Isogeny-based Cryptography School **Summer 2021**

Lecture 5: The Cayley Graph of $\mathrm{Cl}(\mathcal{O}_K)$

Lecturer: Jean-François Biasse *TA: R. Erukulangara and W. Youmans*

This lecture is essentially based on the paper of Jao, Miller and Venkatesan [2]. It is important for isogeny based cryptography because it describes the rapid mixing properties of the isogeny graph of ordinary elliptic curves (and supersingular elliptic curves defined over $\mathbb{Z}_p$).

5.1 The Cayley graph

The Cayley graph can be defined for any group G generated by a subset of elements $S \subseteq G$. Throughout this lecture, we will focus on the case $G = \mathrm{Cl}(\mathcal{O}_K)$, but the main definitions pertaining to Cayley graphs apply to other groups.

Definition 5.1 (Cayley graph of a group) *Let G be a group generated by a subset of elements $S \subseteq G$. The Cayley graph $\mathrm{Cay}(G, S)$ is the graph defined by*

- *The nodes of $\mathrm{Cay}(G, S)$ are the elements of G.*
- *There is an edge between $g_1, g_2 \in G$ if and only if there is $s \in S$ such that $s \cdot g_1 = g_2$.*

To apply this definition to $G = \mathrm{Cl}(\mathcal{O}_K)$, we need to choose a generating set S. From [1], we know that under the Generalized Riemann Hypothesis (GRH), $\mathrm{Cl}(\mathcal{O}_K)$ is generated by the classes of the split prime ideals of norm less than $12\log^2|\Delta|$ where Δ is the discriminant of the number field K. With such a choice of S, we know that the graph $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$ is connected. However, the result from [2] requires a generating set S of cardinality $\log^{2+\varepsilon}|\Delta|$ to prove the rapid mixing properties of $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$. Therefore, our typical choice for S will be

$$S := \{\text{Split prime ideals of norm less than } \log^{2+\varepsilon}|\Delta|\},$$

which satisfies the required property asymptotically. This slight enlargement of the generating set does not impact the overall cost of any of the algorithms we consider.

Now let us analyze the relevance of travels in the Cayley graph with respect to the computational problems that we are concerned about. As we will see in future lectures, the task of finding the group structure of $\mathrm{Cl}(\mathcal{O}_K)$ boils down to the search for vectors $\vec{v} \in \mathbb{Z}^{|S|}$ such that

$$\mathfrak{p}_1^{x_1} \dots \mathfrak{p}_{|S|}^{x_{|S|}} = (\alpha)\mathcal{O}_K \text{ for } \alpha \in K \quad S = (\mathfrak{p}_i).$$

These vectors form a Euclidean lattice Λ which satisfies $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}^{|S|}/\Lambda$. Therefore, the search for elements of Λ is the same as the search for cycles in $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), |S|)$. Some of these cycles are obvious. For example, in a quadratic field, we always have $\mathfrak{p}\overline{\mathfrak{p}} = (p)\mathcal{O}_K$ for a split prime p. These cycles are obtained easily by walking forward, and then backtracking by walking down the path of the conjugates of the edges we just took. Finding non-trivial cycles on the other hand can be computationally hard.

Another really important connection between walks in $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$ and computational problems relevant to isogenies is the decomposition of the class of an input $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_K)$ with respect to the generators of S. Indeed, this can be used to reduce the evaluation of an input isogeny of large degree to the evaluation of a sequence of isogenies of small degree (up to isomorphism). In terms of travel in $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$, this corresponds to finding a path between the class of the input ideal $\mathfrak{a}$ and the trivial class (1) (which is the class of $\mathrm{Cl}(\mathcal{O}_K)$ made of all ideals of the form $(\alpha)\mathcal{O}_K$ for $\alpha \in K$). In general, given two input ideals $\mathfrak{a}, \mathfrak{b}$, we have the correspondence

$$\{\text{Paths from } [\mathfrak{a}] \text{ to } [\mathfrak{b}] \text{ in } \mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)\} \longleftrightarrow \left\{ \text{Vectors } \vec{x} \in \mathbb{Z}^{|S|} \text{ with } \mathfrak{a} \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{x_i} = (\alpha)\mathfrak{b} \text{ for some } \alpha \in K \right\}$$

5.2 Expander graphs

There are two things that we are very interested in regarding travels in $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$, namely

- Ensuring that there are *short* paths between $[\mathfrak{a}]$ and $[\mathfrak{b}]$.
- Ensuring that a short random walk in $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$ ends up in nodes whose random distribution is almost uniform.

The properties of $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$ can lead to the above goals. First we note something that is true for any Cayley graph.

Proposition 5.2 *For a group G, the graph $\mathrm{Cay}(G, S)$ is k-regular for $k = |S|$.*

Indeed, when there are k elements $s_1, \ldots, s_k$ in $S|$, each vertex $g \in G$ is connected to the k distinct nodes $s_1 g, \ldots, s_k g$. To further specify the properties of $\mathrm{Cay}(G, S)$, we turn to its adjacency operator.

Definition 5.3 (Adjacency operator) *The adjacency operator A on a graph $\mathcal{G}$ acts on functions over the vertices of $\mathcal{G}$ by*

$$A \cdot f(x) = \sum_{y \text{ adjacent to } x} f(y).$$

We immediately see that since $\mathrm{Cay}(G, S)$ is k-regular, the constant function $\mathbb{1}(x) = 1$ satisfies $A \cdot \mathbb{1} = k\mathbb{1}$, i.e it is an eigenfunction for A with eigenvalue $\lambda = k$. This is in fact the largest eigenvalue of A, which we denote by λ_{triv}. We use the eigenvalues of A to count the number of paths between sets of vertices. For that, we consider the characteristic function χ_{S_0} of a set of vertices S_0. It is defined by $\chi_{S_0}(x) = 1$ if $x \in S_0$ and 0 otherwise. The inner product of two functions f, g on the vertices of G is defined by $\langle f, g \rangle = \sum_x f(x)g(x)$, and when we apply this to $f = \chi_{S_1}$ and $g = \chi_{S_2}$ for two sets S_1, S_2, we get

$$\langle \chi_{S_1}, \chi_{S_2} \rangle = \sum_x \chi_{S_1}(x)\chi_{S_2}(x) = |S_1 \cap S_2|\,.$$

Now, we would like to know the odds of landing on a subset of vertices S_0 starting from a given vertex v after a random walk of length t. We can show that the length t that ensures a random distribution close to the uniform one is given by properties of the eigenvalues of A, and the size of the graph.

Proposition 5.4 (Lem. 2.1 of [2]) *Let G be a finite k-regular graph such that for all eigenvalue $\lambda \neq \lambda_{triv}$, we have $|\lambda| < c$ for some $c < k$. Then a random walk of length at least $\frac{\log 2|G|/|S_0|^{1/2}}{\log k/c}$ starting from v ends in S_0 with probability between $\frac{|S_0|}{2|G|}$ and $\frac{3|S_0|}{2|G|}$*

Proof: For a given t, the function $A^t\chi_v$ satisfies $A^t\chi_v(x) = 1$ if and only if x is obtained after walking t steps from v in G. Hence the number of paths of length t starting from v and ending in S_0 is given by $\langle \chi_{S_0}, A^t\chi_{\{v\}}\rangle$. Since eigenspaces for different eigenvalues are orthogonal, we can decompose the functions on G according to the direct sum $\mathrm{Func}(G) = V_{\lambda_{\mathrm{triv}}} \oplus V_{\lambda_{\mathrm{triv}}}^{\perp}$. The eigenspace $V_{\lambda_{\mathrm{triv}}}$ consists of the constant functions on G (i.e. generated by the norm-1 eigenfunction $f_{\mathrm{triv}} := \frac{1}{\sqrt{|G|}}\mathbb{1}$), and is stable by the action of A. Let P be the projection onto $V_{\lambda_{\mathrm{triv}}}^{\perp}$, and $P_{\mathrm{triv}} = \mathrm{Id} - P$. We obtain

$$\begin{aligned}
\langle \chi_{S_0}, A^t\chi_{\{v\}}\rangle &= \langle P_{\mathrm{triv}}\chi_{S_0}, P_{\mathrm{triv}}A^t\chi_{\{v\}}\rangle + \langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle \\
&= \langle P_{\mathrm{triv}}\chi_{S_0}, A^tP_{\mathrm{triv}}\chi_{\{v\}}\rangle + \langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle \\
&= \langle \langle \chi_{S_0}, f_{\mathrm{triv}}\rangle f_{\mathrm{triv}}, A^t\langle \chi_{\{v\}}, f_{\mathrm{triv}}\rangle f_{\mathrm{triv}}\rangle + \langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle \\
&= \langle \frac{|S_0|}{\sqrt{|G|}} f_{\mathrm{triv}}, \frac{1}{\sqrt{|G|}} A^t f_{\mathrm{triv}}\rangle + \langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle \\
&= \frac{|S_0|}{|G|}k^t + \langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle
\end{aligned}$$

By the Cauchy-Schwartz inequality, the second term of the sum satisfies the bound

$$\|\langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle\| \leq \|P\chi_{S_0}\|\|PA^t\chi_{\{v\}}\| \leq c^t\|\chi_{S_0}\|\|\chi_{\{v\}}\| = c^t|S_0|^2.$$

Therefore, for $t \geq \frac{\log 2|G|/|S_0|^{1/2}}{\log k/c}$, we have $\|\langle P\chi_{S_0}, PA^t\chi_{\{v\}}\rangle\| \leq \frac{|S_0|}{2|G|}k^t$, and

$$\frac{|S_0|}{2|G|}k^t \leq \langle \chi_{S_0}, A^t\chi_{\{v\}}\rangle \leq \frac{3|S_0|}{2|G|}k^t.$$

The bound on the probability is obtained by dividing the above inequalities by the number k^t of paths of length t. ■

5.3 Mixing properties of the Cayley graph of $\mathrm{Cl}(\mathcal{O}_K)$

To show the rapid mixing properties of $\mathrm{Cay}(\mathrm{Cl}(\mathcal{O}_K), S)$, we need to apply Proposition 5.4. This means that we want to know a bound on k/c where $k = |S|$ is λ_{triv} and $c < k$ is a bound on the absolute value of the other eigenvalues. For finite abelian groups the eigenfunctions of the adjacency operator A are the characters $\chi : G \to \mathbb{C}^*$. Moreover, the eigenvalue λ_χ corresponding to χ is given by

$$\lambda_\chi = \sum_{s\in S} \chi(s).$$

The result from Jao, Miller and Venkatesan [2, Th. 1.1] actually applies to the narrow ray class group of a number field K relative to a conductor $\mathfrak{m}$. The main result [2, Th. 1.1] extends to the quotients of this group, which includes the ray class group of conductor $\mathfrak{m}$, and the ideal class groups of orders $\mathcal{O}$ in K.

Theorem 5.5 (Cor. 1.3 of [2]) *Let K be a number field of degree n and discriminant Δ, $\mathfrak{m}$ be an integral ideal, G be the narrow ray class group relative to $\mathfrak{m}$, $\varepsilon > 0$, and*

$$S := \{\textit{Split prime ideals of norm less than } \log^{2+\varepsilon}(\mathrm{N}(\mathfrak{m})|\Delta|) \textit{ and their inverses}\}.$$

Then there is a constant $C > 0$ *such that for* Δ *sufficiently large, a random walk of length*

$$t \geq C \frac{\log|G|}{\log\log(\mathrm{N}(\mathfrak{m})|\Delta|)}$$

starting from any vertex ends in any $S_0 \subseteq G$ *with probability at least* $\frac{|S_0|}{2|G|}$.

Proof: This result follows from [2, Th. 1.1] which states that non trivial eigenvalues λ satisfy

$$|\lambda| = O\left((\lambda_{\mathrm{triv}} \log \lambda_{\mathrm{triv}})^{1/2+1/B}\right) \quad \text{for } B = 2 + \varepsilon.$$

This comparison is obtained by showing that the eigenvalues satisfy

$$\begin{aligned}\lambda_\chi = \sum_{\mathrm{N}(\mathfrak{p}) \leq x \text{ prime}} \chi(\mathfrak{p}) + \chi(\mathfrak{p})^{-1} &= 2\mathfrak{Re}\left(\sum_{\mathrm{N}(\mathfrak{p}) \leq x \text{ prime}} \chi(\mathfrak{p})\right) \\ &= 2r\,\mathrm{li}(x) + O(nx^{1/2}\log(x\mathrm{N}(\mathfrak{m})|\Delta|),\end{aligned}$$

for $x = \log^B|\Delta|$, $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$, $r = 1$ if χ is trivial and 0 otherwise. We refer to the proof of[2, Th. 1.1] for details on how this identity is obtained. ■

This theorem shows us that asymptotically, random walks of length in $O(\log|\Delta|/\log\log|\Delta|)$ take us to subsets of $\mathrm{Cl}(\mathcal{O}_K)$ that are distributed almost uniformly at random.

References

[1] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[2] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *Journal of Number Theory*, 129(6):1491–1504, 2009.