Radbound University

Decomposition of finite commutative semisimple group algebras over finite fields using the Combinatorial Nullstellensatz

Robert Christian Subroto,

Radboud University (The Netherlands)

June 19, 2023

ESCADA

Introduction

- **Object of interest:** $\mathbb{F}_q[G]$ where G is a finite Abelian group.
- $\mathbb{F}_q[G]$ is semisimple if and only if the order of G is coprime to q
  - **Note:** We only consider semisimple group algebras
- **Goal:** Find the decomposition of $\mathbb{F}_q[G]$ into simple components
- This is done by studying $\mathbb{F}_q[G]$ from an algebraic geometric point of view

Outline

Geometric Interpretation

Circulant Coordinate Rings

- 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)**

- **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 $\mathfrak{a} := (X_1^{m_1} - 1, \ldots, X_n^{m_n} - 1)$ in $R := \mathbb{F}[X_1, \ldots, X_n]$
- 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

Partial Solution: Combinatorial Nullstellensatz

- **Partial solution:** use the **Combinatorial Nullstellensatz (CN)** instead of HN
- **Notation:** $\mathcal{V}_{m_1,\ldots,m_n} := \mu_{m_1} \times \cdots \times \mu_{m_n} \subseteq \mathbb{A}^n_{\mathbb{F}_q}$, where μ_{m_i} are the m_i-th roots of unity
- **Notation:** For an index set I of size m and a ring R, we define $R^{\oplus I}$ as the direct sum of m copies of R, indexed by I

Theorem (Partial Decomposition)

Let $m_1, \ldots, m_n$ be all be coprime to q, and let $\mathbb{L}/\mathbb{F}_q$ such that $\mu_{m_i} \subseteq \mathbb{L}$. Then we have the embedding

$$\tau : R_{m_1,\ldots,m_n}(\mathbb{F}_q) \to \mathbb{L}^{\oplus \mathcal{V}_{m_1,\ldots,m_n}}, \; f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in \mathcal{V}_{m_1,\ldots,m_n}}$$

- τ becomes an isomorphism when $\mu_{m_i} \in \mathbb{F}_q$

- We can refine τ to a **full decomposition** of $R_{m_1,\ldots,m_n}(\mathbb{F}_q)$ without assuming $\mu_{m_i} \subseteq \mathbb{F}_q$!
- Key ingredient: **Galois Theory & Galois Group Actions**

Galois Group Action

Generalized Decomposition Theorem

- For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{A}^n_{\overline{\mathbb{F}}_q}$, define $\mathbb{F}_q(\mathbf{x})$ as the smallest field extension of $\mathbb{F}_q$ containing all $x_1, \dots, x_n$
- For $m := \operatorname{lcm}(m_1, \dots, m_n)$, we consider the group action

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

- The **set of orbits** of $\widetilde{\alpha}$ is denoted by $\Gamma_{\widetilde{\alpha}}$

Generalized Decomposition Theorem

Let $m_1, \dots, m_n$ be all be coprime to q. We have the isomorphism

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

- The orbit structure determines the structure of the group decomposition

An alternative group action

- **Notation:** $\langle q \rangle_m$ is the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ generated by q
- Consider the group action

$$\alpha : \langle q \rangle_m \times \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z}) \to \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z}),$$
$$(q^t, (a_1, \ldots, a_n)) \mapsto (a_1 \cdot q^t \bmod m_1, \ldots, a_n \cdot q^t \bmod m_n)$$

- We denote the **set of orbits** of α by Γ_α
- Orbits of α are easier to compute than $\widetilde{\alpha}$

Equivalence of group actions

- Important one-to-one maps:

$$\iota : \mathrm{Gal}(\mathbb{F}_q(\mu_m)/\mathbb{F}_q) \to \langle q \rangle_m, \;\; \sigma_q^t \mapsto q^t \bmod m$$

$$\gamma : \mathcal{V}_{m_1,\ldots,m_n} \to \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z}), \;\; (\zeta_{m_1}^{a_i}, \ldots, \zeta_{m_n}^{a_n}) \mapsto (a_1, \ldots, a_n),$$

  where $\zeta_{m_1}, \ldots, \zeta_{m_n}$ are fixed primitive roots in $\mu_{m_1}, \ldots, \mu_{m_n}$ respectively
- These maps induces the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{F}_q(\mu_m)/\mathbb{F}_q) \times \mathcal{V}_{m_1,\ldots,m_n} \arrow[r, "\widetilde{\alpha}"] \arrow[d, "\iota\times\gamma"'] & \mathcal{V}_{m_1,\ldots,m_n} \arrow[d, "\gamma"] \\
\langle q \rangle_m \times \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z}) \arrow[r, "\alpha"] & \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})
\end{tikzcd}$$

- **Conclusion:** α and $\widetilde{\alpha}$ are **equivalent group actions!**

- Univariate case: CCR of the form $\mathbb{F}_q[X]/(X^m - 1)$
- **Notation:** $\varphi(n)$ is Euler's totient function
- **Notation:** For $g \in (\mathbb{Z}/m\mathbb{Z})^*$, we denote the order of g as $\mathrm{ord}_m(g)$

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:

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

Orbit Structure: Multivariate Case

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

$$|\,\mathrm{Orb}(\mathbf{y})| \in \{\Delta_{d_1,\ldots,d_n}(q) : (d_1, \ldots, d_n) \in \mathrm{Div}_{m_1,\ldots,m_n}\}$$

- 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 $\Delta_{d_1,\ldots,d_n}(q)$
- Number of orbits:

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

Applications: Invertible Elements

Invertible Elements

- 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 $\mathbf{x} \in \Gamma_{\widetilde{\alpha}}$

Theorem (Counting Invertible Elements)

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

Conclusion

- The Combinatorial Nullstellensatz provides a geometric interpretation
- Galois group actions provided the missing ingredient
- **Mathematical Applications:** representation theory of finite Abelian groups over non-algebraically closed fields
- **Cryptographic Applications:** understanding cryptographic primitives constructed from CCRs like XOODOO and KECCAK-f

Thank you for your attention!