Zeta functions of the joint algebras over finite fields

Tung T. Nguyen

May 27-29, 2022

2022 Zassenhaus Groups and Friends Conference

Muller's Lab, Western University.

Circulant matrices and group rings

Let R be a ring with unity and G a finite group of size n.

Definition

An $n \times n$ G-circulant matrix over R is an $n \times n$ matrix of the form

$$A = (a_{\tau^{-1}\sigma})_{\tau,\sigma \in G},$$

where $a_g \in R$ for all $g \in G$.

Circulant matrices and group rings

Let R be a ring with unity and G a finite group of size n.

Definition

An $n \times n$ G-circulant matrix over R is an $n \times n$ matrix of the form

$$A = (a_{\tau^{-1}\sigma})_{\tau,\sigma \in G},$$

where $a_g \in R$ for all $g \in G$.

We see that A is uniquely determined by the vector $[a_g]_{g \in G}$. For convenience, we can write

$$A = \mathrm{circ}([a_g]_{g \in G}).$$

We will denote by $J_G(R)$ the set of all G-circulant matrices over R.

We can check that $J_G(R)$ is a subring of $M_n(R)$.

We can check that $J_G(R)$ is a subring of $M_n(R)$. Let us also recall

$$R[G] = \{\sum_{g \in G} a_g g\},$$

the group ring of G over R.

We can check that $J_G(R)$ is a subring of $M_n(R)$. Let us also recall

$$R[G] = \{\sum_{g\in G} a_g g\},$$

the group ring of G over R. We have the following

Proposition (Hurley)

The map

$$R[G] \to J_G(R),$$

$$\sum_{g\in G} a_g g \mapsto circ([a_g]_{g\in G}),$$

is a ring isomorphism.

Why G-circulant matrices?

Why G-circulant matrices?

1. Circulant matrices were introduced by Dedekind in his study of normal bases for Galois extensions.

Why G-circulant matrices?

1. Circulant matrices were introduced by Dedekind in his study of normal bases for Galois extensions.
2. In 1886, Frobenius gave a complete factorization of the determinant of $A \in J_G$ into irreducible factors and this was the start of the theory of linear representations and characters of finite groups.

Why G-circulant matrices?

1. Circulant matrices were introduced by Dedekind in his study of normal bases for Galois extensions.
2. In 1886, Frobenius gave a complete factorization of the determinant of $A \in J_G$ into irreducible factors and this was the start of the theory of linear representations and characters of finite groups.
3. Due to (2), many problems involving circulant matrices can have closed-form or analytical solutions.

A motivation from network theory

Let G, H be two graphs. The joint graph $G + H$ of G and H has the following pictorial definition

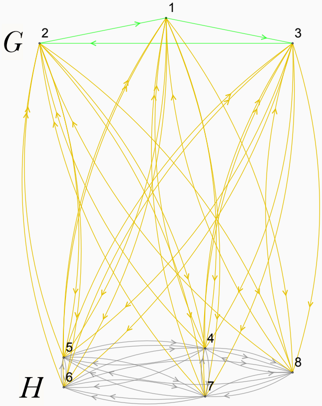

Figure 1: The join of two graphs G and H.

A motivation from network theory

If we denote the adjacency matrix of G, H by A_G, A_H then the adjacency matrix of $G + H$ is

$$A = \begin{pmatrix} A_G & J \\ J & A_H \end{pmatrix},$$

where J is the matrix with all entries equal to 1.

A motivation from network theory

If we denote the adjacency matrix of G, H by A_G, A_H then the adjacency matrix of $G + H$ is

$$A = \begin{pmatrix} A_G & J \\ J & A_H \end{pmatrix},$$

where J is the matrix with all entries equal to 1. This is an example of a multilayer network with two layers.

The joint group ring $J_{G_1,G_2,\ldots,G_d}(R)$

Definition

Let $G_1, G_2, \ldots, G_d$ be groups of size $k_1, k_2, \ldots, k_d$ respectively. A join of circulant matrices R is a matrix of the form

$$A = \left(\begin{array}{c|c|c|c} A_1 & a_{1,2}J & \cdots & a_{1,d}J \\ \hline a_{2,1}J & A_2 & \cdots & a_{2,d}J \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{d,1}J & a_{d,2}J & \cdots & A_d \end{array}\right),$$

where A_i is a G_i-circulant matrix and J denotes the matrix with all entries equal to 1.

The joint group ring $J_{G_1,G_2,\dots,G_d}(R)$

We have the following observation.

Proposition

$J_{G_1,G_2,\dots,G_d}(R)$ is a subring of $M_n(R)$ where $n = \sum_{i=1}^{d} |G_i|$. Furthermore, there is an augmentation map $J_{G_1,G_2,\dots,G_d}(R) \to M_d(R)$ defined by

$$\varepsilon(A) = \begin{bmatrix} \epsilon(A_1) & k_2 a_{12} & \cdots & k_d a_{1d} \\ k_1 a_{21} & \epsilon(A_2) & \cdots & k_d a_{2d} \\ \vdots & \vdots & & \vdots \\ k_1 a_{n1} & k_2 a_{n2} & \cdots & \epsilon(A_d) \end{bmatrix}.$$

Here ϵ is the classical augmentation map on $R[G_i]$.

Zeta functions of $\mathbb{F}_q$-algebras

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements and R an finite dimensional $\mathbb{F}_q$-algebra.

Definition (Following Fukaya, Kato, and Kurokawa)

The zeta function of R is defined as

$$\zeta_R(s) = \prod_{m \subset R} (1 - \#(R/m)^{-s})^{-1}.$$

where m runs over all left maximal ideal of R.

Zeta functions of $\mathbb{F}_q$-algebras

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements and R an finite dimensional $\mathbb{F}_q$-algebra.

Definition (Following Fukaya, Kato, and Kurokawa)

The zeta function of R is defined as

$$\zeta_R(s) = \prod_{m \subset R} (1 - \#(R/m)^{-s})^{-1}.$$

where m runs over all left maximal ideal of R.

This zeta function has an equivalent Euler product presentation

$$\zeta_R(s) = \prod_{M} (1 - q^{-\dim_{\mathbb{F}_q}(M)s})^{-1}$$

where M runs over the set of all simple left modules over R.

Zeta functions of $\mathbb{F}_q$-algebras

Like most other zeta functions in the universe, the zeta function $\zeta_R(s)$ is a "counting" zeta function.

Proposition

Zeta functions of $\mathbb{F}_q$-algebras

Like most other zeta functions in the universe, the zeta function $\zeta_R(s)$ is a "counting" zeta function.

Proposition

Suppose that R is a semi-simple $\mathbb{F}_q$-algebra. Then

$$\zeta_R(s) = \sum_{n=0}^{\infty} \frac{c_n}{q^{ns}} = \sum_{n=0}^{\infty} c_n u^n,$$

where c_n is the number non-isomorphic R-modules of dimension n and $u = q^{-s}$.

Note that for an $\mathbb{F}_q$-algebra, we always have

$$\zeta_R(s) = \zeta_{R^{\mathrm{ss}}}(s),$$

where $R^{\mathrm{ss}} = R/\mathrm{Rad(R)}$ is the semisimplication of R.

Some examples

1. Let $R = M_n(\mathbb{F}_q)$. By the Morita equivalence, we have
$$\zeta_R(s) = \zeta_{\mathbb{F}_q}(s) = (1 - q^{-s})^{-1}.$$

Some examples

1. Let $R = M_n(\mathbb{F}_q)$. By the Morita equivalence, we have
$$\zeta_R(s) = \zeta_{\mathbb{F}_q}(s) = (1 - q^{-s})^{-1}.$$

2. Suppose G is a p-group $R = \mathbb{F}_q[G]$. Then R is a local ring with
$$\mathrm{Rad}(R) = \ker(\epsilon : R \to \mathbb{F}_q).$$
In particular, $R^{\mathrm{ss}} = \mathbb{F}_q$ and $\zeta_R(s) = (1 - q^{-s})^{-1}$.

Some examples

1. Let $R = M_n(\mathbb{F}_q)$. By the Morita equivalence, we have
$$\zeta_R(s) = \zeta_{\mathbb{F}_q}(s) = (1 - q^{-s})^{-1}.$$

2. Suppose G is a p-group $R = \mathbb{F}_q[G]$. Then R is a local ring with
$$\mathrm{Rad}(R) = \ker(\epsilon : R \to \mathbb{F}_q).$$
In particular, $R^{\mathrm{ss}} = \mathbb{F}_q$ and $\zeta_R(s) = (1 - q^{-s})^{-1}$.

3. If $p \nmid |G|$ and G is split over $\mathbb{F}_q$, then by the Artin-Wedderburn theorem
$$R = \mathbb{F}_q[G] \cong \prod_{i=1}^{d} M_{n_i}(\mathbb{F}_q).$$
Therefore
$$\zeta_R(s) = (1 - q^{-s})^{-d}.$$

Zeta function of the joint algebra $J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$

Up to ordering, there exists a (unique) positive integer r such that

- $p \nmid |G_i|, 1 \leq i \leq r$.
- $p \mid |G_i|, r < i \leq d$.

Theorem

The zeta function of of the joint algebra $J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is given by

$$\zeta_{J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)}(s) = (1 - q^{-s})^{r-1} \prod_{i=1}^{d} \zeta_{\mathbb{F}_q[G_i]}(s).$$

Sketch of the proof in the semisimple case

Assume that $|G_i|$ are all invertible in $\mathbb{F}_q$.

Sketch of the proof in the semisimple case

Assume that $|G_i|$ are all invertible in $\mathbb{F}_q$. Let

$$e_{G_i} = \frac{1}{|G_i|} \sum_{g \in G_i} g.$$

Then e_{G_i} is a central idempotent element in $\mathbb{F}_q[G]$.

Sketch of the proof in the semisimple case

Assume that $|G_i|$ are all invertible in $\mathbb{F}_q$. Let

$$e_{G_i} = \frac{1}{|G_i|} \sum_{g \in G_i} g.$$

Then e_{G_i} is a central idempotent element in $\mathbb{F}_q[G]$. Therefore, we have the following decomposition

$$\mathbb{F}_q[G_i] \cong \mathbb{F}_q[G_i]e_{G_i} \times \mathbb{F}_q(1 - e_{G_i}) \cong \mathbb{F}_q \times \Delta_{G_i}(\mathbb{F}_q),$$

where $\Delta_{G_i}(\mathbb{F}_q) = \ker(\mathbb{F}_q[G_i] \to \mathbb{F}_q)$.

Sketch of the proof in the semisimple case

Assume that $|G_i|$ are all invertible in $\mathbb{F}_q$. Let

$$e_{G_i} = \frac{1}{|G_i|} \sum_{g \in G_i} g.$$

Then e_{G_i} is a central idempotent element in $\mathbb{F}_q[G]$. Therefore, we have the following decomposition

$$\mathbb{F}_q[G_i] \cong \mathbb{F}_q[G_i]e_{G_i} \times \mathbb{F}_q(1 - e_{G_i}) \cong \mathbb{F}_q \times \Delta_{G_i}(\mathbb{F}_q),$$

where $\Delta_{G_i}(\mathbb{F}_q) = \ker(\mathbb{F}_q[G_i] \to \mathbb{F}_q)$.

Using these idempotents and the generalized augmentation map, we can show that

$$J_{G_1, G_2, \ldots, G_d}(\mathbb{F}_q) \cong M_d(\mathbb{F}_q) \times \prod_{i=1}^{d} \Delta_{G_i}(\mathbb{F}_q).$$

Sketch of the proof in the semisimple case

Assume that $|G_i|$ are all invertible in $\mathbb{F}_q$. Let

$$e_{G_i} = \frac{1}{|G_i|} \sum_{g \in G_i} g.$$

Then e_{G_i} is a central idempotent element in $\mathbb{F}_q[G]$. Therefore, we have the following decomposition

$$\mathbb{F}_q[G_i] \cong \mathbb{F}_q[G_i]e_{G_i} \times \mathbb{F}_q(1 - e_{G_i}) \cong \mathbb{F}_q \times \Delta_{G_i}(\mathbb{F}_q),$$

where $\Delta_{G_i}(\mathbb{F}_q) = \ker(\mathbb{F}_q[G_i] \to \mathbb{F}_q)$.

Using these idempotents and the generalized augmentation map, we can show that

$$J_{G_1, G_2, \ldots, G_d}(\mathbb{F}_q) \cong M_d(\mathbb{F}_q) \times \prod_{i=1}^{d} \Delta_{G_i}(\mathbb{F}_q).$$

The formula for the zeta function of $J_{G_1, G_2, \ldots, G_d}(\mathbb{F}_q)$ follows easily from this isomorphism.

Sketch of the proof in the general case

In general, we can show that

$$J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)^{\mathrm{ss}} \cong J_{G_1,\ldots,G_r}(\mathbb{F}_q) \times \prod_{i=r+1}^{d} \mathbb{F}_q[G_i]^{\mathrm{ss}}.$$

The zeta function of $J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ can be computed via this isomorphism and the calculations done in the semisimple case.

A corollary

A direct corollary of the above argument is the following.

Theorem (Generalized Maschke theorem)

The joint algebra $J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is semisimple if and only if $|G_i|$ is invertible in $\mathbb{F}_q$ for all $1 \leq i \leq d$.

A corollary

A direct corollary of the above argument is the following.

Theorem (Generalized Maschke theorem)

The joint algebra $J_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is semisimple if and only if $|G_i|$ is invertible in $\mathbb{F}_q$ for all $1 \leq i \leq d$.

Note that this statement holds if we replace $\mathbb{F}_q$ by a semisimple ring R.

Thank you