# An Algebraic Approach to Circulant Column Parity Mixers

Robert Christian Subroto[0000 0001 5534 2655]

*iCIS, Radboud University, Toernooiveld 212, Nijmegen, 6525 EC, The Netherlands.

Corresponding author(s). E-mail(s): bobby.subroto@ru.nl;

**Abstract**

Column Parity Mixers, or CPMs in short, are a particular type of linear maps, used as the mixing layer in permutation-based cryptographic primitives like Keccak-$f$ (SHA3) and Xoodoo. Although being successfully applied, not much is known regarding their algebraic properties. They are limited to invertibility of CCPMs, and that the set of invertible CCPMs forms a group. A possible explanation is due to the complexity of describing CPMs in terms of linear algebra. In this paper, we introduce a new approach to studying CPMs using module theory from commutative algebra. We show that many interesting algebraic properties can be deduced using this approach, and that known results regarding CPMs turn out to be trivial consequences of module theoretic concepts. We also show how this approach can be used to study the linear layer of Xoodoo, and other linear maps with a similar structure which we call DCD-compositions. Using this approach, we prove that every DCD-composition where the underlying vector space with the same dimension as that of Xoodoo has a low order. This provides a solid mathematical explanation for the low order of the linear layer of Xoodoo, which equals 32. We design a DCD-composition using this module-theoretic approach, but with a higher order using a different dimension.

**Keywords:** Column parity mixers, Module theory, Local rings, Linear algebra, Circulant matrices

# 1 Introduction

Column parity mixers [3], or CPMs for short, are a particular type of linear maps which are a generalization of the $\theta$ mixing layers in the cryptographic permutations Xoodoo [1] and Keccak-$f$ [2]. They provide a good trade-off between implementation cost and mixing power, making them well suited for lightweight cryptography.

A formal approach in studying CPMs as a stand alone topic is done in [3], where CPMs were formulated as linear maps between spaces of matrices. Each CPM $\theta$, viewed as an endomorphism of the ring of $m \times n$-matrices, is uniquely determined by an $n \times n$-matrix called the parity folding matrix of $\theta$. There has been some emphasis on studying CPMs where its parity folding matrix belongs to the class of circulant matrices (see [4] for more details about circulant matrices). These CPMs are called circulant CPMs which we abbreviate by CCPMs. Due to the symmetric properties of circulant matrices, CCPMs have a good worst-case behaviour for the purpose of mixing bits. The $\theta$ mixing layers of Xoodoo and Keccak-$f$ are examples of CCPMs.

In [3], a criterion was provided to determine the invertibility of a CCPM by studying the corresponding parity folding matrix. It was also shown that the set of invertible CCPMs forms a group. This is everything that is known so far about the algebraic properties of CCPMs. A reason might be the complexity of describing CCPMs in terms of linear algebra, which at first glance might indicate that no strong conclusions can be drawn regarding their algebraic structure. It turns out that viewing CCPMs as $R$-module homomorphisms, where $R$ is the ring of circulant matrices, is very effective in studying CCPMs. As a result, many interesting properties can be extracted with this approach, and some known results like the invertibility criterion resurfaced as trivial concepts from module theory.

The order of the linear layer in the round function of a cryptographic primitive is relevant in the resistance against invariant subspace attacks, where low order indicates a potential weakness [5]. The linear layer of Xoodoo is a composition of a circulant bit permutation, a CCPM and another circulant bit permutation, and it was numerically determined that the linear layer has an order of only 32. A mathematical explanation for this low order however remained absent. As it turns out, such an explanation can be found by using the module theoretic approach which we used for studying CCPMs. It would be interesting to know if we can find variants of the linear layer of Xoodoo with a higher order, by means of finding new compositions, and/or by changing the dimensions of the state of the permutations.

## Outline

In Section 2, we present a mathematical framework based on commutative algebra as a foundation to studying column parity mixers, which includes module theory and localization of rings.

In Section 3, we introduce circulant rings, which are a generalization of the ring of circulant matrices. We provide a full classification of local circulant rings, as well the corresponding algebraic properties. Moreover, we give a geometric interpretation of circulant rings by considering free modules over these type of rings.

In Section 4, we introduce a generalization of CPMs where we define them as $R$-linear maps of free $R$-modules, where $R$ is a commutative ring with unity. We exploit the algebraic properties of $R$ to gain a deeper understanding of the algebraic structure of CPMs. These include a full description of the eigenspaces of a CPM viewed as an $R$-module homomorphism, and the order of a CPM.

In Section 5, we show that the linear layer of Xoodoo can be interpreted as an $R_{4,32}$-linear map of the free 3-dimensional $R_{4,32}$-module $R_{4,32}^3$, where $R_{4,32}$ is a local circulant ring. We introduce DCD-compositions, which are compositions with a similar structure to that of the linear layer of Xoodoo. We use the results of Sections 3 and 4 to construct DCD-compositions with a higher order.

## Contributions

The main contributions of this paper are the results presented in Sections 3, 4 and 5. These results combined provide a new point of view to CCPMs, which is much more fruitful from an algebraic point of view compared to the original definition .

## Notation

The **cardinality** of a set $S$ is denoted as $\#S$. The set of all positive integers strictly greater than 0 is denoted as $\mathbb{Z}_{>0}$.

Given a commutative ring $R$ with unity, we denote the **multiplicative group of invertible elements** of $R$ by $R^*$. We refer to $\mathrm{Spec}(R)$ as the **set of all proper prime ideals**, and $\mathrm{MaxSpec}(R)$ as the **set of all maximal ideals** of $R$. Given an ideal $\mathfrak{a}$ in $R$, the **radical** of $\mathfrak{a}$ is denoted by $r(\mathfrak{a})$.

The **ring- or set of all $m \times m$-matrices over ring** $R$ is denoted by $\mathrm{M}_m(R)$. The **multiplicative group of $m \times m$-invertible matrices over a ring** $R$ is denoted by $\mathrm{GL}_m(R)$. Moreover, $\mathrm{SL}_m(R)$ is the set of matrices $M \in \mathrm{GL}_m(R)$ where $\det(A) = 1_R$. For a matrix $A \in \mathrm{M}_m(R)$, we say that $A_{ij}$ is the **entry in the $i$-th row and $j$-th column**. Here we use to the convention that the **indexing of coordinates** runs from 0 to $m-1$, hence $0 \leq i, j \leq m-1$. We refer to $I_m$ as the **identity matrix**, and $0_{m\times m}$ as the **zero matrix** in $\mathrm{M}_m(R)$.

For $\mathbb{F}$ a field, we denote $\mathbb{F}^n$ as the $n$-dimensional vector space over $\mathbb{F}$. Its vectors are considered as **column (vertical) vectors**, unless stated otherwise. We **index the coordinates** of a (column) vector $v \in \mathbb{F}^n$ from 0 to $n-1$. Naturally, for $0 \leq i \leq n-1$, $v_i$ is the $i$-th coordinate of $v$. We denote the **transpose** of $v$ by $v^\mathsf{T}$. If for example $v$ is a row vector, $v^\mathsf{T}$ is a column vector. We refer to $\mathsf{e}_y$ as the **$y$-th standard unit vector of** $\mathbb{F}^n$ where $0 \leq y \leq n-1$. The zero vector is defined as $0_n$.

Tor$(G)$ is the **torsion subgroup** of a group $G$, i.e. the elements in $G$ with finite order. For $f$ in some finite group $G$, we denote the **order** of $f$ by ord$(f)$. When $G = (\mathbb{Z}/m\mathbb{Z})^*$, we denote the **multiplicative order** of $g \in (\mathbb{Z}/m\mathbb{Z})^*$ as $\text{ord}_m(g)$. Moreover, gcd and lcm represent the **greatest common divisor** and the **least common multiple** respectively.

# 2 Algebraic Framework

This section contains a brief summary of the required algebraic prerequisites for our research. We heavily rely on concepts from commutative algebra. See [6], [7] and [8] for a more detailed treatment of these topics.

## 2.1 Local Rings and Localization

An important class of rings in commutative algebra are local rings. A ring $R$ is called **local** if it has a unique maximal ideal, which we denote by $\mathfrak{m}$. The field $\mathbb{F} := R/\mathfrak{m}$ is defined as the **residue field** of $R$. We have the natural quotient map

$$q_R : R \to R/\mathfrak{m} \cong \mathbb{F},\ r \mapsto r \bmod \mathfrak{m}. \tag{1}$$

To ease notation, we denote $q_R(r) = r \bmod \mathfrak{m}$ as $\overline{r}$. For local rings, it is known that $r \in R$ is invertible if and only if $r \notin \mathfrak{m}$.

Local rings have been well studied in commutative algebra, resulting into many interesting properties. For example, finitely generated modules over a local ring are closely related to vector spaces over fields due to Nakayama's Lemma [6]. We utilize these properties to non-local commutative rings by applying a technique called **localization**, which is a technique where given a non-local ring $R$ and for a chosen $\mathfrak{p} \in \text{Spec}(R)$, one can construct a local ring $R_\mathfrak{p}$ where its maximal ideal is denoted by $\mathfrak{p} \cdot R_\mathfrak{p}$. Intuitively, we make all elements in $R$ outside $\mathfrak{p}$ invertible. Details about this construction can be found in [6]. For now, it suffices to know that we have a natural ring homomorphism

$$l_\mathfrak{p} : R \to R_\mathfrak{p},\ r \mapsto \frac{r}{1_R}.$$

More about local rings and localization can be found in many books treating commutative algebra, like [7] and [6].

## 2.2 Modules and Linear Algebra

Modules can be considered as a generalization of vector spaces. In its most general form, it is defined as follows:

**Definition 1** ([6]) Let $R$ be a ring. An $R$**-module** consists of the pair $(V, \mu)$ where $V$ is a commutative group and $\mu$ is a mapping of $R \times V$ to $V$ such that, if we write

$ax$ for $\mu(a, x)$ where $a \in R$ and $x \in V$, the following properties are satisfied:

$$\begin{aligned} r(x+y) &= rx + ry \\ (r_1 + r_2)x &= r_1 x + r_2 x \\ (r_1 r_2)x &= r_1(r_2 x) \\ 1x &= x \qquad\qquad (r, r_1, r_2 \in R \text{ and } x, y \in V). \end{aligned}$$

*Remark 1* A trivial but important example of an $R$-module is the ring $R$ itself, considered as a commutative group under addition, and where $\mu : R \times R \to R$ is the multiplication map.

**Definition 2** An $R$-**submodule** $V'$ of $V$ is a subgroup of $V$ such that $r \cdot v' \in V'$ for all $r \in R$ and $v' \in V'$.

*Example 1* Let $\mathfrak{a}$ be an ideal of $R$ and define

$$\mathfrak{a}V := \left\{ \sum_{i=0}^{t} a_i \cdot v_i \mid a_i \in \mathfrak{a}, v_i \in V, t \in \mathbb{Z}_{>0} \right\},$$

which in words means that $\mathfrak{a}V$ consists of finite sums of terms of the form $a \cdot v$ where $a \in \mathfrak{a}$ and $v \in V$. Unless $V = \{0\}$, we have that $\mathfrak{a}V$ is in many cases a proper $R$-submodule of $V$. Nakayama's Lemma [6] is very useful in studying these types of submodules.

We are mainly interested in **free modules** of finite rank. An $R$-module $V$ if called **free** of rank $m$ if there exist elements $\mathsf{e}_0, ..., \mathsf{e}_{m-1} \in V$ such that every element $v \in V$ is **uniquely** expressed as

$$v = \sum_{i=0}^{m-1} r_i \cdot \mathsf{e}_i \qquad\qquad r_i \in R. \tag{2}$$

In algebraic terms, a free module $V$ of rank $m$ is of the form $V = \bigoplus_{i=0}^{m-1} R$, which we also denote as $R^m$. We call $\{\mathsf{e}_0, ..., \mathsf{e}_{m-1}\}$ an $R$-**basis** of $V$. By fixing a basis, every element $v \in V$ is represented by the column vector $v = (r_0, ..., r_{m-1})^{\mathsf{T}}$, where addition is defined coordinate-wise.

## 2.3 Endomorphisms

Free modules have a lot in common with vector spaces. Not only because of the unique representation of elements as in (2), but also in terms of linear transformations.

**Definition 3** Let $V_1$ and $V_2$ be $R$-modules. Then an $R$-**linear map** from $V_1$ to $V_2$ is a map $\theta : V_1 \to V_2$ such that for all $a, b \in V_1$ and $r \in R$, we have

$$\theta(a + b) = \theta(a) + \theta(b)$$

$$\theta(ra) = r\theta(a).$$

When $\theta$ is bijective, we say that $\theta$ is an $R$**-isomorphism**. In the special case when $V_1 = V_2 = V$, we say that $\theta$ is an $R$**-endomorphism** of $V$, and we denote the set of all these endomorphism by $\mathrm{End}_R(V)$.

When considering a free $R$-module $V \cong R^m$, every $R$-endomorphism is uniquely represented by an $m \times m$-matrix with entries in $R$ and vice versa by applying the conventional matrix multiplication. In particular,

$$\mathrm{End}_R(R^m) \cong \mathrm{M}_m(R).$$

For matrices $A, B \in \mathrm{M}_m(R)$, we have for the **determinant** that

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

Invertibility of a matrix in $\mathrm{M}_m(R)$ can be determined by the determinant.

**Proposition 1** *Let $A \in \mathrm{M}_m(R)$. Then $A$ is invertible if and only if $\det(A)$ is invertible in $R$.*

**Lemma 2** *Let $A \in \mathrm{Tor}(\mathrm{GL}_m(R))$. Then $\mathrm{ord}(\det(A)) \mid \mathrm{ord}(A)$.*

The notions of eigenvectors and eigenvalues remain very similar as in linear algebra: $v \in V$ is an **eigenvector** of $\theta$ if there exists $\lambda \in R$ such that $\theta(v) = \lambda \cdot v$. $\lambda$ is called the **eigenvalue** of $v$ under $\theta$. The concept of an eigenbasis is also very similar: $\theta$ has an **eigenbasis** if there exists a basis of $V$ consisting of eigenvectors of $\theta$.

## 2.4 Induced Homomorphisms and Eigenvectors

Let $R$ and $S$ be commutative rings with unity, and let $\varphi : R \to S$ be a ring homomorphism. In particular, $\varphi$ induces on $S$ a natural $R$-homomorphism where we define $r \cdot s := \varphi(r) \cdot s$ for all $r \in R$ and $s \in S$. Hence $\varphi$ is also an $R$-module homomorphism. This naturally extends to an $R$-linear map of free modules, which we also denote by $\varphi$:

$$\varphi : R^m \to S^m,\ (r_0, ..., r_{m-1}) \mapsto (\varphi(r_0), ..., \varphi(r_{m-1})).$$

$\varphi$ also induces the (ring)-homomorphism of matrices

$$\overline{\varphi} : \mathrm{M}_m(R) \to \mathrm{M}_m(S),\ A = (A_{ij})_{0 \le i,j \le m-1} \mapsto \varphi(A) := (\varphi(A_{ij}))_{0 \le i,j \le m-1}. \tag{3}$$

The homomorphism of matrices can be interpreted in terms of endomorphisms, meaning that $\overline{\varphi}$ naturally induces a map

$$\overline{\varphi} : \mathrm{End}_R(R^m) \to \mathrm{End}_S(S^m),\ \theta \mapsto \varphi(\theta),$$

satisfying the commutative diagram:

$$\begin{array}{ccc} R^m & \xrightarrow{\theta} & R^m \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ S^m & \xrightarrow{\overline{\varphi}(\theta)} & S^m \end{array}.$$

For $\theta \in \mathrm{End}_R(R^m)$, we denote $\overline{\varphi}(\theta)$ the **induced $S$-endomorphism** induced by $\varphi$. Induced endomorphisms behave well with respect to eigenvectors.

**Lemma 3** *Let $v \in R^m$ be an eigenvector of $\theta \in \mathrm{End}_R(R^m)$ with eigenvalue $\lambda$. Then $\varphi(v)$ is an eigenvector of $\overline{\varphi}(\theta) \in \mathrm{End}_S(S^m)$ with eigenvalue $\varphi(\lambda)$.*

*Proof* By commutativity of the above diagram, we get

$$\overline{\varphi}(\theta)(\varphi(v)) = \varphi(\theta(v)) = \varphi(\lambda \cdot v) = \varphi(\lambda) \cdot \varphi(v),$$

which concludes the proof. □

If $\theta$ admits an eigenbasis in $R^m$, it is not always the case that $\varphi(\theta)$ also admits an eigenbasis in $S^m$. In this paper however, we only consider two types of induced homomorphisms which do preserve the eigenbases.

### 2.4.1 Type I: Quotient Map of Local Rings

**Definition 4** For $R$ a local ring with the quotient map $q_R : R \to R/\mathfrak{m} \cong \mathbb{F}$, we have the isomorphism $V/\mathfrak{m}V \cong \mathbb{F}^m$, where $V = R^m$. For $\theta \in \mathrm{End}_R(V)$, we denote the **induced $\mathbb{F}$-endomorphism** by $\overline{\theta} \in \mathrm{End}_{\mathbb{F}}(V/\mathfrak{m}V)$.

The induced endomorphism $\overline{\theta}$ satisfies the following commutative diagram:

$$\begin{array}{ccc} R^m & \xrightarrow{\theta} & R^m \\ \downarrow{\scriptstyle q_R} & & \downarrow{\scriptstyle q_R} \\ \mathbb{F}^m & \xrightarrow{\overline{\theta}} & \mathbb{F}^m \end{array}.$$

**Proposition 4** *Let $R$ be a local ring, and assume that $\theta \in \mathrm{M}_m(R)$ has an eigenbasis. Then $\overline{\theta}$ has an eigenbasis over $\mathbb{F}$ in $V/\mathfrak{m}V$.*

**Proposition 5** (**Nakayama's Lemma over local rings**) *Let $R$ be a local ring, and let $V$ be a finitely generated $R$-module. Then any set of generators of $V$ over $R$*

*naturally induces a generating set of the* $\mathbb{F}$*-vector space* $V/\mathfrak{m}V$*. Conversely, any set of generators of* $V$ *over* $R$ *is induced by a unique basis of* $V/\mathfrak{m}V$*.*

*Proof* This is a direct consequence of applying local rings to Nakayama's Lemma [6], which is a well-known result in commutative algebra. □

**Lemma 6** *Let* $R$ *be a local ring with maximal ideal* $\mathfrak{m}$ *and residue field* $\mathbb{F}$*, let* $V = R^m$ *and let* $v \in V \setminus \mathfrak{m}V$ *be an eigenvector of* $\theta \in \mathrm{M}_m(R)$*. Then* $\overline{v}$ *is a non-zero eigenvector of* $\overline{\theta}$ *with eigenvalue* $\overline{\lambda} \in \mathbb{F}$*.*

*Proof* Since $v \notin \mathfrak{m}V$, we have that $\overline{v}$ is non-zero in $V/\mathfrak{m}V$. The rest is an immediate consequence of Lemma 3. □

*Proof (Proposition 4)* This is a direct consequence of Lemmas 5 and 6. □

### 2.4.2 Type II: Localization Map

**Definition 5** Let $R$ be any commutative ring and let $V = R^m$. For $\mathfrak{p} \in \mathrm{Spec}(R)$, we define the localized free $R_\mathfrak{p}$-module $R_\mathfrak{p}^m$ by $V_\mathfrak{p}$, where the ring homomorphism $l_\mathfrak{p} : R \to R_\mathfrak{p}$ induces the $R$-module homomorphism $l_\mathfrak{p} : V \to V_\mathfrak{p}$. For $\theta \in \mathrm{End}_R(V)$, we denote the **induced** $R_\mathfrak{p}$**-endomorphism** by $\theta_\mathfrak{p} \in \mathrm{End}_{R_\mathfrak{p}}(V_\mathfrak{p})$.

The induced endomorphism $\theta_\mathfrak{p}$ satisfies the following commutative diagram:

$$\begin{array}{ccc} R^m & \xrightarrow{\theta} & R^m \\ \downarrow{\scriptstyle l_\mathfrak{p}} & & \downarrow{\scriptstyle l_\mathfrak{p}} \\ R_\mathfrak{p}^m & \xrightarrow{\theta_\mathfrak{p}} & R_\mathfrak{p}^m \end{array}.$$

**Proposition 7** *Assume that* $\theta \in \mathrm{M}_m(R)$ *has an eigenbasis, then* $\theta_\mathfrak{p}$ *has an eigenbasis.*

**Lemma 8** *Let* $\mathfrak{p} \in \mathrm{Spec}(R)$*, and let* $B_V := \{v_0, ..., v_{m-1}\} \subset V$ *a basis of* $V$*, then* $B_{V_\mathfrak{p}} := \left\{\frac{v_0}{1_R}, ..., \frac{v_{m-1}}{1_R}\right\}$ *is a basis of* $V_\mathfrak{p}$*.*

*Proof* Let $v_\mathfrak{p} = \left(\frac{a_0}{b_0}, ..., \frac{a_{m-1}}{b_{m-1}}\right) \in V_\mathfrak{p}$. Define $\hat{b} := \prod_{i=0}^{m-1} b_i$ and $\hat{b}_j := \prod_{0 \le i \le m-1, i \ne j} b_i$, which are elements in $R \setminus \mathfrak{p}$ since this set is multiplicative set. Observe that

$$\hat{b} \cdot v_\mathfrak{p} = \left(\frac{\hat{b}_0 \cdot a_0}{1_R}, ..., \frac{\hat{b}_{m-1} \cdot a_{m-1}}{1_R}\right),$$

which in contained in the image of $l_{\mathfrak{p}}$. Hence there exist $r_0, ..., r_{m-1} \in R$ such that $\hat{b} \cdot v_{\mathfrak{p}} = \sum_{i=0}^{m-1} r_i \cdot \left(\frac{v_i}{1_R}\right)$, which implies that

$$v_{\mathfrak{p}} := \sum_{i=0}^{m-1} \frac{r_i}{\hat{b}} \cdot \left(\frac{v_i}{1_R}\right).$$

Hence $B_{V_{\mathfrak{p}}}$ is a generating set of $V_{\mathfrak{p}}$. Since $B_{V_{\mathfrak{p}}}$ has $m$ elements, and $V_{\mathfrak{p}}$ has dimension $m$ as a free $R_{\mathfrak{p}}$-module, we conclude that $B_{V_{\mathfrak{p}}}$ is a basis of $V_{\mathfrak{p}}$. □

*Proof (Proposition 7)* By Lemma 3, if $v \in V$ is an eigenvector of $\theta \in \mathrm{End}_R(V)$ with eigenvalue $\lambda$, then $l_{\mathfrak{p}}(v)$ is an eigenvector of $\theta_{\mathfrak{p}}$ with eigenvalue $l_{\mathfrak{p}}(\lambda) = \frac{\lambda}{1_R}$. The claim follows directly from the above lemma. □

## 2.5 Useful Matrix Identities

We show some matrix identities which are useful for studying column parity mixers. These identities are valid for all commutative rings $R$ with unity.

**Definition 6** Let $a = (a_0, ..., a_{m-1})^{\mathsf{T}} \in R^m$ be an $m$-tuple viewed as a column vector. We define the **column matrix** of $a$ as the $m \times m$-matrix

$$\mathrm{col}(a) = \begin{pmatrix} a_0 & a_0 & \cdots & a_0 \\ a_1 & a_1 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{m-1} & a_{m-1} & \cdots & a_{m-1} \end{pmatrix} \in \mathrm{M}_m(R).$$

**Lemma 9** *Consider the vector $b = (b_0, ..., b_{m-1})^{\mathsf{T}} \in R^m$, then*

$$\mathrm{col}(a) \cdot b = \left(\sum_{i=0}^{m-1} b_i\right) \cdot a.$$

*Proof* This is a matter of simple verification of matrix multiplication. □

**Corollary 10** *Let $a, b \in R^m$, then*

$$\mathrm{col}(a) \cdot \mathrm{col}(b) = \left(\sum_{i=0}^{m-1} b_i\right) \cdot \mathrm{col}(a).$$

**Proposition 11** *Let $a \in R^m$. Then for any $t \in \mathbb{Z}_{>0}$, we have that*

$$\mathrm{col}(a)^t = \left(\sum_{i=0}^{m-1} a_i\right)^{t-1} \cdot \mathrm{col}(a).$$

*Proof* We use induction on $t$. Let $t = 1$, then

$$\left(\sum_{i=0}^{m-1} a_i\right)^{t-1} \cdot \mathrm{col}(a) = \left(\sum_{i=0}^{m-1} a_i\right)^{0} \cdot \mathrm{col}(a) = 1_R \cdot \mathrm{col}(a) = \mathrm{col}(a)^1,$$

which concludes the first induction step.

Now assume our claim is true for $t = k$ for some $k > 1$. For $t = k + 1$, we get

$$\begin{aligned}
\mathrm{col}(a)^{k+1} &= \mathrm{col}(a)^k \cdot \mathrm{col}(a) \\
&= \left(\sum_{i=0}^{m-1} a_i\right)^{k-1} \cdot \mathrm{col}(a)^2 \\
&= \left(\sum_{i=0}^{m-1} a_i\right)^{k-1} \cdot \left(\sum_{i=0}^{m-1} a_i\right) \cdot \mathrm{col}(a) \\
&= \left(\sum_{i=0}^{m-1} a_i\right)^{k} \cdot \mathrm{col}(a),
\end{aligned}$$

where the second equality is due to the induction hypothesis, and the third equality due to Lemma 9. This concludes the induction hypothesis, and thus the proof. □

# 3 Circulant Rings

We introduce circulant rings, which are defined as follows:

**Definition 7 Circulant rings** are commutative rings of the form

$$R_{m_1,\ldots,m_n} := \mathbb{F}_2[X_1, \ldots, X_n]/\langle X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1\rangle.$$

We denote the set of monomials of $R_{m_1,\ldots,m_n}$ as

$$M_{m_1,\ldots,m_n} := \left\{ \prod_{i=1}^{n} X_i^{q_i} \mid 0 \leq q_i \leq m_i - 1 \right\}$$

In this section, we start by introducing an important class of modules over circulant rings, followed by an algebraic analysis of local circulant rings. To ease notation, we define the ideals

$$\begin{aligned}
\mathfrak{a}_{m_1,\ldots,m_n} &:= \langle X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1\rangle, \\
\mathfrak{m}_n := \mathfrak{a}_{1,\ldots,1} &:= \langle X_1 - 1, \ldots, X_n - 1\rangle,
\end{aligned}$$

both being ideals of $\mathbb{F}_2[X_1, \ldots, X_n]$, and where $\mathfrak{m}_n$ is a maximal ideal.

## 3.1 Circulant Modules: A Geometric Interpretation

Consider the vector space

$$V_{m_1,\ldots,m_n} := \bigotimes_{i=1}^{n} \mathbb{F}_2^{m_i}.$$

We define the standard basis of $V_m$ as

$$B_{m_1,\ldots,m_n} := \{\otimes_{i=1}^{n} \mathsf{e}_{j_i} \mid 0 \leq j_i \leq m_i - 1\}\,.$$

There is a natural $R_{m_1,\ldots,m_n}$-module on the vector space $V_{m_1,\ldots,m_n}$. To see this, consider the map:

$$\begin{aligned} \mu_* : M_{m_1,\ldots,m_n} \times B_{m_1,\ldots,m_n} &\to B_{m_1,\ldots,m_n} \\ \left(\prod_{i=1}^{n} X_i^{q_i}, \otimes_{i=1}^{n} \mathsf{e}_{j_i}\right) &\mapsto \otimes_{i=1}^{n} \mathsf{e}_{j_i - q_i \bmod m_i}, \end{aligned}$$

for all $0 \leq j_i \leq m_i - 1$, which $\mathbb{F}_2$-linearly extends to the map

$$\mu : R_{m_1,\ldots,m_n} \times V_{m_1,\ldots,m_n} \to V_{m_1,\ldots,m_n}.$$

Note that $V_{m_1,\ldots,m_n}$ is an $R_{m_1,\ldots,m_n}$-module under $\mu$.

**Definition 8** The natural $R_{m_1,\ldots,m_n}$-action on $V^{\omega}_{m_1,\ldots,m_n}$ for some $\omega \in \mathbb{Z}_{>0}$ induced by $\mu$ is called the **circulant module** of rank $\omega$.

**Proposition 12** *A circulant module of rank $\omega$ is a free $R_{m_1,\ldots,m_n}$-module of rank $\omega$.*

*Proof* It suffices to show this for circulant modules of rank 1. Consider the following natural 1-to-1 mapping $\vartheta : B_{m_1,\ldots,m_n} \to M_{m_1,\ldots,m_n}$ such that

$$\vartheta_* : B_{m_1,\ldots,m_n} \to M_{m_1,\ldots,m_n} : \otimes_{i=1}^{n} \mathsf{e}_{j_i} \mapsto \prod_{i=1}^{n} X_i^{j_i},$$

which linearly extends to the bijective map

$$\vartheta : V_{m_1,\ldots,m_n} \to R_{m_1,\ldots,m_n}.$$

This map can be easily verified to be a $R_{m_1,\ldots,m_n}$-linear map, hence we have constructed a natural $R_{m_1,\ldots,m_n}$-isomorphism. □

*Remark 2* From the above proposition, we have the commutative diagram

$$\begin{array}{ccc} R_{m_1,\ldots,m_n} \times V_{m_1,\ldots,m_n} & \xrightarrow{\mu} & V_{m_1,\ldots,m_n} \\ \downarrow{\scriptstyle \mathrm{id}\times\vartheta} & & \downarrow{\scriptstyle \vartheta} \\ R_{m_1,\ldots,m_n} \times R_{m_1,\ldots,m_n} & \xrightarrow{\cdot} & R_{m_1,\ldots,m_n} \end{array},$$

where the dot in the lower row is the natural product operation of the ring $R_{m_1,\ldots,m_n}$. The vertical maps are one-to-one correspondences, which implies that the circulant $R_{m_1,\ldots,m_n}$-module $V_{m_1,\ldots,m_n}$ is indeed free of rank one, with corresponding $R_{m_1,\ldots,m_n}$-module isomorphism $\vartheta$.

*Example 2* Consider the ring $R_m = \mathbb{F}_2[X]/\langle X^m - 1\rangle$. The $R_m$-module on $\mathbb{F}_2^m$ is equivalent to the action of $m$-dimensional circulant matrices over $\mathbb{F}_2$.

*Example 3* Consider the ring $R_{4,32}$. An interesting case is the free module action of $R_{4,32}$ over $(\mathbb{F}_2^4 \otimes \mathbb{F}_2^{32})^3$. By Proposition 12, this module is isomorphic to the free module $R_{4,32}^3$, which is in particular useful for studying the linear layer of Xoodoo which will be covered later in this paper.

## 3.2 Classification of Local Circulant Rings

We prove that a circulant ring $R_{m_1,...,m_n}$ is a local ring if and only if $m_i$ is a power of 2 for all $1 \leq i \leq m$.

**Lemma 13** *$\mathfrak{m}_n$ is the unique maximal ideal containing the ideal $\mathfrak{a}_{2^{l_1},...,2^{l_n}}$, where $l_1, ..., l_n \in \mathbb{Z}_{\geq 0}$.*

*Proof* Since $\mathbb{F}_2[X_1, ..., X_n]$ has characteristic 2, we have that

$$X^{2^{l_i}} - 1 = (X-1)^{2^{l_i}}, \tag{4}$$

for each $1 \leq i \leq n$, which immediately implies that $\mathfrak{a}_{2^{l_1},...,2^{l_n}} \subseteq \mathfrak{m}_n$. Note that (4) also implies that $\mathfrak{m}_n$ is contained in the radical of $\mathfrak{a}_{2^{l_1},...,2^{l_n}}$, which in turn implies that $\mathfrak{m}_n = r(\mathfrak{a}_{2^{l_1},...,2^{l_n}})$. Since every maximal ideal containing $\mathfrak{a}_{2^{l_1},...,2^{l_n}}$ must contain $r(\mathfrak{a}_{2^{l_1},...,2^{l_n}})$, it must also contain $\mathfrak{m}_n$. But $\mathfrak{m}_n$ is already maximal, hence uniqueness is proven. □

**Theorem 14** *A circulant ring $R_{m_1,...,m_n}$ is a local ring if and only if $m_i$ is a power of 2 for all $1 \leq i \leq m$.*

*Proof* " $\Leftarrow$ " - Assume that $m_i$ is of the form $2^{l_i}$, where $l_i \in \mathbb{Z}_{\geq 0}$ for all $1 \leq i \leq n$. Since $\mathfrak{m}_n$ is the unique maximal ideal containing $\mathfrak{a}_{2^{l_1},...,2^{l_n}}$ by the above lemma, we have that $\overline{\mathfrak{m}}_n$ must be the unique maximal in $R_{2^{l_1},...,2^{l_n}}$ as shown in [7]. This shows that $R_{2^{l_1},...,2^{l_n}}$ is local.

" $\Rightarrow$ " - Assume that there exists $m_j$ for some $1 \leq j \leq n$ such that $m_j$ is not a power of 2. We may assume without loss of generality that $m_1$ is not a power of 2. Consider the ideal $\mathfrak{m}' := \langle \Phi_{m_1}(X_1), X_2 - 1, ..., X_n - 1\rangle$ where $\Phi_{m_1}$ is the $m_1$-th cyclotomic polynomial. Note that $\Phi_{m_1}$ has degree larger than 1, since $m_1$ is not a power of 2. By the third isomorphism theorem for rings, we get

$$\begin{aligned} R_{m_1,...,m_n}/\overline{\mathfrak{m}}' &= (\mathbb{F}_2[X_1, ..., X_n]/\mathfrak{a}_{m_1,...,m_n})/(\mathfrak{m}'/\mathfrak{a}_{m_1,...,m_n}) \\ &\cong \mathbb{F}_2[X_1, ..., X_n]/\mathfrak{m}' \cong \mathbb{F}_2[X_1]/\Phi_{m_1}(X_1). \end{aligned}$$

Since $\Phi_{m_1}$ is irreducible in $\mathbb{F}_2[X]$, we have that $\mathbb{F}_2[X_1]/\Phi_{m_1}(X_1)$ is a field isomorphic to $\mathrm{GF}(2^{\deg(\Phi_{m_1})})$. Hence $\overline{\mathfrak{m}}'$ is a maximal ideal of $R_{m_1,...,m_n}$ which is not equal to $\mathfrak{m}_n$, thus $R_{m_1,...,m_n}$ is not a local ring. This concludes the proof. □

**Note 15** *For the remainder of this section, we denote $\overline{\mathfrak{m}}_n$ simply by $\mathfrak{m}_n$, which will not cause confusion due to uniqueness of $\mathfrak{m}_n$.*

**Lemma 16** *The residue field of a local circulant ring $R$ is isomorphic to $\mathbb{F}_2$, with quotient map*

$$q_R : R \to \mathbb{F}_2,\ f \mapsto f(1^n).$$

*Proof* By the third isomorphism theorem for rings, we get

$$\begin{aligned} R_{2^{l_1},\ldots,2^{l_n}}/\overline{\mathfrak{m}}_n &= (\mathbb{F}_2[X_1,\ldots,X_n]/\mathfrak{a}_{2^{l_1},\ldots,2^{l_n}})/(\mathfrak{m}_n/\mathfrak{a}_{2^{l_1},\ldots,2^{l_n}}) \\ &\cong \mathbb{F}_2[X_1,\ldots,X_n]/\mathfrak{m}_n \cong \mathbb{F}_2, \end{aligned}$$

where by construction the last isomorphism is indeed the map $f \mapsto f(1^n)$. □

*Remark 3* For $f \in R$, we denote $q_R(f)$ by $\overline{f}$.

**Corollary 17** *For $R$ a local circulant ring, we have that $f \in R$ is invertible if and only if $f(1^n) \neq 0$.*

*Proof* Since $R$ is a local ring, we have that $f$ is invertible if and only if $f \notin \mathfrak{m}_n$. This is indeed equivalent to $f(1^n) \neq 0$ by the above lemma. □

**Corollary 18** *For $R$ a local circulant ring, we have that $f \in R$ is invertible if and only if $f$ contains an odd number of terms.*

*Proof* By the above corollary, we conclude that every term is invertible. If $f$ has $t$ terms, then $f(1^n) \equiv t \bmod 2$ which is not equal to 0 if and only if $t$ is odd. This concludes the proof. □

## 3.3 General Linear Group over Local Circulant Rings

Let $R := R_{2^{l_1},\ldots,2^{l_n}}$ be a local circulant ring, and consider $q_R$ as in Lemma 16. This map can be extended to the map of $m \times m$-matrices

$$q_{m,R} : \mathrm{M}_m(R) \to \mathrm{M}_m(\mathbb{F}_2),\ A := (A_{ij})_{0\leq i,j\leq m-1} \mapsto (\overline{A_{ij}})_{0\leq i,j\leq m-1}.$$

*Remark 4* Just as for the case of $q_R$, for $A \in \mathrm{M}_m(\mathbb{F}_2)$, we denote $q_{m,R}(A)$ by $\overline{A}$.

Observe that $\det(\overline{A}) = \overline{\det(A)}$, since the expression of the determinant consists of finite sums of finite products of entries of $A$, which split under $q_R$. This implies that $q_{m,R}$ maps $\mathrm{GL}_m(R)$ to $\mathrm{GL}_m(\mathbb{F}_2)$. Moreover, we have that the preimage of $\mathrm{GL}_m(\mathbb{F}_2)$ under $q_{m,R}$ is exactly $\mathrm{GL}_m(R)$, as a result from the following lemma:

**Lemma 19** *Let $A \in \mathrm{M}_m(R)$. Then $A \in \mathrm{GL}_m(R)$ if and only if $\overline{A} \in \mathrm{GL}_m(\mathbb{F}_2)$.*

*Proof* Due to locality of $R$, we have the following equivalent statements:

$$A \in \mathrm{GL}_m(R) \Leftrightarrow \det(A) \in R^* \Leftrightarrow \det(A) \notin \mathfrak{m}_n \Leftrightarrow \det(\overline{A}) \in \mathbb{F}_2^* \Leftrightarrow \overline{A} \in \mathrm{GL}_m(\mathbb{F}_2).$$

□

The above lemma implies that $q_{m,R}\,|_{\mathrm{GL}_m(R)}\colon \mathrm{GL}_m(R) \to \mathrm{GL}_m(\mathbb{F}_2)$ is a surjective group homomorphism. Let us denote $q_{m,R}\,|_{\mathrm{GL}_m(R)}$ by $q^*_{m,R}$. From Lemma 19, we conclude that

$$\ker(q^*_{m,R}) = \{I_m + A : A \in \mathrm{M}_m(\mathfrak{m}_n)\}.$$

This implies that

$$\#\ker(q^*_{m,R}) = \#\,\mathrm{M}_m(\mathfrak{m}_n) = (\#\mathfrak{m}_n)^{m^2} = \left(2^{(\prod_{i=1}^n 2^{l_i})-1}\right)^{m^2}, \tag{5}$$

which in particular means that the order of the group $\ker(q^*_{m,R})$ is a power of 2. By Lagrange's theorem, the order of an element $I_m + A \in \ker(q^*_{m,R})$, where $A \in \mathrm{M}_m(\mathfrak{m}_n)$, is of the form $2^\lambda$ where $\lambda \in \mathbb{Z}_{\geq 0}$. Note that

$$(I_m + A)^{2^\lambda} = I_m + A^{2^\lambda},$$

by the binomial theorem of Newton, and since $R$ is of characteristic 2. Hence $\mathrm{ord}(I_m + A)$ is the smallest number of the form $2^\lambda$ such that $A^{2^\lambda} = 0_{m\times m}$. In particular, $A$ is a **nilpotent matrix**.

**Lemma 20** *Let $A \in \mathrm{M}_m(\mathfrak{m}_n)$ and define $l = \max(l_i : 1 \leq i \leq n)$. Then we have $A^{n\cdot 2^l} = 0_{m\times m}$.*

*Proof* In this proof, we use $\mathbb{Z}^n_{\geq 0}$ as an index set, and we let $\mathsf{e}_i$ be the $i$-th unit vector in $\mathbb{Z}^n_{\geq 0}$ where $0 \leq i \leq n-1$.

By assumption of the lemma, there exist matrices $A_{\mathsf{e}_i} \in \mathrm{M}_m(R)$ such that

$$A = \sum_{i=1}^{n} (X_i - 1) \cdot A_{\mathsf{e}_i}. \tag{6}$$

From this, we can construct matrices $A_{j_1\mathsf{e}_1+\cdots+j_n\mathsf{e}_n} \in \mathrm{M}_m(R)$ such that

$$A^2 = \sum_{\substack{0\leq j_1,\ldots,j_n\leq 2\\ j_1+\cdots+j_n=2}} A_{j_1\mathsf{e}_1+\cdots+j_n\mathsf{e}_n} \cdot \prod_{i=1}^{n} (X_i - 1)^{j_i}, \tag{7}$$

where

$$A_{j_1\mathsf{e}_1+\cdots+j_n\mathsf{e}_n} = \sum_{\substack{0\leq j_1,\ldots,j_n\leq 2\\ j_1+\cdots+j_n=2}} A^{j_i}_{\mathsf{e}_i}.$$

Note that the matrices $A_{\mathtt{e}_i}$ satisfying (6) are not unique. For the proof, it suffices to only knowing its existence.

By inductively applying this reasoning, one can show that for all $k \in \mathbb{Z}_{>0}$, there exists a family of matrices $A_{j_1\mathtt{e}_1+\cdots+j_n\mathtt{e}_n} \in \mathrm{M}_m(R)$ where $j_1+\cdots+j_n = k$ such that

$$A^k = \sum_{\substack{0\le j_1,\ldots,j_n\le k \\ j_1+\cdots+j_n=k}} A_{j_1\mathtt{e}_1+\cdots+j_n\mathtt{e}_n} \cdot \prod_{i=1}^{n}(X_i-1)^{j_i}. \tag{8}$$

When $k \ge n\cdot 2^l$, we must have that $j_i \ge 2^{l_i}$ for some $i$, which implies that $\prod_{i=1}^n (X_i - 1)^{j_i} \in \mathfrak{m}_n$ for all $j_1, ..., j_n$ satisfying $j_1+\cdots+j_n = k$. Hence we have $A^{n\cdot 2^l} = 0_{m\times m} \in \mathrm{M}_m(R)$ by applying Equation (8), which concludes the proof. □

**Corollary 21** *For $A \in \ker(q^*_{m,R})$, we have that* $\mathrm{ord}(A) \mid 2^{l+\lceil \log_2(n)\rceil}$.

*Proof* Every element $A \in \ker(q^*_{m,R})$ is of the form $I_m + B$, where $B \in \mathrm{M}_m(\mathfrak{m}_n)$. Observe that

$$2^{l+\lceil \log_2(n)\rceil} = 2^{\lceil \log_2(n)\rceil}\cdot 2^l \ge n\cdot 2^l.$$

From this identity together with the above lemma, we have

$$\begin{aligned} A^{2^{l+\lceil \log_2(n)\rceil}} &= (I_m+B)^{2^{l+\lceil \log_2(n)\rceil}} = I_m^{2^{l+\lceil \log_2(n)\rceil}} + B^{2^{l+\lceil \log_2(n)\rceil}} = I_m + 0_{m\times m} \\ &= I_m, \end{aligned}$$

which concludes the proof. □

# 4 Column Parity Mixers

We introduce a new definition of CPMs which can be viewed as a generalization of the ones defined in [3].

**Definition 9** Let $R$ be a commutative ring with unity. A **column parity mixer** $\theta_z$ (or CPM for short) over $R$ of dimension $m$ where $z = (z_0, ..., z_{m-1})^{\mathsf{T}} \in R^m$, is an $R$-endomorphism over $R^m$ represented by the matrix

$$\theta_z = I_m + \mathrm{col}(z) = \begin{pmatrix} 1_R+z_0 & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1_R+z_1 & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1_R+z_2 & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m-1} & z_{m-1} & z_{m-1} & \cdots & 1_R+z_{m-1} \end{pmatrix}.$$

We say that $z$ is the **parity-folding matrix array**, and $z_0, ..., z_{m-1}$ are the **parity-folding matrices** of $\theta_z$. The set of all CPMs over $R$ of dimension $m$ is denoted by $\mathrm{CPM}_m(R)$.

A CPM over a circulant ring $R$ is called a **circulant column parity mixer**, or CCPM for short.

*Remark 5* The above definition of CPMs is a generalization of the ones defined in [3] since it allows multiple parity-folding matrices. In the special case where $z_0 = z_1 = \cdots = z_{m-1}$, we obtain the original definition of CPMs with only one parity folding matrix.

## 4.1 Characteristic Polynomial and Determinant

In this subsection, we give an expression of the characteristic polynomial and the determinant of a CPM in terms of its parity-folding matrices. We assume for the remainder of this subsection that $\theta_z \in \mathrm{CPM}_m(R)$ for some $m \in \mathbb{Z}_{>0}$ and commutative ring $R$.

**Theorem 22** *The characteristic polynomial $p_{\theta_z}(\lambda)$ of $\theta_z$ is*

$$p_{\theta_z}(\lambda) = \left(\left(1_R + \sum_{i=0}^{m-1} z_i\right) - \lambda\right) \cdot (1_R - \lambda)^{m-1}. \tag{9}$$

*Proof* By definition, $p_{\theta_z}(\lambda) := \det(\theta_z - \lambda \cdot I_m)$. To compute the determinant of $\theta_z - \lambda \cdot I_m$, we use the property that adding up rows (or columns) to **other** rows (or columns) will not affect the determinant. By adding the first column vector to all the other column vectors of $\theta_z$, followed by adding up all the row vectors from the second till the last row vector to the first row vector, we get

$$\begin{aligned}
\det(\theta_z - \lambda \cdot I_m) &= \begin{vmatrix} 1_R + z_0 - \lambda & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1_R + z_1 - \lambda & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1_R + z_2 - \lambda & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m-1} & z_{m-1} & z_{m-1} & \cdots & 1_R + z_{m-1} - \lambda \end{vmatrix} \\
&= \begin{vmatrix} 1_R + z_0 - \lambda & \lambda - 1_R & \lambda - 1_R & \cdots & \lambda - 1_R \\ z_1 & 1_R - \lambda & 0 & \cdots & 0 \\ z_2 & 0 & 1_R - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m-1} & 0 & 0 & \cdots & 1_R - \lambda \end{vmatrix} \\
&= \begin{vmatrix} 1_R + \left(\sum_{i=0}^{m-1} z_i\right) - \lambda & 0 & 0 & \cdots & 0 \\ z_1 & 1_R - \lambda & 0 & \cdots & 0 \\ z_2 & 0 & 1_R - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m-1} & 0 & 0 & \cdots & 1_R - \lambda \end{vmatrix}.
\end{aligned}$$

Denote the last matrix by $A$ and denote $A_{(i,j)}$ as the $m-1 \times m-1$-matrix by removing the $i$-th row and the $j$-th column of $A$. Then

$$\begin{aligned}
\det(\theta_z - \lambda \cdot I_m) &= \det(A) \\
&= \sum_{j=0}^{m-1} (-1)^j \cdot A_{0,j} \cdot \det(A_{(0,j)}) \\
&= A_{0,0} \cdot \det(A_{(0.0)}) + \sum_{j=1}^{m-1} (-1)^j \cdot A_{0,j} \cdot \det(A_{(0,j)}) \\
&= A_{0,0} \cdot \det(A_{(0.0)}),
\end{aligned} \tag{10}$$

where the last equation holds because $A_{0,j} = 0$ for $j > 0$. Observe that $A_{0,0} = \left(1_R + \sum_{i=0}^{m-1} z_i\right) - \lambda$ and $A_{(0,0)} = (1_R - \lambda) \cdot I_{m-1}$, the latter implying that $\det(A_{(0,0)}) = (1_R - \lambda)^{m-1}$. Substituting these values in (10), we obtain

$$\det(\theta_z - \lambda \cdot I_m) = A_{0,0} \cdot \det(A_{(0.0)}) = \left(\left(1_R + \sum_{i=0}^{m-1} z_i\right) - \lambda\right) \cdot (1_R - \lambda)^{m-1},$$

which concludes the proof. □

**Corollary 23** *The determinant of $\theta_z$ equals*

$$\det(\theta_z) = 1_R + \sum_{i=0}^{m-1} z_i.$$

*Proof* The determinant equals the constant term of the characteristic polynomial of $\theta_z$, which from Equation (9) equals $1_R + \sum_{i=0}^{m-1} z_i$. □

**Note 24** *By the above corollary, $p_{\theta_z}(\lambda)$ can be expressed as*

$$p_{\theta_z}(\lambda) = (\det(\theta_z) - \lambda) \cdot (1_R - \lambda)^{m-1}. \tag{11}$$

*We will use this expression for the remainder of this paper.*

## 4.2 Eigenvectors and Eigenspaces

**Lemma 25** *Define*

$$E_1 := \left\{ v = (v_0, ..., v_{m-1})^\mathsf{T} : \sum_{i=0}^{m-1} v_i = 0 \right\}.$$

*Then all elements in $E_1$ have eigenvalue $1_R$, and $E_1$ is a free $R$-module of rank $m-1$.*

*Proof* Observe that for all $v \in E_1$, we have

$$\theta_z(v) = (I_m + \mathrm{col}(z)) \cdot v = v + \left(\sum_{i=0}^{m-1} v_i\right) \cdot z = v + 0 \cdot v = v,$$

which proves that all elements in $E_1$ have eigenvalue $1_R$. Observe that $E_1$ has $m-1$ degrees of freedom, since every $m-1$-tuple of elements in $R$ uniquely determines an element in $E_1$. Hence $E_1$ is a free $R$-module of rank $m-1$. □

**Lemma 26** *The vector $z = (z_0, ..., z_{m-1})^\mathsf{T} \in V$ is an eigenvector of $\theta_z$ with eigenvalue* $\det(\theta_z)$.

*Proof* Observe that

$$\theta_z(z) = (I_m + \mathrm{col}(z)) \cdot z = z + \mathrm{col}(z) \cdot z = z + \left(\sum_{i=0}^{m-1} z_i\right) \cdot z = \left(1_R + \sum_{i=0}^{m-1} z_i\right) \cdot z$$
$$= \det(\theta_z) \cdot z,$$

which finishes the proof. □

**Lemma 27** *Assume that* $\det(\theta_z) - 1_R$ *is invertible in* $R$*, and define*

$$E_2 = \{r \cdot z : r \in R\}.$$

*Then* $E_2$ *is a free* $R$*-submodule of rank* 1*, and* $E_1 \cap E_2 = \{0\}$*.*

*Proof* Observe that for all $r_1, r_2 \in R$ such that $(r_1 - r_2) \cdot z = 0_m$, we have that $(r_1 - r_2) \cdot \left(\sum_{i=0}^{m-1} z_i\right) = 0$. Since $\sum_{i=0}^{m-1} z_i = \det(\theta_z) - 1_R$ is invertible, it must be true that $r_1 = r_2$. This shows that $E_2$ is a free $R$-submodule of rank 1.

Let $x \in E_2$, then there exists $r_x \in R$ such that $x = r_x \cdot z \in E_2$. Note that

$$x = r_x \cdot z \in E_1 \iff \sum_{i=0}^{m-1} r_x \cdot z_i := r_x \cdot \left(\sum_{i=0}^{m-1} z_i\right) := r_x \cdot (\det(\theta_z) - 1_R) = 0. \quad (12)$$

Since by our assumption $\det(\theta_z) - 1_R$ is invertible in $R$, Equation (12) holds if and only if $r_x = 0$, which implies that $x \in E_1$ if and only if $x = 0$. This implies that $E_1 \cap E_2 = \{0\}$, which concludes the proof. □

**Proposition 28** *Assume that* $\det(\theta_z) - 1_R$ *is invertible in* $R$*, then* $V$ *is a direct sum of eigenspaces* $E_1$ *and* $E_2$ *of* $\theta_z$ *with eigenvalues* $1_R$ *and* $\det(\theta_z)$ *respectively.*

*Proof* This is immediate from Lemmas 25, 26 and 27. □

**Theorem 29** *Assume that* $\det(\theta_z) - 1_R$ *is not invertible, then* $\theta_z$ *does not have an eigenbasis.*

*Proof* Since $\det(\theta_z) - 1_R$ is not invertible in $R$, there exists a maximal ideal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$ such that $\det(\theta_z) - 1_R \in \mathfrak{m}$. In particular, $\det(\theta_z) \equiv 1_R \bmod \mathfrak{m}$.

Assume to the contrary that $\theta_z$ has an eigenbasis. Then by Proposition 7, the induced $R_\mathfrak{m}$-endomorphism

$$(\theta_z)_\mathfrak{m} : V_\mathfrak{m} \to V_\mathfrak{m},$$

also has an eigenbasis.

Define the field $\mathbb{F}_\mathfrak{m} := R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$ (this is a field because $R_\mathfrak{m}$ is a local ring) and consider the $\mathbb{F}_\mathfrak{m}$-module $V_\mathfrak{m}/(\mathfrak{m}R_\mathfrak{m})V_\mathfrak{m}$. Note that $V_\mathfrak{m}/(\mathfrak{m}R_\mathfrak{m})V_\mathfrak{m}$ is an $m$-dimensional vector space over $\mathbb{F}_\mathfrak{m}$, which implies that $V_\mathfrak{m}/(\mathfrak{m}R_\mathfrak{m})V_\mathfrak{m} \cong \mathbb{F}_\mathfrak{m}^m$. By Proposition 4, the vector space $\mathbb{F}_\mathfrak{m}^m$ has an eigenbasis of the induced map $\overline{(\theta_z)_\mathfrak{m}} : \mathbb{F}_\mathfrak{m}^m \to \mathbb{F}_\mathfrak{m}^m$. Since $\mathbb{F}_\mathfrak{m} := R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} \cong R/\mathfrak{m}$, the corresponding matrix of $\overline{(\theta_z)_\mathfrak{m}}$ is the matrix of $\theta_z$

where all entries are taken modulo $\mathfrak{m}$. For this reason, the characteristic polynomial of $\overline{(\theta_z)_\mathfrak{m}}$ is the polynomial

$$p_{\overline{(\theta_z)_\mathfrak{m}}}(\lambda) = \left(\overline{\det(\theta_z)} - \lambda\right) \cdot (1-\lambda)^{m-1}. \tag{13}$$

Since $\det(\theta_z) \equiv 1_R \bmod \mathfrak{m}$, we have that $\overline{\det(\theta_z)} = 1$ which implies that the only eigenvalue of $\overline{(\theta_z)_\mathfrak{m}}$ is 1. Let $\overline{E}_1$ be the eigenspace of $\overline{(\theta_z)_\mathfrak{m}}$ with eigenvalue 1. By standard linear algebra over fields, we get

$$\overline{E}_1 := \ker\left(\overline{(\theta_z)_\mathfrak{m}} - I_m\right) = \ker(I_m + \mathrm{col}(\overline{z}) - I_m) = \ker(\mathrm{col}(\overline{z})).$$

Note that $\dim(\overline{E}_1) = m-1$ since $\mathrm{col}(\overline{z})$ has rank 1. But then

$$\dim\left(\overline{E}_1\right) < \dim(V_\mathfrak{m}/(\mathfrak{m}R_\mathfrak{m})V_\mathfrak{m}) = m,$$

which means that $\overline{E}_1$ is not an eigenbasis of $\overline{(\theta_z)_\mathfrak{m}}$. This contradicts our assumption, hence $\theta_z$ does not have an eigenbasis. □

## 4.3 Group of Invertible Column Parity Mixers

**Lemma 30** *Let $\theta_z, \theta_{z'} \in \mathrm{CPM}_m(R)$, then*

$$\theta_z \cdot \theta_{z'} = \theta_{z' + \det(\theta_{z'})z} \in \mathrm{CPM}_m(R),$$

*which in particular implies that $\mathrm{CPM}_m(R)$ is closed under multiplication.*

*Proof* This is due to the following:

$$\begin{aligned}
\theta_z \cdot \theta_{z'} &= (I_m + \mathrm{col}(z)) \cdot (I_m + \mathrm{col}(z')) \\
&= I_m + \mathrm{col}(z) + \mathrm{col}(z') + \mathrm{col}(z) \cdot \mathrm{col}(z') \\
&= I_m + \mathrm{col}(z) + \mathrm{col}(z') + \left(\sum_{i=0}^{m-1} z'_i\right) \cdot \mathrm{col}(z) \\
&= I_m + \mathrm{col}\left(z' + \left(1_R + \sum_{i=0}^{m-1} z'_i\right) \cdot z\right) \\
&= I_m + \mathrm{col}(z' + \det(\theta_{z'}) \cdot z),
\end{aligned}$$

where the third equation is due to Corollary 10. □

**Lemma 31** *Let $\theta_z \in \mathrm{CPM}_m(R)$ be invertible, then*

$$\theta_z^{-1} = \theta_{-z \cdot \det(\theta_z)^{-1}} \in \mathrm{CPM}_m(R).$$

*Proof* Since $\theta_z$ is invertible, we have that $\det(\theta_z)$ is invertible in $R$, hence $\det(\theta_z)^{-1}$ is well-defined. Then

$$\theta_{z'} \cdot \theta_z = I_m \iff z + \det(\theta_z) \cdot z' = 0 \iff z' = -z \cdot \det(\theta_z)^{-1},$$

which concludes the proof. □

**Proposition 32** *The set* $\mathrm{CPM}_m^*(R)$ *consisting of all invertible CPMs forms a subgroup of* $\mathrm{GL}_m(R)$.

*Proof* By Lemma 30, $\mathrm{CPM}_m^*(R)$ is closed under multiplication. Moreover, the inverse of a CPM is also a CPM by Lemma 31. This implies that $\mathrm{CPM}_m^*(R)$ is indeed a subgroup of $\mathrm{GL}_m(R)$. □

**Lemma 33** *Let* $R$ *be a ring of prime characteristic* $p$*, and let* $\theta_z \in \mathrm{CPM}_m^*(R)$ *such that* $\det(\theta_z) = 1_R$ *and* $\theta_z \neq I_m$*. Then* $\mathrm{ord}(\theta_z) = p$.

*Proof* Observe that

$$\theta_z^p = (I_m + \mathrm{col}(z))^p = I_m^p + \mathrm{col}(z)^p = I_m + \left(\sum_{i=0}^{m-1} z_i\right)^{p-1} \cdot \mathrm{col}(z),$$

where the second equation is due to Newtons Binomial Theorem combined with the fact that all multiples of $p$ vanish in rings of characteristic $p$, and where the third equation is due to the identity in Proposition 11. Since $\det(\theta_z) = 1_R$, we have that $\sum_{i=0}^{m-1} z_i = 0$, which implies that $\theta_z^p = I_m$. This means that $\mathrm{ord}(\theta_z) \mid p$, which implies that $\mathrm{ord}(\theta_z)$ equals either 1 or $p$ since $p$ is prime. Because $\theta_z \neq I_m$, we have $\mathrm{ord}(\theta_z) \neq 1$, which means $\mathrm{ord}(\theta_z) = p$. □

**Lemma 34** *Let* $R$ *be a ring of prime characteristic* $p$*, and let* $\theta_z \in \mathrm{CPM}_m^*(R)$*. Then* $\mathrm{ord}(\theta_z)$ *is either* $\mathrm{ord}(\det(\theta_z))$ *or* $p \cdot \mathrm{ord}(\det(\theta_z))$.

*Proof* From Lemma 2, we have that

$$\mathrm{ord}(\det(\theta_z)) \mid \mathrm{ord}(\theta_z).$$

Note that

$$\mathrm{ord}(\theta_z) = \mathrm{ord}(\det(\theta_z)) \cdot \mathrm{ord}\left(\theta_z^{\mathrm{ord}(\det(\theta_z))}\right).$$

Assuming $\mathrm{ord}(\det(\theta_z)) < \infty$, we get

$$\det\left(\theta_z^{\mathrm{ord}(\det(\theta_z))}\right) = \det(\theta_z)^{\mathrm{ord}(\det(\theta_z))} = 1_R.$$

Hence by Lemma 33, $\mathrm{ord}\left(\theta_z^{\mathrm{ord}(\det(\theta_z))}\right)$ is either 1 or $p$, which concludes the proof. □

*Remark 6* The above lemma implies that $\theta_z \in \mathrm{Tor}(\mathrm{CPM}_m^*(R))$ if and only if $\det(\theta_z) \in \mathrm{Tor}(R^*)$.

**Proposition 35** *Let* $\theta_z \in \mathrm{CPM}_m^*(R)$ *such that* $\det(\theta_z) - 1_R \in R^*$*. Then*

$$\mathrm{ord}(\theta_z) = \mathrm{ord}(\det(\theta_z)).$$

*Proof* By Proposition 28, $\theta_z$ admits an eigenbasis with eigenvalues $\lambda_1 = 1_R$ and $\lambda_2 = \det(\theta_z)$. From this, we conclude that

$$\operatorname{ord}(\theta_z) = \operatorname{lcm}(\operatorname{ord}(\lambda_1), \operatorname{ord}(\lambda_2)) = \operatorname{lcm}(1, \operatorname{ord}(\det(\theta_z))) = \operatorname{ord}(\det(\theta_z)),$$

which completes the proof. □

We conclude this section by briefly considering CPMs over $\mathbb{F}_2$ and over local circulant rings.

**Lemma 36** *Let $\theta_z \in \mathrm{CPM}_m^*(\mathbb{F}_2)$ such that $\theta \neq I_m$. Then $\operatorname{ord}(\theta_z) = 2$.*

*Proof* By Lemma 34, we have that $\operatorname{ord}(\theta_z)$ is either equal to $\operatorname{ord}(\det(\theta_z))$ or $2 \cdot \operatorname{ord}(\det(\theta_z))$. Since $\theta_z$ is invertible, we know that $\det(\theta_z) \in \mathbb{F}_2^*$, which means that $\det(\theta_z) = 1_{\mathbb{F}_2}$. Hence $\operatorname{ord}(\det(\theta_z)) = 1$, which means that $\operatorname{ord}(\theta_z)$ is either 1 or 2. Since $\theta_z \neq I_m$, we must have that $\operatorname{ord}(\theta_z) = 2$, which completes the proof. □

**Proposition 37** *Let $R = R_{2^{l_1},\ldots,2^{l_n}}$ be a local circulant ring, and define $l = \max(l_i : 1 \leq i \leq n)$. Then for $\theta_z \in \mathrm{CPM}_m^*(R)$, we have that $\operatorname{ord}(\theta_z) \mid 2^{l+2}$.*

*Proof* $q_{m,R}^*$ restricted to $\mathrm{CPM}_m^*(R)$ induces a surjective map to $\mathrm{CPM}_m^*(\mathbb{F}_2)$.

Let us first consider the case that $\theta_z \in \ker(q_{m,R}^*)$. Since $\theta_z = I_m + \operatorname{col}(z)$, we have that $z_0, \ldots, z_{m-1} \in \mathfrak{m}_n$. Observe that

$$\theta_z^{2^{l+1}} = (I_m + \operatorname{col}(z))^{2^{l+1}} = I_m + \operatorname{col}(z)^{2^{l+1}} = I_m + \left(\sum_{i=0}^{m-1} z_i\right)^{2^{l+1}} \cdot \operatorname{col}(z).$$

Since $\sum_{i=0}^{m-1} z_i \in \mathfrak{m}_n$, we have that $\left(\sum_{i=0}^{m-1} z_i\right)^{2^l} = 0_R$. Hence $\left(\sum_{i=0}^{m-1} z_i\right)^{2^{l+1}} = 0_R$, which implies that $\theta_z^{2^{l+1}} = I_m$.

Now assume that $\theta_z \notin \ker(q_{m,R}^*)$. This means that $q_{m,R}^*(\theta_z) \in \mathrm{CPM}_m^*(\mathbb{F}_2)$ is not the identity, which means that $q_{m,R}^*(\theta_z)$ has order 2. Hence $\theta_z^2 \in \ker(q_{m,R}^*)$, which implies that $\operatorname{ord}(\theta_z^2) \mid 2^{l+1}$ as shown earlier. As a result, we have that $\operatorname{ord}(\theta_z) \mid 2 \cdot 2^{l+1} = 2^{l+2}$, which concludes the proof. □

# 5 Application: The linear layer of Xoodoo

In this section, we show that the linear layer of Xoodoo can be interpreted as a module homomorphism over the local circulant ring $R_{4,32}$. Moreover, we introduce DCD-compositions, which are a type of composition with a similar structure as the linear layer of Xoodoo.

## 5.1 Xoodoo and Local Circulant Modules

An important observation is that the linear layer of Xoodoo is in fact an $R_{4,32}$-linear map of the free circulant module $R_{4,32}^3$. To see this, note that the linear maps $\rho_{\text{west}}$, $\theta$ and $\rho_{\text{east}}$ described in [1] can be represented by the matrices

$$\theta = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}, \quad \rho_{\text{west}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & Y^{11} \end{pmatrix}, \quad \rho_{\text{east}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & X^2Y^8 \end{pmatrix},$$

all contained in $\mathrm{M}_3(R_{4,32})$ where $f = XY^5 + XY^{14} \in R_{4,32}$. Thus the linear layer of Xoodoo is represented by the matrix

$$\begin{aligned} \rho_{\text{west}} \circ \theta \circ \rho_{\text{east}} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & Y^{11} \end{pmatrix} \cdot \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & X^2Y^8 \end{pmatrix} \\ &= \begin{pmatrix} 1+f & Y \cdot f & X^2Y^8 \cdot f \\ X \cdot f & XY \cdot (1+f) & X^3Y^8 \cdot f \\ Y^{11} \cdot f & Y^{12} \cdot f & X^2Y^{19} \cdot (1+f) \end{pmatrix}. \end{aligned}$$

**Proposition 38** *$\rho_{west}$, $\theta$ and $\rho_{east}$ are contained in* $\ker\left(q_{3,R}^*\right)$.

*Proof* Note that $f(1,1) = 1 \cdot 1^5 + 1 \cdot 1^{14} \equiv 2 \equiv 0 \bmod 2$. Using this, we get

$$\begin{aligned} q_{3,R}^*(\theta) = q_{3,R}^* \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix} \\ = \begin{pmatrix} 1+f(1,1) & f(1,1) & f(1,1) \\ f(1,1) & 1+f(1,1) & f(1,1) \\ f(1,1) & f(1,1) & 1+f(1,1) \end{pmatrix} \\ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \end{aligned}$$

hence $\theta \in \ker(q_{3,R}^*)$. In a similar fashion, we conclude that $\rho_{\text{west}}, \rho_{\text{east}} \in \ker(q_{3,R}^*)$. □

By the above proposition together with Corollary 21, we have that

$$\text{ord}(\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}) \mid 2^{5+1} = 2^6 = 64,$$

which is relative low. In fact, we verified using Sagemath that

$$\text{ord}(\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}) = 32.$$

The corresponding code can be found in Appendix A.

## 5.2 DCD-Compositions

In this subsection, we introduce DCD-compositions, which are maps with a similar structure as the linear layer of Xoodoo.

**Definition 10** Define $D_3^*(R)$ as the set of all invertible diagonal matrices in $\mathrm{M}_3(R)$ over a circulant ring $R$, which forms a group under matrix multiplication. We say that a map $\sigma \in \mathrm{GL}_3(R)$ is a **DCD-composition** if there exist $\rho_l, \rho_r \in D_3^*(R)$ and $\theta \in \mathrm{CPM}_3^*(R)$ such that

$$\sigma = \rho_l \circ \theta \circ \rho_r.$$

*Remark 7* The linear layer of Xoodoo is a DCD-composition since $\rho_{\text{east}}, \rho_{\text{west}} \in D_3^*(R_{4,32})$ and $\theta \in \mathrm{CPM}_3^*(R_{4,32})$.

We present two examples of DCD-compositions. In the first example, we construct a DCD-composition with the same bit-state as the linear layer of Xoodoo (also over $R_{4,32}$), but with the highest possible order of such a DCD-composition.

In the second example, we present a DCD-composition over a non-local circulant ring, which resulted in a higher order.

### Example 1: DCD-composition over $R_{4,32}$.

Let $R = R_{4,32}$, and define the group composition $\mathcal{G}_3(R_{4,32}) = D_3^*(R_{4,32}) \cdot \mathrm{CPM}_3^*(R_{4,32})$ which is a subgroup of $\mathrm{GL}_3(R_{4,32})$.

**Theorem 39** *For $\sigma \in \mathcal{G}_3(R_{4,32})$, we have that* $\mathrm{ord}(\sigma) \mid 2^7$.

*Proof* Note that $\sigma$ is of the form $\sigma = \prod_{i=1}^n \rho_i \theta_i$ where $\rho_i \in D_3^*(R_{4,32})$ and $\theta_i \in \mathrm{CPM}_3^*(R_{4,32})$. Observe that $D_3^*(R_{4,32}) \subset \ker(q_{3,R}^*)$, hence $q_{3,R}^*(\sigma) = q_{3,R}^*(\prod_{i=1}^n \theta_i)$ which is contained in $\mathrm{CPM}_3^*(\mathbb{F}_2)$. By Lemma 36, all elements in $\mathrm{CPM}_3^*(\mathbb{F}_2)$ either have order 1 or 2. This implies that $\mathrm{ord}(\theta)$ must divide $2 \cdot 2^6 = 2^7$, since the order of all matrices in $\ker(q_{3,R}^*)$ divide $2^{1+5} = 2^6$ by Corollary 21 (note that $32 = 2^5$). This concludes the proof. □

Every DCD-composition is contained in $\mathcal{G}_3(R_{4,32})$, which implies that the order cannot exceed $2^7 = 128$.

Consider

$$\theta = \begin{pmatrix} 1+f_1 & f_1 & f_1 \\ f_2 & 1+f_2 & f_2 \\ f_3 & f_3 & 1+f_3 \end{pmatrix}, \quad \rho_l = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & Y^{11} \end{pmatrix}, \quad \rho_r = \begin{pmatrix} 1 & 0 & 0 \\ 0 & Y & 0 \\ 0 & 0 & X^2Y^8 \end{pmatrix},$$

where $f_1 = XY^5 + XY^{11} + 1$, $f_2 = XY^5 + XY^{11}$ and $f_3 = XY^5 + XY^{11} + 1$. We verified using SageMath that $\mathrm{ord}(\rho_l \circ \theta \circ \rho_r) = 128$, which is the maximal

possible order of such a composition by the above theorem. The corresponding code can be found in Appendix B.

### Example 2: DCD-composition over $R_n$.

Consider circulant rings of the form $R_n = \mathbb{F}_2[X]/\langle X^n - 1\rangle$, which represents the ring of circulant matrices of dimension $n$.

**Theorem 40** *Let $n$ be an odd number, and let $f \in R_n^*$. Then*

$$\mathrm{ord}(f) \mid 2^{\mathrm{ord}_n(2)} - 1.$$

*Proof* $\mathrm{ord}_n(2)$ is well-defined since $n$ is odd. Let $f = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in R_n^*$. Since we work over $\mathbb{F}_2$, we have

$$f^{2^{\mathrm{ord}_n(2)}} = (a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0)^{2^{\mathrm{ord}_n(2)}} \tag{14}$$

$$= (a_d X^d)^{2^{\mathrm{ord}_n(2)}} + (a_{d-1}X^{d-1})^{2^{\mathrm{ord}_n(2)}} + \cdots + (a_1 X)^{2^{\mathrm{ord}_n(2)}} + a_0^{2^{\mathrm{ord}_n(2)}} \tag{15}$$

$$= a_d \left(X^{2^{\mathrm{ord}_n(2)}}\right)^d + a_{d-1}\left(X^{2^{\mathrm{ord}_n(2)}}\right)^{d-1} + \cdots + a_1 X^{2^{\mathrm{ord}_n(2)}} + a_0 \tag{16}$$

By definition, we have $2^{\mathrm{ord}_n(2)} \equiv 1 \bmod n$, which implies that

$$X^{2^{\mathrm{ord}_n(2)}} \equiv X \bmod \langle X^n - 1\rangle.$$

Hence we can conclude from Expression (16) that $f^{2^{\mathrm{ord}_n(2)}} \equiv f \bmod \langle X^n - 1\rangle$, implying that $f^{2^{\mathrm{ord}_n(2)}-1} \equiv 1 \bmod \langle X^n - 1\rangle$ by invertibility of $f$. Thus the order of $f \in R_n^*$ must divide $2^{\mathrm{ord}_n(2)} - 1$, which concludes the proof. □

Let us choose $n = 167$. Observe that $\mathrm{ord}_{167}(2) = 83$, which by the above theorem means that the highest possible order of elements in $R_{167}^*$ equals $2^{83} - 1$. Consider

$$\theta = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}, \quad \rho_l = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^{11} \end{pmatrix}, \quad \rho_r = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^{10} \end{pmatrix},$$

where $f = X^6 + X^{15}$. Here we have

$$\det(\rho_l \circ \theta \circ \rho_r) = X^{12} \cdot (X^{15} + X^6 + 1) \cdot X^{11} = X^{38} + X^{29} + X^{23}.$$

By using Sagemath, we verified that $X^{27} + X^{18} + X^{12}$ is invertible (see Appendix C for the code). Since $2^{83} - 1$ is a prime number (it is a Mersenne prime number), it must be the order of $X^{27} + X^{18} + X^{12}$. By Lemma 2, we can conclude that $2^{83} - 1$ divides $\mathrm{ord}(\rho_l \circ \theta \circ \rho_r)$.

*Remark 8* We managed to compute the exact order of the composition $\rho_l \circ \theta \circ \rho_r$, which equals $\left(2^{83}-1\right) \cdot \lambda$ where

$$\lambda = 301\,541\,899\,055\,510\,925\,582\,216\,169\,150\,861\,286\,153\,081\,761\,757\,331\,612\,351\,867\,575\,029\,327\,375\,019$$
$$\approx 1.33 \cdot 2^{247}.$$

This is significantly higher than 32. We illustrate a sketch on how we obtained $\lambda$, which requires a bit of mathematical reasoning.

Observe that $R_{167}$ can be naturally embedded in $\mathrm{GF}\left(2^{83}\right)[X]/\langle X^{167}-1\rangle$. Note that $X^{167}-1$ fully splits in $\mathrm{GF}\left(2^{83}\right)$, where we have the decomposition $X^{167}-1 = \prod_{\zeta \in \mu_{167}} X-\zeta$, where $\mu_{167}$ is the set of 167-th roots of unity. Hence by the Chinese Remainder Theorem, we obtain the isomorphism

$$\mathrm{GF}\left(2^{83}\right)[X]/\langle X^{167}-1\rangle \to \bigoplus_{\zeta \in \mu_{167}} \mathrm{GF}\left(2^{83}\right),\ g \mapsto (g(\zeta))_{\zeta \in \mu_{167}}.$$

From this isomorphism, we conclude that

$$\mathrm{GL}_3\left(\mathrm{GF}\left(2^{83}\right)[X]/\langle X^{167}-1\rangle\right) \cong \bigoplus_{\zeta \in \mu_{167}} \mathrm{GL}_3\left(\mathrm{GF}\left(2^{83}\right)\right).$$

By Lagrange, the order of every element in $\mathrm{GL}_3\left(\mathrm{GF}\left(2^{83}\right)[X]/\langle X^{167}-1\rangle\right)$ must divide

$$\#\,\mathrm{GL}_3\left(\mathrm{GF}\left(2^{83}\right)\right) = \left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)\cdot\left(2^{3\cdot 83}-2^{2\cdot 83}\right), \tag{17}$$

hence $\lambda$ must be a divisor of (17).

Using Sagemath, we verified that $\lambda \mid \left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)$. Note that

$$\begin{aligned}
&\left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)\\
&= \left(2^{83}-1\right)\cdot\left(2^{2\cdot 83}+2^{83}+1\right)\cdot 2^{83}\cdot\left(2^{2\cdot 83}-1\right)\\
&= \left(2^{83}-1\right)\cdot\left(2^{2\cdot 83}+2^{83}+1\right)\cdot 2^{83}\cdot(2^{83}+1)\cdot\left(2^{83}-1\right)\\
&= \left(2^{83}-1\right)^2\cdot 2^{83}\cdot\left(\left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)\right).
\end{aligned}$$

Again using Sagemath, we verified that $\lambda \mid \left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)$. By exhaustive search over the divisors of $\left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)$, we managed to find $\lambda$. The details of the code used to compute $\lambda$ can be found in Appendix C.

# 6 Concluding Remarks

There are two main reasons why the order of the linear layer of Xoodoo is relatively low. These being that the linear layer of Xoodoo is contained in $\ker(q^*_{3,R_{4,32}})$, and that the circulant ring $R_{4,32}$ is local. Example 2 demonstrated that for a non-local circulant ring, one can construct DCD-compositions with a much higher order than the linear layer of Xoodoo. An interesting follow up research topic would be to study algebraic properties of non-local circulant rings, and to use these properties to experiment in constructing high order DCD-compositions.

**Acknowledgments.** I would like to thank my PhD supervisor prof. dr. Joan Daemen for providing me with research topics leading to this paper, and for providing valuable feedback.

This work was supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA.

## References

[1] Daemen, J., Hoffert, S., Assche, G.V., Keer, R.V.: The design of xoodoo and xoofff. IACR Trans. Symmetric Cryptol. **2018**(4), 1–38 (2018). https://doi.org/10.13154/tosc.v2018.i4.1-38

[2] Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The Keccak reference. https://keccak.team/papers.html (2011)

[3] Stoffelen, K., Daemen, J.: Column parity mixers. IACR Trans. Symmetric Cryptol. **2018**(1), 126–159 (2018). https://doi.org/10.13154/tosc.v2018.i1.126-159

[4] Gray, R.M.: Toeplitz and circulant matrices: A review (2006)

[5] Beierle, C., Canteaut, A., Leander, G., Rotella, Y.: Proving resistance against invariant attacks: How to choose the round constants. In: Annual International Cryptology Conference, pp. 647–678 (2017). Springer

[6] Atiyah, M.: Introduction to Commutative Algebra. CRC Press, ??? (2018)

[7] Kemper, G.: A Course in Commutative Algebra vol. 256. Springer, ??? (2010)

[8] Lang, S.: Algebra, volume 211 of. Graduate Texts in Mathematics (2004)

# Appendix A Computing the Order of the Linear Layer of Xoodoo

```
#Setting up the ring R_{4,32}
R.<s,t> = GF(2)[]
S.<x,y> = R.quo([s^4 - 1, t^32 - 1])

#Defining \rho_{east}, \rho_{west} and \theta for the linear layer LN
f = x*y^5 + x*y^14

theta = matrix([[1+f,f,f],[f,1+f,f],[f,f,1+f]])
p_l = matrix([[1,0,0],[0,x,0],[0,0,y^11]])
p_r = matrix([[1,0,0],[0,y,0],[0,0,x^2*y^8]])
LN = p_l*theta*p_r

#Naively computing the order of LN using brute force
i = 1
while LN^i != matrix.identity(3):
    i = i + 1

print(i)
```

# Appendix B Computing the Order of Alternative DCD-composition over $R_{4,32}$

```
#Setting up the ring R_{4,32}
R.<s,t> = GF(2)[]
S.<x,y> = R.quo([s^4 - 1, t^32 - 1])

#Defining \rho_l, \rho_r and \theta for the DCD-composition DCD
f1 = x*y^5 + x*y^11 + 1
f2 = x*y^5 + x*y^11
f3 = x*y^5 + x*y^11 + 1

theta = matrix([[1+f1,f1,f1],[f2,1+f2,f2],[f3,f3,1+f3]])
p_l = matrix([[1,0,0],[0,x,0],[0,0,y^11]])
p_r = matrix([[1,0,0],[0,y,0],[0,0,x^2*y^8]])
DCD = p_l*theta*p_r

#Naively computing the order of DCD using brute force
i = 1
while DCD^i != matrix.identity(3):
    i = i + 1
```

```
print(i)
```

# Appendix C Computing the Order of Alternative DCD-composition over $R_{167}$

```
#Setting up the ring R_167
R.<s> = GF(2)[]
S.<x> = R.quo([s^167 - 1])

#Defining \rho_l, \rho_r and \theta for the DCD-composition DCD
f = x^6 + x^15

theta = matrix([[1+f,f,f],[f,1+f,f],[f,f,1+f]])
p_l = matrix([[1,0,0],[0,x,0],[0,0,x^11]])
p_r = matrix([[1,0,0],[0,x,0],[0,0,x^10]])
DCD = p_l*theta*p_r

#Checking/verifying invertibility of DCD
DCD^-1

#Lifting DCD to the order of \det(DCD) = 2^83 - 1, which we call DCD1
ord_det_LN = 2^83 - 1
DCD1 = DCD^ord_det_LN

#Checking/verifying if the order of DCD1 divides a = (2^(2*83) + 2^83
    + 1)*(2^(83) + 1) by verifying if DCD1^a is the indetity matrix
a = (2^(2*83) + 2^83 + 1)*(2^(83) + 1)
DCD1^a

#Naively computing \lambda (the order of DCD1) using brute force
#\lambda must be a divisor of $a$
i = 0
while DCD1^(divisors(a)[i]) != matrix.identity(3):
    i = i + 1

print(divisors(a)[i])
```