Radbound University

Decomposition of finite commutative semisimple group algebras, and some applications in cryptography

Robert Christian Subroto,

Radboud University (The Netherlands)

June 2, 2023

ESCADA

- **Object of interest:** For G a finite Abelian group, consider the group algebra

$$\mathbb{F}_q[G] := \left\{ \sum_{g \in G} c_g \cdot g : c_g \in \mathbb{F}_q \right\}$$

  - **Addition:** $\left(\sum_{g\in G} a_g \cdot g\right) + \left(\sum_{g\in G} b_g \cdot g\right) = \sum_{g\in G}(a_g + b_g) \cdot g$
  - **Multiplication:** $\left(\sum_{g\in G} a_g \cdot g\right) \cdot \left(\sum_{g\in G} b_g \cdot g\right) = \sum_{g,h\in G}(a_g \cdot b_h)(g \cdot h)$
- **Why?** Many applications in coding theory and cryptography!
- **Examples:** Used in the construction of Circulant Column Parity Mixers, which are used in Xoodoo and Keccak-f
- A better understanding of this group algebra leads to a better understanding of their applications

Outline

Part I: Circulant Coordinate Rings

- Circulant Coordinate Rings (CCR)
- Towards the Decomposition
- The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

- Circulant Column Parity Mixers: a brief introduction
- Circulant Column Parity Mixers (CCPM) - New Approach
- Application: Linear Layer of Xoodoo

Part I: Circulant Coordinate Rings

Table of Contents

Part I: Circulant Coordinate Rings

Circulant Coordinate Rings (CCR)

Towards the Decomposition

The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

Circulant Column Parity Mixers: a brief introduction

Circulant Column Parity Mixers (CCPM) - New Approach

Application: Linear Layer of XOODOO

Circulant Coordinate Rings (CCR)

- Let $G = \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$.
- We have the ring isomorphism

$$\Phi_G : \mathbb{F}_q[G] \to \mathbb{F}_q[X_1, \ldots, X_n]/(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)$$
$$f \mapsto \sum_{g \in G} f(g) \cdot \prod_{i=1}^{n} X_i^{g_i}$$

- Applies to any finite Abelian group G, due to the **Fundamental Theorem of finite Abelian groups**
- **Conclusion:** we only need to study coordinate rings of the form

$$R_{m_1,\ldots,m_n}(\mathbb{F}_q) := \mathbb{F}_q[X_1, \ldots, X_n]/(X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1),$$

which we call **circulant coordinate rings** (CCR).

Scope

- When $m_1, \ldots, m_n$ are all coprime to q, then $R_{m_1,\ldots,m_n}(\mathbb{F}_q)$ is a **semisimple** ring
- This means that $R_{m_1,\ldots,m_n}(\mathbb{F}_q)$ is a direct sum of **simple components**
- Simple components are building blocks for semisimple rings, just like prime numbers are the building blocks for any natural number
- **Goal:** find the simple components of $R_{m_1,\ldots,m_n}(\mathbb{F}_q)$

Table of Contents

Part I: Circulant Coordinate Rings

Circulant Coordinate Rings (CCR)

Towards the Decomposition

The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

Circulant Column Parity Mixers: a brief introduction

Circulant Column Parity Mixers (CCPM) - New Approach

Application: Linear Layer of Xoodoo

- **Chinese Remainder Theorem (CRT):** Let $\mathfrak{a}$ be an ideal in R such that $\mathfrak{a} = \bigcap_{j=1}^{t} \mathfrak{p}_j$, where $\mathfrak{p}_j$ are ideals coprime to each other. Then

$$R/\mathfrak{a} \cong \bigoplus_{j=1}^{t} R/\mathfrak{p}_j$$

- **Strategy:** Find the the ideal factorisation of $\mathfrak{a} := (X^{m_1} - 1, \ldots, X^{m_n} - 1)$ in $R := \mathbb{F}[X_1, \ldots, X_n]$, then apply the CRT
- If $\mathbb{F}$ is algebraically closed, this is not hard: **Hilbert's Nullstellensatz (HN)**
- **Problem:** $\mathbb{F}_q$ is not algebraically closed, hence HN does not apply
- **Solution:** apply the Combinatorial Nullstellensatz with Galois Theory

- For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{A}^n_{\mathbb{F}_q}$, define $\mathbb{F}_q(\mathbf{x})$ as the smallest field extension of $\mathbb{F}_q$ containing all $x_1, \dots, x_n$
- $\mathcal{V}_{m_1,\dots,m_n} := \mu_{m_1} \times \cdots \times \mu_{m_n} \subseteq \mathbb{A}^n_{\mathbb{F}_q}$ where μ_{m_i} are the m_i-roots of unity
- For $m := \operatorname{lcm}(m_i : 1 \leq i \leq n)$, consider the group action

$$\alpha : \mathrm{Gal}(\mathbb{F}_q(\mu_m)/\mathbb{F}_q) \times \mathcal{V}_{m_1,\dots,m_n} \to \mathcal{V}_{m_1,\dots,m_n}, \ (\sigma, \mathbf{x}) \mapsto \sigma(\mathbf{x}) := (\sigma(x_1), \dots, \sigma(x_n))$$

- Γ_α: set of orbits of α with a fixed set of representatives in $\mathcal{V}_{m_1,\dots,m_n}$

Decomposition Theorem

We have the isomorphism

$$R_{m_1,\dots,m_n}(\mathbb{F}_q) \to \bigoplus_{\mathbf{y} \in \Gamma_\alpha} \mathbb{F}_q(\mathbf{y}), \ f \mapsto (f(\mathbf{y}))_{\mathbf{y} \in \Gamma_\alpha}$$

Table of Contents

Part I: Circulant Coordinate Rings

Circulant Coordinate Rings (CCR)

Towards the Decomposition

The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

Circulant Column Parity Mixers: a brief introduction

Circulant Column Parity Mixers (CCPM) - New Approach

Application: Linear Layer of Xoodoo

Relating to orbits of α

- The structure of the orbit Γ_α determines the structure of the decomposition
- Luckily, this is not too hard to express in a number-theoretic setting
- **Notation:** for $\mathbf{y} \in \mathcal{V}_{m_1,\ldots,m_n}$, we define $\mathrm{Orb}(\mathbf{y})$ as the orbit of $\mathbf{y}$ under α.
- **Notation:** φ is Euler's totient function
- **Notation:** For $g \in (\mathbb{Z}/m\mathbb{Z})^*$, we denote the order of g as $\mathrm{ord}_m(g)$.

- Univariate case: circulant rings of the form $\mathbb{F}_q[X]/(X^m - 1)$.

Orbit Structure: Univariate Case

- For $\mathrm{Orb}(\mathbf{y}) \in \Gamma_\alpha$:

$$|\mathrm{Orb}(\mathbf{y})| \in \{\mathrm{ord}_d(q) : d \mid m\};$$

- For a fixed $d \mid m$, there exists $\frac{\varphi(m/d)}{\mathrm{ord}_{m/d}(q)}$ orbits of size $\mathrm{ord}_d(m)$;
- Number of orbits:

$$\#\Gamma_\alpha = \sum_{d|m} \frac{\varphi(d)}{\mathrm{ord}_d(q)}.$$

- **Notation:** $\Delta_{d_1,\ldots,d_n}(q) := \mathrm{lcm}_{i=1}^{n}(\mathrm{ord}_{d_i}(q))$
- **Notation:** $\mathrm{Div}_{m_1,\ldots,m_n} := \{(d_1,\ldots,d_n) : d_i \mid m_i\}$

Orbit Structure: Multivariate Case

- For $\mathrm{Orb}(\mathbf{y}) \in \Gamma_\alpha$:

$$|\mathrm{Orb}(\mathbf{y})| \in \{\mathrm{lcm}_{i=1}^{n}(\mathrm{ord}_{d_i}(q)) : d_i \mid m_i\};$$

- For fixed $(d_1,\ldots,d_n) \in \mathrm{Div}_{m_1,\ldots,m_n}$, there exists $\frac{\prod_{i=1}^{n}\varphi(m_i/d_i)}{\Delta_{m_1/d_1,\ldots,m_n/d_n}(q)}$ orbits of size $\mathrm{lcm}_{i=1}^{n}(\mathrm{ord}_{d_i}(q))$.
- Number of orbits:

$$\#\Gamma_\alpha = \sum_{(d_1,\ldots,d_n)\in\mathrm{Div}_{m_1,\ldots,m_n}} \left(\frac{\prod_{i=1}^{n}\varphi(d_i)}{\Delta_{d_1,\ldots,d_n}(q)}\right).$$

- From the orbit structure, we can extract information about the group of invertible elements of $R_{m_1,\ldots,m_n}(\mathbb{F}_q)$.

Theorem (Invertible Criterion)

Let $f \in R_{m_1,\ldots,m_n}(\mathbb{F}_q)$, then f is invertible if and only if $f(\mathbf{x}) \neq 0$ for all $\mathbf{x} \in \Gamma_\alpha$.

Theorem (Counting Invertible Elements)

$$\# R^*_{m_1,\ldots,m_n}(\mathbb{F}_q) = \prod_{(d_1,\ldots,d_n)\in \mathrm{Div}_{m_1,\ldots,m_n}} \left(q^{\Delta_{d_1,\ldots,d_n}(q)} - 1 \right)^{\frac{\prod_{i=1}^n \varphi(d_i)}{\Delta_{d_1,\ldots,d_n}(q)}}$$

Part II: Applications to Circulant Columns Parity Mixers

Table of Contents

Part I: Circulant Coordinate Rings

Circulant Coordinate Rings (CCR)

Towards the Decomposition

The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

Circulant Column Parity Mixers: a brief introduction

Circulant Column Parity Mixers (CCPM) - New Approach

Application: Linear Layer of XOODOO

- Circulant Column Parity Mixers (CCPMs) *[Stoffelen & Daemen, 2018, p.126–159]* are a special type of linear maps
- Used in cryptographic primitives like Xoodoo and Keccak
- They are a good trade-off between implementation cost and mixing power
- CCPMs are defined in terms of linear algebra

Example: θ of Xoodoo

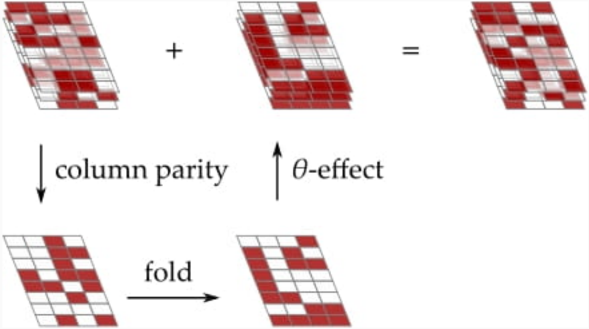
- θ is an example of a circulant column parity mixer (CCPM)
- θ is used in the linear layer of Xoodoo
- θ is a linear map from $V = \mathbb{F}_2^{4\cdot 32\cdot 3} = \mathbb{F}_2^{384}$ to itself
- θ is described in terms of planes, lanes and the specified shifts of bits, as described in detail in the design of Xoodoo *[Daemen et al., 2018, p.1–38]*

Specifications of θ

$$P \leftarrow A_0 + A_1 + A_2$$

$$E \leftarrow P \lll (1,5) + P \lll (1,14)$$

$$A_y \leftarrow A_y + E, \qquad y \in \{0,1,2\}$$



Introduction & Motivation (continued)

- CCPMs in terms of linear algebra: complex and difficult for studying algebraic properties
- **Solution:** study CCPMs using module theory
- **Outline:**
  1. Briefly introducing basics of module theory
  2. Introducing new definition of CCPMs in terms of module theory
  3. Show some consequences/results of this new definition
  4. Show how θ translates into this new definition
  5. Show an interesting application of the linear layer of Xoodoo

Notation

- For a vector space V over $\mathbb{F}_2$ with dimension n, we index the coordinates of $v \in V$ from 0 to $n-1$
- $\mathrm{e}_i \in V$ is the i-th unit vector with $0 \leq i \leq n-1$
- For vector spaces V and W over $\mathbb{F}_2$, the **tensor product** over $\mathbb{F}_2$ is denoted by $V \otimes_{\mathbb{F}_2} W$
- We have the map $V \times W \to V \otimes_{\mathbb{F}_2} W, \ (v, w) \mapsto v \otimes w$
- $\dim(V \otimes_{\mathbb{F}_2} W) = \dim(V) \cdot \dim(W)$ with basis

$$\{\mathrm{e}_i \otimes \mathrm{e}_j \mid 0 \leq i \leq \dim(V) - 1, 0 \leq j \leq \dim(W) - 1\}$$

- **Vector spaces:** scalars over a field $\mathbb{F}$
- **Modules:** scalars over a ring R
- R^m: Consists of m-tuples $v := (v_0, \ldots, v_{m-1})^\mathsf{T}$ with $v_i \in R$
- For $c \in R$, we have the scalar operation

$$c \cdot v = c \cdot \begin{pmatrix} v_0 \\ \vdots \\ v_{m-1} \end{pmatrix} = \begin{pmatrix} c \cdot v_0 \\ \vdots \\ c \cdot v_{m-1} \end{pmatrix}$$

- This concept is useful for CCPMs when R is a CCR.

R-linear map

- We say that a map $F : R^m \to R^m$ is R-**linear** if:
  1. For $v, u \in R^m$, we have $F(u + v) = F(u) + F(v)$
  2. For $v \in R^m$ and $c \in R$, we have $F(c \cdot v) = c \cdot F(v)$
- **Important result:** All R-linear maps are uniquely represented by an $m \times m$-matrix with entries in R, and vice versa!

Table of Contents

Part I: Circulant Coordinate Rings

- Circulant Coordinate Rings (CCR)
- Towards the Decomposition
- The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

- Circulant Column Parity Mixers: a brief introduction
- Circulant Column Parity Mixers (CCPM) - New Approach
- Application: Linear Layer of Xoodoo

Redifining CCPMs

- Let R be a CCR, and let $z = (z_0, \ldots, z_{m-1})^{\mathsf{T}} \in R^m$.
- A **circulant columns parity mixer (CCPM)** θ_z is an R-linear map of the form

$$\theta_z = \begin{pmatrix} 1 + z_0 & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1 + z_1 & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1 + z_2 & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{m_1} & z_{m-1} & z_{m-1} & \cdots & 1 + z_{m-1} \end{pmatrix}.$$

- θ_z is uniquely determined by z, which we call the **parity folding matrix array**
- $z_0, \ldots, z_{m-1}$ are the **parity folding matrices** of θ_z.
- $\mathrm{CCPM}_m(R)$: set of all CCPMs over R of dimension m

Properties CCPMs

- **Characteristic polynomial** of θ_z:

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

- **Determinant** of θ_z:

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

- θ_z is **invertible** if and only if $1 + \sum_{i=0}^{m-1} z_i$ is **invertible** in R
- θ_z has an **eigenbasis** over R if and only if $\sum_{i=0}^{m-1} z_i$ is **invertible**

- The planes in a CCPM are modelled as the vector space $\mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32}$
- We have a the group isomorphism (additive)

$$\vartheta : \mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32} \to R_{4,32}(\mathbb{F}_2), \;\; \mathrm{e}_i \otimes \mathrm{e}_j \mapsto X_1^i X_2^j$$

- The shifts $(a, b) \lll$ is equivalent by scaling with $X_1^a X_2^b$
- **Important observation:** The map $\theta : R_{4,32}(\mathbb{F}_2)^3 \to R_{4,32}(\mathbb{F}_2)^3$ is an $R_{4,32}(\mathbb{F}_2)$-linear map!
- We obtain the following commutative diagram:

$$\begin{tikzcd}
R_{4,32}(\mathbb{F}_2)^3 \arrow[r, "\theta_z"] & R_{4,32}(\mathbb{F}_2)^3 \\
(\mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32})^3 \arrow[u, "\overline{\vartheta}"] \arrow[r, "\theta"] & (\mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32})^3 \arrow[u, "\overline{\vartheta}"]
\end{tikzcd}$$

The map θ revisited (2/2)

- $\theta : (\mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32})^3 \to (\mathbb{F}_2^4 \otimes_{\mathbb{F}_2} \mathbb{F}_2^{32})^3$ is equivalent to $\theta_z : R_{4,32}(\mathbb{F}_2)^3 \to R_{4,32}(\mathbb{F}_2)^3$ with matrix representation

$$\theta_z = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}, \; f = X_1 X_2^5 + X_1 X_2^{14}$$

- Even better: we can do this for the whole linear layer of Xoodoo!
- How? See next part of the presentation

Table of Contents

Part I: Circulant Coordinate Rings

Circulant Coordinate Rings (CCR)

Towards the Decomposition

The Orbit Structure

Part II: Applications to Circulant Columns Parity Mixers

Circulant Column Parity Mixers: a brief introduction

Circulant Column Parity Mixers (CCPM) - New Approach

Application: Linear Layer of Xoodoo

Modules and The Linear Layer of Xoodoo (1/2)

- Linear layer of Xoodoo consists of the composition $\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}$
- **Observation:** ρ_{west}, θ and ρ_{east} are all invertible $R_{4,32}(\mathbb{F}_2)$-linear maps, thus having matrix representations!

Modules and The Linear Layer of Xoodoo (2/2)

- The linear layer is also $R_{4,32}(\mathbb{F}_2)$-linear over $R_{4,32}(\mathbb{F}_2)^3$ with the following matrix representation:

$$\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_1 & 0 \\ 0 & 0 & X_2^{11} \end{pmatrix} \cdot \begin{pmatrix} 1+f & 1 & 1 \\ 1 & 1+f & 1 \\ 1 & 1 & 1+f \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_2 & 0 \\ 0 & 0 & X_1^2 X_2^8 \end{pmatrix}$$

$$= \begin{pmatrix} 1+f & X_2 \cdot f & X_1^2 X_2^8 \cdot f \\ X_1 \cdot f & X_1 X_2 \cdot (1+f) & X_1^3 X_2^8 \cdot f \\ X_2^{11} \cdot f & X_2^{12} \cdot f & X_1^2 X_2^{19} \cdot (1+f) \end{pmatrix}$$

- Using the module-theoretical approach, some algebraic properties of the linear layer of Xoodoo can be explained by the algebraic structure of $R_{4,32}(\mathbb{F}_2)$!

Some results

- Order of Linear Layer equals 32, which is relatively low
- Possible threat against invariant subspace attacks *[Beierle et al., 2017, p.647–678]*
- Reason of this low order: choice of the CCR $R_{4,32}(\mathbb{F}_2)$
- Using the theory of CCRs, we can construct linear maps of a similar structure with high order
- Think of orders around 2^{247}!

Conclusion

- CCRs are interesting from both a mathematical and cryptographic point of view
- Can be useful in designing and understanding cryptographic primitives based on CCRs
- Maybe useful for cryptanalysis?

Thank you for your attention!