j_1,i_1}(\mathtt{B}_1^T) \cdots E_{j_l,i_l}(\mathtt{B}_l^T)D^T P^T$;
3. $(M^T)^{-1} = P(D^T)^{-1}E_{j_l,i_l}(\mathtt{B}_l^T) \cdots E_{j_1,i_1}(\mathtt{B}_1^T)Q$.

Now one can easily see that

1. $M \in \mathbf{M}_{\mathcal{B}}$ if and only if $M^{-1} \in \mathbf{M}_{Rev(\mathcal{B})}$.
2. $M \in \mathbf{M}_{\mathcal{B}}$ if and only if $M^T \in \mathbf{M}_{Irc(Rev(\mathcal{B}))}$.
3. $M \in \mathbf{M}_{\mathcal{B}}$ if and only if $(M^{-1})^T = (M^T)^{-1} \in \mathbf{M}_{Irc(\mathcal{B})}$.

Consequently, we get the following results.

1. For $\mathcal{B}_1 \in \mathbf{EC}_{\mathcal{B}}$ and $\mathcal{B}_2 \in \mathbf{EC}_{Rev(\mathcal{B})}$, we have $M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $M^{-1} \in \mathbf{M}_{\mathcal{B}_2}$.
2. For $\mathcal{B}_1 \in \mathbf{EC}_{\mathcal{B}}$ and $\mathcal{B}_2 \in \mathbf{EC}_{Irc(Rev(\mathcal{B}))}$, we have $M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $M^T \in \mathbf{M}_{\mathcal{B}_2}$.
3. For $\mathcal{B}_1 \in \mathbf{EC}_{\mathcal{B}}$ and $\mathcal{B}_2 \in \mathbf{EC}_{Irc(\mathcal{B})}$, we have $M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $(M^{-1})^T \in \mathbf{M}_{\mathcal{B}_2}$.

Now we extend the equivalence class of $\mathcal{B}$ by joining together the equivalence classes of $\mathcal{B}$, $Rev(\mathcal{B})$, $Irc(\mathcal{B})$ and $Rev(Irc(\mathcal{B}))$.

Definition 9. Let $\mathcal{B} = (E_{i_1,j_1}, E_{i_2,j_2}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$. Then the extended equivalence class containing the path $\mathcal{B}$ is given by

$$\mathbf{EEC}_{\mathcal{B}} = \mathbf{EC}_{\mathcal{B}} \cup \mathbf{EC}_{Rev(\mathcal{B})} \cup \mathbf{EC}_{Irc(\mathcal{B})} \cup \mathbf{EC}_{Rev(Irc(\mathcal{B}))}.$$

From the discussion above, we get the following result.

Theorem 2. *Let $\mathcal{B} = (E_{i_1,j_1}, E_{i_2,j_2}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$. If $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{EEC}_{\mathcal{B}}$ then at least one of the following is true.*

1. *$M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $M \in \mathbf{M}_{\mathcal{B}_2}$.*
2. *$M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $M^{-1} \in \mathbf{M}_{\mathcal{B}_2}$.*
3. *$M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $M^T \in \mathbf{M}_{\mathcal{B}_2}$.*
4. *$M \in \mathbf{M}_{\mathcal{B}_1}$ if and only if $(M^T)^{-1} \in \mathbf{M}_{\mathcal{B}_2}$.*

Now observe that if $M \in \mathbf{M}_{\mathcal{B}_1}$ is MDS then M, M^T and $(M^T)^{-1}$ are also MDS by Fact 2.1. Moreover, by Proposition 5, we have

$$\mathcal{C}_{sw}(M) = \mathcal{C}_{sw}(M^{-1}) = \mathcal{C}_{sw}(M^T) = \mathcal{C}_{sw}((M^T)^{-1}).$$

Therefore we get the following result.

Theorem 3. *Let $\mathcal{B} = (E_{i_1,j_1}, E_{i_2,j_2}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n,m)$. Let $\mathcal{B}_1, \mathcal{B}_2 \in \mathbf{EEC}_{\mathcal{B}}$ be two paths in the extended equivalence class of $\mathcal{B}$. If $M_1 \in \mathbf{M}_{\mathcal{B}_1}$ is MDS then there exists an MDS matrix $M_2 \in \mathbf{M}_{\mathcal{B}_2}$ such that $\mathcal{C}_{sw}(M_1) = \mathcal{C}_{sw}(M_2)$*

By using the tools developed above, next we show that the lower bound on the *sw*-XOR of 4×4 block matrices over $\mathcal{M}_n$ is $8n + 3$.

3.1 The case of 4×4 block matrices

We consider the case of $m = 4$, i.e., the ring $\mathcal{M}(n, 4)$ of 4×4 block matrices over $\mathcal{M}_n$. It has been shown in [WLTZ21, Section 5] that if a path over $\mathcal{M}(n, 4)$ can generate an MDS matrix then its length must be at least 8. They have also shown that the lower bound on the sw-XOR cost of 4×4 matrices over a finite field $\mathbb{F}_q$ (i.e, $\mathcal{M}(4, \mathbb{F}_q)$) is $8n + 3$, and they have established that this bound is tight by exhibiting matrices for $n = 4, 8$. But it is not known whether the same is true for the case of block matrices in $\mathcal{M}(n, 4)$. Based on the ideas discussed above, we below establish that the lower bound on sw-XOR cost is in fact $8n + 3$ even for block matrices in $\mathcal{M}(n, 4)$ and show that there does not exist an MDS matrix in $\mathcal{M}(n, 4)$ with sw-XOR cost equal to $8n + 2$. We first present some useful results. The following result can be used to verify the non-singularity of 2×2 block submatrices.

Proposition 7. *[Mey00, p. 475] Let $S = (\mathtt{S}_{ij})$ be a 2×2 block matrix such that the block entries $\mathtt{S}_{ij}$ are non-singular. Then S is non-singular if and only if the matrices $\mathtt{S}_{22} + \mathtt{S}_{21}\mathtt{S}_{11}^{-1}\mathtt{S}_{12}$, $\mathtt{S}_{11} + \mathtt{S}_{12}\mathtt{S}_{22}^{-1}\mathtt{S}_{21}$, $\mathtt{S}_{12} + \mathtt{S}_{11}\mathtt{S}_{21}^{-1}\mathtt{S}_{22}$ and $\mathtt{S}_{21} + \mathtt{S}_{22}\mathtt{S}_{12}^{-1}\mathtt{S}_{11}$ are non-singular.*

We first present a method to search for potential paths that can generate (low cost) MDS matrices. In fact, we will show that for the case of $m = 4$, it is enough to consider two paths to perform the cost analysis to establish the lower bound.

Let $\mathcal{B} = (E_{i_1,j_1}, E_{i_2,j_2}, \ldots, E_{i_l,j_l})$ be a path of length l over $\mathcal{M}(n, m)$. A matrix $M \in \mathbf{M}_{\mathcal{B}}$ generated by the path $\mathcal{B}$ is given by

$$M = PDE_{i_l,j_l}(\mathtt{B}_l) \cdots E_{i_1,j_1}(\mathtt{B}_1)Q,$$

where $P, Q \in \mathcal{P}(n, m)$, $D \in \mathcal{D}(n, m)$ and $\mathtt{B}_t \in \mathcal{M}_n$ for $1 \leq t \leq l$. Then by Fact 2.1 we can see that if M is MDS then $M' = E_{i_l,j_l}(\mathtt{B}_l) \cdots E_{i_1,j_1}(\mathtt{B}_1)$ is also MDS. Also observe that $M' \in \mathbf{M}_{\mathcal{B}}$ and it is a product of only Type III elementary block matrices of $\mathcal{B}$. So we have the following result.

Proposition 8. *If a path $\mathcal{B} = (E_{i_1,j_1}, \ldots, E_{i_l,j_l})$ can generate MDS matrices then there exist $\mathtt{B}_1, \mathtt{B}_2, \ldots, \mathtt{B}_l \in \mathcal{M}_n$ such that the matrix $M = E_{i_l,j_l}(\mathtt{B}_l) \cdots E_{i_2,j_2}(\mathtt{B}_2)E_{i_1,j_1}(\mathtt{B}_1)$ is MDS.*

If a path $\mathcal{B}$ can generate MDS matrices then by Definition 9 and Theorem 2 we can see that each path in the extended equivalence class of $\mathcal{B}$ can generate MDS matrices. So it is enough to verify one path (a representative path) in each extended equivalence class whether it can generate MDS matrices. In fact, we can see by Proposition 8 that it is enough to verify matrices which are products of only elementary block matrices of Type III generated by the representative paths.

As shown in [WLTZ21, Section 5], the length of a path over $\mathcal{M}(n, 4)$ must be at least 8 if it can generate MDS matrices. Note also that it is true even with singular coefficient matrices for Type III elementary block matrices, though they have only considered non-singular coefficient matrices. By using the ideas presented above, we were also able to verify quickly that the same is true. Suppose $M \in \mathcal{M}(n, 4)$ is MDS and it is not generated by a path of length 8. That means the length of the shortest path that can generate M is at least 9. So the sw-XOR cost of M is greater than $9n$. For $n \geq 3$, we have $9n \geq 8n + 3$. Therefore it is enough to consider paths of length 8 to find potential paths that can generate MDS matrices with sw-XOR cost less than $8n + 3$. As there are 12 different elementary block matrices of Type III over $\mathcal{M}(n, 4)$ (ignoring the coefficients), we can form 12^8 different paths of length 8 over $\mathcal{M}(n, 4)$. To find potential paths, we follow an elimination process, and it can be divided into several steps as described in Algorithm 2. First, note that a path of length 8 cannot generate MDS matrices if it can be shortened by applying Proposition 6. So we can eliminate all such paths. Note also that if a path can be shortened, then any path in its extended equivalence class can also be shortened. We then identify a set of representative paths of the extended equivalence classes of paths of length 8 (that cannot be shortened) over $\mathcal{M}(n,4)$. We then find potential paths by symbolically verifying MDS property of the matrices generated by the representative paths considering the form given in Proposition 8.

Algorithm 2 Finding Potential Paths of Length 8 over $\mathcal{M}(n,4)$

```
    Input: Set of all paths of length 8 over $\mathcal{M}(n,4)$
    Output: The set of potential paths of length 8 that can generate MDS matrices
1: From the set of all paths, eliminate all those paths of length 8 that can be shortened
   by applying Proposition 6.
2: Group the remaining paths into extended equivalence classes using Algorithm 1. Let
   $\mathbf{R}$ be a set of representative paths of the extended equivalence classes.
3: For each representative path $\mathcal{B} = (E_{i_1,j_1}, \ldots, E_{i_8,j_8}) \in \mathbf{R}$, by symbolic computation
   (treating the coefficient matrices as variables) we verify the impossibility of generating
   MDS matrices by $\mathcal{B}$.
    (i) Consider
              $M = E_{i_8,j_8}(\mathtt{B}_8) \cdots E_{i_2,j_2}(\mathtt{B}_2) E_{i_1,j_1}(\mathtt{B}_1)$
        and its inverse
              $M^{-1} = E_{i_1,j_1}(\mathtt{B}_1) E_{i_2,j_2}(\mathtt{B}_2) \cdots E_{i_8,j_8}(\mathtt{B}_8).$
        The entries of $M$ and $M^{-1}$ are from the free algebra on 8 indeterminates $\mathtt{B}_1, \ldots, \mathtt{B}_8$
        over $\mathbb{F}_2$ which is a noncommutative ring. After simplifying, if any of the entries of
        $M$ or $M^{-1}$ is zero then that particular block entry will always be the zero matrix
        for any choice of the matrices in $\mathcal{M}_n$ for the variables $\mathtt{B}_1, \mathtt{B}_2, \ldots, \mathtt{B}_8$. In that case,
        the path $\mathcal{B}$ cannot generate MDS matrices. If all the entries of both $M$ and $M^{-1}$
        are nonzero then proceed with testing $2 \times 2$ submatrices of $M$ and $M^{-1}$.
   (ii) For each $2 \times 2$ submatrix of $M$, we verify any of the four expressions as given
        in Proposition 7 is zero or not in the cases where the inverses can be canceled
        out symbolically. Similarly, we verify $2 \times 2$ submatrices of $M^{-1}$. If any of the
        expressions is zero, then for any choice of the matrices in $\mathcal{M}_n$ for the variables
        $\mathtt{B}_1, \mathtt{B}_2, \ldots, \mathtt{B}_8$, the corresponding $2 \times 2$ will be singular, and so the path cannot
        generate MDS matrices.
4: Output the set of all paths that survive the elimination process.
```

We have performed the search using Algorithm 2. We see that out of the $12^8 = 429,981,696$ paths of length 8 over $\mathcal{M}(n,4)$, the number of paths remain after the first step is $147,122,868$. The other paths are eliminated in the first step as they can be shortened. From these $147,122,868$ paths, we can form $121,499$ extended equivalence classes. Taking a set of representative paths of these extended equivalence classes, only 236 paths remain after Step 3-(i). We finally see that exactly two paths (in the set of representative paths of the extended equivalence classes) remain after Step 3-(ii). So, out of the 12^8 paths of length 8 over $\mathcal{M}(n,4)$, only paths that can generate MDS matrices are from these two extended equivalence classes. We see that each extended equivalence class contains 192 paths, and so there are exactly 394 distinct paths of length 8 over $\mathcal{M}(n,4)$ that can generate MDS matrices. We consider the following representatives of the extended equivalences classes:

$$\boxed{\begin{array}{c} \mathcal{B}_1 : E_{1,2}\, E_{3,4}\, E_{2,3}\, E_{3,1}\, E_{4,2}\, E_{1,4}\, E_{2,1}\, E_{4,3}; \\ \mathcal{B}_2 : E_{1,2}\, E_{3,4}\, E_{2,3}\, E_{4,1}\, E_{1,2}\, E_{3,4}\, E_{2,3}\, E_{4,1}. \end{array}}$$

Fig 1: Representative Paths of the Extended Equivalence Classes over $\mathcal{M}(n,4)$

It was established in [WLTZ21] that there does not exist an MDS matrix in $\mathcal{M}(n,4)$ with sw-XOR cost $8n+1$ and there exist MDS matrices in $\mathcal{M}(n,4)$ with sw-XOR cost $8n+3$ for some values of n. But it is not known whether there exists an MDS matrix with sw-XOR cost $8n+2$, and the authors could not verify this even for the case of $n=4$ as the search space is huge. Suppose that if there exists an MDS matrix M with sw-XOR cost $8n+2$, then it must be generated by a path of length 8 over $\mathcal{M}(n,4)$, and this path must be in the extended equivalence class of either $\mathcal{B}_1$ or $\mathcal{B}_2$ given in Fig 1. Therefore, by Theorem 3, we must have a matrix M' in either $\mathbf{M}_{\mathcal{B}_1}$ or $\mathbf{M}_{\mathcal{B}_2}$ which is MDS and the sw-XOR cost of M' is equal to $8n+2$. Below we show that there does not exist such a matrix and hence the lower bound on the sw-XOR cost of MDS matrices in $\mathcal{M}(n,m)$ is $8n+3$. The following well-known facts on permutation matrices are useful in our proof.

Fact 3.1. *The sum of two permutation matrices over fields of characteristic* 2 *is singular. The product of two permutation matrices is also a permutation matrix. The inverse of a permutation matrix is a permutation matrix. Moreover, $P^{-1}=P^T$ for $P\in\mathcal{P}(n,m)$.*

The main result of the paper is as follows.

Theorem 4. *Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the paths mentioned in Fig 1. There is no matrix M in either $\mathbf{M}_{\mathcal{B}_1}$ or $\mathbf{M}_{\mathcal{B}_2}$ such that M is MDS and the sw-XOR cost of M is equal to $8n+2$.*

Proof. We will first consider the path $\mathcal{B}_1$ and establish that there cannot be an MDS matrix M generated by $\mathcal{B}_1$ such that the sw-XOR cost of M is $8n+2$.

Case – Path $\mathcal{B}_1$:
For simplicity, we consider the path $\mathcal{B}_1$ to be the ordered list of tuples of row/column indices

$$\mathcal{B}_1=[(1,2),(3,4),(2,3),(3,1),(4,2),(1,4),(2,1),(4,3)].$$

As we are interested in finding an MDS matrix in $\mathbf{M}_{\mathcal{B}_1}$ with the least sw-XOR cost, by Fact 2.1 and Proposition 4, it is enough to consider a matrix $M\in\mathbf{M}_{\mathcal{B}_1}$ in the format given below (with $l=8$ and D_0, D_8, P and Q are all equal to the identity matrix in (11)).

$$M=E_{4,3}(\mathtt{B}_8)D_7E_{2,1}(\mathtt{B}_7)D_6E_{1,4}(\mathtt{B}_6)D_5E_{4,2}(\mathtt{B}_5)D_4E_{3,1}(\mathtt{B}_4)D_3E_{2,3}(\mathtt{B}_3)D_2E_{3,4}(\mathtt{B}_2)D_1E_{1,2}(\mathtt{B}_1),$$

where $D_k=\prod_{j=1}^4 D_{kj}$ is a diagonal matrix with $D_{kj}=E_j(\mathtt{A}_{kj})$. Denote the set of variables or coefficient matrices appearing in the above decomposition by

$$\mathcal{V}_M=\{\mathtt{A}_{11},\ldots,\mathtt{A}_{14},\mathtt{A}_{21},\ldots,\mathtt{A}_{24},\mathtt{A}_{31},\ldots,\mathtt{A}_{74},\mathtt{B}_1,\ldots,\mathtt{B}_8\}.$$

Our aim is to know whether there exists a choice for the coefficient matrices, i.e., $\mathcal{V}_M\subseteq GL(n,\mathbb{F}_2)$ such that the matrix M is MDS and the sw-XOR cost of M is equal to $8n+2$. We show that there is no such choice by symbolically verifying MDS property using Fact 3.1. First, observe that the sw-XOR cost of the matrix M satisfies

$$\begin{aligned}\mathcal{C}_{sw}(M)&=\sum_{k=1}^{7}\sum_{j=1}^{4}\mathcal{C}_s(E_j(\mathtt{A}_{kj}))+\sum_{k=1,(i_k,j_k)\in\mathcal{B}_1}^{8}\mathcal{C}_s(E_{i_k,j_k}(\mathtt{B}_i))\\&\le 8n+\sum_{k=1}^{7}\sum_{j=1}^{4}\mathcal{C}_s(\mathtt{A}_{kj})+\sum_{k=1}^{8}\mathcal{C}_d(\mathtt{B}_i),\end{aligned}$$

where the inequality is due to the identity (9). By Proposition 3, it is clear that the sw-XOR cost of M is equal to $8n+2$ only if $\mathcal{V}_M$ contains at most two non-permutation matrices and all others are permutation matrices. Next we show that with such a choice of coefficient matrices the matrix M cannot be MDS.

Observe that $E_{i,j}(\mathtt{B})$ is involutory and so the inverse of M can be given by

$$M^{-1} = E_{1,2}(\mathtt{B}_1)C_1E_{3,4}(\mathtt{B}_2)C_2E_{2,3}(\mathtt{B}_3)C_3E_{3,1}(\mathtt{B}_4)C_4E_{4,2}(\mathtt{B}_5)C_5E_{1,4}(\mathtt{B}_6)C_6E_{2,1}(\mathtt{B}_7)C_7E_{4,3}(\mathtt{B}_8),$$

where $C_k = \prod_{j=1}^{4} E_j(\mathtt{A}_{kj}^{-1})$ is the inverse of D_k for $k = 1, \ldots, 7$.

We use SageMath software for symbolic computation. The elements of the matrix M are symbolic expressions in the free algebra over $\mathbb{F}_2$ with generating set $\mathcal{V}_M$. Now consider the expression of the element $M[1,4]$ of M in terms of the coefficient matrices

$$\begin{aligned} M[1,4] &= \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64}\,\mathtt{A}_{74} + \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{B}_7\,\mathtt{A}_{74} \\ &= \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\big(\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64} + \mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{B}_7\big)\mathtt{A}_{74} \end{aligned}$$

As all the coefficient matrices in $\mathcal{V}_M$ are non-singular, the block entry $M[1,4]$ is non-singular if and only if

$$\mathtt{M}_{14} = \big(\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64} + \mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{B}_7\big)$$

is non-singular. By Fact 3.1, the matrix $\mathtt{M}_{14}$ will be singular if all the matrices appearing in the expression $\mathtt{M}_{14}$ are permutation matrices. So at least one of the coefficient matrices appearing in the expression $\mathtt{M}_{14}$ must be a non-permutation matrix for $M[1,4]$ to be non-singular. In other words, it is necessary that at least one of the elements in the set

$$\mathcal{S}_{14} = \{\mathtt{A}_{44}, \mathtt{A}_{54}, \mathtt{A}_{64}, \mathtt{B}_4, \mathtt{A}_{42}, \mathtt{A}_{52}, \mathtt{B}_6, \mathtt{A}_{63}, \mathtt{B}_7\}$$

is a non-permutation matrix in $GL(n, \mathbb{F}_2)$. Also, we have 4 more elements in M which are also sum of two monomials.

$$\begin{aligned} M[1,2] &= \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{A}_{41}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_8 + \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} \\ &= \mathtt{A}_{11}\,\mathtt{A}_{21}\big(\mathtt{A}_{31}\,\mathtt{A}_{41}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_8 + \mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72}\big) \\ M[2,3] &= \mathtt{A}_{12}\,\mathtt{A}_{22}\,\mathtt{A}_{32}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{A}_{73} + \mathtt{A}_{12}\,\mathtt{B}_2\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{A}_{73} \\ &= \mathtt{A}_{12}\big(\mathtt{A}_{22}\,\mathtt{A}_{32} + \mathtt{A}_{12}\,\mathtt{B}_2\,\mathtt{A}_{21}\,\mathtt{B}_3\,\mathtt{A}_{34}\,\mathtt{B}_4\big)\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{A}_{73} \\ M[4,2] &= \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{B}_1\,\mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{B}_5\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_8 \\ &= \big(\mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{B}_1\,\mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{B}_5\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_8\big) \\ M[4,3] &= \mathtt{B}_1\,\mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53}\,\mathtt{A}_{63}\,\mathtt{A}_{73} + \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\,\mathtt{A}_{63}\,\mathtt{A}_{73} \\ &= \big(\mathtt{B}_1\,\mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53} + \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{B}_4\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_6\big)\mathtt{A}_{63}\,\mathtt{A}_{73} \end{aligned}$$

Similarly, in the inverse matrix M^{-1} we have the following 5 elements which are also sum of two monomials. Let $\mathtt{C}_{kj} = \mathtt{A}_{kj}^{-1}$.

$$\begin{aligned} M^{-1}[1,4] &= \mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51}\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14} + \mathtt{B}_8\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14} \\ &= \big(\mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51} + \mathtt{B}_8\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{B}_5\big)\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14} \\ M^{-1}[2,1] &= \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{C}_{52}\,\mathtt{C}_{42}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_2\,\mathtt{C}_{11} + \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} \\ &= \mathtt{C}_{72}\,\mathtt{C}_{62}\big(\mathtt{C}_{52}\,\mathtt{C}_{42}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_2 + \mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\big)\mathtt{C}_{11} \\ M^{-1}[2,3] &= \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\,\mathtt{C}_{13} + \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_1 \\ &= \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_6\,\mathtt{C}_{53}\big(\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\,\mathtt{C}_{13} + \mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_1\big) \\ M^{-1}[3,1] &= \mathtt{C}_{73}\,\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} + \mathtt{C}_{73}\,\mathtt{B}_7\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{B}_4\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_2\,\mathtt{C}_{11} \\ &= \mathtt{C}_{73}\big(\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21} + \mathtt{B}_7\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{B}_4\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_2\big)\mathtt{C}_{11} \\ M^{-1}[3,4] &= \mathtt{C}_{73}\,\mathtt{B}_7\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{C}_{34}\,\mathtt{C}_{24}\,\mathtt{C}_{14} + \mathtt{C}_{73}\,\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\,\mathtt{C}_{24}\,\mathtt{C}_{14} \\ &= \mathtt{C}_{73}\big(\mathtt{B}_7\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{C}_{34} + \mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{B}_5\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{B}_3\big)\mathtt{C}_{24}\,\mathtt{C}_{14} \end{aligned}$$

If M is MDS then M^{-1} is also MDS, so all the elements of M and M^{-1} are non-singular. By the same argument as discussed above, it is necessary that at least one of the elements appearing in the expressions/sums in brackets above must be a non-permutation matrix. As the inverse of a permutation matrix is also a permutation matrix, we can see that either both $\mathtt{A}_{ij}$ and $\mathtt{C}_{ij} = \mathtt{A}_{ij}^{-1}$ are permutation matrices or both are non-permutation matrices. By Fact 3.1 at least one of the matrices in $\mathcal{T}_{14} = \{\mathtt{A}_{71}, \mathtt{A}_{61}, \mathtt{A}_{51}, \mathtt{B}_8, \mathtt{A}_{72}, \mathtt{A}_{62}, \mathtt{B}_6, \mathtt{A}_{53}, \mathtt{B}_5\}$ must be a non-permutation matrix for $M^{-1}[1,4]$ to be non-singular. In this sense (that is the variable $\mathtt{C}_{ij}$ is replaced with $\mathtt{A}_{ij}^{-1}$), observe that there is no single element that appears in all the above expressions/sums in brackets, and there is exactly one pair of elements, namely $\{\mathtt{B}_4, \mathtt{B}_5\}$, such that at least one of them appears in all those expressions/sums in brackets. So if $\mathcal{C}_{sw}(M) = 8n + 2$ and all the block entries of M and M^{-1} are non-singular, then we must have $\mathtt{B}_4$ and $\mathtt{B}_5$ to be (non-singular) non-permutation matrices and all other coefficient matrices in $\mathcal{V}_M$ must be permutation matrices. Assume that the elements of $\mathcal{V}_M$ satisfy this property. Now we will show that even with such a choice of matrices the matrix M cannot be MDS. For this purpose, we consider the following transformation of the matrix M which preserves the MDS property. We then verify the non-singularity of 2×2 block submatrices of the matrix $\hat{M}$ obtained.

$$\begin{aligned}\hat{M} = T_8^{-1} M T_1 &= T_8^{-1}\Big(E_{i_8,j_8}(\mathtt{B}_8)\big(\prod_{k=1}^{7} D_k\, E_{i_k,j_k}(\mathtt{B}_k)\big)\Big)T_1\\ &= \big(T_8^{-1}\, E_{i_8,j_8}(\mathtt{B}_8)T_8\big)\Big(\prod_{k=1}^{7}(T_{k+1}^{-1} D_k T_k)(T_k^{-1} E_{i_k,j_k}(\mathtt{B}_k)T_k)\Big),\end{aligned}$$

where $T_k = Diag(\mathtt{T}_{k1}, \mathtt{T}_{k2}, \mathtt{T}_{k3}, \mathtt{T}_{k4})$'s are block diagonal matrices and the diagonal blocks $\mathtt{T}_{kl} \in \mathcal{P}_n$ are permutation matrices for $1 \le l \le 4$. First, note that if M is MDS then $\hat{M}$ is also MDS. Now observe that $\mathtt{A}_{kj}$'s are permutation matrices, and so for any choice of T_1, by choosing $T_{k+1} = D_k T_k$ we get $(T_{k+1}^{-1} D_k T_k) = I_{n,m}$ for $1 \le k \le 7$. With such a choice and setting $\mathtt{H}_k = \mathtt{T}_{ki_k}^{-1} \mathtt{B}_k \mathtt{T}_{kj_k}$ for $k = 1, \ldots, 8$, by Lemma 7 we get $T_k^{-1} E_{i_k,j_k}(\mathtt{B}_k) T_k = E_{i_k,j_k}(\mathtt{H}_k)$. Consequently,

$$\hat{M} = (T_8^{-1}\, E_{i_8,j_8}(\mathtt{B}_8)T_8)\big(\prod_{k=1}^{7}(T_k^{-1} E_{i_k,j_k}(\mathtt{B}_k)T_k)\big) = \big(\prod_{k=1}^{8} E_{i_k,j_k}(\mathtt{H}_k)\big).$$

By our assumption, we have $\mathtt{B}_4$ and $\mathtt{B}_5$ are non-permutation matrices and the other matrices in $\{\mathtt{B}_1, \mathtt{B}_2, \mathtt{B}_3, \mathtt{B}_6, \mathtt{B}_7, \mathtt{B}_8\}$ are permutation matrices. Observe that $\mathcal{C}_d(\mathtt{H}_k) = \mathcal{C}_d(\mathtt{B}_k)$ for $1 \le k \le 8$ since $\mathtt{T}_{kt}$, $1 \le t \le 4$, are permutation matrices. Therefore, the matrices $\mathtt{H}_4$ and $\mathtt{H}_5$ are non-permutation matrices and $\mathtt{H}_k$, $k \in \{1, 2, 3, 6, 7, 8\}$, are permutation matrices. Now consider the following 2×2 submatrix of $\hat{M}$

$$S = \begin{pmatrix} \hat{M}[1,2] & \hat{M}[1,4] \\ \hat{M}[2,2] & \hat{M}[2,4] \end{pmatrix}$$

Observe that if M is MDS then $\hat{M}$ is also MDS, and so all the block submatrices of $\hat{M}$ are also non-singular. By Proposition 7, if S is non-singular then

$$\mathtt{S} = \hat{M}[2,4] + \hat{M}[2,2](\hat{M}[1,2])^{-1}\hat{M}[1,4]$$

is non-singular. Simplifying the expression of $\mathtt{S}$, we get

$$\begin{aligned}\mathtt{S} &= (\mathtt{H}_2\,\mathtt{H}_3 + \mathtt{H}_6\,\mathtt{H}_7 + \mathtt{H}_2\,\mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7) + (1 + \mathtt{H}_2\,\mathtt{H}_8 + \mathtt{H}_2\,\mathtt{H}_3\,\mathtt{H}_4)(\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)^{-1}(\mathtt{H}_3 + \mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7)\\ &= (\mathtt{H}_2\,\mathtt{H}_3 + \mathtt{H}_6\,\mathtt{H}_7 + \mathtt{H}_2\,\mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7) + \big((\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)^{-1} + \mathtt{H}_2\big)(\mathtt{H}_3 + \mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7)\\ &= \mathtt{H}_6\,\mathtt{H}_7 + (\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)^{-1}(\mathtt{H}_3 + \mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7)\\ &= (\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)^{-1}\big((\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)\,\mathtt{H}_6\,\mathtt{H}_7 + (\mathtt{H}_3 + \mathtt{H}_3\,\mathtt{H}_4\,\mathtt{H}_6\,\mathtt{H}_7)\big)\\ &= (\mathtt{H}_8 + \mathtt{H}_3\,\mathtt{H}_4)^{-1}(\mathtt{H}_8\,\mathtt{H}_6\,\mathtt{H}_7 + \mathtt{H}_3).\end{aligned}$$

The matrices $\mathtt{H}_3, \mathtt{H}_6, \mathtt{H}_7$ and $\mathtt{H}_8$ are permutation matrices since $\mathtt{B}_3, \mathtt{B}_6, \mathtt{B}_7$ and $\mathtt{B}_8$ are permutation matrices. So the matrix $\mathtt{S}$ cannot be non-singular as $(\mathtt{H}_8\,\mathtt{H}_6\,\mathtt{H}_7 + \mathtt{H}_3)$ is a sum of two permutation matrices. This implies that the matrix S cannot be non-singular. Hence with such a choice of $\mathtt{H}_k$'s the matrix $\hat{M}$ cannot be MDS and so the matrix M cannot be MDS. Therefore, there cannot be an MDS matrix $M \in \mathbf{M}_{\mathcal{B}_1}$ such that the sw-XOR cost of M is equal to $8n+2$. Next we consider the second path and show the same.

Case – Path $\mathcal{B}_2$:
For simplicity, we consider the path $\mathcal{B}_2$ to be the ordered list of tuples of row/column indices

$$\mathcal{B}_2 = [(1,2),(3,4),(2,3),(4,1),(1,2),(3,4),(2,3),(4,1)].$$

As discussed in the case of path $\mathcal{B}_1$, it is enough to consider a matrix $M \in \mathbf{M}_{\mathcal{B}_2}$ in the format given below.

$$M = E_{4,1}(\mathtt{B}_8)D_7E_{2,3}(\mathtt{B}_7)D_6E_{3,4}(\mathtt{B}_6)D_5E_{1,2}(\mathtt{B}_5)D_4E_{4,1}(\mathtt{B}_4)D_3E_{2,3}(\mathtt{B}_3)D_2E_{3,4}(\mathtt{B}_2)D_1E_{1,2}(\mathtt{B}_1),$$

where $D_k = \prod_{j=1}^{4} D_{kj}$ is a diagonal matrix with $D_{kj} = E_j(\mathtt{A}_{kj})$. Denote the set of variables or coefficient matrices appearing in the above decomposition by

$$\mathcal{V}_M = \{\mathtt{A}_{11}, \ldots, \mathtt{A}_{14}, \mathtt{A}_{21}, \ldots, \mathtt{A}_{24}, \mathtt{A}_{31}, \ldots, \mathtt{A}_{74}, \mathtt{B}_1, \ldots, \mathtt{B}_8\}.$$

Our aim is to know whether there exists a choice for the coefficient matrices, i.e., $\mathcal{V}_M \subseteq GL(n, \mathbb{F}_2)$ such that the matrix M is MDS and the sw-XOR cost of M is equal to $8n+2$. The proof is similar to the proof as in the case of path $\mathcal{B}_1$. In fact, by observing the entries of M and the entries of its inverse M^{-1}, we will be able to conclude that there cannot be such a choice for the coefficient matrices.

We can see that there are 6 entries in M that are sum of two monomials. Similarly, there 6 entries in the inverse matrix M^{-1} that are also sum of two monomials. The symbolic expressions of these entries are presented in Appendix C. The block entries of M and M^{-1} are non-singular if at least one of the variables/coefficient matrices appearing in each expression/sum in brackets is a non-permutation matrix. Replacing $\mathtt{C}_{kj} = \mathtt{A}_{kj}^{-1}$, observe that there is no variable that appears in all those 12 expressions in brackets (of M and M^{-1}). Also, there is no pair of variables/coefficient matrices such that at least one of them appears in those 12 expressions in brackets. By the same argument as in the case of path $\mathcal{B}_1$, we can see that there cannot be an MDS matrix $M \in \mathbf{M}_{\mathcal{B}_2}$ such that the sw-XOR cost of M is equal to $8n+2$. □

4 Conclusion

We have presented an extensive study on the metric sw-XOR and proved that the minimum possible implementation cost under this metric is $8n+3$ for 4×4 MDS matrices over the general linear group $GL(n, \mathbb{F}_2)$. We have also shown that it is, essentially, enough to consider only two paths to search exhaustively for MDS matrices with sw-XOR cost equal to $8n+3$. In the case of $n = 4$ or 8, this bound is tight and the values are 35 and 67 respectively, existence of such matrices are known due to [DL18]. Therefore, our result puts an end to the quest for such block MDS matrices under the sw-XOR metric and thus suggests to give a fresh look at the implementation cost of MDS matrices to be able to cross the limit of $8n+3$.

In future, it will be interesting to find low cost implementations of the MDS matrices that are of practical interest like AES MixColumns under the sw-XOR metric similar to the work of [XZL$^+$20]. Another important parameter in hardware implementation of MDS matrices is the depth of the circuit which is not considered in our work. Establishing lower bounds under the metrics s-XOR or g-XOR and also considering depth is an interesting future work.

References

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015*, pages 411–436, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[Ber09] Daniel J Bernstein. Optimizing linear maps modulo 2. In *Workshop Record of SPEED-CC: Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers*, pages 3–18, 2009.

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 625–653. Springer, 2016.

[BMP08] Joan Boyar, Philip Matthews, and René Peralta. On the shortest linear straight-line program for computing linear forms. In Edward Ochmanski and Jerzy Tyszkiewicz, editors, *Mathematical Foundations of Computer Science 2008, 33rd International Symposium, MFCS 2008, Torun, Poland, August 25-29, 2008, Proceedings*, volume 5162 of *Lecture Notes in Computer Science*, pages 168–179. Springer, 2008.

[BP10] Joan Boyar and René Peralta. A new combinational logic minimization technique with applications to cryptology. In Paola Festa, editor, *Experimental Algorithms, 9th International Symposium, SEA 2010, Ischia Island, Naples, Italy, May 20-22, 2010. Proceedings*, volume 6049 of *Lecture Notes in Computer Science*, pages 178–189. Springer, 2010.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A small present - towards reaching the limit of lightweight encryption. In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017.

[CDL15] Anne Canteaut, Sébastien Duval, and Gaëtan Leurent. Construction of lightweight S-boxes using Feistel and MISTY structures. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*, volume 9566 of *Lecture Notes in Computer Science*, pages 373–393. Springer, 2015.

[DL18] Sébastien Duval and Gaëtan Leurent. MDS matrices with lightweight circuits. *IACR Trans. Symmetric Cryptol.*, 2018(2):48–78, 2018.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *Advances in Cryptology -*

CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.

[JPST17] Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux. Optimizing implementations of lightweight building blocks. *IACR Trans. Symmetric Cryptol.*, 2017(4):130–168, 2017.

[KLSW17] Thorsten Kranz, Gregor Leander, Ko Stoffelen, and Friedrich Wiemer. Shorter linear straight-line programs for MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2017(4):188–211, 2017.

[KPPY14] Khoongming Khoo, Thomas Peyrin, Axel Y. Poschmann, and Huihui Yap. FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 433–450. Springer Berlin Heidelberg, 2014.

[KPSV21] Abhishek Kesarwani, Sumit Kumar Pandey, Santanu Sarkar, and Ayineedi Venkateswarlu. Recursive MDS matrices over finite commutative rings. *Discret. Appl. Math.*, 304:384–396, 2021.

[KSV19] Abhishek Kesarwani, Santanu Sarkar, and Ayineedi Venkateswarlu. Exhaustive search for various types of MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2019(3):231–256, 2019.

[LS16] Meicheng Liu and Siang Meng Sim. Lightweight MDS generalized circulant matrices. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 101–120. Springer, 2016.

[LW16] Yongqiang Li and Mingsheng Wang. On the construction of lightweight circulant involutory MDS matrices. In Thomas Peyrin, editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 121–139. Springer, 2016.

[LW17] Chaoyun Li and Qingju Wang. Design of lightweight linear diffusion layers from near-MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2017(1):129–155, 2017.

[LWC18] NIST lightweight cryptography project. 2018. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf.

[LWL18] Qiuping Li, Baofeng Wu, and Zhuojun Liu. Direct constructions of (involutory) MDS matrices from block vandermonde and cauchy-like matrices. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields - 7th International Workshop, WAIFI 2018, Bergen, Norway, June 14-16, 2018, Revised Selected Papers*, volume 11321 of *Lecture Notes in Computer Science*, pages 275–290. Springer, 2018.

[Max19] Alexander Maximov. AES mixcolumn with 92 XOR gates. *IACR Cryptol. ePrint Arch.*, 2019. https://eprint.iacr.org/2019/833.

[Mey00] Carl D Meyer. *Matrix Analysis and Applied Linear Algebra*, volume 71. Siam, 2000.

[MSST22] Kalikinkar Mandal, Dhiman Saha, Sumanta Sarkar, and Yosuke Todo. Sycon: a new milestone in designing ASCON-like permutations. *J. Cryptogr. Eng.*, 12(3):305–327, 2022.

[Paa97] Christof Paar. Optimized arithmetic for Reed-Solomon encoders. In *Proceedings of IEEE international symposium on information theory*, pages 250–. IEEE, 1997.

[SKOP15] Siang Meng Sim, Khoongming Khoo, Frédérique E. Oggier, and Thomas Peyrin. Lightweight MDS involution matrices. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 471–493. Springer, 2015.

[SS16a] Sumanta. Sarkar and Siang Meng Sim. A deeper understanding of the XOR count distribution in the context of lightweight cryptography. In D. Pointcheval, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa, Fes, Morocco, April 13-15, 2016, Proceedings*, volume 9646 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 2016.

[SS16b] Sumanta Sarkar and Habeeb Syed. Lightweight diffusion layer: Importance of Toeplitz matrices. *IACR Trans. Symmetric Cryptol.*, 2016(1):95–113, 2016.

[SS17] Sumanta Sarkar and Habeeb Syed. Analysis of toeplitz MDS matrices. In Josef Pieprzyk and Suriadi Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, volume 10343 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2017.

[WLTZ21] Shi Wang, Yongqiang Li, Shizhu Tian, and Xiangyong Zeng. Four by four MDS matrices with the fewest XOR gates based on words. *Advances in Mathematics of Communications*, 2021. https://doi.org/10.3934/amc.2021025.

[XZL+20] Zejun Xiang, Xiangyong Zeng, Da Lin, Zhenzhen Bao, and Shasha Zhang. Optimizing implementations of linear layers. *IACR Trans. Symmetric Cryptol.*, 2020(2):120–145, 2020.

[YZW21] Yumeng Yang, Xiangyong Zeng, and Shi Wang. Construction of lightweight involutory MDS matrices. *Design, Codes and Cryptography*, 89(7):1453–1483, 2021.

[ZWS18] Lijing Zhou, Licheng Wang, and Yiru Sun. On efficient constructions of lightweight MDS matrices. *IACR Trans. Symmetric Cryptol.*, 2018(1):180–200, 2018.

[ZWZZ16] Ruoxin Zhao, Baofeng Wu, Rui Zhang, and Qian Zhang. Designing optimal implementations of linear layers (full version). *IACR Cryptol. ePrint Arch.*, 2016. http://eprint.iacr.org/2016/1118.

A Proof of Lemma 1

First note that a matrix M in $\mathcal{M}(n, m)$ can be interpreted as an $mn \times mn$ matrix over $\mathbb{F}_2$. Suppose that M is non-singular, then it is well-known that the matrix M can be decomposed as a product of elementary matrices over $\mathbb{F}_2$. Observe that the identity matrix is the only elementary matrix of Type II over $\mathbb{F}_2$. Also, for elementary matrices over $\mathbb{F}_2$, we have $E(i, j) = E_{i,j}(1)E_{j,i}(1)E_{i,j}(1)$. Therefore, over $\mathbb{F}_2$, the matrix M can be decomposed as a product of elementary matrices of Type III. Now we show that any $mn \times mn$ elementary matrix of Type III over $\mathbb{F}_2$ can be written as a product of two elementary block matrices in $\mathcal{M}(n, m)$. Suppose that $n \geq 2$ and $i = i_1 n + i_2$ and $j = j_1 n + j_2$. Then there exist $\mathtt{B}, \mathtt{B}' \in GL(n, \mathbb{F}_2)$ such that $\mathtt{B} + \mathtt{B}' = \mathtt{B}_{i_2 j_2}$, where $\mathtt{B}_{i_2 j_2}$ is the matrix with (i_2, j_2)-th entry is 1 and 0 elsewhere. Observe that $E_{i,j}(1) = E_{i_1,j_1}(\mathtt{B})E_{i_1,j_1}(\mathtt{B}')$ by (1). Hence the result.

In the above proof, we have $i \neq j$. Suppose $i_1 \neq j_1$ and $i_2 = j_2$. In this case, we cannot have a matrix $\mathtt{B}' \in GL(n, \mathbb{F}_2)$ such that $\mathtt{I}_n + \mathtt{B}' = \mathtt{B}_{i_2 j_2}$ as mentioned in the proof of [WLTZ21, Corollary 1].

B Proof of Lemma 9

Let $E_{i,j}(\mathtt{B}) = I_{n,m} + B_{i,j}$ and $E_{i',j'}(\mathtt{B}') = I_{n,m} + B'_{i',j'}$, where $B_{i,j}$ ($B'_{i',j'}$) is the matrix with $[i, j]$-th ($[i', j']$-th) entry is $\mathtt{B}$ ($\mathtt{B}'$) and all other entries are zero. Then

$$\begin{aligned}
E_{i,j}(\mathtt{B})E_{i',j'}(\mathtt{B}') &= I_{n,m} + B_{i,j} + B'_{i',j'} + B_{i,j}B'_{i',j'},\\
E_{i',j'}(\mathtt{B}')E_{i,j}(\mathtt{B}) &= I_{n,m} + B_{i,j} + B'_{i',j'} + B'_{i',j'}B_{i,j}.
\end{aligned}$$

Now observe that

$$B_{i,j}B'_{i',j'} = \begin{cases} F_{i,j'}, & j = i' \\ \mathbf{0}, & j \neq i' \end{cases} \quad \text{and} \quad B'_{i',j'}B_{i,j} = \begin{cases} G_{i',j}, & i = j' \\ \mathbf{0}, & i \neq j', \end{cases}$$

where $F_{i,j'}$ ($G_{i',j}$) is the matrix with $[i, j']$-th ($[i', j]$-th) entry is $\mathtt{B}\,\mathtt{B}'$ ($\mathtt{B}'\mathtt{B}$) and all others are zero. Therefore, if $i \neq j'$ and $j \neq i'$ then the last component in the above sum is the zero matrix and hence they are equal. Hence the result.

C Symbolic Expressions of the Entries of M and M^{-1}

We can see that there are 6 entries in M that are sum of two monomials and they are:

$$\begin{aligned}
M[1,2] &= \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{B}_{4}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{A}_{41}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_{8}\\
&= \mathtt{A}_{11}\,\mathtt{A}_{21}(\mathtt{A}_{31}\,\mathtt{B}_{4}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{A}_{31}\,\mathtt{A}_{41}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_{8})\\
M[2,2] &= \mathtt{A}_{12}\,\mathtt{A}_{22}\,\mathtt{A}_{32}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{A}_{12}\,\mathtt{B}_{2}\,\mathtt{A}_{23}\,\mathtt{B}_{3}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{B}_{5}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_{8}\\
&= \mathtt{A}_{12}(\mathtt{A}_{22}\,\mathtt{A}_{32}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{A}_{62}\,\mathtt{A}_{72} + \mathtt{B}_{2}\,\mathtt{A}_{23}\,\mathtt{B}_{3}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{B}_{5}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\,\mathtt{B}_{8})\\
M[2,3] &= \mathtt{A}_{12}\,\mathtt{B}_{2}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53}\,\mathtt{A}_{63}\,\mathtt{A}_{73} + \mathtt{A}_{12}\,\mathtt{A}_{22}\,\mathtt{A}_{32}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_{6}\,\mathtt{A}_{63}\,\mathtt{A}_{73}\\
&= \mathtt{A}_{12}(\mathtt{B}_{2}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53} + \mathtt{A}_{22}\,\mathtt{A}_{32}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_{6})\mathtt{A}_{63}\,\mathtt{A}_{73}\\
M[3,4] &= \mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{B}_{3}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64}\,\mathtt{A}_{74} + \mathtt{A}_{13}\,\mathtt{A}_{23}\,\mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53}\,\mathtt{A}_{63}\,\mathtt{B}_{7}\,\mathtt{A}_{74}\\
&= \mathtt{A}_{13}\,\mathtt{A}_{23}\ (\mathtt{B}_{3}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64} + \mathtt{A}_{33}\,\mathtt{A}_{43}\,\mathtt{A}_{53}\,\mathtt{A}_{63}\,\mathtt{B}_{7})\ \mathtt{A}_{74}\\
M[4,1] &= \mathtt{B}_{1}\,\mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{A}_{41}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71} + \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{B}_{5}\,\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\\
&= (\mathtt{B}_{1}\,\mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{A}_{41} + \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{B}_{5})\mathtt{A}_{51}\,\mathtt{A}_{61}\,\mathtt{A}_{71}\\
M[4,4] &= \mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64}\,\mathtt{A}_{74} + \mathtt{B}_{1}\,\mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{B}_{4}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_{6}\,\mathtt{A}_{63}\,\mathtt{B}_{7}\,\mathtt{A}_{74}\\
&= (\mathtt{A}_{14}\,\mathtt{A}_{24}\,\mathtt{A}_{34}\,\mathtt{A}_{44}\,\mathtt{A}_{54}\,\mathtt{A}_{64} + \mathtt{B}_{1}\,\mathtt{A}_{11}\,\mathtt{A}_{21}\,\mathtt{A}_{31}\,\mathtt{B}_{4}\,\mathtt{A}_{42}\,\mathtt{A}_{52}\,\mathtt{B}_{6}\,\mathtt{A}_{63}\,\mathtt{B}_{7})\mathtt{A}_{74}
\end{aligned}$$

Similarly, there 6 entries in the inverse matrix M^{-1} that are also sum of two monomials. Let $\mathtt{C}_{kj} = \mathtt{A}_{kj}^{-1}$.

$$\begin{aligned}
M^{-1}[1,1] &= \mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51}\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} + \mathtt{B}_{8}\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_{6}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{B}_{3}\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_{1}\\
&= (\mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51}\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} + \mathtt{B}_{8}\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_{6}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{B}_{3}\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_{1})\\
M^{-1}[1,2] &= \mathtt{B}_{8}\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{C}_{52}\,\mathtt{C}_{42}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{C}_{12} + \mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51}\,\mathtt{C}_{41}\,\mathtt{B}_{4}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{C}_{12}\\
&= (\mathtt{B}_{8}\,\mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{C}_{52}\,\mathtt{C}_{42}\ + \mathtt{C}_{71}\,\mathtt{C}_{61}\,\mathtt{C}_{51}\,\mathtt{C}_{41}\,\mathtt{B}_{4})\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{C}_{12}\\
M^{-1}[2,3] &= \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{B}_{6}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\,\mathtt{C}_{13} + \mathtt{C}_{72}\,\mathtt{C}_{62}\,\mathtt{C}_{52}\,\mathtt{C}_{42}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_{2}\,\mathtt{C}_{13}\\
&= \mathtt{C}_{72}\,\mathtt{C}_{62}\,(\mathtt{B}_{6}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\ + \mathtt{C}_{52}\,\mathtt{C}_{42}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_{2})\,\mathtt{C}_{13}\\
M^{-1}[3,3] &= \mathtt{C}_{73}\,\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\,\mathtt{C}_{13} + \mathtt{C}_{73}\,\mathtt{B}_{7}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{B}_{5}\,\mathtt{C}_{41}\,\mathtt{B}_{4}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_{2}\,\mathtt{C}_{13}\\
&= \mathtt{C}_{73}\,(\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{C}_{23}\ + \mathtt{B}_{7}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{B}_{5}\,\mathtt{C}_{41}\,\mathtt{B}_{4}\,\mathtt{C}_{32}\,\mathtt{C}_{22}\,\mathtt{B}_{2})\,\mathtt{C}_{13}\\
M^{-1}[3,4] &= \mathtt{C}_{73}\,\mathtt{B}_{7}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{C}_{34}\,\mathtt{C}_{24}\,\mathtt{C}_{14} + \mathtt{C}_{73}\,\mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{B}_{3}\,\mathtt{C}_{24}\,\mathtt{C}_{14}\\
&= \mathtt{C}_{73}\,(\mathtt{B}_{7}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{C}_{34}\ + \mathtt{C}_{63}\,\mathtt{C}_{53}\,\mathtt{C}_{43}\,\mathtt{C}_{33}\,\mathtt{B}_{3})\,\mathtt{C}_{24}\,\mathtt{C}_{14}\\
M^{-1}[4,1] &= \mathtt{C}_{74}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{B}_{5}\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} + \mathtt{C}_{74}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,\mathtt{C}_{44}\,\mathtt{C}_{34}\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_{1}\\
&= \mathtt{C}_{74}\,\mathtt{C}_{64}\,\mathtt{C}_{54}\,(\mathtt{B}_{5}\,\mathtt{C}_{41}\,\mathtt{C}_{31}\,\mathtt{C}_{21}\,\mathtt{C}_{11} + \mathtt{C}_{44}\,\mathtt{C}_{34}\,\mathtt{C}_{24}\,\mathtt{C}_{14}\,\mathtt{B}_{1})
\end{aligned}$$