Unramified graph covers of finite degree

Dynamics and Graphs over Finite Fields: Algebraic, Number Theoretic and Algorithmic Aspects

in honor of Igor Shparlinski's 60th birthday

CIRM, Luminy, March 30, 2016

Winnie Li

Pennsylvania State University

Unramified covers of a graph

All graphs are connected and undirected.

- An unramified cover of a graph X is a surjective graph homo. $\alpha : Y \to X$ which is a local isom. All covers are unramified.
- The group of automorphisms of α is

$$Aut(\alpha) = \{\gamma : Y \to Y \text{ automorphism} | \alpha = \alpha \circ \gamma\}.$$

An auto. is determined by its action on the fiber $\alpha^{-1}(x)$ above any vertex x of X.

- Call α a normal cover if $Aut(\alpha)$ acts transitively on one and hence all fibers. Its Galois group $G_\alpha = Aut(\alpha)$.
- If a fiber $\alpha^{-1}(x)$ is a finite set, its cardinality is called the *degree* of α. A finite degree cover α is normal if and only if $|Aut(\alpha)| = \deg \alpha$.

- The universal cover $\tilde{X}$ of X is a tree. The natural projection $pr_X : \tilde{X} \to X$ is a normal cover with $Aut(pr_X) = \pi_1(X, x)$, the fundamental group of X.

  (So $X \leftrightarrow F$, $\tilde{X} \leftrightarrow \bar{F}$, and $\pi_1(X, x) \leftrightarrow G_F$.)

- A cover $\beta : Y \to Z$ is called a *subcover* of the cover $\alpha : Y \to X$ if α factors through β, that is, there is a cover $\gamma : Z \to X$ such that $\alpha = \gamma \circ \beta$. Denote γ by α/β.

- Two subcovers $\beta : Y \to Z$ and $\beta' : Y \to Z'$ of $\alpha : Y \to X$ are *equivalent* if there exists a graph isomorphism $\gamma : Z \to Z'$ such that $\gamma \circ \beta = \beta'$ and $\alpha/\beta = (\alpha/\beta') \circ \gamma$.

  (cover $\alpha \leftrightarrow$ field extension $K \supseteq F$, and equivalence classes of subcovers $\leftrightarrow$ intermediate fields)

Galois theory for graph covers

Let $\alpha : Y \to X$ be a normal cover with Galois group G_α. Denote by $[\beta]_\alpha$ the subcovers of α equivalent to β. Then

(1) The map $[\beta]_\alpha \mapsto G_\beta$ is a bijection from the set of equiv. classes of subcovers of α to the set of subgroups of G_α.

(2) Let β be a subcover of α. Then α/β is a normal cover if and only if G_β is a normal subgroup of G_α. In this case

$$G_{\alpha/\beta} \cong G_\alpha / G_\beta.$$

Call such β a *normal subcover* of α.

(3) $\pi_1(Y, y)$ can be imbedded as a subgroup of $\pi_1(X, x)$ so that

$$G_\alpha \cong \pi_1(X, x)/\pi_1(Y, y).$$

Here $y \in \alpha^{-1}(x)$.

The fundamental group of X

Suppose X is a finite graph with n vertices and m edges. Each element in the fundamental group $\pi_1(X, x)$ is represented by a backtrackless walk in X starting and ending at x.

$\pi_1(X, x)$ is a free group of rank $r(X) = m - n + 1$.

To find a set of generators, choose a spanning tree T in X, which uses $n - 1$ edges of X. Adding an unused edge e_i to T yields a loop L_i, which in turn yields a backtrackless walk C_i in $\pi_1(X, x)$. These C_i's generate $\pi_1(X, x)$, each of length $\leq 2n - 1$.

$r(X) = 0$ implies X is a tree, hence no covers;
$r(X) = 1$ implies X is homotopic to a circle. For each d, there is one cover of degree d.

Assume $r(X) \geq 2$ *and each vertex has degree at least* 2.

Prime ideals in a number field

Let F be a number field.

- The set of elements in F integral over $\mathbb{Z}$ form a ring $\mathbb{Z}_F$. Usually it is not a UFD, but each nonzero ideal in $\mathbb{Z}_F$ is a finite product of max'l ideals, called the "primes" of F, unique up to order.
- Given a finite extension K of F and a prime $\mathfrak{p}$ of F,

$$\mathfrak{p}\mathbb{Z}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_1, ..., \mathfrak{P}_r$ are distinct primes of K and $e_j \geq 1$. The primes $\mathfrak{P}_1, ..., \mathfrak{P}_r$ are called the primes of K over $\mathfrak{p}$.

Say $\mathfrak{p}$ unramified in K if all $e_j = 1$. An unram. $\mathfrak{p}$ splits completely in K if all primes $\mathfrak{P}_j$ over $\mathfrak{p}$ have same norm as $\mathfrak{p}$.
- Finite Galois extensions K of F are determined by the set of primes of F splitting completely in K.

Primes in a finite graph

Let X be a finite connected undirected graph.

- A geodesic cycle of X is a closed walk which is backtrackless when traveled along it twice. It has a starting vertex and orientation.
- A geodesic cycle is *primitive* if it is not obtained by traveling along a shorter geodesic cycle more than once. So a geodesic cycle is either primitive or a power of a primitive cycle.
- A "prime" of X is a primitive geodesic cycle in X up to equivalence, i.e. ignoring the starting point (but keeping the orientation).
- $r(X) \geq 2$ implies that X has infinitely many primes.

Decomposition of primes of a graph

Let $\alpha : Y \to X$ be a finite unramified cover.

- Let $\mathfrak{P}$ be a prime of Y. Then $\alpha(\mathfrak{P}) = \mathfrak{p}^k$ for a prime $\mathfrak{p}$ of X and an integer $k \geq 1$. Say $\mathfrak{P}$ lies above $\mathfrak{p}$. Then $\ell(\mathfrak{P}) = k\ell(\mathfrak{p})$.
- Given a prime $\mathfrak{p}$ of X, there are finitely many primes $\mathfrak{P}$ of Y lying above $\mathfrak{p}$ (arising from lifting $\mathfrak{p}$ in Y). Say $\mathfrak{p}$ splits completely in Y if all primes $\mathfrak{P}$ of Y above $\mathfrak{p}$ have the same length as $\mathfrak{p}$. In other words, all liftings of $\mathfrak{p}$ in Y are closed.

Characterizing finite normal covers

Suppose $|X| = n$. Let $\alpha : Y \to X$ be a finite normal cover. For a subcover $\beta : Y \to Z$ of α, let

$P_\ell(\beta) = \{$primes of X with length $\leq \ell$ which split completely in $\beta(Y) = Z\}$.

Theorem [Huang-L] *Assume $r(X) \geq 2$. Two normal subcovers β and β' of α are equiv. iff*

$$P_{4nd-d-1}(\beta) = P_{4nd-d-1}(\beta'),$$

where $d = lcm(\deg(\alpha/\beta), \deg(\alpha/\beta'))$.

In particular, equiv classes of degree d normal covers of X are characterized by the primes of X of length $\leq 4nd - d - 1$ that split completely.

Characterizing equivalent subcovers

Suppose $|X| = n$. Let $\alpha : Y \to X$ be a finite normal cover. Fix a vertex x of X. Choose a vertex $y \in \alpha^{-1}(x)$.

For a subcover $\beta : Y \to Z$ of α and integer $\ell > 0$, let

$C_\ell(\beta) = \{$cycles in X starting at x with length $\leq \ell$ which lift (via α/β) to cycles in $\beta(Y) = Z$ starting at $\beta(y)$ $\}$.

Theorem [Huang-L] *Two subcovers β and β' of α are equiv. iff*

$$C_{2nd-1}(\beta) = C_{2nd-1}(\beta'),$$

where $d = \max(\deg(\alpha/\beta), \deg(\alpha/\beta'))$.

Cebotarev density theorem for number fields

Given a modulus m, the arithmetic progressions $r+m\mathbb{Z}$ partition the integers into m sets. The primes, except finitely many of them, are contained in the progressions with remainder r coprime to m. There are $\phi(m)$ such progressions.

Dirichlet's theorem: The primes are uniformly distributed among these arithmetic progressions in the sense that the primes contained in any $r+m\mathbb{Z}$ with $(r,m)=1$ has natural density $1/\phi(m)$.

The Cebotarev density theorem extends Dirichlet's theorem.

- Let K/F be a finite Galois extension with Galois group G. To each prime $\mathfrak{p}$ of F unramified in K we associate a Frobenius conjugacy class of G, denoted $\mathrm{Frob}(\mathfrak{p})$.

- Given a conjugacy class $\mathcal{C}$ of G, let

$$P(\mathcal{C}) = \{\mathfrak{p} \text{ prime of } F : \mathrm{Frob}(\mathfrak{p}) = \mathcal{C}\}.$$

- Cebotarev density theorem (CDT): The Frobenius conjugacy classes are uniformly distributed. More precisely, for each conjugacy class $\mathcal{C}$ of G, the set $P(\mathcal{C})$ has natural density $\frac{|\mathcal{C}|}{|G|}$, i.e.,

$$\lim_{r\to\infty} \frac{\#\{\mathfrak{p} \in P(\mathcal{C}) : N(\mathfrak{p}) \leq r\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) \leq r\}} = \frac{|\mathcal{C}|}{|G|}.$$

When $K = \mathbb{Q}(\zeta_m)$ and $F = \mathbb{Q}$, the Galois group G is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, hence $|G| = \phi(m)$. Each conjugacy class $\mathcal{C}$ is a singleton. For each $p \nmid m$, $\mathrm{Frob}(p) = p$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then CDT reduces to Dirichlet's theorem.

Frobenius conjugacy classes for graph covers

Let $\alpha : Y \to X$ be a finite normal cover with Galois group G_α, which acts transitively on any fiber.

- Let $\mathfrak{p}$ be a prime of X through the vertex x. Let $y \in \alpha^{-1}(x)$. Then $\mathfrak{p}$ has a unique lifting to a backtrackless path P in Y starting at y. The end point z of P also lies in $\alpha^{-1}(x)$.
- There is a unique element σ_y in G_α sending y to z.
- If we choose a different starting point y' in $\alpha^{-1}(x)$, then $\sigma_{y'}$ is conjugate to σ_y.
- The conjugacy class of σ_y depends on $\mathfrak{p}$ and not the choice of y, called the Frobenius conjugacy class of $\mathfrak{p}$ in G_α and denoted by $\mathrm{Frob}(\mathfrak{p})$.

Cebotarev density theorem for graph covers

Let $\alpha : Y \to X$ be a finite normal cover with Galois group G_α. For each conjugacy class $\mathcal{C}$ of G_α, let

$$P(\alpha; \mathcal{C}) = \{\text{primes } \mathfrak{p} \text{ of } X \ : \ \text{Frob}(\mathfrak{p}) = \mathcal{C}\}.$$

Terras: The Frobenius conjugacy classes are uniformly distributed w.r.t. the Dirichlet density, i.e., for each conjugacy class $\mathcal{C}$ of G_α,

$$\lim_{u \to (1/\lambda_X)^-} \frac{\sum_{\mathfrak{p} \in P(\alpha, \mathcal{C})} u^{\ell(\mathfrak{p})}}{\sum_{\mathfrak{p} \textit{ prime of } X} u^{\ell(\mathfrak{p})}} = \frac{|\mathcal{C}|}{|G_\alpha|}.$$

Here $1/\lambda_X$ is the radius of convergence of the zeta function of X:

$$Z(X, u) = \prod_{\mathfrak{p} \text{ prime of } X} \frac{1}{1 - u^{\ell(\mathfrak{p})}}.$$

Cebotarev density theorem in natural density for graphs

For a graph X, let

$$\Delta_X = gcd_{\text{primes } \mathfrak{p} \text{ of } X}(\ell(\mathfrak{p})).$$

A subset P of primes of X has natural density δ if

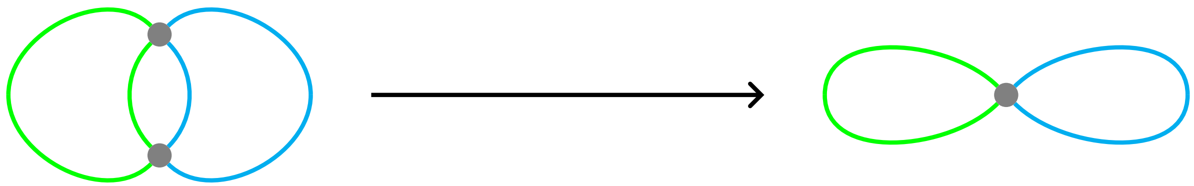
$$\lim_{r\to\infty} \frac{|\{\mathfrak{p} \in P | \ell(\mathfrak{p}) < r\}|}{|\{\text{primes } \mathfrak{p} \text{ of } X | \ell(\mathfrak{p}) < r\}|} = \delta.$$

Theorem [Huang-L] *Assume $r(X) \geq 2$. Let $\alpha : Y \to X$ be a finite normal cover with Galois group G_α. Then the natural density of $P(\alpha; \mathcal{C})$ exists ($= |\mathcal{C}|/|G_\alpha|$) for one conjugacy class $\mathcal{C}$ of G_α iff it exists for all $\mathcal{C}$ iff $\Delta_X = \Delta_Y$.*

Remark. Stark-Terras proved that either $\Delta_Y = \Delta_X$ or $\Delta_Y = 2\Delta_X$, and both cases occur. Our proof did not use this fact.

Illustration of the proof by an example

Consider the degree 2 normal cover $\alpha : Y \to X$ as follows:



- $r(X) = 2$, $\Delta_X = 1$ and $\Delta_Y = 2$.
- $G_\alpha = \{\pm id\}$ has two conjugacy classes

$$\mathcal{C}_+ = \{id\} \text{ and } \mathcal{C}_- = \{-id\}.$$

- $P(\alpha; \mathcal{C}_+)$ (resp. $P(\alpha; \mathcal{C}_-)$) consists of primes of X with even (resp. odd) length, and each set has Dirichlet density $1/2$.

Claim: Neither $P(\alpha; \mathcal{C}_+)$ nor $P(\alpha; \mathcal{C}_-)$ has natural density.

Assume the natural density of $P(\alpha;\mathcal{C}_+)$ exists (hence $=1/2$), and derive a contradiction. Ditto for $P(\alpha;\mathcal{C}_-)$.

Therefore

$$\lim_{r\to\infty}\frac{\left|\{\mathfrak{p}\in P(\alpha;\mathcal{C}_+)\mid \ell(p)\le 2r\}\right|}{\left|\{\mathfrak{p}\text{ is a prime of }X\mid \ell(p)\le 2r\}\right|} = \lim_{r\to\infty}\frac{\left|\{\mathfrak{p}\in P(\alpha;\mathcal{C}_+)\mid \ell(p)\le 2r+1\}\right|}{\left|\{\mathfrak{p}\text{ is a prime of }X\mid \ell(p)\le 2r+1\}\right|}=\frac{1}{2},$$

which implies

$$\lim_{r\to\infty}\frac{\left|\{\mathfrak{p}\text{ is a prime of }X\mid \ell(p)\le 2r\}\right|}{\left|\{\mathfrak{p}\text{ is a prime of }X\mid \ell(p)\le 2r+1\}\right|}=1. \tag{1}$$

The Prime Number Theorem for graphs asserts that

$$\left|\{\text{primes } \mathfrak{p} \text{ of } X : \ \ell(\mathfrak{p}) = r\Delta_X\}\right| \sim \frac{(\lambda_X)^{r\Delta_X}}{r} \quad \text{as } r \to \infty$$

and

$$\left|\{\text{primes } \mathfrak{p} \text{ of } X : \ell(\mathfrak{p}) < r\Delta_X\}\right| \sim \frac{(\lambda_X)^{r\Delta_X}}{r((\lambda_X)^{\Delta_X} - 1)} \quad \text{as } r \to \infty,$$

in which λ_X is the largest eigenvalue in absolute value of the adjacency matrix of directed edges in X.

Hence the left hand side of (1) is $1/\lambda_X^{\Delta_X}$.

In our case the edge adjacency matrix is

$$\begin{array}{c} \\ e_1 \\ \overline{e}_1 \\ e_2 \\ \overline{e}_2 \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & \overline{e}_1 & e_2 & \overline{e}_2 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \end{array},$$

where $e_1, \overline{e}_1$ (resp. $e_2, \overline{e}_2$) are the cyan (resp. green) edges of X with opposite orientations. We find $\lambda_X = 3$, and the limit (1) is equal to 1/3, a contradiction.

To each finite-dimensional irreducible representation ρ of G_α, define the Artin L-function by

$$L(X, \rho, u) = \prod_{[\gamma] \text{ primitive}} \frac{1}{\det(I - \rho(\gamma) u^{\ell(\gamma)})}.$$

Here $[\gamma]$ denotes the conjugacy class of $\gamma \in G_\alpha$. When ρ is the trivial representation, $L(X, \rho, u) = Z(X, u)$. Recall that $Z(X, u)$ is holomorphic on $|u| < 1/\lambda_X$ and it has a simple pole at $1/\lambda_X$.

Hashimoto showed that when $\Delta_X = \Delta_Y$, for all nontrivial irreducible ρ, $L(X, \rho, u)$ is holomorphic on $|u| \leq 1/\lambda_X$.
If $h = \Delta_Y/\Delta_X > 1$, then there are $h - 1$ nontrivial irreducible ρ such that $L(X, \rho, u)$ is holomorphic on $|u| < 1/\lambda_X$ and has a pole on $|u| = 1/\lambda_X$. The analytic behavior of the Artin L-functions is used to prove the theorem.

Isospectral number fields

Two finite extensions K and K' of a number field F are *isospectral* if for each prime $\mathfrak{p}$ of F, there is a norm preserving bijection from the primes of K above p to those of K'.

Take a finite Galois extension L of F containing K and K' as subfields. Write $G = Gal(L/F)$ and let H and H' be the subgroups of G with fixed fields K and K'. Then

Theorem K and K' are isospectral iff

(a) H and H' are locally conjugate in G, i.e., for each conjugacy class $[g]$ of G, we have

$$\#([g] \cap H) = \#([g] \cap H').$$

Further $K \cong K'$ iff H and H' are conjugate in G.

This criterion was extended by Sunada to compact Riemannian manifolds.

Isospectral graphs

Let $\alpha : Y \to X$ be a finite normal cover with Galois group G_α, and $\beta : Y \to Z$ and $\beta' : Y \to Z'$ two subcovers of α.

Theorem [Somodi 2015] TFAE:

(a) G_β and $G_{\beta'}$ are locally conjugate in G_α;

(b) For every prime $\mathfrak{p}$ of X, there is a length preserving bijection from the primes of $Z = \beta(Y)$ above $\mathfrak{p}$ to those of $Z' = \beta'(Y)$;

((b) implies that Z and Z' are isospectral, i.e., their adjacency matrices have the same eigenvalues.)

(c) For every prime $\mathfrak{p}$ of X, the number of primes of Z above $\mathfrak{p}$ with the same length as $\mathfrak{p}$ agrees with that of Z'.

Theorem [Huang-L] In (c) only need primes $\mathfrak{p}$ of length $\leq 2|X| \deg \alpha$.

Reasons for graph isospectrality theorems

"(a) iff (b)" follows from Sunada's argument for manifolds. Sunada also showed that (a) is equivalent to
(d)

$$\rho := \mathrm{Ind}_{\mathrm{G}_\beta}^{\mathrm{G}_\alpha} 1_{\mathrm{G}_\beta} \cong \mathrm{Ind}_{\mathrm{G}_{\beta'}}^{\mathrm{G}_\alpha} 1_{\mathrm{G}_{\beta'}} =: \rho'.$$

Two representations are equivalent iff they have the same trace on all conjugacy classes. Condition (c) says that the traces of ρ and ρ' agree on Frobenius conjugacy classes. The Cebotarev density theorem in Dirichlet density implies that each conjugacy class $\mathcal{C}$ of G_α is equal to $\mathrm{Frob}(\mathfrak{p})$ for infinitely many $\mathfrak{p}$. Hence (a), (b), (c), (d) are equivalent. The theorem of Huang-Li is to show the shortest length of $\mathfrak{p}$ with $\mathrm{Frob}(\mathfrak{p}) = \mathcal{C}$ is $\leq 2|X| \deg \alpha$. For this we use the bound on a set of generators of $\pi_1(X, x)$ and $G_\alpha = \pi_1(X, x)/\pi_1(Y, y)$ mentioned before.