Cycles in (abstract) isogeny graphs: How many are there, and where can you find them?

Eli Orvis

University of Colorado Boulder

June 26, 2025

Why study cycles in isogeny graphs

Let $G(p, \ell)$ be the supersingular ℓ-isogeny graph modulo p.

Why study cycles in isogeny graphs

Let $G(p, \ell)$ be the supersingular ℓ-isogeny graph modulo p.

Why should we care about cycles in $G(p, \ell)$?

Why study cycles in isogeny graphs

Let $G(p, \ell)$ be the supersingular ℓ-isogeny graph modulo p.

Why should we care about cycles in $G(p, \ell)$?

1. Cycles provide security failures (i.e. CGL hash function) [1]

Why study cycles in isogeny graphs

Let $G(p, \ell)$ be the supersingular ℓ-isogeny graph modulo p.

Why should we care about cycles in $G(p, \ell)$?

1. Cycles provide security failures (i.e. CGL hash function) [1]
2. Cycles can be used to compute endomorphisms [2]

Why study cycles in isogeny graphs

Let $G(p, \ell)$ be the supersingular ℓ-isogeny graph modulo p.

Why should we care about cycles in $G(p, \ell)$?

1. Cycles provide security failures (i.e. CGL hash function) [1]
2. Cycles can be used to compute endomorphisms [2]
3. Cycles are fun!

Orientations and Cycles

We are particularly interested in *non-backtracking* cycles:

Orientations and Cycles

We are particularly interested in *non-backtracking* cycles:

Definition

Let $\phi_1, \ldots, \phi_n$ be isogenies representing a cycle in $G(p, \ell)$. The cycle is *non-backtracking* if $\phi_{i+1} \circ \phi_i \neq [\ell]$ for all $1 \leq i < n$.

Orientations and Cycles

We are particularly interested in *non-backtracking* cycles:

Definition

Let $\phi_1, \ldots, \phi_n$ be isogenies representing a cycle in $G(p, \ell)$. The cycle is *non-backtracking* if $\phi_{i+1} \circ \phi_i \neq [\ell]$ for all $1 \leq i < n$.

The paper *Orientations and cycles in supersingular ℓ-isogeny graphs* [3] introduced "isogeny cycles":

Orientations and Cycles

We are particularly interested in *non-backtracking* cycles:

Definition

Let $\phi_1, \ldots, \phi_n$ be isogenies representing a cycle in $G(p, \ell)$. The cycle is *non-backtracking* if $\phi_{i+1} \circ \phi_i \neq [\ell]$ for all $1 \leq i < n$.

The paper *Orientations and cycles in supersingular ℓ-isogeny graphs* [3] introduced "isogeny cycles":

Definition

An *isogeny cycle* is a closed walk, forgetting basepoint, in $G(p, \ell)$ containing no backtracking, which is not a power of another closed walk.

Orientations and Cycles

The main result of [3] establishes a bijection between isogeny cycles in $G(p, \ell)$ and rims of oriented isogeny volcanoes:

Orientations and Cycles

The main result of [3] establishes a bijection between isogeny cycles in $G(p, \ell)$ and rims of oriented isogeny volcanoes:

Theorem

Let $r > 2$. There is a bijection between isogeny cycles of length r and directed rims of size r in $\mathcal{G}_{K,\ell}$ where K ranges over all imaginary quadratic fields.

Orientations and Cycles

The main result of [3] establishes a bijection between isogeny cycles in $G(p, \ell)$ and rims of oriented isogeny volcanoes:

Theorem

Let $r > 2$. There is a bijection between isogeny cycles of length r and directed rims of size r in $\mathcal{G}_{K,\ell}$ where K ranges over all imaginary quadratic fields.

Corollary

Let $p \equiv 1 \pmod{12}$. Then the number of isogeny cycles of length r in $G(p, \ell)$ is asymptotically $\ell^r/2r$ as $r \to \infty$.

Orientations and Cycles

Questions:

Orientations and Cycles

Questions:

1. Where do these cycles live in $G(p, \ell)$?

Orientations and Cycles

Questions:

1. Where do these cycles live in $G(p, \ell)$?
2. Can we remove the $p \equiv 1 \pmod{12}$ condition in Corollary 4?

Orientations and Cycles

Questions:

1. Where do these cycles live in $G(p, \ell)$?
2. Can we remove the $p \equiv 1 \pmod{12}$ condition in Corollary 4?
3. Can we extend any of these results to other isogeny graphs?

Finding cycles

The spine

In order to answer the question of *where* you can find cycles, we need a reference point:

The spine

In order to answer the question of *where* you can find cycles, we need a reference point:

Definition

The *spine* of $G(p, \ell)$ is the subgraph induced by the $\mathbb{F}_p$ vertices.

The spine

In order to answer the question of *where* you can find cycles, we need a reference point:

Definition

The *spine* of $G(p, \ell)$ is the subgraph induced by the $\mathbb{F}_p$ vertices.

Note: In a vague sense this is "all" you can use.

The spine

In order to answer the question of *where* you can find cycles, we need a reference point:

Definition

The *spine* of $G(p, \ell)$ is the subgraph induced by the $\mathbb{F}_p$ vertices.

Note: In a vague sense this is “all” you can use.

Basic question: How many cycles intersect the spine?

Results

Results

Theorem (O.)

Fix ℓ and r, $r \neq 2^k$. Let

$$R_1 = \frac{\#\text{ vertices in } \mathcal{G}_{\ell,p} \text{ contained in an } r\text{-cycle}}{\#\text{ of vertices in } \mathcal{G}_{\ell,p}},$$

and

$$R_2 = \frac{\#\text{ vertices in } \mathcal{S} \text{ contained in an } r\text{-cycle}}{\#\text{ of vertices in } \mathcal{S}}.$$

Then for each sufficiently large p, either

1. $R_2 = 0$, *or,*
2. $R_1 < R_2$.

Results

Theorem (O.)

Fix ℓ and r, $r \neq 2^k$. Let

$$R_1 = \frac{\#\text{ vertices in } \mathcal{G}_{\ell,p} \text{ contained in an } r\text{-cycle}}{\#\text{ of vertices in } \mathcal{G}_{\ell,p}},$$

and

$$R_2 = \frac{\#\text{ vertices in } \mathcal{S} \text{ contained in an } r\text{-cycle}}{\#\text{ of vertices in } \mathcal{S}}.$$

Then for each sufficiently large p, either

1. $R_2 = 0$, *or,*
2. $R_1 < R_2$.

In other words, for large enough primes p, r-cycles are disproportionately likely to occur along the spine.

Results

We will give formulas for

1. the number of r-cycles along the spine,
2. the average number of r-cycles as $p \to \infty$.

Results

We will give formulas for

1. the number of r-cycles along the spine,
2. the average number of r-cycles as $p \to \infty$.

Definition

Let

$$X_r = \{\text{imaginary quadratic discriminants } \Delta, \text{ where...}\}$$

1. $\ell = [\mathfrak{l}][\bar{\mathfrak{l}}]$ in $cl(\mathcal{O}_\Delta)$,
2. $o([\mathfrak{l}]) \mid r$,
3. and the conductor of $\mathcal{O}_\Delta$ is not divisible by ℓ.

Results

Definition

Let $H_{\mathcal{O}_\Delta}(x) =$ Hilbert Class Polynomial of $\mathcal{O}_\Delta$. Define

$$\delta_p(\Delta) = \begin{cases} 1 & \text{if } \left(\frac{\Delta}{p}\right) = -1 \text{ and } H_{\mathcal{O}_\Delta}(x) \text{ has a solution in } \mathbb{F}_p, \\ 0 & \text{otherwise.} \end{cases}$$

Results

Theorem (O.)

Fix p, ℓ, r, with $p \gg 0$. Then

$$\#\{r\text{-cycles intersecting } \mathcal{S}\} = 2\sum_{d|r} \mu(d) \sum_{\Delta \in X_{\frac{r}{d}}} \delta_p(\Delta) h_2(\Delta),$$

where $h_2(\Delta) = |cl(\mathcal{O}_\Delta)[2]|$.

Results

We can compute the average number of r-cycles along $\mathcal{S}$:

Results

We can compute the average number of r-cycles along $\mathcal{S}$:

Theorem (O.)

Fix ℓ, r. Let $(p_i)_{i=1}^{\infty}$ be an increasing sequence of consecutive primes. Then

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \#\{r\text{-cycles intersecting } \mathcal{S}_{\ell,p_i}\} = \sum_{d|r} \mu(d) \# X_{\frac{r}{d}}.$$

Techniques

Restricting to odd r, we can outline our strategy as follows:

Techniques

Restricting to odd r, we can outline our strategy as follows:

1. By results of [3], all r-cycles come from orders in X_r.

Techniques

Restricting to odd r, we can outline our strategy as follows:

1. By results of [3], all r-cycles come from orders in X_r.
2. Lift the problem to the oriented isogeny graph.

Techniques

Restricting to odd r, we can outline our strategy as follows:

1. By results of [3], all r-cycles come from orders in X_r.
2. Lift the problem to the oriented isogeny graph.
3. Use Kaneko's bound [4] to show that for large enough p, all of the oriented r-cycles produce disjoint unoriented cycles.

Techniques

Restricting to odd r, we can outline our strategy as follows:

1. By results of [3], all r-cycles come from orders in X_r.
2. Lift the problem to the oriented isogeny graph.
3. Use Kaneko's bound [4] to show that for large enough p, all of the oriented r-cycles produce disjoint unoriented cycles.
4. Show that, for sufficiently large p, each oriented r-cycle contains at most one $\mathbb{F}_p$-vertex.

Techniques

Restricting to odd r, we can outline our strategy as follows:

1. By results of [3], all r-cycles come from orders in X_r.
2. Lift the problem to the oriented isogeny graph.
3. Use Kaneko's bound [4] to show that for large enough p, all of the oriented r-cycles produce disjoint unoriented cycles.
4. Show that, for sufficiently large p, each oriented r-cycle contains at most one $\mathbb{F}_p$-vertex.

Together, these give us:

$$r\text{-cycles on } \mathcal{S} \leftrightarrow \mathbb{F}_p \text{ roots of } H_{\mathcal{O}}(x), \text{ for } \mathcal{O} \in X_r$$

.

Example

Example: 3-cycles in $\mathcal{G}_{3,p}$.

Example

Example: 3-cycles in $\mathcal{G}_{3,p}$.

By results of ACLSST [3], every 3-cycle in $\mathcal{G}_{3,p}$ is obtained from one of the following orders:

$$\{-23, -44, -59, -83, -92, -104, -107\}.$$

Example

Theorem (Kaneko [4])

Suppose that

$$\mathcal{O}_{D_1} \hookrightarrow O \quad \text{and} \quad \mathcal{O}_{D_2} \hookrightarrow O$$

for O a maximal order of $B_{p,\infty}$. Then

$$D_1 D_2 \geq 4p.$$

If $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$, then

$$D_1 D_2 \geq p^2.$$

Example

Theorem (Kaneko [4])

Suppose that

$$\mathcal{O}_{D_1} \hookrightarrow O \quad \text{and} \quad \mathcal{O}_{D_2} \hookrightarrow O$$

for O *a maximal order of* $B_{p,\infty}$*. Then*

$$D_1 D_2 \geq 4p.$$

If $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$*, then*

$$D_1 D_2 \geq p^2.$$

Using this gives that the 3-cycles in $\mathcal{G}_{3,p}$ are disjoint for $p > \frac{(-104)(-107)}{4}$.

Example

Theorem (Chen & Xue [5])

Let $\mathcal{H}_p = \{\mathbb{F}_p \text{ roots of } H_{\mathcal{O}}(x)\}$. If $\mathcal{H}_p \neq \emptyset$, then $cl(\mathcal{O})[2]$ acts freely and transitively on $\mathcal{H}_p$.

Example

Theorem (Chen & Xue [5])

Let $\mathcal{H}_p = \{\mathbb{F}_p$ roots of $H_{\mathcal{O}}(x)\}$. If $\mathcal{H}_p \neq \emptyset$, then $cl(\mathcal{O})[2]$ acts freely and transitively on $\mathcal{H}_p$.

Consequence: There are 2^k many $\mathbb{F}_p$-roots.

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

1. Frobenius fixes the vertex set of C.

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

1. Frobenius fixes the vertex set of C.
2. Thus there are 0 or 2 $\mathbb{F}_{p^2}$-vertices in C.

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

1. Frobenius fixes the vertex set of C.
2. Thus there are 0 or 2 $\mathbb{F}_{p^2}$-vertices in C.
3. Each 3-cycle contains the same number of $\mathbb{F}_p$-vertices.

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

1. Frobenius fixes the vertex set of C.
2. Thus there are 0 or 2 $\mathbb{F}_{p^2}$-vertices in C.
3. Each 3-cycle contains the same number of $\mathbb{F}_p$-vertices.
4. The total number of $\mathbb{F}_p$-vertices is a power of 2.

Example

Let C be an 3-cycle intersecting $\mathcal{S}$, and $p \gg 0$:

1. Frobenius fixes the vertex set of C.
2. Thus there are 0 or 2 $\mathbb{F}_{p^2}$-vertices in C.
3. Each 3-cycle contains the same number of $\mathbb{F}_p$-vertices.
4. The total number of $\mathbb{F}_p$-vertices is a power of 2.

Thus there is exactly 1 $\mathbb{F}_p$-vertex on C.

Example

For $p \gg 0$, we can count the $\mathbb{F}_p$-vertices by counting the $\mathbb{F}_p$-vertices for each order in

$$\{-23, -44, -59, -83, -92, -104, -107\},$$

where p does not split.

Example

For $p \gg 0$, we can count the $\mathbb{F}_p$-vertices by counting the $\mathbb{F}_p$-vertices for each order in

$$\{-23, -44, -59, -83, -92, -104, -107\},$$

where p does not split.

Here we use either Chen and Xue [5], or Li, Li, and Ouyang [6].

Example

For $p \gg 0$, we can count the $\mathbb{F}_p$-vertices by counting the $\mathbb{F}_p$-vertices for each order in

$$\{-23, -44, -59, -83, -92, -104, -107\},$$

where p does not split.

Here we use either Chen and Xue [5], or Li, Li, and Ouyang [6].

Note: The number of such vertices depends only on congruence conditions on p!

Open questions

Open questions

1. What is the "right" generalization to vertices that are "near" the spine?

Open questions

1. What is the “right” generalization to vertices that are “near” the spine?
2. Can the same results be deduced from the recent paper of He-Korpal-Tran-Vincent on Gross lattices of curves over $\mathbb{F}_p$?

Counting cycles

Ihara zeta functions

This part of the talk is joint work with Jun Bo Lau, Travis Morrison, Gabrielle Scullard, and Lukas Zobernig.

Ihara zeta functions

This part of the talk is joint work with Jun Bo Lau, Travis Morrison, Gabrielle Scullard, and Lukas Zobernig.

A natural object to study the *number* of cycles in a graph G is the *Ihara zeta function*:

Definition

Ihara zeta functions

This part of the talk is joint work with Jun Bo Lau, Travis Morrison, Gabrielle Scullard, and Lukas Zobernig.

A natural object to study the *number* of cycles in a graph G is the *Ihara zeta function*:

Definition

Let G be an (undirected) graph. The *Ihara zeta function* of G is the function

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1}$$

Ihara zeta functions

Facts about Ihara zeta functions:

1. $u\frac{d}{du}\log\zeta_G(u) = \sum_{m\geq 1} N_m u^m$, where N_m is the number of non-backtracking cycles of length m.

Ihara zeta functions

Facts about Ihara zeta functions:

1. $u\frac{d}{du}\log\zeta_G(u) = \sum_{m\geq 1} N_m u^m$, where N_m is the number of non-backtracking cycles of length m.
2. (Bass determinant formula): Suppose that G is a d-regular graph, and let A be the adjacency matrix of G. Then we have:

$$\zeta_G(u) = \frac{(1-u^2)^{1-\chi(G)}}{\det(I - Au + (d-1)u^2)}.$$

Abstract isogeny graphs

We would like to study cycles not only in $G(p, \ell)$ but in other isogeny graphs:

Abstract isogeny graphs

We would like to study cycles not only in $G(p, \ell)$ but in other isogeny graphs:

1. Level H-structure, $G(p, \ell, H)$

Abstract isogeny graphs

We would like to study cycles not only in $G(p, \ell)$ but in other isogeny graphs:

1. Level H-structure, $G(p, \ell, H)$
2. Higher dimensional $(\ell, \ldots, \ell)$-graphs

Abstract isogeny graphs

We would like to study cycles not only in $G(p, \ell)$ but in other isogeny graphs:

1. Level H-structure, $G(p, \ell, H)$
2. Higher dimensional $(\ell, \ldots, \ell)$-graphs

In order to study all of these at once, we introduce the notion of an *abstract isogeny graph*.

Abstract isogeny graphs

Definition

An *abstract isogeny graph* is the following collection of data:

- A set X of vertices;
- a set Y of edges;
- functions, $s, t : Y \to X \times X$;
- a function $J : Y \to Y$; and
- a function $L : X \to X$,

such that $J(s(e)) = t(e)$ and $t(J(e)) = L(s(e))$ for all $e \in Y$.

Motivating abstract isogeny graphs

First, we should motivate the L function.

Motivating abstract isogeny graphs

First, we should motivate the L function. In the level structure graph $G(p, \ell, H)$, the dual map takes $\phi : (E, \iota) \to (E', \iota')$ to $\hat{\phi} : (E', \iota') \to (E, [\ell] \circ \iota)$.

Motivating abstract isogeny graphs

First, we should motivate the L function. In the level structure graph $G(p, \ell, H)$, the dual map takes $\phi : (E, \iota) \to (E', \iota')$ to $\hat{\phi} : (E', \iota') \to (E, [\ell] \circ \iota)$.

But if H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} \notin H$, then $(E, [\ell] \circ \iota) \neq (E, \iota)$!

Motivating abstract isogeny graphs

First, we should motivate the L function. In the level structure graph $G(p, \ell, H)$, the dual map takes $\phi : (E, \iota) \to (E', \iota')$ to $\hat{\phi} : (E', \iota') \to (E, [\ell] \circ \iota)$.

But if H is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} \notin H$, then $(E, [\ell] \circ \iota) \neq (E, \iota)$!

The operator L keeps track of how the target of J depends on the source of the edge.

Motivating abstract isogeny graphs

Theorem (Bo Lau, Morrison, O., Scullard, Zobernig)

Choosing appropriate representatives for the dual map in order to define J, we can realize $G(p, \ell, H)$ as an abstract isogeny graph for any H. The same is true for $(\ell, \ldots, \ell)$-isogeny graphs.

Ihara zeta function for abstract isogeny graphs

We define the Ihara zeta function of an abstract isogeny graph as

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.

Ihara zeta function for abstract isogeny graphs

We define the Ihara zeta function of an abstract isogeny graph as

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.
We will give the Ihara zeta function in two ways:

Ihara zeta function for abstract isogeny graphs

We define the Ihara zeta function of an abstract isogeny graph as

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.

We will give the Ihara zeta function in two ways:

1. by combinatorial data,

Ihara zeta function for abstract isogeny graphs

We define the Ihara zeta function of an abstract isogeny graph as

$$\zeta_G(u) = \prod_{\text{prime cycles } P} (1 - u^{|P|})^{-1},$$

where the primes are non-backtracking with respect to the J function.

We will give the Ihara zeta function in two ways:

1. by combinatorial data,
2. by relation to zeta functions of modular curves.

Ihara zeta function - combinatorial formula

For a function $f : S \to S$ acting on a finite set S, we define $C_k(f)$ to be the number of k-cycles in the largest permutation induced by f.

Ihara zeta function - combinatorial formula

For a function $f : S \to S$ acting on a finite set S, we define $C_k(f)$ to be the number of k-cycles in the largest permutation induced by f.

Theorem (Bo Lau, Morrison, O., Scullard, Zobernig)

Let $\Gamma = (X, Y, J, L)$ be an abstract isogeny graph with regular out degree d and adjacency matrix A. Then $\zeta_\Gamma(u)$ is given by:

$$\frac{(1-u^2)^{C_1(L)}(1+u)^{-C_1(J)} \prod_{k>1}(1-(-1)^k u^{2k})^{C_k(L)}(1-u^k)^{-C_k(J)}}{\det(1 - Au + u^2(d-1)L)}$$

Hasse-Weil Zeta functions

Our next goal is to relate Ihara zeta functions of abstract isogeny graphs to Hasse Weil zeta functions of modular curves. This will allow us to understand asymptotics of cycles in graphs with level structure.

Hasse-Weil Zeta functions

Our next goal is to relate Ihara zeta functions of abstract isogeny graphs to Hasse Weil zeta functions of modular curves. This will allow us to understand asymptotics of cycles in graphs with level structure.

Definition

Let X be a smooth, irreducible, projective variety defined over $\mathbb{F}_\ell$. The **Hasse-Weil zeta function** for X is defined as:

$$Z(X,u) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{\ell^n})}{n} u^n\right) = \prod_{x \in [X]} \frac{1}{1 - u^{\deg(x)}},$$

where the product is defined over the closed points of X.

Orientable graphs associated to abstract isogeny

Our formula relating the Ihara zeta function to Hasse-Weil zeta functions of modular curves will use the Euler characteristics of some auxiliary graphs, the *orientable graphs* associated to an abstract isogeny graph Γ.

Definition

Let $\Gamma = (X, Y, J, L)$ be an abstract isogeny graph. We define $\sim_X$ to be the smallest equivalence relation on X such that $x \sim_X Lx$ for all $x \in X$, and $\sim_Y$ to be the smallest equivalence relation on Y such that $y \sim_Y J^2 y$ for all $y \in Y$. The *orientable graphs associated to* Γ are
$\Gamma^+ = (X/\sim_X, Y/\sim_Y - \{[y] : J[y] = [y]\}, J)$ and
$\Gamma^- = (X/\sim_X, Y/\sim_Y \sqcup \{[y] : J[y] = [y]\}, J)$

Ihara zeta function - modular curves formula

Theorem

Let G be the ℓ-isogeny graph with Borel level structure. Let $X_0(pN)_{\mathbb{F}_\ell}$ and $X_0(N)_{\mathbb{F}_\ell}$ denote the modular curves over $\mathbb{F}_\ell$. Then we have that

$$Z(X_0(pN)_{\mathbb{F}_\ell}, u)Z(X_0(N)_{\mathbb{F}_\ell}, u)^{-2}\zeta_G(u) = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}$$

where G^{+1}, G^{-1} are the orientable graphs associated to G.

Ihara zeta function - modular curves formula

Theorem

Let G be the ℓ-isogeny graph with Borel level structure. Let $X_0(pN)_{\mathbb{F}_\ell}$ and $X_0(N)_{\mathbb{F}_\ell}$ denote the modular curves over $\mathbb{F}_\ell$. Then we have that

$$Z(X_0(pN)_{\mathbb{F}_\ell}, u)Z(X_0(N)_{\mathbb{F}_\ell}, u)^{-2}\zeta_G(u) = (1+u)^{\chi(G^{-1})}(1-u)^{\chi(G^{+1})}$$

where G^{+1}, G^{-1} are the orientable graphs associated to G.

Note: We can generalize this to much more general H.

Asymptotics for graphs with level structure in arbitrary characteristic

Finally, we use this product to deduce asymptotics for the number of cycles of length r as $r \to \infty$, for arbitrary p, and in the presence of level structure.

Asymptotics for graphs with level structure in arbitrary characteristic

Finally, we use this product to deduce asymptotics for the number of cycles of length r as $r \to \infty$, for arbitrary p, and in the presence of level structure.

Theorem (Bo Lau, Morrison, O., Scullard, Zobernig)

Let G be the ℓ-isogeny graph with Borel level structure, and N_r be the number of non-backtracking tailless cycles of length r in G. Then we have that

$$N_r = 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) - \chi(G^{+1}) + (-1)^{r-1}\chi(G^{-1}).$$

Asymptotics for graphs with level structure in arbitrary characteristic

The previous theorem gives the following asymptotic:

Asymptotics for graphs with level structure in arbitrary characteristic

The previous theorem gives the following asymptotic:

Theorem (Bo Lau, Morrison, O., Scullard, Zobernig)

Let G be the ℓ-isogeny graph with N-level structure for an arbitrary prime p. Let N_r be the number of non-backtracking cycles of length r in G. Then N_r asymptotically approaches ℓ^r as $r \to \infty$.

The one proof

Proof.

1. By the product formula for the zeta functions, we have constants C_1, C_2 such that

$$2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_1 \leq N_r$$

and

$$N_r \leq 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_2.$$

The one proof

Proof.

1. By the product formula for the zeta functions, we have constants C_1, C_2 such that

$$2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_1 \leq N_r$$

and

$$N_r \leq 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_2.$$

2. By Hasse's bound

$$\#X_0(pN)(\mathbb{F}_{\ell^r})/\ell^r \to 1$$

as $r \to \infty$.

The one proof

Proof.

1. By the product formula for the zeta functions, we have constants C_1, C_2 such that

$$2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_1 \leq N_r$$

and

$$N_r \leq 2\#X_0(N)(\mathbb{F}_{\ell^r}) - \#X_0(pN)(\mathbb{F}_{\ell^r}) + C_2.$$

2. By Hasse's bound

$$\#X_0(pN)(\mathbb{F}_{\ell^r})/\ell^r \to 1$$

as $r \to \infty$.

3. So $N_r/\ell^r \to 2 - 1 = 1$ as $r \to \infty$.

Open questions

Open questions

1. Can the formula for the Ihara zeta function of an abstract isogeny graph be simplified? (in progress)

Open questions

1. Can the formula for the Ihara zeta function of an abstract isogeny graph be simplified? (in progress)
2. Can one give a version of the "graph theory prime number theorem" for abstract isogeny graphs?

Open questions

1. Can the formula for the Ihara zeta function of an abstract isogeny graph be simplified? (in progress)
2. Can one give a version of the "graph theory prime number theorem" for abstract isogeny graphs?
3. Can the zeta function product formula be generalized to $(\ell, \ldots, \ell)$-isogeny graphs?

Open questions

1. Can the formula for the Ihara zeta function of an abstract isogeny graph be simplified? (in progress)
2. Can one give a version of the "graph theory prime number theorem" for abstract isogeny graphs?
3. Can the zeta function product formula be generalized to $(\ell, \ldots, \ell)$-isogeny graphs?
4. Are there other interesting properties of isogeny graphs that can be understood from their zeta functions?

References I

[1] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic hash functions from expander graphs". In: *J. Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790,1432-1378. DOI: 10.1007/s00145-007-9002-x. URL: https://doi.org/10.1007/s00145-007-9002-x.

[2] Kirsten Eisenträger et al. "Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs". In: *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 215–232. ISBN: 978-1-935107-08-8; 978-1-935107-07-1. DOI: 10.2140/obs.2020.4.215. URL: https://doi.org/10.2140/obs.2020.4.215.

References II

[3] Sarah Arpin et al. *Orientations and cycles in supersingular isogeny graphs*. 2022. arXiv: 2205.03976 [math.NT].

[4] Masanobu Kaneko. "Supersingular j-invariants as singular moduli $\mod p$". In: *Osaka J. Math.* 26.4 (1989), pp. 849–855. ISSN: 0030-6126. URL: http://projecteuclid.org/euclid.ojm/1200781857.

[5] Mingjie Chen and Jiangwei Xue. *On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p*. 2022. arXiv: 2202.04317 [math.NT].

[6] Jianing Li, Songsong Li, and Yi Ouyang. *Factorization of Hilbert class polynomials over prime fields*. 2021. arXiv: 2108.00168 [math.NT].