On Constructions of a Sort of MDS Block Diffusion Matrices for Block Ciphers and Hash Functions

Ruoxin Zhao[1,2], Rui Zhang[1], Yongqiang Li[1], and Baofeng Wu[1]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences
[2] University of Chinese Academy of Sciences
zhaoruoxin@iie.ac.cn

Abstract

Many modern block ciphers use maximum distance separate (MDS) matrices as their diffusion layers. In this paper, we propose a new method to verify a sort of MDS diffusion block matrices whose blocks are all polynomials in a certain primitive block over the finite field $\mathbb{F}_2$. And then we discover a new kind of transformations that can retain MDS property of diffusion matrices and generate a series of new MDS matrices from a given one. Moreover, we get an equivalence relation from this kind of transformation. And MDS property is an invariant with respect to this equivalence relation which can greatly reduce the amount of computation when we search for MDS matrices. The minimal polynomials of matrices play an important role in our strategy. To avoid being too theoretical, we list a series of MDS diffusion matrices obtained from our method for some specific parameters. Furthermore, we talk about MDS recursive diffusion layers with our method and extend the corresponding work of M. Sajadieh et al. published on FSE 2012 and the work of S. Wu published on SAC 2012.

Keywords: Diffusion layer, linear transformation, branch numbers, MDS matrix, minimal polynomial, equivalence relation.

1 Introduction

Block ciphers are one of the most important building blocks in many cryptosystems. Modern block ciphers are often iterations of several rounds and each round consists of a confusion layer and a diffusion layer. From the viewpoint of mathematics, the confusion layers are usually formed by nonlinear functions (S-boxes) while the diffusion layers are formed by linear functions. The diffusion layers play an significant role in block ciphers as well as in other cryptographic primitives such as hash functions. On one hand, the diffusion layers can provide resistance against many well-known attacks on block ciphers such as differential cryptanalysis [3] and linear cryptanalysis [19]; on the other hand, they greatly influence the efficiency of implementations.

The security of a diffusion layer is measured by its differential branch number and the linear branch number. The larger the two branch numbers are, the stronger a diffusion layer is. The diffusion layers with the optimal branch numbers are called being maximum distance separable (MDS) [18]. This name comes from the theory of error-correcting codes because

the problems about branch numbers can be transferred into some problems on the error-correcting codes relevant to the diffusion layers. For more details about MDS codes and MDS matrices, please refer to [4, 18, 17, 5, 13]. However, they do not become easier even from the viewpoint of coding theory. Therefore, how to construct diffusion layers with large branch numbers is still a challenge to the cryptosystem designers.

By now, there are two main types of diffusion layers with high efficiency: recursive diffusion layers and involutory diffusion layers. As we know, the diffusion layer used in AES cannot be implemented very efficiently, especially on hardware. Thus, in [10], J. Guo et al. presented a new strategy for designing diffusion layers with bundle-based linear feedback shift registers (LFSRs). From their strategy, a diffusion layer can be divided into several steps. In each step, the last bundle is updated by a linear combination of all the bundles while other bundles are merely obtained by shifting the state vector by one bundle (see Figure 1). A diffusion layer designed with this strategy is called a recursive diffusion layer. In [25], M. Sajadieh et al. extended the linear combinations in this strategy to combinations of linear transformations. For more details about recursive diffusion layers, please consult [25, 26, 1, 6]. A diffusion layer is called involutory if its inverse mapping is the same as itself. Obviously, this property saves the storage of systems because the encryption diffusion mapping and the decryption diffusion mapping are identical. Most designers prefer two approaches to directly design involutory MDS diffusion layers: constructions from Cauchy matrices [27] and constructions from Vandermonde matrices [15]. However, they can merely get a few special types of involutory MDS diffusion layers. For more details about involutory diffusion layers, please consult [11, 24, 20].

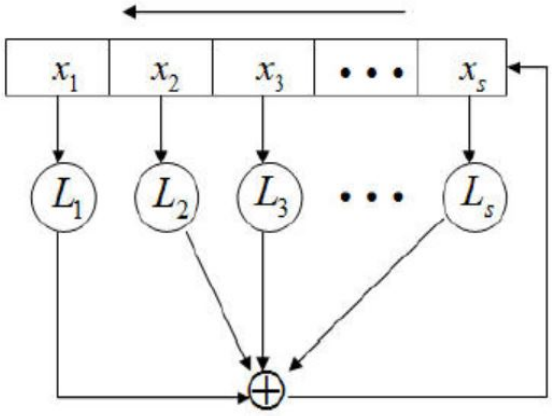

Figure 1: Linear feedback shift register

In general, a diffusion layer can be regarded as an $\mathbb{F}_2$-linear transformation over the vector space $\mathbb{F}_2^n$ for certain parameter n. However, some diffusion layers can be lifted to some finite fields larger than $\mathbb{F}_2$. For example, the diffusion layer of AES is indeed an $\mathbb{F}_2$-linear transformation over the vector space $\mathbb{F}_2^{128}$. However, it is essentially an $\mathbb{F}_q$-linear transformation over $\mathbb{F}_q^{16}$ where q is equal to 2^8. Notice that multiplications with elements in $\mathbb{F}_{2^n}$ are still $\mathbb{F}_2$-linear transformations over the vector space $\mathbb{F}_2^n$. Thus, the diffusion layers in AES-like ciphers are just a small part of $\mathbb{F}_2$-linear transformations.

In this paper, we focus on the constructions of a sort of $\mathbb{F}_2$-linear MDS diffusion layers whose blocks are all polynomials in a primitive block. We present a new method to test whether a diffusion layer is MDS. Note that the minimal polynomials of matrices play an important role in our method. Then, more significantly, we expand our method into a more generalized case. We discover a new kind of transformations that retains MDS property of diffusion matrices and can generate many MDS matrices from a fixed one. With this method, we find out a series of MDS diffusion layers with some fixed parameters. Furthermore, we discuss the recursive diffusion layers and involutory diffusion layers with our method and extend the results of [25] and [26].

The rest of this paper is organized as follows. In Section 2, we introduce some definitions and previous results about linear transformations, determinants, matrices and branch numbers. In Section 3, we present our method to find out MDS diffusion layers. To avoid being too theoretical, We also illustrate some experimental results. In Section 4, we expand our method into a more generalized case and present a modified algorithm. In Section 5, we discuss the recursive diffusion layers with our method and extend the results of [25] and [26]. Finally, we conclude this paper in Section 6.

2 Preliminaries

In this section, we introduce some definitions and previous results we need.

2.1 Linear Algebra

In this paper, $\mathcal{M}_{s\times t}(F)$ usually denotes the set consisting of all the $(s \times t)$ matrices over the field F.

Let $\mathbb{F}_q$ (or $GF(q)$) be the finite field with q elements where q is a prime power and V be an n-dimensional $\mathbb{F}_q$-linear space. A mapping $L : V \to V$ is an $\mathbb{F}_q$-linear transformation over V if for every $u, v \in \mathbb{F}_q$, for every $\alpha, \beta \in V$,

$$L(u\alpha + v\beta) = uL(\alpha) + vL(\beta).$$

From linear algebra, we know that there exists a bijection between the set consisting of all the $\mathbb{F}_q$-linear transformation over V and the set $\mathcal{M}_{n\times n}(\mathbb{F}_q)$ under a fixed basis of V. Furthermore, if we regard the two sets as two algebras, the bijection is an algebra isomorphism. Thus, in this paper, we identify every $\mathbb{F}_q$-linear transformation over V with a matrix in $\mathcal{M}_{n\times n}(\mathbb{F}_q)$. Specifically, if L is a matrix in $\mathcal{M}_{n\times n}(\mathbb{F}_q)$, the mapping which maps every row vector $\boldsymbol{x} \in \mathbb{F}_q^n$ to $\boldsymbol{x}L$ is an $\mathbb{F}_q$-linear transformation over $\mathbb{F}_q^n$ uniquely determined by L, so we also denote this linear transformation by L.

Let $\mathbb{F}_{q^n}$ be an extension of $\mathbb{F}_q$. Then $\mathbb{F}_{q^n}$ is an n-dimensional $\mathbb{F}_q$-linear space. Notice that multiplication with an element in $\mathbb{F}_{q^n}$ is a special $\mathbb{F}_q$-linear transformation over $\mathbb{F}_{q^n}$. More precisely, for every $\alpha \in \mathbb{F}_{q^n}$, the mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ defined as $f(x) = \alpha x$ is an $\mathbb{F}_q$-linear transformation over $\mathbb{F}_{q^n}$.

For every vector $\boldsymbol{x} \in \mathbb{F}_q^m$, the Hamming weight of $\boldsymbol{x}$ is defined as the number of non-zero coordinates of $\boldsymbol{x}$ and is denoted by $w_H(\boldsymbol{x})$. Suppose $\boldsymbol{y} \in \mathbb{F}_q^{bn}$ for some positive integers b and n. We may divide $\boldsymbol{y}$ into n segments, namely, $\boldsymbol{y} = (\boldsymbol{y}_1, \cdots, \boldsymbol{y}_n)$ where $\boldsymbol{y}_i \in \mathbb{F}_q^b$, $i = 1, \cdots, n$. Then each $\boldsymbol{y}_i$ is called a bundle of $\boldsymbol{y}$. The bundle weight of $\boldsymbol{y}$ is defined as the number of

non-zero bundles of $\boldsymbol{y}$ and is denoted by $w_b(\boldsymbol{y})$. If $\boldsymbol{z} \in \mathbb{F}_q^{bn}$ is another vector, the bundle distance between $\boldsymbol{y}$ and $\boldsymbol{z}$ is defined as $w_b(\boldsymbol{y}-\boldsymbol{z})$ and denoted by $d_b(\boldsymbol{y},\boldsymbol{z})$. Note that $w_b(\boldsymbol{y})$ and $w_H(\boldsymbol{y})$ are distinct in most cases.

Suppose $\boldsymbol{x} \in \mathbb{F}_q^{bn}$ be a row vector and $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_q)$ is a matrix. Let $\boldsymbol{y} = \boldsymbol{x}L$ be the image of $\boldsymbol{x}$ under the linear transformation L. From matrix theory, it is convenient to express the multiplication of $\boldsymbol{x}$ and L if we divide $\boldsymbol{x}$ into bundles and divide L into blocks. That is, we may write $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$ where $\boldsymbol{x}_i \in \mathbb{F}_q^b$, $i = 1, \cdots, n$ and

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

where $L_{i,j} \in \mathcal{M}_{b\times b}(\mathbb{F}_q)$ is a matrix, $i, j = 1 \cdots, n$. Then

$$\begin{aligned} \boldsymbol{y} &= (\boldsymbol{y}_1, \boldsymbol{y}_2 \cdots, \boldsymbol{y}_n) \\ &= (\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_n) \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix} \end{aligned}$$

where each $\boldsymbol{y}_j \in \mathbb{F}_q^b$ and $\boldsymbol{y}_j = \sum_{i=1}^n \boldsymbol{x}_i L_{i,j}$, $j = 1, \cdots, n$. In this paper, the techniques dealing with block matrices play an important role.

As mentioned in Section 1, minimal polynomials of matrices play a significant role in this paper. So we are presenting some knowledge about minimal polynomials. Let F and E be two fields such that $F \subseteq E$ or $E \subseteq F$. For a square matrix $H \in \mathcal{M}_{b\times b}(E)$, a polynomial $f(x) \in F[x]$ is called an annihilator polynomial of H in $F[x]$ if $f(H) = O_b$ where O_b is the zero matrix in $\mathcal{M}_{b\times b}(F)$. For example, from Hamilton-Cayley theorem, we know that the characteristic polynomial of H is an annihilator polynomial of H in $E[x]$. A polynomial $g(x) \in F[x]$ is called the minimal polynomial of H in $F[x]$ if $g(x)$ is the monic annihilator polynomial of H in $F[x]$ with the lowest degree. The minimal polynomial of H is usually denoted by $m_H(x)$. In fact, the minimal polynomial of a matrix has some relation to its annihilator polynomials.

Proposition 1 ([22]). *The minimal polynomial of a matrix A divides all the annihilator polynomials of it.*

For two matrices $A, B \in \mathcal{M}_{b\times b}(F)$, we say that A is similar to B (or B is similar to A) if there exists a nonsingular matrix $P \in \mathcal{M}_{b\times b}(F)$ such that $P^{-1}AP = B$. An elementary property of minimal polynomial is stated in the following lemma.

Proposition 2 ([22]). *Two similar matrices have the same minimal polynomial.*

In matrix theory, there is a proposition useful to us.

Proposition 3 ([8]). *The minimal polynomial and the characteristic polynomial of a matrix over a field F have the same irreducible factors in $F[x]$.*

According to Proposition 1 and 3, we may test the factors of the characteristic polynomial of H one by one to seek the minimal polynomial of H. But along with the increase of the degree of characteristic polynomial, the amount of computation for this approach will skyrocket rapidly. Thus, for those matrices with large sizes, we need other methods to compute their minimal polynomials. For example, the following proposition brings us an effective approach.

Proposition 4 ([8]). *Let $A : V \to V$ be linear. Suppose $W_1, \cdots, W_k$ are subspaces of V such that $V = W_1 + \cdots + W_k$, $A(W_i) \subseteq W_i$ for all i, and the restriction of A to W_i has minimal polynomial $m_i(x)$. Then the minimal polynomial of A on V is* $\mathrm{lcm}(m_1, \cdots, m_k)$.

In Proposition 4, $\mathrm{lcm}(m_1, \cdots, m_k)$ denotes the least common multiple of $m_1, \cdots, m_k$. As we mentioned, Proposition 4 leads to an algorithm for computing the minimal polynomial of any square matrix $A \in \mathcal{M}_{n\times n}(E)$. Pick any column vector $v \neq \mathbf{0}$ in $V = E^n$ and consider the sequence of vectors $\{v, Av, A^2v, \cdots\}$. They span a subspace of V that is denoted by W, so $W = \{f(A)v : f(x) \in E[x]\}$. The nice feature of W is that $A(W) \subseteq W$, so A makes sense as a linear operator on W. To determine the minimal polynomial of A on W, find the smallest positive integer d such that the vectors $v, Av, \cdots, A^dv$ are linearly dependent. Since $v, Av, \cdots, A^{d-1}v$ are linearly independent, the linear relation

$$b_{d-1}A^{d-1}v + \cdots b_1Av + b_0v = \mathbf{0}$$

with $b_i \in E$, $i = 1, \cdots, d-1$ implies that $b_i = 0$, $i = 1, \cdots, d-1$. Hence for every nonzero polynomial $f(x) \in E[x]$ with degree less than d, $f(A)v \neq 0$, and then $f(A) \neq O_n$ as an operator on W where O_n denotes the zero matrix in $\mathcal{M}_{n\times n}(E)$, which means the minimal polynomial of A acting on W has degree at least d. There is a linear dependence relation on the set $v, Av, \cdots, A^dv$, and the coefficient of A^dv in the relation must be nonzero since the other vectors are linearly independent. We can make the coefficient of A^dv to be 1, say

$$A^dv + c_{d-1}A^{d-1}v + \cdots + c_1Av + c_0v = \mathbf{0}$$

where $c_i \in E$, $i = 0, 1, \cdots, d-1$. This tells us the polynomial

$$m(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$$

satisfies $m(A)v = \mathbf{0}$, so for every $f(x) \in E[x]$ we have $m(A)f(A)v = f(A)m(A)v = f(A)\mathbf{0} = \mathbf{0}$. Since every element in W is $f(A)v$ for some $f(x)$, so $m(A)$ annihilates all the elements in W. Thus $m(A)$ is just the minimal polynomial of A acting on W. Incidentally, this also shows $\dim W = d$ and W has basis $v, Av, \cdots, A^{d-1}v$. Set $W_1 = W$ and $m_1(x) = m(x)$. If $W_1 \neq V$, pick a column vector $v_2 \notin W_1$ and run through the same argument for the subspace W_2 of V spanned by the vectors $\{v_2, Av_2, A^2v_2, \cdots\}$ to get a minimal polynomial $m_2(x)$ for A on W_2. Since $v_2 \notin W_1$, $\dim(W_1 + W_2) > \dim W_1$. If $W_1 + W_2 \neq V$, proceed this procedure. Since V is finite-dimensional, eventually we will get a sequence of subspaces $W_1, W_2, \cdots, W_k$ where $A(W_i) \subseteq W_i$ for $i = 1, \cdots, k$ and $W_1 + \cdots + W_k = V$. Then the minimal polynomial of A on V is the least common multiple of $m_1(x), \cdots, m_k(x)$ from Proposition 4.

2.2 Diffusion Layers

The diffusion layers in block ciphers and hash functions are essentially $\mathbb{F}_2$-linear transformations, so sometime we just call them linear transformations or just diffusion matrices.

Now we present the definitions of the branch numbers.

Definition 1 (Differential Branch Number). *Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion matrix for certain positive integers b and n. The differential branch number of L is defined as*

$$\mathcal{B}_d(L) = \min_{\boldsymbol{x}\in\mathbb{F}_2^{bn},\boldsymbol{x}\neq\mathbf{0}} \{w_b(\boldsymbol{x}) + w_b(L(\boldsymbol{x}))\},$$

where each bundle of vectors in $\mathbb{F}_2^{bn}$ is in $\mathbb{F}_2^b$ and $L(\boldsymbol{x}) = \boldsymbol{x}L$ if we write $\boldsymbol{x}$ as a row vector in $\mathbb{F}_2^{bn}$.

Definition 2 (Linear Branch Number). *Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion matrix for certain positive integers b and n. The linear branch number of L is defined as*

$$\mathcal{B}_l(L) = \min_{\boldsymbol{x}\in\mathbb{F}_2^{bn},\boldsymbol{x}\neq\mathbf{0}} \{w_b(\boldsymbol{x}) + w_b(L^T(\boldsymbol{x}))\},$$

where each bundle of vectors in $\mathbb{F}_2^{bn}$ is in $\mathbb{F}_2^b$ and L^T is the transposition of L and $L^T(\boldsymbol{x}) = \boldsymbol{x}L^T$ if we write $\boldsymbol{x}$ as a row vector in $\mathbb{F}_2^{bn}$.

The larger the branch numbers are, the stronger the diffusion layer is against differential and linear cryptanalyses.

We may consider the branch numbers from the viewpoint of coding theory. It is not hard to verify that the set $\{(\boldsymbol{x}, \boldsymbol{x}L)|\boldsymbol{x} \in \mathbb{F}_2^{bn}\}$ is a $\mathbb{F}_2$-linear code with length $2bn$, namely, a $\mathbb{F}_2$-linear subspace of $\mathbb{F}_2^{2bn}$. Let C_L denote this code. The dimension of C_L is bn and a standard generator matrix of it is $(I_{bn}\ \ L)$ where I_{bn} is the identity matrix in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$. Then it is easy to discover that $\mathcal{B}_d(L)$ is equal to the minimum bundle weight of all nonzero codewords in C_L while $\mathcal{B}_l(L)$ is equal to the minimum bundle weight of all nonzero codewords in the dual code of C_L. Unfortunately, if we only regard C_L as a $\mathbb{F}_2$-linear code with length $2bn$ over $\mathbb{F}_2$, it is hard to handle the bundle weight or bundle distance explicitly. Therefore, in [5] M. Blaum et al. treated C_L as a $\mathbb{F}_2$-linear group code over $\mathbb{F}_2^b$ with length $2n$ and dimension bn. With this notion, it is clear that the differential branch number of L is just equal to the minimum distance d of C_L. From coding theory, we know $d \leq 2n - \log_{2^b} |C_L| + 1 = n + 1$ which is called the Singleton bound (see [18]). The codes attaining the Singleton bound are called maximum distance separable (MDS) codes. So the diffusion layers attaining this bound are also called MDS and they are the optimal primitives in cryptosystems.

Definition 3 (MDS Diffusion Layer). *Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion matrix for certain positive integers b and n where b is the length of bundles. Then L is called a MDS diffusion layer if $\mathcal{B}_d(L) = n + 1$.*

In the rest of this subsection, we recall some previous results useful for this paper. The proofs of these results are similar to those about the ordinary MDS linear codes.

The result of [5] may be redescribed as the following proposition.

Proposition 5. *Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion matrix for certain positive integers b and n where b is the length of bundles. Suppose L is divided into n^2 blocks such that*

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

where $L_{i,j} \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, $i, j = 1, \cdots, n$. Then L is MDS if and only if every submatrix of L consisting of some of these blocks is nonsingular.

Proposition 6 ([9])**.** *A linear diffusion layer D has a maximum differential branch number if and only if it has a maximum linear branch number.*

2.3 Equivalence Relation

For two sets X and Y, a relation from X to Y is a subset $R \subseteq X \times Y$. If $(x, y) \in R$, we say y is R-related to x and usually write xRy. Especially, if $X = Y$, we call R a relation on X.

Suppose R is a relation on a set X. Then we call R an equivalence relation if it has the following three properties.

- reflexivity: for every $x \in X$, xRx;
- symmetry: for all $x, y \in X$, xRy implies yRx;
- transitivity: for all $x, y, z \in X$, xRy and yRz imply xRz.

And in this case, we usually say x is equivalent to y if xRy. For $a \in X$, the subset of X consisting of all the element equivalent to a is called an equivalence class containing a and is usually denoted by $\overline{a}$ or $[a]$.

For a set X, $\{A_i\}_{i\in I}$ is a collection of subsets of it. Then $\{A_i\}_{i\in I}$ is called a partition of X if $A_i \cap A_j = \emptyset$ for all $i \neq j$ and $\cup_{i\in I} A_i = X$.

Actually, every equivalence relation on a set X corresponds to a partition of X.

Proposition 7 ([21])**.** *If "$\equiv$" is an equivalence relation on a set X, then the equivalence classes form a partition of X. Conversely, given a partition $\{A_i : i \in I\}$ of X, there is an equivalence relation on X whose equivalence classes are the blocks A_i.*

3 Our Strategy for Constructing MDS Block Diffusion Matrices

In this section, we present our method for constructions a sort of MDS diffusion layers.

First of all, we state a lemma about block matrices that is often treated as an exercise in the textbooks of matrix theory. Because it is not very trivial and for completeness of this paper, we give the proof of this lemma here.

Lemma 1. *Let F be a field, $L \in \mathcal{M}_{bn\times bn}(F)$ be a block matrix for some positive integers b and n such that*

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

where $L_{i,j} \in \mathcal{M}_{b\times b}(F)$, $i, j = 1, \cdots, n$ and they commute pairwise. Then

$$\det(L) = \det\left(\sum (-1)^{\tau(i_1 i_2 \cdots i_n)+\tau(j_1 j_2 \cdots j_n)} L_{i_1,j_1} L_{i_2,j_2} \cdots L_{i_n,j_n}\right), \tag{1}$$

where $\det(L)$ denotes the determinant of L, the sum on the right side consists of all the products of n blocks having distinct row indices and distinct column indices and a sign, $\tau(i_1 i_2 \cdots i_n)$ denotes the number of inverse-ordered pairs in the permutation $(i_1 i_2 \cdots i_n)$ where an inverse-ordered pair is a pair whose number on the left side is larger than its number on the right side. In other words, if we let

$$\det_s(L) = \sum (-1)^{\tau(i_1 i_2 \cdots i_n)+\tau(j_1 j_2 \cdots j_n)} L_{i_1,j_1} L_{i_2,j_2} \cdots L_{i_n,j_n}, \tag{2}$$

which is the determinant of the block matrix L if we regard all of its blocks $L_{i,j}$, $i, j = 1, \cdots, n$ as entries and regard L as a $(n \times n)$ matrix (we call $\det_s(L)$ the symbolic determinant of L), then

$$\det(L) = \det(\underset{s}{\det}(L)).$$

Proof. To prove $\det(L) = \det(\det_s(L))$, we use induction on n.

In case when $n = 1$, we do not need to prove anything.

To clarify the general case, we illustrate the case when $n = 2$ for simplicity. When $n = 2$,

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix}. \tag{3}$$

From the multiplication of block matrices, we get

$$\begin{pmatrix} I_b & O_b \\ -L_{2,1} & I_b \end{pmatrix} \begin{pmatrix} I_b & O_b \\ O_b & L_{1,1} \end{pmatrix} \begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix} = \begin{pmatrix} L_{1,1} & L_{1,2} \\ O_b & L_{1,1}L_{2,2} - L_{1,2}L_{2,1} \end{pmatrix}, \tag{4}$$

where I_b denotes the identity matrix in $\mathcal{M}_{b\times b}(F)$ and O_b denotes the zero matrix in $\mathcal{M}_{b\times b}(F)$. By calculating the determinants of both sides of equation (4) we get

$$\det(L_{1,1}) \det(L) = \det(L_{1,1}) \det(L_{1,1}L_{2,2} - L_{1,2}L_{2,1}). \tag{5}$$

If $\det(L_{1,1}) \neq 0$, the equation (1) is proved immediately. If $\det(L_{1,1}) = 0$, we have to use a trick. Specifically, we can regard L as a matrix over the polynomial ring $F[x]$ where x is an indeterminant of F and substitute $xI_b + L_{1,1}$ for $L_{1,1}$ in L. From this viewpoint, equation (5) becomes

$$\det(xI_b + L_{1,1}) \det(L) = \det(xI_b + L_{1,1}) \det((xI_b + L_{1,1})L_{2,2} - L_{1,2}L_{2,1}). \tag{6}$$

Note that $\det(xI_b + L_{1,1})$, $\det(L)$, $\det(xI_b + L_{1,1})$ and $\det((xI_b + L_{1,1})L_{2,2} - L_{1,2}L_{2,1})$ all become polynomials in $F[x]$ now. Obviously, $\det(xI_b + L_{1,1}) \neq 0$, so

$$\det(L) = \det((xI_b + L_{1,1})L_{2,2} - L_{1,2}L_{2,1}). \tag{7}$$

If two polynomials are equal, their corresponding coefficients are equal too. So if we assign $x = 0$ in the equation (7), we prove the equation (1) in case when $n = 2$.

Now we suppose equation (1) is true for $1, 2, \cdots, n-1$. From the multiplication of block matrices, we get

$$\begin{pmatrix} I_b & O_b & \cdots & O_b \\ -L_{2,1} & I_b & \cdots & O_b \\ \cdots & \cdots & \ddots & \cdots \\ -L_{n,1} & O_b & \cdots & I_b \end{pmatrix} \begin{pmatrix} I_b & O_b & \cdots & O_b \\ O_b & L_{1,1} & \cdots & O_b \\ \cdots & \cdots & \ddots & \cdots \\ O_b & O_b & \cdots & L_{1,1} \end{pmatrix} L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ O_b & & & \\ \vdots & & A & \\ O_b & & & \end{pmatrix}, \tag{8}$$

where $A \in \mathcal{M}_{b(n-1)\times b(n-1)}(F)$. Let U, V, W denote

$$\begin{pmatrix} I_b & O_b & \cdots & O_b \\ -L_{2,1} & I_b & \cdots & O_b \\ \cdots & \cdots & \ddots & \cdots \\ -L_{n,1} & O_b & \cdots & I_b \end{pmatrix}, \begin{pmatrix} I_b & O_b & \cdots & O_b \\ O_b & L_{1,1} & \cdots & O_b \\ \cdots & \cdots & \ddots & \cdots \\ O_b & O_b & \cdots & L_{1,1} \end{pmatrix}, \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ O_b & & & \\ \vdots & & A & \\ O_b & & & \end{pmatrix}$$

respectively. Then we can write the equation (8) as $UVL = W$. On one hand, by taking symbolic determinant of both sides of $UVL = W$, we get

$$\det_s(UVL) = \det_s(W). \tag{9}$$

From the definition of symbolic determinant, we can easily get

$$\det_s(UVL) = \det_s(U)\det_s(V)\det_s(L). \tag{10}$$

Thus we have

$$\det_s(U)\det_s(V)\det_s(L) = \det_s(W). \tag{11}$$

By computing the symbolic determinants of the both sides of equation (11), we get

$$L_{1,1}^{n-1}\det_s(L) = L_{1,1}\det_s(A). \tag{12}$$

Then by taking the determinants of both sides of equation (12), we have

$$\det(L_{1,1})^{n-1}\det(det_s(L)) = \det(L_{1,1})\det(\det_s(A)). \tag{13}$$

On the other hand, by directly taking the determinants of both sides of $UVL = W$, we get

$$\det(U)\det(V)\det(L) = \det(UVL) = \det(W). \tag{14}$$

By computing the determinants of both sides of equation (14), we have

$$\det(L_{1,1})^{n-1}\det(L) = \det(L_{1,1})\det(A). \tag{15}$$

From the induction hypothesis, we know $\det(\det_s(A)) = \det(A)$. Thus,

$$\det(L_{1,1})^{n-1} \det(\det_s(L)) = \det(L_{1,1})^{\,n-1} \det(L). \tag{16}$$

If $\det(L_{1,1}) \neq 0$, we get $\det(\det_s(L)) = \det(L)$, and the equation (1) is proved immediately. If $\det(L_{1,1}) = 0$, we just need to use the same technique as in case when $n = 2$. Specifically, we also regard L as a matrix over the polynomial ring $F[x]$ where x is an indeterminant of F and substitute $xI_b + L_{1,1}$ for $L_{1,1}$ in L. Finally, by assigning $x = 0$, we complete the proof of equation (1).

□

Remark 1. *Another expression of the determinant of L often arises in many papers, that is*

$$\det(L) = \det\left(\sum_{\sigma \in S_n} (-1)^{\tau(\sigma(1)\sigma(2)\cdots\sigma(n))} L_{1,\sigma(1)} L_{2,\sigma(2)} \cdots L_{n,\sigma(n)}\right), \tag{17}$$

where S_n is the symmetric group on n elements. It is easy to see that equation (17) is just a special case of equation (1), because in equation (17) the permutation of row indices is $(12\cdots n)$ and $\tau(12\cdots n) = 0$.

Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion matrix for certain positive integers b and n where b is the length of bundles, and L be divided into n^2 blocks such that

$$L = \begin{pmatrix} L_{1,1} & L_{1,2} & \cdots & L_{1,n} \\ L_{2,1} & L_{2,2} & \cdots & L_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ L_{n,1} & L_{n,2} & \cdots & L_{n,n} \end{pmatrix}$$

where $L_{i,j} \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, $i, j = 1, \cdots, n$. From Proposition 5, in order to judge whether L is MDS, we need to check the determinants of all the submatrices of L composed of some of these blocks. If one wants to calculate these determinants by Lemma 1, all of the blocks $L_{i,j}$, $i, j = 1, 2, \cdots, n$, need to commute pairwise. But pairwise commutativity is such a high requirement that most sets of matrices cannot meet it. Therefore, in this paper, we focus on a specific sort of matrices whose blocks are all polynomials of a certain primitive block. In detail, we only consider such a situation when each block $L_{i,j}$, $i, j = 1, 2, \cdots, n$ of the diffusion matrices is a polynomial in certain $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$. In [25] and [26], M. Sajadieh et al. and S. Wu et al. also mentioned this situation. In comparison with their strategies, ours has such advantages:

- They just discussed the recursive diffusion layers, while we consider more general diffusion layers as well as recursive ones.
- They just found out the conditions for MDS diffusion layers but didn't point out how to construct the building primitive A (denoted by L in their papers), while we figure out not only the conditions for MDS diffusion matrices but also the constructions of A explicitly.
- We use some techniques to increase the efficiency of search algorithms.

In this section and following sections, we will explain the advantages of our method.

As mentioned in the previous paragraphs, we will focus on the block diffusion layers whose blocks are all polynomials in certain block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$. Let each block $L_{i,j} = f_{i,j}(A)$, where $f_{i,j}(x) \in \mathbb{F}_2[x]$, $i, j = 1, 2, \cdots, n$. In this paper, we call the polynomial matrix

$$\begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$$

the external matrix of L. For MDS property, we need to check every determinant of the submatrices consisting of some of the blocks of the diffusion matrix. Of course, we can conventionally calculate these determinants. Alternatively, we may calculate them with Lemma 1 because all of the blocks are obviously pairwise commutative. For example, to calculate the determinant of the submatrix

$$B = \begin{pmatrix} L_{1,1} & L_{1,2} & L_{1,3} \\ L_{2,1} & L_{2,2} & L_{2,3} \\ L_{3,1} & L_{3,2} & L_{3,3} \end{pmatrix},$$

we may work out the symbolic determinant $\det_s(B)$ firstly, and then calculate $\det(\det_s(B))$. Note that $\det_s(B)$ is also a polynomial in A. Actually, the symbolic determinant of every submatrix consisting of those blocks is a polynomial in A. This is an important clue for us. Actually, if we know the minimal polynomial of A, there is a more efficient technique to determine whether such submatrices are nonsingular. Let us look at the following lemma.

Lemma 2. *Let F be a field, $A \in \mathcal{M}_{b\times b}(F)$, $m_A(x)$ be the minimal polynomial of A in the polynomial ring $F[x]$, $g(x) \in F[x]$. Then* $\det(g(A)) \neq 0$ *if and only if* $\mathrm{GCD}(g(x), m_A(x)) = 1$, *where* $\mathrm{GCD}(g(x), m_A(x))$ *denotes the greatest common divisor of $g(x)$ and $m_A(x)$.*

Proof. To begin with, if the greatest common divisor of a family of polynomials is equal to 1, we say they are coprime.

Suppose $g(A)$ is nonsingular. Assume $\mathrm{GCD}(g(x), m_A(x)) = d(x)$ and $\deg(d) > 1$. Then there exists $u(x), v(x) \in F[x]$ such that $g(x) = u(x)d(x)$, $m_A(x) = v(x)d(x)$. Consequently, we have $g(A) = u(A)d(A)$, $m_A(A) = v(A)d(A)$. From $O_b = m_A(A) = v(A)d(A)$ and $\deg(v) < \deg(m_A)$, we get $v(A) \neq O_b$. And then we get $d(A)$ is singular, otherwise $v(A)$ would be equal to O_b. Because $g(A) = u(A)d(A)$ and $g(A)$ is nonsingular, we get $d(A)$ is nonsingular. A contradiction! Thus, $\mathrm{GCD}(g(x), m_A(x))$ must be 1.

Conversely, suppose $\mathrm{GCD}(g(x), m_A(x)) = 1$. Then there exists $u(x), v(x) \in F[x]$ such that $g(x)u(x) + m_A(x)v(x) = 1$. If we assign $x = A$, we get $g(A)u(A) = I_b$. Thus $g(A)$ is nonsingular. □

As mentioned before, the symbolic determinant of every submatrix consisting of those blocks of the diffusion matrix L is a polynomial in A. From Lemma 2, instead of calculating the determinant of every such submatrix, we present a new technique: to judge whether such a submatrix is nonsingular, the only thing we need to do is to calculate the symbolic determinant and to check whether the symbolic determinant (treated as a polynomial in x)

is coprime with $m_A(x)$. For example, for a submatrix of L

$$H = \begin{pmatrix} I_b & A \\ I_b + A & I_b + A^2 \end{pmatrix},$$

we firstly calculate $det_s(H) = I_b + A$, and then check whether $\mathrm{GCD}(1 + x, m_A(x)) = 1$. It is faster than calculating the determinant of H directly. However, one should note that in order to exploit this technique, we have to know the minimal polynomial of A in advance. This is not a trivial task. Meanwhile our goal is to definitely obtain a series of MDS diffusion layers which requires us to clearly figure out the building block A. In other words, we need a matrix $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ together with its minimal polynomial $m_A(x) \in \mathbb{F}_2[x]$.

To show our main guideline and avoid getting into the complicated situation too early, we merely consider a special case in this section, namely, when the minimal polynomial of the primitive block is irreducible in $\mathbb{F}_2[x]$, and leave the general case to Section 4. For example, suppose

$$g(x) = a_0 + a_1 x + \cdots + a_{b-1}x^{b-1} + x^b$$

is a monic irreducible polynomial in $\mathbb{F}_2[x]$. Then the companion matrix of $g(x)$ is

$$A = \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ & & & -a_1 \\ & I_{b-1} & & \vdots \\ & & & -a_{b-1} \end{pmatrix}$$

(of course we know $-a_i = a_i$ here). It is well known that $g(x)$ is just the characteristic polynomial of A in $\mathbb{F}_2[x]$. From Hamilton-Cayley theorem ([23]), we know $g(A) = O_b$. Then $m_A(x) \mid g(x)$. But $g(x)$ has only two monic factors, namely 1 and $g(x)$ itself, and 1 is surely not the annihilator polynomial of any matrix. So $g(x)$ must be the minimal polynomial of A in $\mathbb{F}_2[x]$. Hence, we have attained a matrix $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ together with its irreducible minimal polynomial $m_A(x) \in \mathbb{F}_2[x]$.

When the minimal polynomial of a primitive block A is irreducible in $\mathbb{F}_2[x]$, it is obvious that a polynomial $f(x) \in \mathbb{F}_2[x]$ is coprime with $m_A(x)$ if and only if $f(x) \not\equiv 0 \mod m_A(x)$. Hence, we get an easier way to check whether a polynomial in A is nonsingular: for a polynomial $f(x) \in \mathbb{F}_2[x]$, $f(A)$ is nonsingular if and only if $f(x) \not\equiv 0 \mod m_A(x)$. From the above statement, for a given primitive block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ whose minimal polynomial $m_A(x)$ is irreducible in $\mathbb{F}_2[x]$, the external matrices of MDS diffusion matrices L are just determined by $m_A(x)$ but not by A itself or b. More Specifically, if $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ and $A' \in \mathcal{M}_{b'\times b'}(\mathbb{F}_2)$ are two primitive blocks having the same irreducible minimal polynomial, the polynomial matrix

$$\begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$$

makes

$$\begin{pmatrix} f_{1,1}(A) & f_{1,2}(A) & \cdots & f_{1,n}(A) \\ f_{2,1}(A) & f_{2,2}(A) & \cdots & f_{2,n}(A) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(A) & f_{n,2}(A) & \cdots & f_{n,n}(A) \end{pmatrix}$$

MDS if and only if it makes

$$\begin{pmatrix} f_{1,1}(A') & f_{1,2}(A') & \cdots & f_{1,n}(A') \\ f_{2,1}(A') & f_{2,2}(A') & \cdots & f_{2,n}(A') \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(A') & f_{n,2}(A') & \cdots & f_{n,n}(A') \end{pmatrix}$$

MDS.

In summary of the above statements, now we present Algorithm 1 that can find out all MDS diffusion matrices L such that

- $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ for the given parameters b and n;
- L can be divided to n^2 blocks and each block $L_{i,j} \in M_{b\times b}(\mathbb{F}_2)$ is a polynomial in a given primitive block $A \in M_{b\times b}(\mathbb{F}_2)$ whose minimal polynomial is an irreducible polynomial in $\mathbb{F}_2[x]$.

In Algorithm 1, from Step 7 to Step 32 we intend to check all the matrices $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ whose entries are polynomials in A but not 0. Note that because $m_A(x) = g(x)$, all polynomials in A are in the sense of modulo $g(x)$. At an algebraic standpoint, we consider these entries in the quotient ring $\frac{\mathbb{F}_2[x]}{<g(x)>}$ where $< g(x) >$ denotes the ideal generated by $g(x)$. Since $\mathbb{F}_2[x]$ is a primary ideal domain and $g(x)$ is an irreducible element in $\mathbb{F}_2[x]$, $< g(x) >$ is a maximal ideal of $\mathbb{F}_2[x]$. Consequently, $\mathbb{F}_2[x]/< g(x) >$ is a field and actually isomorphic to $\mathbb{F}_{2^m}$ where m is the degree of $g(x)$. From Step 10 to Step 32, our aim is to check whether the determinant of every square submatrix of a fixed matrix L_1 is nonzero. Here, to improve the efficiency, we make use of another technique which was already mentioned in [12]. In order to make sure all the square submatrices of L_1 is nonsingular, we might check them one by one. For example, we might firstly check 1 $(n \times n)$ submatrices of L_1 and secondly check $\binom{n}{n-1}^2$ $((n-1)\times(n-1))$ submatrices and go on. There are $\binom{n}{r}^2$ $(r \times r)$ submatrices for each r and totally

$$\sum_{r=1}^{n} \binom{n}{r}^2 = \binom{2n}{n} - 1$$

submatrices of L_1. The number of these submatrices is too large. Therefore, in this paper, we do not check them one by one. Instead, we firstly check the $(n \times n)$ submatrices of L_1. For each $(n \times n)$ submatrices (of course there is only 1 such submatrix), if it passes the test, we will compute the inverse of it (by means of elementary operations) and check all the entries of the inverse matrix. This is because for an $(n \times n)$ nonsingular matrix B, $B^{-1} = \frac{1}{\det(B)} B^*$ where

$$B^* = \begin{pmatrix} B_{1,1} & B_{2,1} & \vdots & B_{n,1} \\ B_{1,2} & B_{2,2} & \vdots & B_{n,2} \\ \vdots & \vdots & \vdots & \vdots \\ B_{1,n} & B_{2,n} & \vdots & B_{n,n} \end{pmatrix}$$

and each $B_{i,j}$ is equal to the product of $(-1)^{i+j}$ and the minor determinant derived from B by removing the i-th row and the j-th column. Similarly, we can check all the $((n-3)\times(n-3))$

Algorithm 1 Search for MDS Diffusion Matrices 1

Input: two integers $b, n \in \mathbb{Z}^+$, a matrix $A \in M_{b\times b}(\mathbb{F}_2)$ together with its irreducible minimal polynomial $g(x) \in \mathbb{F}_2[x]$.

Output: some polynomial matrices, an integer k.

define an integer k and $k \leftarrow 0$;
define a set $PS(m) := \{h(x) \in \mathbb{F}_2[x] \mid h(x) \neq 0, \deg(h) < m\}$ where $m = \deg(\mathrm{g})$;
define a matrix $L \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and $L \leftarrow O_n$;
define an integer r and $r \leftarrow 0$;
define $f(x) \in \frac{\mathbb{F}_2[x]}{<g(x)>}$ and $f(x) \leftarrow 0$;
print "The $(n \times n)$-size external matrices of MDS diffusion matrices in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ are:";
for $L \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ where $L_{i,j} \in PS(m)$, $i, j = 1, \cdots, n$ **do**
  turn L into $L_1 \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]/< g(x) >)$ by a ring homomorphism $\eta : \mathbb{F}_2[x] \rightarrow \mathbb{F}_2[x]/< g(x) >$ such that $\eta(h(x)) = h(x) + < g(x) >$;
  $r \leftarrow n$;
  while $r \geq 2$ **do**
    define a matrix $B \in \mathcal{M}_{r\times r}(\mathbb{F}_2[x]/< g(x) >)$ and $B \leftarrow O_r$;
    for B runs over all the $(r \times r)$-size submatrices of L_1 **do**
      $f(x) \leftarrow \det(B)$;
      if $f(x) = 0$ **then**
        goto Step 31;
      else
        if $r \geq 3$ **then**
          compute B^{-1};
          for $f(x)$ runs over all the entries of B^{-1} **do**
            if $f(x) = 0$ **then**
              goto Step 31;
            end if
          end for
        end if
      end if
    end for
    $r \leftarrow r - 2$;
  end while
  print L;
  $k \leftarrow k + 1$;
  switch to the next L;
end for
print "where $x = A$.";
print "There are k such MDS diffusion matrices.".

submatrices along with all the $((n-2)\times(n-2))$ submatrices. This technique benefits from a fact that elementary operations are much faster than calculating determinants. On Step 36, we mean the diffusion matrices can be obtained by assigning the primitive block A to x for each entry of the output polynomial matrices. Moreover, as mentioned in Section 2, two similar matrices have the same minimal polynomial. Thus, in fact, we may assign x with $P^{-1}AP$ for every nonsingular matrix $P \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$.

4 Our Strategy for a More Generalized Case

In Section 3, we explained our strategy to find out a sort of MDS diffusion layers for the fixed parameters and presented an algorithm. Note that we assumed a condition there: the minimal polynomial of the primitive block A in $\mathbb{F}_2[x]$ is irreducible. Subsequently, that case is virtually identical to looking for MDS diffusion matrices in $\mathcal{M}_{n\times n}(\mathbb{F}_{2^m})$. But, in practice, it is not true for most matrices because matrix rings contain zero divisors (see [21], page 573). How many matrices in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$ have irreducible minimal polynomials? Let us figure out the proportion with the following lemma.

Lemma 3. *Let $A \in \mathcal{M}_{b\times b}(\mathbb{F}_q)$, $m_A(x)$ be the minimal polynomial of A in $\mathbb{F}_q[x]$. Then $m_A(x)$ is irreducible in $\mathbb{F}_q[x]$ if and only if $A \in \mathbb{F}_{q^b}$.*

Proof. Let $f(x)$ denote the characteristic polynomial of A. Then $\deg(f) = b$ where $\deg(f)$ denotes the degree of $f(x)$.

Suppose $m_A(x)$ be irreducible in $\mathbb{F}_q[x]$. Let $\deg(m_A) = d$ and $\mathbb{F}_q(\alpha)$ denote the smallest extension field of $\mathbb{F}_q$ that includes α. Then, from field theory,

$$\mathbb{F}_q(A) \cong \mathbb{F}_q[x]/< m_A(x) > = \mathbb{F}_{q^d}$$

where "$\cong$" means "isomorphic to" and $< m_A(x) >$ is the ideal generated by $m_A(x)$. Because $f(x)$ is the characteristic polynomial of A, $f(A) = O_b$ from Hamilton-Cayley theorem. Then $m_A(x) \mid f(x)$ from Proposition 1. Meanwhile, according to Proposition 3, $f(x)$ is necessarily a power of $m_A(x)$. Consequently, $d \mid b$. And it is followed by $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^b}$. Thus, $A \in \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^b}$.

Conversely, suppose $A \in \mathbb{F}_{q^b}$. Assume $m_A(x)$ is reducible in $\mathbb{F}_q[x]$. Then there exists two polynomials $u(x), v(x) \in \mathbb{F}_q[x]$ such that $m_A(x) = u(x)v(x)$ and $\deg(u) < \deg(m_A)$ and $\deg(u) < \deg(m_A)$. Because $m_A(x)$ is the minimal polynomial of A, $u(A) \neq 0$ and $v(A) \neq 0$. But $u(A)v(A) = m_A(A) = 0$. It is a contradiction since any field does not contain zero divisors. Thus $m_A(x)$ must be irreducible in $\mathbb{F}_q[x]$. □

From Lemma 3, the number of matrices in $\mathcal{M}_{b\times b}(\mathbb{F}_q)$ whose minimal polynomials are irreducible in $\mathbb{F}_q[x]$ is q^b, while the cardinality of $\mathcal{M}_{b\times b}(\mathbb{F}_q)$ is q^{b^2}. The proportion is too small. If we only focus on those primitive blocks whose minimal polynomials are irreducible in $\mathbb{F}_2[x]$, we will miss a large amount of MDS candidates. Therefore, in this section, we will remove this condition and consider a more generalized case: the minimal polynomial of the primitive block A is reducible in $\mathbb{F}_2[x]$.

Just as in Section 3, we also suppose every block of the diffusion matrix $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ is a polynomial of certain primitive block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$. Then every minor determinant of L consisting of its blocks is equal to the determinant of a polynomial in A. In Section 3, for every polynomial $f(x) \in \mathbb{F}_2[x]$, $f(A)$ is nonsingular if and only if $f(x) \not\equiv 0 \mod m_A(x)$

because $m_A(x)$ is irreducible in $\mathbb{F}_2[x]$. Now, in this section, we suppose $m_A(x)$ is reducible in $\mathbb{F}_2[x]$. Then we can get the standard factorization of $m_A(x)$ by Berlekamp's algorithm ([4]). Suppose

$$m_A(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s}$$

is the standard factorization of $m_A(x)$ where $p_1(x), \cdots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$. From Lemma 2, for a polynomial $f(x) \in \mathbb{F}_2[x]$, $f(A)$ is nonsingular if and only if $\mathrm{GCD}(f(x), m_A(x)) = 1$. Then, in this case, $\mathrm{GCD}(f(x), m_A(x)) = 1$ if and only if $\mathrm{GCD}(f(x), p_i(x)) = 1$ for $i = 1, \cdots, s$. Moreover, because each $p_i(x)$ is irreducible in $\mathbb{F}_2[x]$, we only need to check whether $f(x) \equiv 0 \mod p_i(x)$ for $i = 1, \cdots, s$. From an algebraic viewpoint, for a polynomial $f(x) \in \mathbb{F}_2[x]$, $f(A)$ is a nonsingular matrix in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$ if and only if $f(x)$ is a invertible element in the fields $\mathbb{F}_2[x]/< p_i(x) >$ for $i = 1, \cdots, s$. Therefore, for a external matrix

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}\left(\mathbb{F}_2[x]/< m_A(x) >\right),$$

if we want to argue whether $H(A)$ is an MDS block matrix with block size $(b \times b)$, what we need to do is just to regard $H(x)$ as a matrix over $\mathbb{F}_2[x]/< p_i(x) >$, $i = 1, \cdots, s$ and check whether it is MDS over these field respectively. From the above statement and Lemma 2, we have the following theorem.

Theorem 1. *Let $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ with the minimal polynomial $m_A(x) \in \mathbb{F}_2[x]$. Suppose $m_A(x)$ has the standard factorization*

$$m_A(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s},$$

where $p_1(x), \cdots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$ and $e_1, \cdots, e_s$ are positive integers. Let

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]).$$

Then the following three statements are equivalent.

1. *$H(A)$ is an MDS block matrix with block size $(b \times b)$;*
2. *every minor determinant of $H(x)$ is coprime with $m_A(x)$;*
3. *every minor determinant of $H(x)$ is coprime with $p_i(x)$ for $i = 1, \cdots, n$.*

From the discussion above and in Section 3, for a given primitive block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, the external matrices of MDS diffusion matrices $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ are absolutely determined by $m_A(x)$ but not by A itself or b, no matter whether $m_A(x)$ is reducible or not. We formally state this conclusion in the following theorem.

Theorem 2. *Suppose $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ and $A' \in \mathcal{M}_{b'\times b'}(\mathbb{F}_2)$ are two primitive blocks having the same minimal polynomial. Then the external matrix*

$$\begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$$

makes

$$\begin{pmatrix} f_{1,1}(A) & f_{1,2}(A) & \cdots & f_{1,n}(A) \\ f_{2,1}(A) & f_{2,2}(A) & \cdots & f_{2,n}(A) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(A) & f_{n,2}(A) & \cdots & f_{n,n}(A) \end{pmatrix} \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$$

be an MDS diffusion matrix if and only if it makes

$$\begin{pmatrix} f_{1,1}(A') & f_{1,2}(A') & \cdots & f_{1,n}(A') \\ f_{2,1}(A') & f_{2,2}(A') & \cdots & f_{2,n}(A') \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(A') & f_{n,2}(A') & \cdots & f_{n,n}(A') \end{pmatrix} \in \mathcal{M}_{b'n\times b'n}(\mathbb{F}_2)$$

be an MDS diffusion matrix.

For a matrix $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ and a polynomial matrix

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]),$$

let us think about two kinds of elementary operations on $H(x)$, namely, interchanging two rows (or columns) and multiplying a row (or a column) with a polynomial $g(x) \in \mathbb{F}_2[x]$ coprime to $m_A(x)$. If we obtain another polynomial matrix $H'(x) \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ from $H(x)$ via interchanging two rows (or columns) of $H(x)$, according to the properties of determinants, we know every minor determinant $D'(x)$ of $H'(x)$ is equal to certain minor determinant $D(x)$ of $H(x)$ multiplied by 1 or -1. If $D(x)$ is coprime to $m_A(x)$, $D'(x)$ is coprime to $m_A(x)$ obviously. Thus interchanging two rows (or columns) of $H(x)$ does not change MDS property of it. Likewise, if we multiply a row (or a column) of $H(x)$ with a polynomial $g(x) \in \mathbb{F}_2[x]$ coprime to $m_A(x)$, every minor determinant $D'(x)$ of obtained polynomial matrix $H'(x)$ will be equal to certain minor determinant $D(x)$ of $H(x)$ multiplied by $g(x)$. If $D(x)$ is coprime to $m_A(x)$, $D'(x) = D(x)g(x)$ must be coprime to $m_A(x)$ since $g(x)$ is also coprime to $m_A(x)$. So multiplying a row (or a column) with a polynomial $g(x) \in \mathbb{F}_2[x]$ coprime to $m_A(x)$ does not change MDS property of $H(x)$ either. By contrast, the third kind of elementary operation on matrices, namely, adding a row (or column) multiplied by a polynomial to another row (or column) cannot retain MDS property of $H(x)$, because it might make some entries become zero. However, we discover another operation on $H(x)$ that is a little similar to the third kind of elementary operation mentioned above and can retain MDS property of $H(x)$. Let us clarify this kind of operation in the following theorem.

Theorem 3. *Let A be a matrix in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$ with the minimal polynomial $m_A(x) \in \mathbb{F}_2[x]$. Suppose the standard factorization of $m_A(x)$ in $\mathbb{F}_2[x]$ is*

$$m_A(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s},$$

where $p_1(x), \cdots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$ and $e_1, \cdots, e_s$ are positive integers. Let

$$g(x) = p_1(x)p_2(x)\cdots p_s(x).$$

Let

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$$

and

$$H'(x) = H(x) + g(x) \begin{pmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ h_{n,1}(x) & h_{n,2}(x) & \cdots & h_{n,n}(x) \end{pmatrix},$$

where

$$\begin{pmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ h_{n,1}(x) & h_{n,2}(x) & \cdots & h_{n,n}(x) \end{pmatrix}$$

is any polynomial matrix in $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$. In other words, every (i,j)-th entry of $H'(x)$ is equal to $f_{i,j}(x) + g(x)h_{i,j}(x)$, $i,j = 1, \cdots, n$. Then $H(A)$ is MDS if and only if $H'(A)$ is MDS.

Proof. Obviously, the transformation from $H(x)$ to $H'(x)$ is invertible. So we only need to prove MDS property of $H(A)$ implies MDS property of $H'(A)$.

Suppose $H(A)$ is MDS. According to Theorem 1, what we need to do is to prove every minor determinant of $H'(x)$ is coprime to $p_i(x)$ for $i = 1, \cdots, s$. Without loss of generality, let us think of a square submatrix $M'(x)$ of $H'(x)$ obtained by choosing the i-th rows for $i = 1, \cdots, m$ and the j-th columns for $j = 1, \cdots, m$ of $H'(x)$, where m is a positive integer and $m \leq n$. Then

$$\det(M'(x)) = \begin{vmatrix} f_{1,1}(x) + g(x)h_{1,1}(x) & f_{1,2}(x) + g(x)h_{1,2}(x) & \cdots & f_{1,m}(x) + g(x)h_{1,m}(x) \\ f_{2,1}(x) + g(x)h_{2,1}(x) & f_{2,2}(x) + g(x)h_{2,2}(x) & \cdots & f_{2,m}(x) + g(x)h_{2,m}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{m,1}(x) + g(x)h_{m,1}(x) & f_{m,2}(x) + g(x)h_{m,2}(x) & \cdots & f_{m,m}(x) + g(x)h_{m,m}(x) \end{vmatrix}.$$

According to the properties of determinant, we may write $\det(M'(x))$ as the sum of a series of m-order determinants. More specifically, for every $j = 1, \cdots, m$, we can split the j-th column of $\det(M'(x))$ into two columns

$$\begin{pmatrix} f_{1,j}(x) \\ f_{2,j}(x) \\ \vdots \\ f_{m,j}(x) \end{pmatrix}$$

and

$$\begin{pmatrix} g(x)h_{1,j}(x) \\ g(x)h_{2,j}(x) \\ \vdots \\ g(x)h_{m,j}(x) \end{pmatrix}.$$

Finally, $\det(M'(x))$ can be written as the sum of 2^m determinants. For instance, one of these determinants is

$$\begin{vmatrix} g(x)h_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) \\ g(x)h_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,m}(x) \\ \cdots & \cdots & \cdots & \cdots \\ g(x)h_{m,1}(x) & f_{m,2}(x) & \cdots & f_{m,m}(x) \end{vmatrix},$$

which is equal to

$$g(x)\begin{vmatrix} h_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) \\ h_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,m}(x) \\ \cdots & \cdots & \cdots & \cdots \\ h_{m,1}(x) & f_{m,2}(x) & \cdots & f_{m,m}(x) \end{vmatrix}.$$

Obviously, all of these 2^m determinants are multiples of $g(x)$ expect one determinant, namely,

$$\begin{vmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,m}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{m,1}(x) & f_{m,2}(x) & \cdots & f_{m,m}(x) \end{vmatrix}.$$

Let $M(x)$ denote the submatrix

$$\begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,m}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,m}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{m,1}(x) & f_{m,2}(x) & \cdots & f_{m,m}(x) \end{pmatrix}.$$

Then

$$\det(M'(x)) = \det(M(x)) + g(x)q(x), \tag{18}$$

where $q(x) \in \mathbb{F}_2[x]$. Since $H(A)$ is MDS, $\det(M(x))$ is coprime to $p_i(x)$ for $i = 1, \cdots, s$. Thus, $\det(M'(x))$ is also coprime to $p_i(x)$ for $i = 1, \cdots, s$ because $g(x)$ is a multiple of $p_i(x)$ for $i = 1, \cdots, s$. Similarly, every minor determinant of $H'(x)$ is coprime to $p_i(x)$ for $i = 1, \cdots, s$. Therefore, $H'(A)$ is MDS according to Theorem 1. □

Remark 2. *Theorem 3 gives us an approach to construct new MDS diffusion matrices from a fixed MDS matrix. Obviously, it is useless to the case when the multiplicity of every irreducible factor of $m_A(x)$ is 1 (including the case when $m_A(x)$ is irreducible in $\mathbb{F}_2[x]$). In this case, $g(x) = m_A(x)$. Then for every entry $f_{i,j}(x)$ of $H(x)$, $f_{i,j}(A) + g(A)h_{i,j}(A)$ has no difference from $f_{i,j}(A)$. But it does make sense when there exists a irreducible factor of $H(x)$ having a multiplicity greater than 1. In this case, the approach coming from Theorem 3 can give us at least $2^l - 1$ extra options for every entry of the external matrix of an MDS block matrix, where $l = \deg(m_A) - \deg(g)$. In detail, if $H(A)$ is MDS, for every entry $f_{i,j}(x)$*

of the external matrix of $H(A)$, we may randomly pick a polynomial $h_{i,j} \in \mathbb{F}_2[x]$ such that $\deg(\mathrm{h_{i,j}}) < \deg(\mathrm{m_A}) - \deg(\mathrm{g})$ and substitute $f_{i,j}(x) + g(x)h_{i,j}(x)$ for $f_{i,j}(x)$. This kind of operation on $H(x)$ does not alter MDS property of $H(A)$. Furthermore, as mentioned in the proof of Theorem 3, the transformation from $H(x)$ to $H'(x)$ is invertible. Let γ denote the binary relation on the set $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ such that for two matrices $H(x)$ and $H'(x)$ in $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$, $H(x)$ is γ-related to $H'(x)$ if there exists a matrix

$$\begin{pmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ h_{n,1}(x) & h_{n,2}(x) & \cdots & h_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$$

making

$$H'(x) = H(x) + g(x) \begin{pmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n}(x) \\ h_{2,1}(x) & h_{2,2}(x) & \cdots & h_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ h_{n,1}(x) & h_{n,2}(x) & \cdots & h_{n,n}(x) \end{pmatrix}.$$

It is easy to check γ is an equivalence relation (a relation holding reflexivity, symmetry and transitivity). So we can partition $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ into equivalence classes by γ. And according to Theorem 3, if one polynomial matrix $H(x)$ makes $H(A)$ MDS, every polynomial matrix $H'(x)$ in the same class as $H(x)$'s makes $H'(A)$ MDS. In other words, MDS property is an invariant on every equivalence class obtained from γ. Besides, from the definition of the relation γ, it is not hard to calculate the numbers of equivalence classes obtained from it. We merely need to consider the entries of external matrices as the residues with respect to modulo $\mod g(x)$. Thus, there are totally $2^{\deg(g)\cdot n^2}$ equivalence classes obtained from γ. If we restrict the degree of entries of external matrices to a range $[0, \deg(m_A) - 1]$ (regard every entry as a residue modulo $m_A(x)$), the cardinality of every equivalence class is $2^{l\cdot n^2}$ where $l = \deg(m_A) - \deg(g)$. Therefore, if we want to search for all the external matrices of MDS matrices (or a part of them), we may only take the representatives of the equivalence classes obtained form γ into account. And this approach will greatly reduce the amount of search when $2^{l\cdot n^2}$ is large. In practice, the less nonzero entries a diffusion matrix has, the more efficient implementation it has. As the Hamming weight of a sequence, we may extend the notion of Hamming weight to matrices. For a matrix $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$, we define its Hamming weight $w_H(L)$ as the number of its nonzero entries. Then for a matrix $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ and a polynomial matrix

$$H(x) = \begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & \cdots & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & \cdots & f_{2,n}(x) \\ \cdots & \cdots & \cdots & \cdots \\ f_{n,1}(x) & f_{n,2}(x) & \cdots & f_{n,n}(x) \end{pmatrix} \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]),$$

obviously

$$w_H(H(A)) = \sum_{i,j=1}^{n} w_H(f_{i,j}(A)).$$

So, if we need a diffusion matrix with a Hamming weight as small as possible, we may manage to reduce the Hamming weight of each block $f_{i,j}(A)$, $i, j = 1, \cdots, n$ respectively. With respect

to a equivalence class obtained from γ, we can choose the one with the smallest Hamming weight from

$$\{f_{i,j}(A) + g(A)h_{i,j}(A) \mid h_{i,j}(x) \in \mathbb{F}_2[x], \deg(h) < \deg(m_A) - \deg(g)\}$$

for each (i,j), $i,j = 1, \cdots, n$, and then we will get the most efficient diffusion matrix in this equivalence class.

From Theorem 3 and Remark 2, we have the following corollary.

Corollary 1. *Let A be a matrix in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$ with the minimal polynomial $m_A(x) \in \mathbb{F}_2[x]$. Suppose the standard factorization of $m_A(x)$ in $\mathbb{F}_2[x]$ is*

$$m_A(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_s(x)^{e_s},$$

where $p_1(x), \cdots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$ and $e_1, \cdots, e_s$ are positive integers. Let

$$g(x) = p_1(x)p_2(x)\cdots p_s(x).$$

Let γ be the binary relation defined in Remark 2 on the set $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$. And let $MDSEM_{n\times n}(\mathbb{F}_2[x], A)$ denote the set

$$\{H(x) \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]) \mid H(A) \text{ is } MDS\}.$$

Then γ is an equivalence relation on the set $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and partition $\mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ into $2^{\deg(g)\cdot n^2}$ equivalence classes. Moreover, $MDSEM_{n\times n}(\mathbb{F}_2[x], A)$ is the union of some of the equivalence classes obtained from γ.

In summary of the above statements, now we present Algorithm 2 that can find out all the MDS diffusion matrices L such that

- $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ for given parameters b and n;
- L can be divided to n^2 blocks and each block $L_{i,j} \in M_{b\times b}(\mathbb{F}_2)$ is a polynomial in given primitive block $A \in M_{b\times b}(\mathbb{F}_2)$.

Algorithm 2 is similar to Algorithm 1. We modify several steps. And it is easy to find out the reasons from the above explanations. On Step 39, like the situation in Algorithm 1, we may actually assign x with $P^{-1}AP$ for every nonsingular matrix $P \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$.

4.1 Some Experimental Results

We conduct our experiment with MAGMA (version 2.19-9) on a computer whose hardware and software conditions are listed in Table 1.

We search with Algorithm 2 for parameters $b = 8$ and $n = 4$. We choose the primitive block

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{8\times 8}(\mathbb{F}_2)$$

Algorithm 2 Search for MDS Diffusion Matrices 2

Input: two integers $b, n \in \mathbb{Z}^+$, a matrix $A \in M_{b\times b}(\mathbb{F}_2)$ together with its minimal polynomial $m(x) \in \mathbb{F}_2[x]$, $m(x)$'s standard factorization $m(x) = p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_s(x)^{e_s}$ in $\mathbb{F}_2[x]$, $g(x) = p_1(x)p_2(x)\cdots p_s(x)$.

Output: some polynomial matrices, an integer k.

1: define an integer k and $k \leftarrow 0$;
2: $d := \deg(g)$;
3: define a set $PS(d) := \{h(x) \in \mathbb{F}_2[x] \mid \deg(h) < d, \mathrm{GCD}(h(x), p_i(x)) = 1, \forall i = 1, \cdots, s\}$;
4: define a matrix $L \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and $L \leftarrow O_n$;
5: define an integer r and $r \leftarrow 0$;
6: define $f_i(x) \in \mathbb{F}_2[x]/ < p_i(x) >$ and $f_i(x) \leftarrow 0$, $i = 1, \cdots, s$;
7: print "The $(n \times n)$-size external matrices of MDS diffusion matrices in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ are:";
8: **for** $L \in \mathcal{M}_{n\times n}(PS(d))$ **do**
9: **for** $i = 1, \cdots, s$ **do**
10: turn L into $L_i \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]/ < p_i(x) >)$ by a ring homomorphism $\eta : \mathbb{F}_2[x] \rightarrow \mathbb{F}_2[x]/ < p_i(x) >$ such that $\eta(h(x)) = h(x) + < p_i(x) >$;
11: $r \leftarrow n$;
12: **while** $r \geq 2$ **do**
13: define a matrix $B \in \mathcal{M}_{r\times r}(\mathbb{F}_2[x]/ < p_i(x) >)$ and $B \leftarrow O_r$;
14: **for** B runs over all the $(r \times r)-$size submatrices of L_i **do**
15: $f_i(x) \leftarrow \det(B)$;
16: **if** $f_i(x) = 0$ **then**
17: goto Step 34;
18: **else**
19: **if** $r \geq 3$ **then**
20: compute B^{-1};
21: **for** $f_i(x)$ runs over all the entries of B^{-1} **do**
22: **if** $f_i(x) = 0$ **then**
23: goto Step 34;
24: **end if**
25: **end for**
26: **end if**
27: **end if**
28: **end for**
29: $r \leftarrow r - 2$;
30: **end while**
31: **end for**
32: print L;
33: $k \leftarrow k + 1$;
34: switch to the next L;
35: **end for**
36: print "where $x = A$.";
37: print "There are k such MDS diffusion matrices.".

Table 1: Computer Hardware and Software

processor	Intel Xeon E5620 @ 2.40GHz
RAM	DDR3, 32G, 2133.4MHz
operation system	Windows 7, 64 bit

with the minimal polynomial $m_A(y) = (y^4 + y + 1)^2 \in \mathbb{F}_2[y]$. Then

$$g(y) = \frac{m_A(y)}{\mathrm{GCD}(m_A(y), m'_A(y))} = y^4 + y + 1,$$

where $m'_A(y)$ denotes the derivative of $m_A(y)$. We want to find out the external matrices of MDS matrices. If we really searched all external matrices in $\mathcal{M}_{4\times n}(\mathbb{F}_2[y])$ whose entries are in the sense of modulo $g(y)$, we would have to check $15^{16} = 6568408355712890625$ polynomial matrices (we omit those matrices at least one of whose entries is 0). It is too large! We do not have a supercomputer to handle such computations. So we restrict ourselves to only four variable entries and just search the external matrices having the form

$$\begin{pmatrix} 1 & y & 1+y & y^2 \\ y^2 & 1+y & y & 1 \\ f_{3,1}(y) & f_{3,2}(y) & f_{3,3}(y) & f_{3,4}(y) \\ f_{3,4}(y) & f_{3,1}(y) & f_{3,2}(y) & f_{3,3}(y) \end{pmatrix} \in \mathcal{M}_{4\times 4}(\mathbb{F}_2[x])$$

where $f_{3,1}(y), f_{3,2}(y), f_{3,3}(y)f_{3,4}(y)$ are in the sense of modulo $g(y)$. Hence we only need to check $15^4 = 50625$ external matrices.

After running a series of MAGMA codes, we find out 1395 external matrices of MDS diffusion matrices. And it takes 10.920 seconds. We list a part of these candidates in Appendix A (note that we just list the third rows of them).

Note that we are searching for the representatives of equivalence classes obtained from the equivalence relation γ mentioned in Remark 2. If we treat the entries of external matrices as residues modulo $m_A(y)$, every equivalence class contains $(2^4)^{16} = 2^{64}$ polynomial matrices. For example, the external matrix

$$H(y) = \begin{pmatrix} 1 & y & 1+y & y^2 \\ y^2 & 1+y & y & 1 \\ y^2+1 & 1 & y^2+y & y^2+y \\ y^2+y & y^2+1 & 1 & y^2+y \end{pmatrix}$$

makes $H(A)$ MDS according to our experiment. Then the equivalence class of $H(y)$ contains all the polynomial matrices having the form

$$H(y) + g(y) \begin{pmatrix} h_{1,1}(y) & h_{1,2}(y) & h_{1,3}(y) & h_{1,4}(y) \\ h_{2,1}(y) & h_{2,2}(y) & h_{2,3}(y) & h_{2,4}(y) \\ h_{3,1}(y) & h_{3,2}(y) & h_{3,3}(y) & h_{3,4}(y) \\ h_{4,1}(y) & h_{4,2}(y) & h_{4,3}(y) & h_{4,4}(y) \end{pmatrix}$$

where $h_{i,j} \in \mathbb{F}_2[y]$, $\deg(h_{i,j}) < 4$ or $h_{i,j}(y) = 0$ for $i = 1, 2, 3, 4$ and $j = 1, 2, 3, 4$. All of these external matrices are MDS when assigning A to y.

5 Constructing Recursive MDS Diffusion Layers with Our Strategy

In section, we discuss the constructions of recursive diffusion layers with our method.

As mentioned in section 1, recursive diffusion layers are a sort of diffusion layers with high efficiency because they make use of LFSRs. Let $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ be a diffusion layer for certain positive integers b and n where b is the length of bundles, then L is recursive if there exists n matrices (or $\mathbb{F}_2-$linear transformations) $B_1, \cdots, B_n \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ such that for every input row vector $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$, the corresponding output row vector $\boldsymbol{y} = (\boldsymbol{y}_1, \cdots, \boldsymbol{y}_n)$ is just the $(n+1)$-th state vector of the linear recursive sequence that has the relation

$$\begin{aligned} \boldsymbol{x}_{l+n+1} &= B_1(\boldsymbol{x}_{l+1}) + B_2(\boldsymbol{x}_{l+2}) + \cdots + B_n(\boldsymbol{x}_{l+n}) \\ &= \boldsymbol{x}_{l+1}B_1 + \boldsymbol{x}_{l+2}B_2 + \cdots + \boldsymbol{x}_{l+n}B_n \end{aligned} \tag{19}$$

and the initial state vector $\boldsymbol{x} = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$. In other words, if we input $(\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$ to the LFSR with the relation (19), we will take $(\boldsymbol{x}_{n+1}, \cdots, \boldsymbol{x}_{2n})$ as the output vector of the diffusion layer L. If we express this procedure by matrices, we can define a matrix

$$B = \begin{pmatrix} O_b & \cdots & O_b & B_1 \\ I_b & \cdots & O_b & B_2 \\ \vdots & \ddots & \vdots & \vdots \\ O_b & \cdots & I_b & B_n \end{pmatrix} \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$$

where $B_1, \cdots, B_n \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, O_b denotes the zero matrix in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$ and I_b denotes the identity matrix in $\mathcal{M}_{b\times b}(\mathbb{F}_2)$. Then it is easy to get the diffusion matrix $L = B^n$. We name $B_1, \cdots, B_n \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$ the recursive coefficient matrices after the common recursive coefficients in a certain field. Note that the first block column of L is

$$\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}.$$

Thus at least we need $B_1, \cdots, B_n$ to be nonsingular if we want a MDS diffusion matrix.

In [25] and [26], the authors talked about several recursive diffusion layers whose recursive coefficient matrices are all polynomials in certain primitive block (denoted by L in their papers). But they just gave the sufficient and necessary conditions for those diffusion layers being MDS without talking about the construction of the primitive block in detail. Obviously, if every recursive coefficient matrix is a polynomial in certain primitive block $A \in \mathcal{M}_{b\times b}(\mathbb{F}_2)$, every block of the received diffusion matrix will be a polynomial in A too. So those diffusion layers discussed in [25] and [26] are merely special cases of the situation discussed in Section 3 and 4. Consequently, we may construct recursive diffusion matrices with our strategy.

In summary of the above statements, now we present Algorithm 3 that can find out all the MDS recursive diffusion matrices L such that

- $L \in \mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ for the given parameters b and n;
- L can be divided to n^2 blocks and each block $L_{i,j} \in M_{b\times b}(\mathbb{F}_2)$, $i, j = 1, \cdots, n$;

Algorithm 3 Search for Recursive MDS Diffusion Matrices

Input: two integers $b, n \in \mathbb{Z}^+$, a matrix $A \in M_{b\times b}(\mathbb{F}_2)$ together with its minimal polynomial $m(x) \in \mathbb{F}_2[x]$, $m(x)$'s standard factorization $m(x) = p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_s(x)^{e_s}$ in $\mathbb{F}_2[x]$, $g(x) = p_1(x)p_2(x)\cdots p_s(x)$.

Output: some polynomial matrices, an integer k.

1: define an integer k and $k \leftarrow 0$;
2: $d := \deg(g)$;
3: define a set $PS(d) := \{h(x) \in \mathbb{F}_2[x] \mid \deg(h) < d, \mathrm{GCD}(h(x), p_i(x)) = 1, \forall i = 1, \cdots, s\}$;
4: define $L \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and $L \leftarrow O_n$;
5: define $B_1(x), \cdots, B_n(x) \in \mathbb{F}_2[x]$ and $B_1(x) \leftarrow 0, \cdots, B_n(x) \leftarrow 0$;
6: define a matrix $B \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x])$ and $B \leftarrow O_n$;
7: define an integer r and $r \leftarrow 0$;
8: define $f_i(x) \in \mathbb{F}_2[x]/ < p_i(x) >$ and $f_i(x) \leftarrow 0$, $i = 1, \cdots, s$;
9: print "The $(n \times n)$ round external matrices of MDS recursive diffusion matrices in $\mathcal{M}_{bn\times bn}(\mathbb{F}_2)$ are:";
10: **for** $(B_1(x), \cdots, B_n(x))$ run over $PS(d)^n$ **do**
11: $B \leftarrow \begin{pmatrix} O_b & \cdots & O_b & B_1 \\ I_b & \cdots & O_b & B_2 \\ \vdots & \ddots & \vdots & \vdots \\ O_b & \cdots & I_b & B_n \end{pmatrix}$;
12: $L \leftarrow B^n$;
13: **for** $i = 1, \cdots, s$ **do**
14: turn L into $L_i \in \mathcal{M}_{n\times n}(\mathbb{F}_2[x]/ < p_i(x) >)$ by a ring homomorphism $\eta : \mathbb{F}_2[x] \to \mathbb{F}_2[x]/ < p_i(x) >$ such that $\eta(h(x)) = h(x) + < p_i(x) >$;
15: **for** $f_i(x)$ runs over all the entries of L_i **do**
16: **if** $f_i(x) = 0$ **then**
17: goto Step 43;
18: **end if**
19: **end for**
20: $r \leftarrow n$;
21: **while** $r \geq 2$ **do**
22: define a matrix $H \in \mathcal{M}_{r\times r}(\mathbb{F}_2[x]/ < p_i(x) >)$ and $H \leftarrow O_r$;
23: **for** H runs over all the $(r \times r)$ submatrices of L_i **do**
24: $f_i(x) \leftarrow \det(H)$;
25: **if** $f_i(x) = 0$ **then**
26: goto Step 43;
27: **else**
28: **if** $r \geq 3$ **then**
29: compute H^{-1};
30: **for** $f_i(x)$ runs over all the entries of H^{-1} **do**
31: **if** $f_i(x) = 0 \mod p_i(x)$ **then**
32: goto Step 43;
33: **end if**
34: **end for**
35: **end if**
36: **end if**
37: **end for**
38: $r \leftarrow r - 2$;
39: **end while**
40: **end for**
41: print B;
42: $k \leftarrow k + 1$;
43: switch to the next $(B_1(x), \cdots, B_n(x))$;
44: **end for**
45: print "where $x = A$.";
46: print "There are k such MDS diffusion matrices.".

- every recursive coefficient matrix is a polynomial in given primitive block $A \in M_{b\times b}(\mathbb{F}_2)$.

Note that every matrix output by Algorithm 3 is a matrix corresponding to each round of the diffusion layer but not the diffusion matrix itself.

5.1 Some Experimental Results

We conduct our experiment with MAGMA (version 2.19-9) on a computer whose hardware and software conditions are listed in Table 1.

We search with Algorithm 3 for parameters $b = 8$ and $n = 6$. We choose the primitive block

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_{8\times 8}(\mathbb{F}_2)$$

with the minimal polynomial $m_A(y) = (y^4 + y + 1)^2 \in \mathbb{F}_2[y]$. Then

$$g(y) = \frac{m_A(y)}{\mathrm{GCD}(m_A(y), m'_A(y))} = y^4 + y + 1,$$

where $m'_A(y)$ denotes the derivative of $m_A(y)$. We want to find out the round external matrices

$$B(y) = \begin{pmatrix} 0 & \cdots & 0 & B_1(y) \\ 1 & \cdots & 0 & B_2(y) \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & B_6(y) \end{pmatrix} \in \mathcal{M}_{6\times 6}(\mathbb{F}_2[y])$$

of recursive MDS matrices, where $\deg(B_i) < 4$ for $i = 1, \cdots, 6$. So we need to check $15^6 = 11390625$ external matrices totally.

After running a series of MAGMA codes, we find out 180 external matrices of recursive MDS matrices. And it takes 5373.766 seconds. We list all the round external matrices in Appendix B (note that we just list the transpose of the 6th columns of them).

Similar to Section 4.1, we just search for the representatives of equivalence classes obtained from the equivalence relation γ. And it is easy to generate the whole equivalence class of each representative with the method mentioned in Remark 2.

6 Conclusion

In this paper, we propose a new method to verify a sort of MDS diffusion block matrices whose blocks are all polynomials in a certain primitive block over the finite field $\mathbb{F}_2$. And then we discover a new kind of transformations that can retain MDS property of diffusion matrices and generate a series of new MDS matrices from a given one. Moreover, we get an equivalence relation from this kind of transformation. And MDS property is an invariant with

respect to this equivalence relation which can greatly reduce the amount of computation when we search for MDS matrices. With this method, we list a series of MDS diffusion matrices for some specific parameters. Finally, we discuss MDS recursive diffusion layers with our method and extend the results of the corresponding work of FSE 2012 and SAC 2012. We expect that our proposal will be helpful in designing the diffusion layers of block ciphers and hash functions.

References

[1] D. Augot, M. Finiasz. Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes. FSE 2014. To appear.

[2] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, T. Yaçin. Block Ciphers - Focus on the Linear Layer (feat. PRIDE)*. CRYPTO 2014, Part I, LNCS, vol. 8616, pp. 57-76, Springer, 2014.

[3] E. Biham, A. Shamir. Differential Cryptanalysis of DES-Like Cryptosystems. CRYPTO '90, LNCS, vol. 537, pp. 2-21, Springer, 1991.

[4] E. R. Berlekamp. Algebraic Coding Theory. McGraw-Hill, 1968.

[5] M. Blaum, R. M. Roth. On Lowest Density MDS Codes. IEEE Transactions on Information Theory, vol. 45(1), pp. 46-59, 1999.

[6] T. P. Berger. Constructions of Recursive MDS Diffusion Layers from Gabidulin Codes. INDOCRYPT 2013, LNCS, vol. 8250, pp. 274-285, Springer, 2013.

[7] F. Chabaud, S. Vaudenay. Links between Differential and Linear Crytanalysis. EUROCRYPT '94, LNCS, vol. 950, pp. 356-365, Springer, 1995.

[8] K. Conrad. The Minimal Polynomial and Some Applications. http://www.math.uconn.edu/ kconrad/blurbs/linmultialg/minpolyandappns.pdf

[9] J. Daemen, V. Rijmen. The Design of Rijndael AES - The Advanced Encryption Standard. Springer, 2002.

[10] J. Guo, T. Peyrin, A. Poschmann. The PHOTON Family of Lightweight Hash Functions. CRYPTO 2011, LNSC, vol. 6841, pp. 222-239, Springer, 2011.

[11] K. C. Gupta, I. G. Ray. On Constructions of Involutory MDS Matrices. AFRICACRYPT 2013, LNCS, vol. 7918, pp. 43-60, Springer, 2013.

[12] K. C. Gupta, I. G. Ray. On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography. CD-ARES 2013 Workshops, LNCS, vol. 8128, pp. 29-43, Springer, 2013.

[13] P. Junod, S. Vaudenay. Perfect Diffusion Primitive for Block Ciphers. SAC 2004, LNCS, vol. 3357, pp. 84-99, Springer, 2004.

[14] D. C. Lay. Linear Algebra and Its Applications, Fourth Edition. Pearson Education, 2012.

[15] J. Lacan, J. Fimes. Systematic MDS Erasure Codes Based on Vandermonde Matrices. IEEE Trans. Commun. Lett., vol 8(9), pp. 570-572, 2004.

[16] R. Lidl and H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.

[17] S. Ling, C. Xing. Coding Theory A First Course. Cambridge University Press, 2004.

[18] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. North-Holland Publishing Company, 1977.

[19] M. Matsui. Linear Cryptanalysis Method for DES Cipher. EUROCRYPT '93, LNCS, vol. 765, pp. 386-397, Springer, 1994.

[20] J. Nakahara Jr., E. Abrahao. A New Involutory MDS Matrix for the AES. International Journal of Network Security, vol. 9(2), pp. 109-116, National Chung Hsing University, 2009.

[21] J. J. Rotman. Advanced Modern Algebra. Prentice Hall, 2003.

[22] D. Serre. Matrices Theory and Applications. Springer-Verlag, 2002.

[23] G. Strang. Linear Algebra and Its Applications, Fourth Edition. Cengage Learning, 2005.

[24] M. Sajadieh, M. Dakhilalian, H Mala, B. Omoomi. On Construction of Involutory MDS Matrices from Vandermond Matrices in $GF(2^q)$. Des. Codes Cryptogr., vol. 64, pp. 287-308, Springer, 2012.

[25] M. Sajadieh, M. Dakhilalian, H. Mala, P. Sepehrdad. Recursive Diffusion Layers for Block Ciphers and Hash Functions. FSE 2012, LNCS, vol. 7549, pp. 385-401, Springer, 2012.

[26] S. Wu, M. Wang, W. Wu. Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions. SAC 2012, LNCS, vol. 7707, pp. 355-371, Springer, 2013.

[27] A. M. Youssef, S. Mister, S. E. Tavares. On the Design of Linear Transformations for Substitute Permutation Encryption Networks. SAC'97, pp. 1-9, 1997.

Appendices

A

$[y^2+y, y^2+y, y^3+y^2+y, 1]$, $[y^2+y, y^2+y, y^3+y^2+y+1, y^2+1]$, $[y^2+y, y^2+y, y^3+y^2+y+1, y^2]$,
$[y^2+y, y^2+y, y^3+1, y^3+y]$, $[y^2+y, y^2+y, y^3+1, y^2+y+1]$, $[y^2+y, y^2+y, 1, y^3+y^2+y]$,
$[y^2+y, y^2+y, 1, y^3+y^2+y+1]$, $[y^2+y, y^2+y, 1, y^2+1]$, $[y^2+y, y^3+y^2+y, y^2+y, y^3+y^2+1]$,

$[y^2+y, y^3+y^2+y, y^2+y, y^2+y+1]$, $[y^2+y, y^3+y^2+y, y^3+y^2+y, y]$, $[y^2+y, y^3+y^2+$
$y, y^3+y^2+y, 1]$, $[y^2+y, y^3+y^2+y, y^3+y^2+y+1, 1]$, $[y^2+y, y^3+y^2+y, y^3+y+1, y]$,
$[y^2+y, y^3+y^2+y, y^3+y+1, y^2+1]$, $[y^2+y, y^3+y^2+y, y^3+y+1, 1]$, $[y^2+y, y^3+y^2+y, y^3, y^2+1]$,
$[y^2+y, y^3+y^2+y, 1, 1]$, $[y^2+y, y, y^2+y, y^3+y^2+y]$, $[y^2+y, y, y^2+y, y^3+1]$, $[y^2+y, y, y^3+y^2+$
$y, y]$, $[y^2+y, y, y^3+y^2+y, 1]$, $[y^2+y, y, y^2, y^2+1]$, $[y^2+y, y, y^2+y+1, y^2+y]$, $[y^2+y, y, y^3, y^2+1]$,
$[y^2+y, y, y^3, 1]$, $[y^2+y, y^3+y^2+y+1, y^2+y, y^3+y^2+y]$, $[y^2+y, y^3+y^2+y+1, y^2+y, y^2]$,
$[y^2+y, y^3+y^2+y+1, y^2+y, y^3+1]$, $[y^2+y, y^3+y^2+y+1, y^2+1, y]$, $[y^2+y, y^3+y^2+$
$y+1, y^2, y^3+y^2]$, $[y^2+y, y^3+y^2+y+1, y^2, y^2]$, $[y^2+y, y^3+y^2+y+1, y^2, y^2+y+1]$,
$[y^2+y, y^3+y^2+y+1, y^3, y^3+y^2+y+1]$, $[y^2+y, y^3+y^2+y+1, y^3+1, y^3+y^2+y]$,
$[y^2+y, y^3+y^2+1, y^3+y^2+1, y]$, $[y^2+y, y^3+y^2+1, y^3+y^2+1, y^2+y+1]$, $[y^2+y, y^3+y^2+$
$1, y^3+y+1, y^2+y+1]$, $[y^2+y, y^3+y^2+1, y^3, y^3+y^2+1]$, $[y^2+y, y+1, y^2+y, y^3+y^2+y]$,
$[y^2+y, y+1, y^2+y, y^3+y^2+1]$, $[y^2+y, y+1, y^2+1, y^3+y^2+y]$, $[y^2+y, y+1, y^3+y^2+1, y^2+1]$,
$[y^2+y, y+1, y^2+y+1, y^3+y^2+y]$, $[y^2+y, y+1, y^3+1, y^3+y^2+y]$, $[y^2+y, y+1, 1, y^3+y^2+y+1]$,
$[y^2+y, y^3+y, y^2+y, y^3+y^2+y]$, $[y^2+y, y^3+y, y^2+y, y^3+y^2]$, $[y^2+y, y^3+y, y^2+y, y^2]$,
$[y^2+y, y^3+y, y^2+y, 1]$, $[y^2+y, y^3+y, y^3+y^2+y, y^3+y^2+y]$, $[y^2+y, y^3+y, y^2, y^3+y^2+1]$,
$[y^2+y, y^3+y, y^2+y+1, y^2]$, $[y^2+y, y^3+y, y^3, y^3+y^2]$, $[y^2+y, y^3+y, y^3, y^3+y^2+1]$,
$[y^2+y, y^3+y, y^3, y^3+1]$, $[y^2+y, y^3+y, 1, y^3+y^2+y]$, $[y^2+y, y^3+y, 1, y^3+y^2+y+1]$,
$[y^2+y, y^3+y, 1, 1]$, $[y^2+y, y^2+y+1, y^2+y, y^2]$, $[y^2+y, y^2+y+1, y^3+y^2+y, y^2]$, $[y^2+$
$y, y^2+y+1, y^3+y^2+y+1, y^2+1]$, $[y^2+y, y^2+y+1, y^3+y^2+y+1, y^3+y]$, $[y^2+y, y^2+y+$
$1, y^2+y+1, y]$, $[y^2+y, y^2+y+1, y^2+y+1, y^3+y^2+1]$, $[y^2+y, y^2+y+1, y^2+y+1, y^2]$,
$[y^2+y, y^2+y+1, y^3+1, y^3+y]$, $[y^2+y, y^2+y+1, y^3+1, y^2+y+1]$, $[y^2+y, y^3, y^3+y^2+y, y^2]$,
$[y^2+y, y^3, y^2+1, y^3+y]$, $[y^2+y, y^3, y^3+y^2+1, y]$, $[y^2+y, y^3, y^3+y^2+1, y^2]$, $[y^2+y, y^3, y^3+y+$
$1, y^2]$, $[y^2+y, y^3, y^3+y+1, y^2+y+1]$, $[y^2+y, y^3, y^3+1, y^2+y]$, $[y^2+y, y^3+1, y^2+y, y^3+y^2+1]$,
$[y^2+y, y^3+1, y^2+y, y^2]$, $[y^2+y, y^3+1, y^2+y, y^3+y]$, $[y^2+y, y^3+1, y^3+y+1, y^3+1]$,
$[y^2+y, y^3+1, y^2+y+1, y^2+y]$, $[y^2+y, y^3+1, y^2+y+1, y]$, $[y^2+y, y^3+1, y^2+y+1, y^2]$,
$[y^2+y, y^3+1, y^3+1, y^3+y]$, $[y^2+y, y^3+1, 1, y^3+y^2]$, $[y^2+y, 1, y^2+y, y^3+y^2+y+1]$,
$[y^2+y, 1, y^2+y, y^3+y^2]$, $[y^2+y, 1, y^2+y, y^3+y^2+1]$, $[y^2+y, 1, y^2+y, y^2]$, $[y^2+y, 1, y^2+1, y^2+y]$,
$[y^2+y, 1, y^2+1, y^3+y^2+1]$, $[y^2+y, 1, y^2+1, y^3+y]$, $[y^2+y, 1, y^2, y^3+y^2]$, $[y^2+y, 1, y^3+y+1, 1]$,
$[y^3+y^2+y, y^2+y, y^2+y, 1]$, $[y^3+y^2+y, y^2+y, y^3+y^2+y, y^2+1]$, $[y^3+y^2+y, y^2+y, y^3+y^2+y, y+$
$1]$, $[y^3+y^2+y, y^2+y, y^3+y^2+y, 1]$, $[y^3+y^2+y, y^2+y, y, y^3+y^2+y]$, $[y^3+y^2+y, y^2+y, y, y^2+1]$,
$[y^3+y^2+y, y^2+y, y, y^3+y+1]$, $[y^3+y^2+y, y^2+y, y^3+y^2, y^3+y^2+y+1]$, $[y^3+y^2+y, y^2+$
$y, y^3+y^2+1, y^2+y]$, $[y^3+y^2+y, y^3+y^2+y, y^2+y, y]$, $[y^3+y^2+y, y^3+y^2+y, y^2+y, 1]$,
$[y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^2]$, $[y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^3]$, $[y^3+y^2+y, y^3+$
$y^2+y, y^3+y^2, y^3+1]$, $[y^3+y^2+y, y^3+y^2+y, y^2, y^3+y^2]$, $[y^3+y^2+y, y^3+y^2+y, y^3, y^2+1]$,
$[y^3+y^2+y, y^3+y^2+y, y^3, y^3+1]$, $[y^3+y^2+y, y, y^2+y, y]$, $[y^3+y^2+y, y, y^2+y, 1]$,
$[y^3+y^2+y, y, y^3+y^2+y, y^2+1]$, $[y^3+y^2+y, y, y, y^2+1]$, $[y^3+y^2+y, y, y, y+1]$, $[y^3+y^2+$
$y, y, y, y^3+y+1]$, $[y^3+y^2+y, y, y^2, y^2+1]$, $[y^3+y^2+y, y, y^3, y^3+1]$, $[y^3+y^2+y, y, y^3, 1]$,
$[y^3+y^2+y, y^3+y^2, y^3+y^2+y, y^3+y^2+y+1]$, $[y^3+y^2+y, y^3+y^2, y^3+y^2+y, y^2+1]$,
$[y^3+y^2+y, y^3+y^2, y^3+y^2+y, y+1]$, $[y^3+y^2+y, y^3+y^2, y^3+y^2+y, y^3]$, $[y^3+y^2+y, y^3+y^2, y^2+$
$1, y^3+y^2+y+1]$, $[y^3+y^2+y, y^3+y^2, y^3+y^2+1, y^3+y^2]$, $[y^3+y^2+y, y^3+y^2, y^3+1, y^3+y^2+y]$,
$[y^3+y^2+y, y^3+y^2, y^3+1, y+1]$, $[y^3+y^2+y, y^3+y^2, y^3+1, 1]$, $[y^3+y^2+y, y^2, y^3+y^2+y, y]$,
$[y^3+y^2+y, y^2, y^3+y^2+y, y+1]$, $[y^3+y^2+y, y^2, y^3+y^2, y^3+y^2]$, $[y^3+y^2+y, y^2, y^3+y^2+1, y^3+y^2]$,
$[y^3+y^2+y, y^2, y^3+y^2+1, y^3+y+1]$, $[y^3+y^2+y, y^2, y^3+y^2+1, y^3+1]$, $[y^3+y^2+y, y^2, y^2, y^3+y^2]$,
$[y^3+y^2+y, y^2, y^2, y^3+y+1]$, $[y^3+y^2+y, y^2, y^3+y, y^3+1]$, $[y^3+y^2+y, y^2, y^3, y^3+y^2]$,
$[y^3+y^2+y, y+1, y^3+y^2+1, y]$, $[y^3+y^2+y, y+1, y+1, y]$, $[y^3+y^2+y, y+1, y+1, y^3+y+1]$,

$[y^3+y^2+y, y+1, y^3+y, y+1]$, $[y^3+y^2+y, y^3+y, y^2+y, y^3+y^2+y]$, $[y^3+y^2+y, y^3+y, y^3+y^2+1, y]$,
$[y^3+y^2+y, y^3+y, y^3+y^2+1, y^2+1]$, $[y^3+y^2+y, y^3+y, y^2, y^2+1]$, $[y^3+y^2+y, y^3+y, y+1, y^2+1]$,
$[y^3+y^2+y, y^3+y, y+1, y^3+y+1]$, $[y^3+y^2+y, y^3+y, y^3+1, 1]$, $[y^3+y^2+y, y^3+y+1, y^3+$
$y^2+y, y^2+y]$, $[y^3+y^2+y, y^3+y+1, y^3+y^2+y, y^2]$, $[y^3+y^2+y, y^3+y+1, y, y^3+y^2+y]$,
$[y^3+y^2+y, y^3+y+1, y^2+1, y^3+1]$, $[y^3+y^2+y, y^3+y+1, y^2, y^3+y^2]$, $[y^3+y^2+y, y^3+y+$
$1, y^2, y^3+y+1]$, $[y^3+y^2+y, y^3+y+1, y^3+y, y^3+y^2]$, $[y^3+y^2+y, y^3+y+1, y^3+y, y^3+1]$,
$[y^3+y^2+y, y^2+y+1, y^2+y, y^2]$, $[y^3+y^2+y, y^2+y+1, y^3+y^2+y, y^2]$, $[y^3+y^2+y, y^2+$
$y+1, y^3+y^2+y, y+1]$, $[y^3+y^2+y, y^2+y+1, y, y^2]$, $[y^3+y^2+y, y^2+y+1, y^3+y^2, y^3]$,
$[y^3+y^2+y, y^2+y+1, y+1, y^3+1]$, $[y^3+y^2+y, y^2+y+1, y^3+1, y^2]$, $[y^3+y^2+y, y^3, y^2+y, y^2]$,
$[y^3+y^2+y, y^3, y^3+y^2+y, y^2+y]$, $[y^3+y^2+y, y^3, y^3+y^2+y, y^2+1]$, $[y^3+y^2+y, y^3, y^3+y^2+y, y^2]$,
$[y^3+y^2+y, y^3, y^2+1, y]$, $[y^3+y^2+y, y^3, y^2+1, y^3+y^2+y+1]$, $[y^3+y^2+y, y^3, y^2+1, y^2+1]$,
$[y^3+y^2+y, y^3, y^3+y, y^3]$, $[y^3+y^2+y, y^3, y^3+1, y^3+y+1]$, $[y^3+y^2+y, 1, y^3+y^2+y, y^3+y^2+y+1]$,
$[y^3+y^2+y, 1, y^3+y^2+y, y^2+1]$, $[y^3+y^2+y, 1, y^3+y^2+y, y^3+y^2]$, $[y^3+y^2+y, 1, y^3+y^2+y, y^2]$,
$[y^3+y^2+y, 1, y, y^2+1]$, $[y^3+y^2+y, 1, y^2+1, y+1]$, $[y^3+y^2+y, 1, y^3+y^2, y^3+y^2]$, $[y^3+y^2+$
$y, 1, y^3+y^2, y^2]$, $[y^3+y^2+y, 1, y^3+y^2, y^3]$, $[y^3+y^2+y, 1, y^2, y^2]$, $[y^3+y^2+y, 1, y^3+y, y^2+y]$,
$[y^3+y^2+y, 1, y^3+y, y^3+y^2+y+1]$, $[y^3+y^2+y, 1, y^3+y, y+1]$, $[y, y^2+y, y^3+y^2+y, y^3+y^2+y]$,
$[y, y^2+y, y^3+y^2+y, y^2+1]$, $[y, y^2+y, y^3+y^2+y, y^3+y+1]$, $[y, y^2+y, y, y^3+y^2+y]$,
$[y, y^2+y, y, y^3+y^2+1]$, $[y, y^2+y, y, y^2]$, $[y, y^2+y, y, y^3+y+1]$, $[y, y^2+y, y^3+y^2, y^3+y^2+1]$,
$[y, y^2+y, y^3+y^2+1, y^3+y]$, $[y, y^2+y, y^3+y+1, y^3+y+1]$, $[y, y^2+y, y^3+1, y^2]$, $[y, y^2+y, y^3+$
$1, y^3+y]$, $[y, y^2+y, y^3+1, y^2+y+1]$, $[y, y^3+y^2+y, y, y^2+1]$, $[y, y^3+y^2+y, y, y^3+y^2+1]$,
$[y, y^3+y^2+y, y, y^2]$, $[y, y^3+y^2+y, y, y^3+y]$, $[y, y^3+y^2+y, y^3+y^2+1, y^2]$, $[y, y^3+y^2+y, y+$
$1, y^2+y]$, $[y, y^3+y^2+y, y+1, y]$, $[y, y^3+y^2+y, y+1, y^3+y]$, $[y, y^3+y^2+y, y^3, y^3+y^2+y]$,
$[y, y, y^3+y^2+y, y^2+1]$, $[y, y, y^3+y^2+y, y+1]$, $[y, y, y^3+y^2+y, y^3+y+1]$, $[y, y, y^2+1, y^3+y^2+1]$,
$[y, y, y^2+1, y+1]$, $[y, y, y^3+y+1, y^3+y^2+y]$, $[y, y, y^2+y+1, y^2+y]$, $[y, y, y^2+y+1, y^3+y^2]$,
$[y, y^3+y^2+y+1, y, y^3+y+1]$, $[y, y^3+y^2+y+1, y, y^2+y+1]$, $[y, y^3+y^2+y+1, y^3+y^2, y]$,
$[y, y^3+y^2+y+1, y^3+y^2+1, y+1]$, $[y, y^3+y^2+y+1, y^3+y+1, y^3+y^2+y]$, $[y, y^3+y^2+y+$
$1, y^3+y+1, y^3+y^2+y+1]$, $[y, y^3+y^2+y+1, y^3+1, y^3+y^2+y]$, $[y, y^3+y^2+y+1, y^3+1, y+1]$,
$[y, y^2+1, y, y^3+y^2+1]$, $[y, y^2+1, y, y^3+y+1]$, $[y, y^2+1, y, y^2+y+1]$, $[y, y^2+1, y^3+y^2+1, y^3+y^2]$,
$[y, y^2+1, y^3+y^2+1, y^3+y^2+1]$, $[y, y^2+1, y^3+y^2+1, y^2]$, $[y, y^2+1, y+1, y^3+y^2+y+1]$, $[y, y^2+$
$1, y^2+y+1, y^3+y+1]$, $[y, y^2+1, y^3+1, y^2+1]$, $[y, y^3+y^2, y, y^3+y^2+1]$, $[y, y^3+y^2, y^2+1, y^2+y]$,
$[y, y^3+y^2, y^2+1, y+1]$, $[y, y^3+y^2, y^3+y^2, y^3+y^2+y+1]$, $[y, y^3+y^2, y^3+y^2, y^3+y^2+1]$,
$[y, y^3+y^2, y^3+y^2, y^3+y]$, $[y, y^3+y^2, y^3+y+1, y^3+y^2+1]$, $[y, y^3+y^2, y^2+y+1, y^2+y]$,
$[y, y^3+y^2, y^2+y+1, y^3+y^2]$, $[y, y^3+y, y^3+y, y^3+y^2+y+1]$, $[y, y^3+y, y^3+y, y^3+y^2]$,
$[y, y^3+y, y^3, y^3+y^2]$, $[y, y^3+y, y^3+1, y^3+y]$, $[y, y^3+y+1, y^3+y^2+y, y^3+y^2+y]$,
$[y, y^3+y+1, y, y^3+y^2]$, $[y, y^3+y+1, y, y^3+y]$, $[y, y^3+y+1, y^2+1, y^3+y^2+y]$, $[y, y^3+y+$
$1, y^3+y+1, y^3+y^2+y]$, $[y, y^3+y+1, y^3+y+1, y^3+y^2+y+1]$, $[y, y^3+y+1, y^3, y^3+y^2+y]$,
$[y, y^3+y+1, y^3, y^3+y^2+y+1]$, $[y, y^3+y+1, y^3, y+1]$, $[y, y^3+y+1, y^3+1, y+1]$, $[y, y^2+y+$
$1, y^3+y^2+y, y^2]$, $[y, y^2+y+1, y, y^2+y]$, $[y, y^2+y+1, y, y^3+y^2+1]$, $[y, y^2+y+1, y, y^3+y]$,
$[y, y^2+y+1, y^3+y^2, y]$, $[y, y^2+y+1, y^3+y^2, y^3+y^2+y+1]$, $[y, y^2+y+1, y^3+y^2, y^3+y^2+1]$,
$[y, y^2+y+1, y^2+y+1, y^2+y]$, $[y, y^2+y+1, y^3, y^2+y+1]$, $[y, y^3+1, y+1, y^2+y]$,
$[y, y^3+1, y^3+y, y^3+y^2+y+1]$, $[y, y^3+1, y^3+y, y^3+y^2+1]$, $[y, y^3+1, y^3+y+1, y^3+y^2+1]$,
$[y, y^3+1, y^2+y+1, y]$, $[y, y^3+1, y^3, y^3+y^2]$, $[y, y^3+1, y^3, y^3+y^2+1]$, $[y, 1, y^3+y^2+y, y^2+1]$,
$[y, 1, y, y^3+y]$, $[y, 1, y, y^3+y+1]$, $[y, 1, y^3+y^2, y^3+y+1]$, $[y, 1, y+1, y^3+y+1]$, $[y, 1, y^3+y, y+1]$,
$[y, 1, y^2+y+1, y^3+y+1]$, $[y^3+y^2+y+1, y^2+y, y^2+y, y^2+1]$, $[y^3+y^2+y+1, y^2+$
$y, y^2+y, y^2]$, $[y^3+y^2+y+1, y^2+y, y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y^2+y, y^3+1, y^2]$,

$[y^3+y^2+y+1, y^3+y^2+y, y^2+y, 1]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2+y+1, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y, y^2, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y+1, y+1]$, $[y^3+y^2+y+1, y^3+y^2+y, 1, y^3]$, $[y^3+y^2+y+1, y, y^3+y^2+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y, y^3+y^2+y+1, y^3+y]$, $[y^3+y^2+y+1, y, y^3+y^2+y+1, y^3+y+1]$, $[y^3+y^2+y+1, y, y^3+y^2+y+1, y^3]$, $[y^3+y^2+y+1, y, y^2, y^3+y]$, $[y^3+y^2+y+1, y, y^3+y, y^2+y]$, $[y^3+y^2+y+1, y, y^3+y+1, y+1]$, $[y^3+y^2+y+1, y, y^3+y+1, y^3+y+1]$, $[y^3+y^2+y+1, y, y^3+y+1, y^3]$, $[y^3+y^2+y+1, y, y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y, y^2+y+1, y^3+y^2]$, $[y^3+y^2+y+1, y, y^2+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y, y^3, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2, y]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2, y^2]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y+1, y^3+y]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y+1, 1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, 1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3, y^3+y+1]$, $[y^3+y^2+y+1, y^2+1, y^3+y^2+y+1, y^3+y^2]$, $[y^3+y^2+y+1, y^2+1, y^3+y^2+y+1, y^3]$, $[y^3+y^2+y+1, y^2+1, y^2, y^3+y^2+y+1]$, $[y^3+y^2+y+1, y^2+1, y^2+1, y^3+y, 1]$, $[y^3+y^2+y+1, y^2+1, y^2+y+1, y^3+y+1]$, $[y^3+y^2+y+1, y^2+1, y^2+y+1, 1]$, $[y^3+y^2+y+1, y^2+1, y^3, y^2+1]$, $[y^3+y^2+y+1, y^2+1, y^3, y^3+y+1]$, $[y^3+y^2+y+1, y^2+1, y^3+y^2, y^3+y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2+y+1, y]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2+y+1, y^3+y]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2, y]$, $[y^3+y^2+y+1, y^3+y^2, y^2, y^3+y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2, y^2, y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y^2, y^3+y]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y^3+1, y^3+y^2]$, $[y^3+y^2+y+1, y^2, y^3+y^2+y+1, y^3+y]$, $[y^3+y^2+y+1, y^2, y^3+y^2, y^3]$, $[y^3+y^2+y+1, y^2, y^3+y^2, y^2]$, $[y^3+y^2+y+1, y^2, y^2, y^2+y]$, $[y^3+y^2+y+1, y^2, y^2, y^2+1]$, $[y^3+y^2+y+1, y^2, y^2, y^3+y]$, $[y^3+y^2+y+1, y^2, y+1, y]$, $[y^3+y^2+y+1, y^2, y+1, 1]$, $[y^3+y^2+y+1, y^2, y^3, y^3+y]$, $[y^3+y^2+y+1, y+1, y^3+y^2+y+1, y^3+y^2]$, $[y^3+y^2+y+1, y+1, y^3+y^2+y+1, y^3+y]$, $[y^3+y^2+y+1, y+1, y^3+y^2+y+1, y^3]$, $[y^3+y^2+y+1, y+1, y^3+y^2, y^3]$, $[y^3+y^2+y+1, y+1, y^3+y, y^3+y^2+1]$, $[y^3+y^2+y+1, y+1, y^3+y, y^2]$, $[y^3+y^2+y+1, y+1, y^3+y, y^3+y]$, $[y^3+y^2+y+1, y+1, y^2+y+1, y+1]$, $[y^3+y^2+y+1, y+1, 1, y^2+1]$, $[y^3+y^2+y+1, y^3+y+1, y^3+y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y^3+y+1, y^3+y^2+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y+1, y^3+y^2+y+1, y+1]$, $[y^3+y^2+y+1, y^3+y+1, y^3+y, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y+1, 1, y^3+y]$, $[y^3+y^2+y+1, y^3+y+1, 1, y]$, $[y^3+y^2+y+1, y^3+y+1, 1, y^3+y^2+y+1]$, $[y^3+y^2+y+1, y^2+y+1, y^2+y, y^2+1]$, $[y^3+y^2+y+1, y^2+y+1, y^2+y, y^3+y]$, $[y^3+y^2+y+1, y^2+y+1, y^3+y^2, y^3+y^2+y+1]$, $[y^3+y^2+y+1, y^2+y+1, y^3, y^3+y]$, $[y^3+y^2+y+1, y^2+y+1, y^3+1, y^2]$, $[y^3+y^2+y+1, y^2+y+1, y^3+1, y^3+y]$, $[y^3+y^2+y+1, y^2+y+1, 1, y]$, $[y^3+y^2+y+1, y^3, y^3+y^2+y+1, y^2+y]$, $[y^3+y^2+y+1, y^3, y^3+y^2+y+1, y^2]$, $[y^3+y^2+y+1, y^3, y+1, y^3+y+1]$, $[y^3+y^2+y+1, y^3, y^3+y+1, y^3+y+1]$, $[y^3+y^2+y+1, y^3, y^2+y+1, 1]$, $[y^3+y^2+y+1, y^3, y^3, y^2+1]$, $[y^3+y^2+y+1, y^3, y^3, y^3+y+1]$, $[y^3+y^2+y+1, y^3, y^3+1, y^2+1]$, $[y^3+y^2+y+1, y^3, y^3+1, y^3+y+1]$, $[y^3+y^2+y+1, y^3, y^3+1, 1]$, $[y^2+1, y, y, y^3+y^2+1]$, $[y^2+1, y, y, y+1]$, $[y^2+1, y, y^3+y^2, y]$, $[y^2+1, y, y^2+y+1, y^3+y^2+1]$, $[y^2+1, y^3+y^2+y+1, y^2+y, y]$, $[y^2+1, y^3+y^2+y+1, y^2+1, y^2+y]$, $[y^2+1, y^3+y^2+y+1, y^2+1, y^3+y]$, $[y^2+1, y^3+y^2+y+1, y^2+1, y^3]$, $[y^2+1, y^3+y^2+y+1, y^2+1, y^3+1]$, $[y^2+1, y^3+y^2+y+1, y^3+y^2, y]$, $[y^2+1, y^3+y^2+y+1, y^3+y^2, y^2]$, $[y^2+1, y^3+y^2+y+1, y^3+y^2, y^3+y]$, $[y^2+1, y^3+y^2+y+1, y^3+y^2+1, y^2+y]$, $[y^2+1, y^3+y^2+y+1, y^3, y^3]$, $[y^2+1, y^3+y^2+y+1, y^3, y^3+1]$, $[y^2+1, y^3+y^2+y+1, y^3, y^3+y+1]$, $[y^2+1, y^2+1, y^2, y^3+y^2+y+1]$, $[y^2+1, y^2+1, y^2, y^3+y^2+1]$, $[y^2+1, y^2+1, y^3, y^3+y^2+y]$, $[y^2+1, y^2+1, y^3, y^3+1]$,

$[y^2+1, y^2+1, y^3, 1]$, $[y^2+1, y^2+1, y^3+1, y^3]$, $[y^2+1, y^2+1, 1, y^2+y]$, $[y^2+1, y^2+1, 1, y^3+y^2+y]$, $[y^2+1, y^3+y^2, y^3+y^2+y, y^3+y^2+y+1]$, $[y^2+1, y^3+y^2, y, y^2+y]$, $[y^2+1, y^3+y^2, y, y+1]$, $[y^2+1, y^3+y^2, y^2, y^2+1]$, $[y^2+1, y^3+y^2, y^2+y+1, y^2+y]$, $[y^2+1, y^3+y^2, y^2+y+1, y^3+y^2+1]$, $[y^2+1, y^3+y^2, y^3+1, y^2+y]$, $[y^2+1, y^3+y^2+1, y^2+1, y^2+y]$, $[y^2+1, y^3+y^2+1, y^3+y^2+1, y^2+y]$, $[y^2+1, y^3+y^2+1, y^3+y^2+1, y]$, $[y^2+1, y^3+y^2+1, y^3+y^2+1, y+1]$, $[y^2+1, y^3+y^2+1, y^2, y^3+y^2+1]$, $[y^2+1, y^3+y^2+1, y^2, y^3+y^2]$, $[y^2+1, y^3+y^2+1, 1, y^3+y^2+y]$, $[y^2+1, y^3+y^2+1, 1, y^3+y^2+y+1]$, $[y^2+1, y^2, y^2+1, y^2+y]$, $[y^2+1, y^2, y^2+1, y]$, $[y^2+1, y^2, y^2+1, y^3+y^2+y+1]$, $[y^2+1, y^2, y^3+y^2+1, y^2+y]$, $[y^2+1, y^2, y^3+y^2+1, y^2+1]$, $[y^2+1, y^2, y^3+y^2+1, y+1]$, $[y^2+1, y^2, y^2, y^3+y^2+y+1]$, $[y^2+1, y^2, y^2+y+1, y^2]$, $[y^2+1, y^2, y^3, y^3+y]$, $[y^2+1, y+1, y^2+y, y^3+y^2+y]$, $[y^2+1, y+1, y^2+1, y^2]$, $[y^2+1, y+1, y^2+1, y^3+1]$, $[y^2+1, y+1, y^3+y^2, y^3+y^2+y]$, $[y^2+1, y+1, y^3+y^2, y^3]$, $[y^2+1, y+1, y^3+y^2+1, y^2+1]$, $[y^2+1, y+1, y^3+1, y+1]$, $[y^2+1, y+1, y^3+1, y^3]$, $[y^2+1, y^3+y+1, y^3+y^2+y, y^3+1]$, $[y^2+1, y^3+y+1, y, y^3+y^2+y]$, $[y^2+1, y^3+y+1, y^2+1, y]$, $[y^2+1, y^3+y+1, y^2+1, y^3+1]$, $[y^2+1, y^3+y+1, y^3+y^2+1, y^3+1]$, $[y^2+1, y^3+y+1, y^2, y^3+1]$, $[y^2+1, y^3+y+1, y^2, y^3]$, $[y^2+1, y^3, y^2+y, y^3+y]$, $[y^2+1, y^3, y^3+y^2, y]$, $[y^2+1, y^3, y^3+y^2+y, y^3+y^2+y+1]$, $[y^2+1, y^3, y^3+y^2+y, y^2+1]$, $[y^2+1, y^3, y^2+1, y^2+y]$, $[y^2+1, y^3, y^2+1, y]$, $[y^2+1, y^3, y^2+1, y^3+y]$, $[y^2+1, y^3, y^2+1, 1]$, $[y^2+1, y^3, y^2+y+1, y^3]$, $[y^2+1, y^3+1, y^2+1, y]$, $[y^2+1, y^3+1, y^2+1, y^3+y^2+1]$, $[y^2+1, y^3+1, y^3+y^2, y^3+y^2+y]$, $[y^2+1, y^3+1, y^2+y+1, y^3+y^2+y]$, $[y^2+1, y^3+1, y^2+y+1, y+1]$, $[y^2+1, y^3+1, y^2+y+1, y^3]$, $[y^2+1, y^3+1, y^3, y^3]$, $[y^2+1, y^3+1, y^3+1, y+1]$, $[y^2+1, y^3+1, y^3+1, y^3]$, $[y^2+1, y^3+1, 1, y^3]$, $[y^2+1, 1, y^2+y, y^2+y]$, $[y^2+1, 1, y^2+y, y^3+y^2+1]$, $[y^2+1, 1, y^2+y, y^3+y]$, $[y^2+1, 1, y^3+y^2+y, y+1]$, $[y^2+1, 1, y^2+1, y^2+y]$, $[y^2+1, 1, y^2+1, y^2]$, $[y^2+1, 1, y^2+1, y^3+1]$, $[y^2+1, 1, y^3+y^2, 1]$, $[y^2+1, 1, y^2, y^3+1]$, $[y^3+y^2, y^2+y, y^3+y^2+y, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y, y, y^3+y^2+1]$, $[y^3+y^2, y^2+y, y^3+y^2, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y, y^3+y^2, y^3+1]$, $[y^3+y^2, y^2+y, y^3+y, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y, y^3+1, y^3+y]$, $[y^3+y^2, y^2+y, 1, y^3+y^2+y+1]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y, y^2]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y, y^3]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y, y^3+1]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y+1, y^3]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2, y^3]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+1, y^3+y]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y, y^2+y+1]$, $[y^3+y^2, y^3+y^2+y, 1, y^3+y^2+y]$, $[y^3+y^2, y^3+y^2+y, 1, y^2+y+1]$, $[y^3+y^2, y, y^2+1, y]$, $[y^3+y^2, y, y^3+y^2, y^3+y^2+1]$, $[y^3+y^2, y, y^3+y^2, y^3+y+1]$, $[y^3+y^2, y, y^3+y^2, y^3]$, $[y^3+y^2, y, y^3+y^2, y^3+1]$, $[y^3+y^2, y, y^3+y, y^3+y^2]$, $[y^3+y^2, y, y^3+y, y^2+y+1]$, $[y^3+y^2, y, y^3+y, y^3+1]$, $[y^3+y^2, y, y^3, y^3+y+1]$, $[y^3+y^2, y^3+y^2+y+1, y, y]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y^2+y+1, y]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y^2+y+1, y^2]$, $[y^3+y^2, y^3+y^2+y+1, y^2+1, y]$, $[y^3+y^2, y^3+y^2+y+1, y^2+1, y^2]$, $[y^3+y^2, y^3+y^2+y+1, y^2+1, y^3+y]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y^2, y^3+y^2+y]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y^2, y^3+1]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y^2+1, y]$, $[y^3+y^2, y^3+y^2+y+1, y+1, y^3+y]$, $[y^3+y^2, y^3+y^2, y, y^3+y^2+y+1]$, $[y^3+y^2, y^3+y^2, y, y^3+y^2+1]$, $[y^3+y^2, y^3+y^2, y, y^3+y]$, $[y^3+y^2, y^3+y^2, y^3+y^2+y+1, y]$, $[y^3+y^2, y^3+y^2, y^3+y^2+1, y^3+y]$, $[y^3+y^2, y^3+y^2, y^3+y^2+1, y^3]$, $[y^3+y^2, y^3+y^2, 1, y^3+y^2+y]$, $[y^3+y^2, y^3+y^2, 1, y^2+y+1]$, $[y^3+y^2, y^3+y^2+1, y^3+y^2, y^3+y^2+y+1]$, $[y^3+y^2, y^3+y^2+1, y^3+y^2, y^3]$, $[y^3+y^2, y^3+y^2+1, y^3+y^2, 1]$, $[y^3+y^2, y^3+y^2+1, y+1, y^3+y^2+1]$, $[y^3+y^2, y^3+y^2+1, y^3+y, y^2]$, $[y^3+y^2, y^3+y^2+1, y^3, y^3+y^2+y]$, $[y^3+y^2, y^3+y^2+1, y^3, y^3+y+1]$, $[y^3+y^2, y^3+y^2+1, y^3, y^3]$, $[y^3+y^2, y^3+y^2+1, 1, y^3+y^2+y+1]$, $[y^3+y^2, y^2, y^3+y^2+y, y^3+y^2]$, $[y^3+y^2, y^2, y^3+y^2+y+1, y]$, $[y^3+y^2, y^2, y^3+y^2+y+1, y^2]$, $[y^3+y^2, y^2, y^3+y^2+y+1, y^3+y^2+y]$, $[y^3+y^2, y^2, y^3+y^2+y+1, y^3+1]$, $[y^3+y^2, y^2, y^3+y^2, 1]$, $[y^3+y^2, y^2, y+1, y]$, $[y^3+y^2, y^2, y+1, y^3+y]$, $[y^3+y^2, y^2, y^3, y^3+y]$, $[y^3+y^2, y+1, y^3+y^2+y+1, y^3]$, $[y^3+y^2, y+1, y^2+1, y^3+y^2+y]$, $[y^3+y^2, y+1, y^2+1, y^3]$, $[y^3+y^2, y+1, y^3+1, y^3+y]$,

$y, y^2+y+1]$, $[y^3+y^2, y+1, y^3+1, y^2]$, $[y^3+y^2, y+1, y^3+1, y^3]$, $[y^3+y^2, y+1, 1, y^3+y^2]$, $[y^3+y^2, y^2+y+1, y^3+y^2+y, y^3]$, $[y^3+y^2, y^2+y+1, y, y]$, $[y^3+y^2, y^2+y+1, y, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y+1, y, y^3+y^2+1]$, $[y^3+y^2, y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y+1, y^3+y^2, y]$, $[y^3+y^2, y^2+y+1, y^3+y^2, y^3+y^2+y+1]$, $[y^3+y^2, y^2+y+1, y^3+y^2, y^3+y+1]$, $[y^3+y^2, y^2+y+1, y^3+y^2, y^3]$, $[y^3+y^2, y^2+y+1, y+1, y^3+y+1]$, $[y^3+y^2, y^2+y+1, y+1, y^3+1]$, $[y^3+y^2, y^2+y+1, y+1, 1]$, $[y^3+y^2, y^2+y+1, y^3, y^3+1]$, $[y^3+y^2, y^3+1, y^2+1, y^3+y^2+y]$, $[y^3+y^2, y^3+1, y+1, y^3+1]$, $[y^3+y^2, y^3+1, y^3+1, y^3+y^2+y]$, $[y^3+y^2, y^3+1, y^3+1, y^2]$, $[y^3+y^2, 1, y^3+y^2+y, y^3+y^2]$, $[y^3+y^2, 1, y^3+y^2+y, y^2]$, $[y^3+y^2, 1, y^3+y^2+y, y^3]$, $[y^3+y^2, 1, y, y^3+y+1]$, $[y^3+y^2, 1, y^2+1, 1]$, $[y^3+y^2, 1, y^3+y^2, y^2+y+1]$, $[y^3+y^2, 1, y^3+y^2, y^3]$, $[y^3+y^2, 1, y^3+y^2, y^3+1]$, $[y^3+y^2, 1, 1, y^2+y+1]$, $[y^3+y^2+1, y^2+y, y^3+y^2+y, y^2+y]$, $[y^3+y^2+1, y^2+y, y, y^3+y]$, $[y^3+y^2+1, y^2+y, y^3+y^2+1, y+1]$, $[y^3+y^2+1, y^2+y, y^3+y^2+1, y^3+y+1]$, $[y^3+y^2+1, y^2+y, y^3+y+1, y+1]$, $[y^3+y^2+1, y^2+y, y^2+y+1, y^2+y+1]$, $[y^3+y^2+1, y^2+y, y^2+y+1, y^3]$, $[y^3+y^2+1, y^2+y, y^2+y+1, y^3+1]$, $[y^3+y^2+1, y^3+y^2+y, y, y^2]$, $[y^3+y^2+1, y^3+y^2+y, y^3+y^2, y^3+y]$, $[y^3+y^2+1, y^3+y^2+y, y^3+y^2, y^2+y+1]$, $[y^3+y^2+1, y^3+y^2+y, y+1, y^2+y+1]$, $[y^3+y^2+1, y^3+y^2+y, y^3+y+1, y^3+y^2+1]$, $[y^3+y^2+1, y^3+y^2+y, 1, y^2+y+1]$, $[y^3+y^2+1, y^3+y^2+y, 1, y^3]$, $[y^3+y^2+1, y^3+y^2+y+1, y, y+1]$, $[y^3+y^2+1, y^3+y^2+y+1, y^2+1, y^2+y]$, $[y^3+y^2+1, y^3+y^2+y+1, y^2+y]$, $[y^3+y^2+1, y^3+y^2+y+1, y^3+y^2+1, y^3+y^2]$, $[y^3+y^2+1, y^3+y^2+y+1, y^3+y^2+1, y+1]$, $[y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y+1]$, $[y^3+y^2+1, y^3+y^2+y+1, y^3, y+1]$, $[y^3+y^2+1, y^2+1, y, y^3+y^2]$, $[y^3+y^2+1, y^2+1, y, y^3+y^2+1]$, $[y^3+y^2+1, y^2+1, y, y^2]$, $[y^3+y^2+1, y^2+1, y^3+y^2+1, y^2+y]$, $[y^3+y^2+1, y^2+1, y^3+y^2+1, y^3+y^2]$, $[y^3+y^2+1, y^2+1, y^3+y^2+1, y^2+y+1]$, $[y^3+y^2+1, y^2+1, y^3+y^2+1, y^3+1]$, $[y^3+y^2+1, y^2+1, y^2+y+1, y^3+1]$, $[y^3+y^2+1, y^2+1, 1, y^2+1]$, $[y^3+y^2+1, y^3+y^2, y^3+y^2+y, y^3]$, $[y^3+y^2+1, y^3+y^2, y^3+y^2, y^3+y]$, $[y^3+y^2+1, y^3+y^2, y^3+y^2, y^3]$, $[y^3+y^2+1, y^3+y^2, 1, y^3]$, $[y^3+y^2+1, y^3+y^2+y, y^2+y]$, $[y^3+y^2+1, y^3+y^2+y, y^2+y+1]$, $[y^3+y^2+1, y^3+y^2+1, y^2+1, y^2+y]$, $[y^3+y^2+1, y^3+y^2+1, y^2+1, y]$, $[y^3+y^2+1, y^3+y^2+1, y^2+1, y+1]$, $[y^3+y^2+1, y^3+y^2+1, y+1, y^2+1]$, $[y^3+y^2+1, y^3+y^2+1, y^3+y+1, y^2]$, $[y^3+y^2+1, y^3+y^2+1, y^3+y+1, y^3]$.

B

$[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2+y, y^3+1, y^3+y+1, y^3]$, $[y^3+y^2+y+1, y^3+y^2+y, y, y^2+y+1, y^3+y+1, y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+y, y^3+y^2, y^2+1, y^3+y^2+y+1, y^2+1]$, $[y^3+y^2+y+1, y, y^3+y^2+y, y^2+y+1, y^3+y^2+y+1, y^3]$, $[y^3+y^2+y+1, y, y, y^2+1, y^2, y^3]$, $[y^3+y^2+y+1, y, y^3+y^2, y^3+1, y^3+y^2+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y+1, y^2+y+1, y^2+y, y^3+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y^3+y+1, y^2+1, y^2+y]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+1, y^3+y+1, y^2+y+1, y+1]$, $[y^3+y^2+y+1, y^2+1, y^3+y^2+y+1, y^2+y+1, y^3, y^2+y]$, $[y^3+y^2+y+1, y^2+1, y^2, y^3+y+1, y^3+y^2+1, 1]$, $[y^3+y^2+y+1, y^2+1, y^3+y+1, y^2+1, y^3, 1]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2+y, y^2+1, y^3+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y, y^3+1, y^2, y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2, y^2+y+1, y^2, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^3, y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^2+1, y^2, y^3+y+1, y^3+y^2+1, 1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y^2+1, y^3, 1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y^3+y^2+y, y^2+1, y^3+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2, y, y^3+1, y^2, y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2, y^3+y^2, y^2+y+1, y^2, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^3, y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^2+1, y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2+y+1, y^3+y+1, y^3+y+1, y^2+1, y^2+y+1]$, $[y^3+y^2+y+1, y^2+1, y^3+y^2+y+1, y^2+y+1, y^3, y^2+y+1]$, $[y^3+y^2+y+1, y^2+1, y^2, y^3+y+1, y^3+y^2+1, 1]$, $[y^3+y^2+y+1, y^2+1, y^3+y+1, y^2+1, y^3, 1]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2+y, y^2+1, y^3+y+1, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y, y^3+1, y^2, y^2+1]$, $[y^3+y^2+y+1, y^3+y^2, y^3+y^2, y^2+y+1, y^2, y^3+y^2+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^3, y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^2+1, y^2+y+1]$, $[y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+y+1, y^3+y+1, y^3+y^2, y^3+y^2]$, $[y^3+y^2+y+1, y+1, y^2+y+1, y^3+1, y^3+y^2+y, y^3+y^2]$, $[y^3+y^2+y+1, y+1, 1, y^2+1, y^3+y^2, y]$,

$[y^3+y^2+y+1, y^3+y, y^2+y, y^3+1, y, y]$, $[y^3+y^2+y+1, y^3+y, y^2+y+1, y^2+1, y^3+y^2+y, y^3+y^2+y]$, $[y^3+y^2+y+1, y^3+y, 1, y^3+y+1, y^3+y^2+y, y]$, $[y^3+y^2+y+1, y^3+y+1, y+1, y^3+y+1, y^2+y, y^3+y]$, $[y^3+y^2+y+1, y^3+y+1, y^3+y, y^2+y+1, 1, y+1]$, $[y^3+y^2+y+1, y^3+y+1, y^3+1, y^3+1, y^2+y, y+1]$, $[y^3+y^2+y+1, y^3, y^3+y^2+y+1, y^2+1, y^3+y^2+y]$, $[y^3+y^2+y+1, y^3, y^2, y^2+y+1, y^3+y^2+1, y^2+y+1]$, $[y^3+y^2+y+1, y^3, y^3+y+1, y^3+y+1, y^2+1, y^2+y]$, $[y^3+y^2+y+1, y^3+1, y^2+y, y^2+1, y, y^3+y^2]$, $[y^3+y^2+y+1, y^3+1, y^2+y+1, y^3+y+1, y, y^3+y^2+y]$, $[y^3+y^2+y+1, y^3+1, 1, y^3+1, y^3+y^2, y^3+y^2+y]$, $[y^3+y^2, y^3+y^2+y, y^3+y^2+y+1, y^2+y, 1, y^2]$, $[y^3+y^2, y^3+y^2+y, y^2, y^3+y^2+y, y^2+y+1, y^3+y^2+y+1]$, $[y^3+y^2, y^3+y^2+y, y^3+y+1, y^3+y+1, y^2+y+1, y^2]$, $[y^3+y^2, y, y^3+y^2+y+1, y^3+y^2+y, 1, y^3+y+1]$, $[y^3+y^2, y, y^2, y^3+y+1, 1, y^3+y^2+y+1]$, $[y^3+y^2, y, y^3+y+1, y^2+y, y^2+y, y^3+y^2+y+1]$, $[y^3+y^2, y^3+y^2+y+1, y^3+y+1, y^2+1, y^2+1]$, $[y^3+y^2, y^3+y^2+y+1, 1, y^3+y^2+y, y^3+y^2+1, y^2+1]$, $[y^3+y^2, y^2+1, y^2+1, y+1, y, y^3+y]$, $[y^3+y^2, y^2+1, y^3+y^2+1, y^2+y, y^3+y^2, y^3+y]$, $[y^3+y^2, y^2+1, y^3, y^3+y+1, y^3+y^2, y^3+1]$, $[y^3+y^2, y^3+y^2, y^3+y^2+y+1, y^3+y+1, y^2+y, y^3+y+1]$, $[y^3+y^2, y^3+y^2, y^2, y^2+y, y^2+y+1, y^3+y+1]$, $[y^3+y^2, y^3+y^2, y^3+y+1, y^3+y^2+y, y^2+y, y^2]$, $[y^3+y^2, y^3+y^2+1, y^2+1, y^2+y, y^3+y^2+y, y+1]$, $[y^3+y^2, y^3+y^2+1, y^3+y^2+1, y^3+y+1, y^3+y^2+y, y^3+y]$, $[y^3+y^2, y^3+y^2+1, y^3, y+1, y^3+y^2, y+1]$, $[y^3+y^2, y^2, y^2+y, y^3+y+1, y^3+y^2+1, y^3]$, $[y^3+y^2, y^2, y^2+y+1, y^3+y^2+y, y^3, y^3]$, $[y^3+y^2, y^2, 1, y+1, y^3, y^2+1]$, $[y^3+y^2, y+1, y^3+y^2+y, y+1, y^3+y, 1]$, $[y^3+y^2, y+1, y, y^3+y^2+y, y^3+1, 1]$, $[y^3+y^2, y+1, y^3+y^2, y^2+y, y^3+y, y^2+y+1]$, $[y^3+y^2, y^3+y, y^3+y^2+y, y^3+y^2+y, y+1, y^2+y+1]$, $[y^3+y^2, y^3+y, y, y^2+y, y^3+1, y^2+y]$, $[y^3+y^2, y^3+y, y^3+y^2, y+1, y^3+1, y^2+y+1]$, $[y^3+y^2, y^3+y+1, y^2+y, y^3+y^2+y, y^2+1, y^3+y^2+1]$, $[y^3+y^2, y^3+y+1, y^2+y, y^3+y^2+y, y^2+1, y^3+y^2+1]$, $[y^3+y^2, y^3+y+1, 1, y^3+y+1, y^2+y+1, y^3]$, $[y^3+y^2, y^3+y+1, 1, y^3+y^2+1, y^3, y^3+y^2+1]$, $[y^3+y^2, y^3, y^2+1, y^3+y+1, y^3+y^2+y+1, y^2+1]$, $[y^3+y^2, y^3, y^3, y^2+y, y, y^3+1]$, $[y^3+y^2, y^3+1, y^3+y^2+y, y^2+y, y+1, 1]$, $[y^3+y^2, y^3+1, y, y+1, y+1, y^2+y]$, $[y^3+y^2, y^3+1, y^3+y^2, y^3+y^2+y, y^3+y, y^2+y]$, $[y^3+y, y^3+y^2+y, y+1, y, y, y^2+y]$, $[y^3+y, y^3+y^2+y, y^3+y, y^3+1, y^3+y^2, y^2+y]$, $[y^3+y, y^3+y^2+y, y^3+1, y^2+y, y^3+y^2+y+1, 1]$, $[y^3+y, y, y+1, y^3+1, y^3+y^2+y, 1]$, $[y^3+y, y, y^3+y, y^2+y, y^3+y^2, y^2+y+1]$, $[y^3+y, y, y^3+1, y, y^3+y^2, 1]$, $[y^3+y, y^3+y^2+y+1, y^3+y^2+y+1, y^2+y, y+1, y^3+y^2+y]$, $[y^3+y, y^3+y^2+y+1, y^2, y^3+y^2+1, y+1, y]$, $[y^3+y, y^3+y^2+y+1, y^3+y+1, y, y^3+y^2+y]$, $[y^3+y, y^2+1, y^2+y, y^3+y^2+1, y^3+y+1, y^3+y^2+y+1]$, $[y^3+y, y^2+1, y^2+y+1, y^3+1, y^3+y^2+y+1, y^2]$, $[y^3+y, y^3+y^2, y+1, y^2+y, y^3+y^2+y, y^2+y]$, $[y^3+y, y^3+y^2, y^3+y, y, y^3+y^2+y, y^2+y+1]$, $[y^3+y, y^3+y^2, y^3+1, y^3+1, y, y^2+y+1]$, $[y^3+y, y^3+y^2+1, y^2+y, y^3+1, y^2, y^3+y+1]$, $[y^3+y, y^3+y^2+1, y^2+y+1, y, y^2, y^3+y^2+y+1]$, $[y^3+y, y^3+y^2+1, 1, y^3+y^2+y+1, y^3+y+1]$, $[y^3+y, y^2, y^3+y^2+y+1, y^3+y^2+1, y^3+y, y^3+y^2+y]$, $[y^3+y, y^2, y^2, y, y+1, y^3+y^2]$, $[y^3+y, y^2, y^3+y+1, y^2+y, y^3+y, y^3+y^2]$, $[y^3+y, y+1, y^2+1, y^3+y^2+1, 1, y^3]$, $[y^3+y, y+1, y^3+y^2+1, y^2+y, y^2+y, y^3]$, $[y^3+y, y+1, y^3, y^3+1, 1, y^3+y^2+1]$, $[y^3+y, y^3+y, y^2+1, y^2+y, y^2+y+1, y^3+y^2+1]$, $[y^3+y, y^3+y, y^3+y^2+1, y^3+1, y^2+y, y^2+1]$, $[y^3+y, y^3+y, y^3, y^3+y^2+1, y^2+y, y^3+y^2+1]$, $[y^3+y, y^3+y+1, y^2+y+1, y, y^3+y, y]$, $[y^3+y, y^3+y+1, y^2, y^2+y, y^3+1, y]$, $[y^3+y, y^3+y+1, y^3+y+1, y^3+y^2+1, y^3+1, y^3+y^2]$, $[y^3+y, y^3, y^2+y, y, y^3+y+1, y^3+1]$, $[y^3+y, y^3+1, y^2+1, y^3+1, y^2+y+1, y^3]$, $[y^3+y, y^3+1, y^3+y^2+1, y^3+y^2+1, y^2+y+1, y^2+1]$, $[y^3+y, y^3+1, y^3, y^2+y, 1, y^2+1]$, $[y^3, y^3+y^2+y, y^2+y, y^2, y+1, y^3+y]$, $[y^3, y^3+y^2+y, y^2+y+1, y^3+y^2+1, y+1, y^3+1]$, $[y^3, y^3+y^2+y, 1, y^3+y^2+y, y^3+$

$y, y^3+1]$, $[y^3, y, y^2+y, y^3+y^2+1, y^3+y, y^3+y]$, $[y^3, y, y^2+y+1, y^3+y^2+y, y^3+1, y^3+y]$, $[y^3, y, 1, y^2, y^3+y, y+1]$, $[y^3, y^3+y^2+y+1, y^2+1, y^2+y+1, y^3+y+1, y^2+y+1]$, $[y^3, y^3+y^2+y+1, y^3+y^2+1, y^3+y^2+1, y^2, y^2+y]$, $[y^3, y^3+y^2+y+1, y^3, y^2, y^3+y+1, y^2+y]$, $[y^3, y^2+1, y^3+y^2+y, y^2+y+1, y^2+y+1, y^3+y^2]$, $[y^3, y^2+1, y, y^3+y^2+y, 1, y^3+y^2]$, $[y^3, y^2+1, y^3+y^2, y^3+y^2+1, 1, y^3+y^2+y]$, $[y^3, y^3+y^2, y^2+y, y^3+y^2+y, y+1, y+1]$, $[y^3, y^3+y^2, y^2+y+1, y^2, y^3+1, y^3+1]$, $[y^3, y^3+y^2, 1, y^3+y^2+1, y^3+1, y+1]$, $[y^3, y^3+y^2+1, y^3+y^2+y, y^3+y^2+y, y^2+y, y]$, $[y^3, y^3+y^2+1, y, y^3+y^2+1, y^2+y, y^3+y^2]$, $[y^3, y^3+y^2+1, y^3+y^2, y^2+y+1, 1, y]$, $[y^3, y^2, y^2+1, y^3+y^2+1, y^3+y+1, 1]$, $[y^3, y^2, y^3+y^2+1, y^2, y^3+y^2+y+1, 1]$, $[y^3, y^2, y^3, y^2+y+1, y^3+y^2+y+1, y^2+y]$, $[y^3, y+1, y+1, y^2, y^2+1, y^3+y^2+y+1]$, $[y^3, y+1, y^3+y, y^3+y^2+y, y^3, y^3+y+1]$, $[y^3, y+1, y^3+1, y^2+y+1, y^3, y^3+y^2+y+1]$, $[y^3, y^3+y, y+1, y^3+y^2+y, y^2+1, y^2]$, $[y^3, y^3+y, y^3+y, y^2+y+1, y^2+1, y^3+y+1]$, $[y^3, y^3+y, y^3+1, y^2, y^3+y^2+1, y^3+y+1]$, $[y^3, y^3+y+1, y^2+1, y^2, y^2, y^2+y+1]$, $[y^3, y^3+y+1, y^3+y^2+1, y^2+y+1, y^2, 1]$, $[y^3, y^3+y+1, y^3, y^3+y^2+1, y^3+y^2+y+1, y^2+y+1]$, $[y^3, y^3, y^3+y^2+y, y^3+y^2+1, y^2+y+1, y]$, $[y^3, y^3, y, y^2+y+1, y^2+y, y^3+y^2+y]$, $[y^3, y^3, y^3+y^2, y^3+y^2+y, y^2+y+1, y^3+y^2+y]$, $[y^3, y^3+1, y+1, y^2+y+1, y^3+y^2+1, y^2]$, $[y^3, y^3+1, y^3+y, y^2, y^3, y^2]$, $[y^3, y^3+1, y^3+1, y^3+y^2+y, y^3+y^2+1, y^3+y^2+y+1]$, $[1, y^3+y^2+y, y^2+1, y^2+1, y^3+y^2, y^2+1]$, $[1, y^3+y^2+y, y^3+y^2+1, y^2+1, y^3+y^2, y^2+1]$, $[1, y^3+y^2+y, y^3+y^2+1, y^2, y^3+y^2, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^2+1, y^3+y^2, y^2]$, $[1, y^3+y^2+y, y^3+y^2+y, y^2, y^3+y^2, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^2, y^3, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^3+y^2, y^2]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^3, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^3+y^2, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2, y^3+y^2+y, y^2]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y+1]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y+1, y^3+y^2+y+1]$, $[1, y^3+y^2+y, y^3+y^2+y, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1]$, $[1, y^3+y^2+y, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1]$, $[1, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1, y^3+y^2+y+1]$.