Cohomology of Shimura curves in quasi-linear time : A topological approach.

Rayane Baït - Aurel Page

January 16th, 2026

Diophantine equations

The modular method

Fermat equation : $a^p + b^p = c^p$. $\Rightarrow$ Frey (elliptic) curve/$\mathbb{Q}$: $y^2 = (x^2 - a^p)(x + b^p)$. $\xrightarrow{\textit{Modularity}}$ Cusp modular form : f in $S_2(2) - \{0\}$.

Compute $S_2(2)$ and find out that $S_2(2) = \{0\}$.

- *No such solution to the Fermat equation can exist !*

Diophantine equations

The modular method

Fermat equation : $a^p + b^p = c^p$. $\Rightarrow$ Frey (elliptic) curve/$\mathbb{Q}$: $y^2 = (x^2 - a^p)(x + b^p)$. $\xrightarrow{\textit{Modularity}}$ Cusp modular form : f in $S_2(2) - \{0\}$.

Compute $S_2(2)$ and find out that $S_2(2) = \{0\}$.

- *No such solution to the Fermat equation can exist !*

Diophantine equations

The modular method

Fermat equation : $a^p + b^p = c^p$. $\Rightarrow$ Frey (elliptic) curve/$\mathbb{Q}$: $y^2 = (x^2 - a^p)(x + b^p)$. $\xrightarrow{\textit{Modularity}}$ Cusp modular form : f in $S_2(2) - \{0\}$.

Compute $S_2(2)$ and find out that $S_2(2) = \{0\}$.

- *No such solution to the Fermat equation can exist !*

Diophantine equations

The modular method

Fermat equation : $a^p + b^p = c^p$. $\Rightarrow$ Frey (elliptic) curve/$\mathbb{Q}$: $y^2 = (x^2 - a^p)(x + b^p)$. $\xrightarrow{\text{Modularity}}$ Cusp modular form : f in $S_2(2) - \{0\}$.

Compute $S_2(2)$ and find out that $S_2(2) = \{0\}$.

- *No such solution to the Fermat equation can exist !*

Diophantine equations

The modular method

Fermat equation : $a^p + b^p = c^p$. $\Rightarrow$ Frey (elliptic) curve/$\mathbb{Q}$: $y^2 = (x^2 - a^p)(x + b^p)$. $\xrightarrow{\text{Modularity}}$ Cusp modular form : f in $S_2(2) - \{0\}$.

Compute $S_2(2)$ and find out that $S_2(2) = \{0\}$.

- *No such solution to the Fermat equation can exist !*

Generalized Fermat equations

→ Darmon's program for $Ax^p + By^q = Cz^r$

Solution to $Ax^p + By^q = Cz^r$. $\Rightarrow$ Frey variety/F of GL_k-type and conductor η. $\xrightarrow{\text{Modularity}}$ Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Generalized Fermat equations

→ Darmon's program for $Ax^p + By^q = Cz^r$

Solution to $Ax^p + By^q = Cz^r$. $\Rightarrow$ Frey variety/F of GL_k-type and conductor η. $\xrightarrow{Modularity}$ Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Generalized Fermat equations

→ Darmon's program for $Ax^p + By^q = Cz^r$

Solution to $Ax^p + By^q = Cz^r$. $\Rightarrow$ Frey variety/F of GL_k-type and conductor η. $\xrightarrow{\text{Modularity}}$ Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Generalized Fermat equations

→ **Darmon's program for $Ax^p + By^q = Cz^r$**

Solution to $Ax^p + By^q = Cz^r$. $\Rightarrow$ Frey variety$/F$ of GL_k-type and conductor η. $\xrightarrow{\text{Modularity}}$ Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Generalized Fermat equations

→ Darmon's program for $Ax^p + By^q = Cz^r$

Solution to $Ax^p + By^q = Cz^r$. $\Rightarrow$ Frey variety/F of GL_k-type and conductor η. $\xrightarrow{Modularity}$ Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Generalized Fermat equations

→ Darmon's program for $Ax^p + By^q = Cz^r$

Solution to $Ax^p + By^q = Cz^r$.	$\Rightarrow$	Frey variety/F of GL_k-type and conductor η.	$\xrightarrow{\textit{Modularity}}$	Automorphic form π of weight k and level η.

Compute the "space of automorphic forms of weight k and level η" and prove that it doesn't contain π.

For $(A, B, C) = (1, 1, 1)$, Darmon has built hyperelliptic/superelliptic Frey curves of GL_2-type over a totally real field F. In this case, many modularity theorems are known where π is a Hilbert modular form of weight 2 and level η.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta) \backslash \mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree$/\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree$/\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree$/\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree/$\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

Computing Hilbert modular forms

Following the work of Greenberg-Voight [GV10]

Let

- $F \neq \mathbb{Q}$ be a totally real number field of odd degree$/\mathbb{Q}$,
- $\mathbb{Z}_F$ its ring of integers,
- $\eta \subset \mathbb{Z}_F$ a level.

There exist

- a quaternion algebra B/F with discriminant $(1) \subset \mathbb{Z}_F$
- a subgroup of units $B^\times \supset \Gamma_0(\eta) \to PGL_2(\mathbb{R})$

Such that (when F has strict class number 1) $X := X_0(\eta) = \Gamma_0(\eta)\backslash\mathfrak{h}$ is a compact and complex curve and there are Hecke equivariant isomorphisms

$$S_k(\eta) \simeq S_k^B(\eta) \simeq H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$$

Where $2 \leq k$ is a weight and $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$.

Idea :

Compute $H^1(\Gamma_0^B(\eta), W_k(\mathbb{C}))$ with its Hecke action using the topology of X.

In this talk

Problem :

Given a weight $2 \leq k$ and a co-finite discrete subgroup $\Gamma \subset PSL_2(\mathbb{R})$, compute

$$H^1(\Gamma, W_k(\mathbb{C}))$$

where $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$. When $k = 2$ we recover $W_k(\mathbb{C}) = \mathbb{C}$ with a trivial Γ action.

Initial idea of approach :

Compute a presentation of Γ and solve linear systems $\rightarrow \tilde{O}(n^3)$

Our approach

Compute a better-chosen presentation of Γ and solve a structured linear system $\rightarrow \tilde{O}(n)$

In this talk

Problem :

Given a weight $2 \leq k$ and a co-finite discrete subgroup $\Gamma \subset PSL_2(\mathbb{R})$, compute

$$H^1(\Gamma, W_k(\mathbb{C}))$$

where $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$. When $k = 2$ we recover $W_k(\mathbb{C}) = \mathbb{C}$ with a trivial Γ action.

Initial idea of approach :

Compute a presentation of Γ and solve linear systems $\rightarrow \tilde{O}(n^3)$

Our approach

Compute a better-chosen presentation of Γ and solve a structured linear system $\rightarrow \tilde{O}(n)$

In this talk

Problem :

Given a weight $2 \leq k$ and a co-finite discrete subgroup $\Gamma \subset PSL_2(\mathbb{R})$, compute

$$H^1(\Gamma, W_k(\mathbb{C}))$$

where $W_k(\mathbb{C}) = Sym_{k-2}(\mathbb{C}^2)$. When $k = 2$ we recover $W_k(\mathbb{C}) = \mathbb{C}$ with a trivial Γ action.

Initial idea of approach :

Compute a presentation of Γ and solve linear systems $\rightarrow \tilde{O}(n^3)$

Our approach

Compute a better-chosen presentation of Γ and solve a structured linear system $\rightarrow \tilde{O}(n)$

Theorem :

Assume $X_\Gamma := \Gamma\backslash\mathfrak{h}$ *has signature* $(g, \nu_1, \dots, \nu_f)$. *Then the group* Γ *has for any* $1 \leq m$ *presentations of the form :*

- $\langle e_1, \dots, e_{2g}, \gamma_1, \dots, \gamma_f \,|\, \prod_{i=1}^{4g} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$
- $$\langle a_1, b_1, \dots, a_m, b_m, e_1, \dots, e_{2(g-k)}, \gamma_1, \dots, \gamma_f \,| \prod_{i=1}^{m}[a_i, b_i] \prod_{j=1}^{4(g-k)} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$$
- $\langle a_1, b_1, \dots, a_g, b_g, \gamma_1, \dots, \gamma_f \,|\, \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$

which are respectively one word, m-handles and geometric presentations of Γ.

In [Imb01; Imb99] Imbert gives a combinatorial procedure to compute *geometric* presentations of Fuchsian groups from the data of a fundamental domain with a side pairing. Following Imbert we show how to algorithmically retrieve intermediate presentations in quasi-linear time and the geometric presentation in quasi-quadratic time.

Theorem :

Assume $X_\Gamma := \Gamma\backslash\mathfrak{h}$ has signature $(g, \nu_1, \ldots, \nu_f)$. Then the group Γ has for any $1 \leq m$ presentations of the form :

- $\langle e_1, \ldots, e_{2g}, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{4g} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$
-
$$\langle a_1, b_1, \ldots, a_m, b_m, e_1, \ldots, e_{2(g-k)}, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{m}[a_i, b_i] \prod_{j=1}^{4(g-k)} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$$
- $\langle a_1, b_1, \ldots, a_g, b_g, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$

which are respectively one word, m-handles and geometric presentations of Γ.

In [Imb01; Imb99] Imbert gives a combinatorial procedure to compute *geometric* presentations of Fuchsian groups from the data of a fundamental domain with a side pairing. Following Imbert we show how to algorithmically retrieve intermediate presentations in quasi-linear time and the geometric presentation in quasi-quadratic time.

Theorem :

Assume $X_\Gamma := \Gamma \backslash \mathfrak{h}$ has signature $(g, \nu_1, \dots, \nu_f)$. Then the group Γ has for any $1 \leq m$ presentations of the form :

- $\langle e_1, \dots, e_{2g}, \gamma_1, \dots, \gamma_f \,|\, \prod_{i=1}^{4g} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j \rangle$
- $$\langle a_1, b_1, \dots, a_m, b_m, e_1, \dots, e_{2(g-k)}, \gamma_1, \dots, \gamma_f \,| \prod_{i=1}^{m} [a_i, b_i] \prod_{j=1}^{4(g-k)} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j \rangle$$
- $\langle a_1, b_1, \dots, a_g, b_g, \gamma_1, \dots, \gamma_f \,|\, \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j \rangle$

which are respectively one word, m-handles and geometric presentations of Γ.

In [Imb01; Imb99] Imbert gives a combinatorial procedure to compute *geometric* presentations of Fuchsian groups from the data of a fundamental domain with a side pairing. Following Imbert we show how to algorithmically retrieve intermediate presentations in quasi-linear time and the geometric presentation in quasi-quadratic time.

Theorem :

Assume $X_\Gamma := \Gamma\backslash\mathfrak{h}$ has signature $(g, \nu_1, \ldots, \nu_f)$. Then the group Γ has for any $1 \leq m$ presentations of the form :

- $\langle e_1, \ldots, e_{2g}, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{4g} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$
- $$\langle a_1, b_1, \ldots, a_m, b_m, e_1, \ldots, e_{2(g-k)}, \gamma_1, \ldots, \gamma_f \,| \prod_{i=1}^{m}[a_i, b_i] \prod_{j=1}^{4(g-k)} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$$
- $\langle a_1, b_1, \ldots, a_g, b_g, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$

which are respectively one word, m-handles and geometric presentations of Γ.

In [Imb01; Imb99] Imbert gives a combinatorial procedure to compute *geometric* presentations of Fuchsian groups from the data of a fundamental domain with a side pairing. Following Imbert we show how to algorithmically retrieve intermediate presentations in quasi-linear time and the geometric presentation in quasi-quadratic time.

Theorem :

Assume $X_\Gamma := \Gamma\backslash\mathfrak{h}$ *has signature* $(g, \nu_1, \ldots, \nu_f)$*. Then the group* Γ *has for any* $1 \leq m$ *presentations of the form :*

- $\langle e_1, \ldots, e_{2g}, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{4g} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$
- $$\langle a_1, b_1, \ldots, a_m, b_m, e_1, \ldots, e_{2(g-k)}, \gamma_1, \ldots, \gamma_f \,| \prod_{i=1}^{m}[a_i, b_i] \prod_{j=1}^{4(g-k)} e_{\varphi(i)}^{\epsilon_i} \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$$
- $\langle a_1, b_1, \ldots, a_g, b_g, \gamma_1, \ldots, \gamma_f \,|\, \prod_{i=1}^{g}[a_i, b_i] \prod_{j=1}^{f} \gamma_j = 1,\ \gamma_j^{\nu_j};\ j\rangle$

which are respectively one word, m-handles and geometric presentations of Γ*.*

In [Imb01; Imb99] Imbert gives a combinatorial procedure to compute *geometric* presentations of Fuchsian groups from the data of a fundamental domain with a side pairing. Following Imbert we show how to algorithmically retrieve intermediate presentations in quasi-linear time and the geometric presentation in quasi-quadratic time.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$
  $\rightarrow$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \rightarrow$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\rightarrow (\nu_1, \ldots, \nu_f)$
- signature $(g, \nu_1, \ldots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} .z = \frac{az+b}{cz+d}$
  $\rightarrow$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \rightarrow$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\rightarrow (\nu_1, \ldots, \nu_f)$
- signature $(g, \nu_1, \ldots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} .z = \frac{az+b}{cz+d}$
  $\rightarrow$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \rightarrow$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\rightarrow (\nu_1, \ldots, \nu_f)$
- signature $(g, \nu_1, \ldots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$

  $\rightarrow$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \rightarrow$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\rightarrow (\nu_1, \ldots, \nu_f)$
- signature $(g, \nu_1, \ldots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} .z = \frac{az+b}{cz+d}$
  $\to$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \to$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\to (\nu_1, \dots, \nu_f)$
- signature $(g, \nu_1, \dots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Some notations/conventions :

All of our Fuchsian groups are *co-compact*.

- $\mathfrak{h}$ upper half plane $\mathfrak{h} := \{\tau \in \mathbb{C} | 0 < Im(\tau)\}$
- $PSL_2(\mathbb{R})$ projective special linear group Acts on $\mathfrak{h}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$
  $\rightarrow$ *orientation preserving* isometries.
- Co-compact Fuchsian group $\Gamma \hookrightarrow PSL_2(\mathbb{R})$ *Discrete* subgroup of $PSL_2(\mathbb{R})$ s.t $\Gamma \backslash \mathfrak{h}$ is *compact*.
- hyperbolic elements of Γ generate free part of $\Gamma^{ab} \rightarrow$ genus g
- elliptic elements of Γ elements of finite order, f conjugacy classes of maximal finite cyclic subgroups with orders $\rightarrow (\nu_1, \ldots, \nu_f)$
- signature $(g, \nu_1, \ldots, \nu_f)$ *Uniquely* determines Γ up to isomorphism.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v : $\to B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho\colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*. Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma\backslash\mathfrak{h}$ is **good complex 1-orbifold** and in particular a **Riemann surface**. We call any such S a **Shimura curve**.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v : $\rightarrow B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho \colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*. Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma \backslash \mathfrak{h}$ is **good complex 1-orbifold** and in particular a **Riemann surface**. We call any such S a **Shimura curve**.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v :
  $\to B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho\colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*. Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma\backslash\mathfrak{h}$ is **good complex 1-orbifold** and in particular a **Riemann surface**. We call any such S a **Shimura curve**.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v : $\rightarrow B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho \colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*.
Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma \backslash \mathfrak{h}$ is **good complex 1-orbifold** and in particular a **Riemann surface**. We call any such S a **Shimura curve**.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v : $\rightarrow B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho\colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*. Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma\backslash\mathfrak{h}$ is good complex 1-orbifold and in particular a Riemann surface. We call any such S a Shimura curve.

Shimura curves

A Fuchsian group is **arithmetic** if it is obtained as follows, we need

- A **totally real** field F with $1 < [F : \mathbb{Q}]$ odd.
- A **quaternion algebra** B/F *splitting* at exactly 1 place v :
  $\to B_v \simeq M_2(F_v) = M_2(\mathbb{R})$.
- An **order** $O \subset B$ with units of norm 1 denoted O^1.

As shown in [Kat93] from the embedding

$$B \otimes_F \mathbb{R} \hookrightarrow \mathbb{H}^{n-1} \times M_2(\mathbb{R})$$

we obtain an embedding $\rho \colon O^1 \hookrightarrow PSL_2(\mathbb{R})$ which is *discrete* and *co-compact*. Any Γ *commensurable* with a $\rho(O^1)$ is called an **arithmetic** Fuchsian group.

Shimura curves

Given an *arithmetic* Fuchsian group Γ, the quotient $S := \Gamma\backslash\mathfrak{h}$ is **good complex 1-orbifold** and in particular a **Riemann surface**. We call any such S a **Shimura curve**.

Representing Γ

Fundamental domains and side pairings

Fundamental domain : Family of polygons $(P_i)_{i=1,\ldots,f}$, $D := \sqcup_i P_i$ with $\overline{B(0,1)} \cong P_i \subset \mathfrak{h}$.

- s.t. $\sqcup_{g\in\Gamma} g.D = \mathfrak{h}$
- $g.\mathring{D} \cap \mathring{D} = \emptyset$

Representing a Fuchsian group :

- Fundamental domain P for $\Gamma \curvearrowright \mathfrak{h}$ with $\partial P = e_1 \ldots e_n$, $E = \{e_i\}_i$ edges of P.
- Side pairing $\sigma_1 \colon E \to E$, a fixed-point free involution representing the gluing.
- Map $\varphi \colon E \hookrightarrow \Gamma$ such that $\varphi(e) = \varphi(\sigma_1(e))^{-1}$ and defined by $P \cap \varphi(e)P = \{e\}$.

Further let $\sigma_2 \curvearrowright E$ by clock-wise rotation of the polygons.

Theorem :

$\mathrm{im}\varphi$ generates Γ and if $\sigma_1\sigma_2^{-1}$ has cycles $\{c_i\}_{i=1,\ldots,f}$ then a a cycle c is either a relation for Γ or an elliptic so that $\{c^{\nu_c}\}$ is a complete set of relations where ν_c is the order of c in Γ.

Representing Γ

Fundamental domains and side pairings

Fundamental domain : Family of polygons $(P_i)_{i=1,\dots,f}$, $D := \sqcup_i P_i$ with $\overline{B(0,1)} \cong P_i \subset \mathfrak{h}$.

- s.t. $\sqcup_{g\in\Gamma} g.D = \mathfrak{h}$
- $g.\mathring{D} \cap \mathring{D} = \emptyset$

Representing a Fuchsian group :

- Fundamental domain P for $\Gamma \curvearrowright \mathfrak{h}$ with $\partial P = e_1 \dots e_n$, $E = \{e_i\}_i$ edges of P.
- Side pairing $\sigma_1 \colon E \to E$, a fixed-point free involution representing the gluing.
- Map $\varphi \colon E \hookrightarrow \Gamma$ such that $\varphi(e) = \varphi(\sigma_1(e))^{-1}$ and defined by $P \cap \varphi(e)P = \{e\}$.

Further let $\sigma_2 \curvearrowright E$ by clock-wise rotation of the polygons.

Theorem :

$\mathrm{im}\varphi$ generates Γ and if $\sigma_1\sigma_2^{-1}$ has cycles $\{c_i\}_{i=1,\dots,f}$ then a a cycle c is either a relation for Γ or an elliptic so that $\{c^{\nu_c}\}$ is a complete set of relations where ν_c is the order of c in Γ.

Representing Γ

Fundamental domains and side pairings

Fundamental domain : Family of polygons $(P_i)_{i=1,\dots,f}$, $D := \sqcup_i P_i$ with $\overline{B(0,1)} \cong P_i \subset \mathfrak{h}$.

- s.t. $\sqcup_{g\in\Gamma} g.D = \mathfrak{h}$
- $g.\mathring{D} \cap \mathring{D} = \emptyset$

Representing a Fuchsian group :

- Fundamental domain P for $\Gamma \curvearrowright \mathfrak{h}$ with $\partial P = e_1 \dots e_n$, $E = \{e_i\}_i$ edges of P.
- Side pairing $\sigma_1 \colon E \to E$, a fixed-point free involution representing the gluing.
- Map $\varphi \colon E \hookrightarrow \Gamma$ such that $\varphi(e) = \varphi(\sigma_1(e))^{-1}$ and defined by $P \cap \varphi(e)P = \{e\}$.

Further let $\sigma_2 \curvearrowright E$ by clock-wise rotation of the polygons.

Theorem :

$\mathrm{im}\varphi$ generates Γ and if $\sigma_1\sigma_2^{-1}$ has cycles $\{c_i\}_{i=1,\dots,f}$ then a a cycle c is either a relation for Γ or an elliptic so that $\{c^{\nu_c}\}$ is a complete set of relations where ν_c is the order of c in Γ.

Representing elements of Γ

Straight line programs

Let $\{g_1, \ldots, g_n\} = \mathrm{im}(\varphi)$ generate Γ. A **straight line program** is a vector of instructions v with an out vector o, evaluating in Γ, such that

- $o(1) = g_1, \ldots, o(n) = g_n$.
- $v(k)$ gives group instructions to compute $o(k+n)$ in terms of $(o(i))_{i<k+n}$.

From the function φ, one can write v using only the edges E, stored as integers for example, without evaluating in Γ.

Why ?

- Can represent redondant words in quasi-linear space instead of exponential space.
- Can evaluate in any group.

Representing elements of Γ

Straight line programs

Let $\{g_1, \ldots, g_n\} = \mathrm{im}(\varphi)$ generate Γ. A straight line program is a vector of instructions v with an out vector o, evaluating in Γ, such that

- $o(1) = g_1, \ldots, o(n) = g_n$.
- $v(k)$ gives group instructions to compute $o(k+n)$ in terms of $(o(i))_{i<k+n}$.

From the function φ, one can write v using only the edges E, stored as integers for example, without evaluating in Γ.

Why ?

- Can represent redondant words in quasi-linear space instead of exponential space.
- Can evaluate in any group.

Main algorithm

Let Γ be an arithmetic Fuchsian group of genus g.

Algorithm :

There exist a $\tilde{O}(g)$ algorithm that given a fundamental domain P and a side pairing (σ_1, φ) for Γ outputs a straight line program expressing one-word and $O(1)$-handles presentation of Γ.

The same algorithm can compute a geometric presentation in time $\tilde{O}(g^2)$.

Main algorithm

Let Γ be an arithmetic Fuchsian group of genus g.

Algorithm :

There exist a $\tilde{O}(g)$ algorithm that given a fundamental domain P and a side pairing (σ_1, φ) for Γ outputs a straight line program expressing one-word and $O(1)$-handles presentation of Γ.

The same algorithm can compute a geometric presentation in time $\tilde{O}(g^2)$.

Application to Cohomology

Recall : Given a totally real field F we wish to compute $S_2(\eta)$, the space of Hilbert modular forms of parallel weight 2 over F and level η. Do as follows :

- Build a suitable quaternion algebra B and an arithmetic fuchsian group $\Gamma_0^B(\eta)$ of signature $(g, \nu_1, \ldots, \nu_f)$, represented as a fundamental domain P and side pairing (σ_1, φ).
- Compute a one-word presentation

$$\Gamma_0^B(\eta) \simeq \langle e_1, \ldots, e_{2g}, \gamma_1, \ldots, \gamma_f | \prod_{j=1}^{4g} e_{\phi(j)}^{\epsilon_j} \prod_{i=1}^{f} \gamma_i = 1,\ \gamma_i^{\nu_i} = 1;\ i = 1, \ldots, f \rangle$$

It has the property that each e_i appears exactly twice, once with $\epsilon_{\varphi(j_1)} = 1$ and the other with $\epsilon_{\varphi(j_2)} = -1$.

Application to Cohomology

Endow $\mathbb{C}$ with the trivial $\Gamma_0^B(\eta)$ structure. From the previous parts with need to compute

$$H^1(\Gamma_0^B(\eta), \mathbb{C})$$

the space of 1-cocycles from $\Gamma_0^B(\eta) \to \mathbb{C}$ modulo 1-coboundaries. As $\mathbb{C}$ is trivial we have

$$H^1(\Gamma_0^B(\eta), \mathbb{C}) \simeq Hom(\Gamma_0^B, \mathbb{C}) \simeq ((\Gamma_0^B)^{ab})^*$$

And from the one word presentation we obtain

$$\left(\Gamma_0^B\right)^{ab} \simeq \mathbb{Z}^{2g} \oplus \left(\prod_{i=1}^{f} \mathbb{Z}/\nu_i\mathbb{Z}\right) / (1, \ldots, 1).\mathbb{Z}$$

and using the dual basis we get

$$H^1((\Gamma_0^B)^{ab}, \mathbb{C}) \simeq \mathbb{Z}^{2g}$$

Application to Cohomology

Endow $\mathbb{C}$ with the trivial $\Gamma_0^B(\eta)$ structure. From the previous parts with need to compute

$$H^1(\Gamma_0^B(\eta), \mathbb{C})$$

the space of 1-cocycles from $\Gamma_0^B(\eta) \to \mathbb{C}$ modulo 1-coboundaries. As $\mathbb{C}$ is trivial we have

$$H^1(\Gamma_0^B(\eta), \mathbb{C}) \simeq Hom(\Gamma_0^B, \mathbb{C}) \simeq ((\Gamma_0^B)^{ab})^*$$

And from the one word presentation we obtain

$$\left(\Gamma_0^B\right)^{ab} \simeq \mathbb{Z}^{2g} \oplus \left(\prod_{i=1}^{f} \mathbb{Z}/\nu_i\mathbb{Z}\right) /(1, \ldots, 1).\mathbb{Z}$$

and using the dual basis we get

$$H^1((\Gamma_0^B)^{ab}, \mathbb{C}) \simeq \mathbb{Z}^{2g}$$

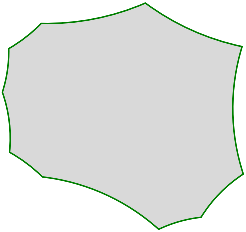
A real example : fundamental domain

- $F = \mathbb{Q}(\sqrt{8})$,
- $B = \left(\frac{-\frac{\sqrt{8}}{2}, -3}{F}\right)$,
- O the order generated by the columns of
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1/2 & 1/2 & 1/2 & 1/2 \\ 0 & 0 & 1 & 0 & 1/2 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1 & 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \end{pmatrix}$$
as a $\mathbb{Z}$-module.

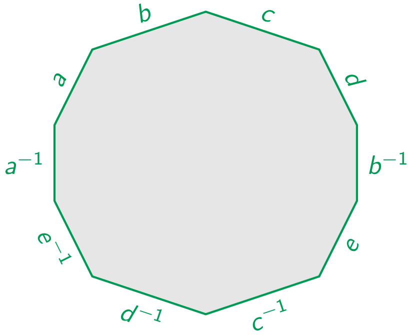
now let $\Gamma := O^1$.

A real example : fundamental domain

Using J. Rickards software for fundamental domains of arithmetic Fuchsian groups [Ric22] we obtain



It also ouputs a side pairing (σ_1, φ) with



where $E = \{a, b, c, d, e, a^{-1}, b^{-1}, c^{-1}, d^{-1}, e^{-1}\}$ and $x^{-1} = \sigma_1(x)$. The polygon with gluing (P, σ_1) is represented as the word $w = abcdb^{-1}ec^{-1}d^{-1}e^{-1}a^{-1}$.

Presentation of Γ

From before, a presentation of Γ is given by

$$\{\varphi(a), \varphi(b), \varphi(c), \varphi(d), \varphi(e)\}$$

and if σ_2 is the cycle $(abcdb^{-1}ec^{-1}d^{-1}e^{-1}a^{-1})$, then relations can be read off of the cycles of

$$\sigma_1 \circ \sigma_2^{-1} = (a)(bA^{-1}e)(cb^{-1}d^{-1})(dc^{-1}e^{-1})$$

in this case, the only elliptic is a with order 3 and we will see that Γ has signature $(g, \nu) = (1, 3)$.

Where do the relations come from ?

Easy case

If Γ has signature (g), meaning no elliptics, then Γ acts totally discontinuously on $\mathfrak{h}$ so that by covering space theory $\Gamma \simeq \pi_1(\Gamma\backslash\mathfrak{h})$.

- Let P be a fundamental polygon for Γ represented by the word $w = e_{\phi(1)}^{\epsilon_1} \dots e_{\phi(n)}^{\epsilon_n}$.
- Assume $G := \Gamma\backslash\partial P$ has a single vertex v, then $n = 4g$ and by the Van Kampen theorem $\pi_1(\Gamma\backslash\mathfrak{h}, v) = \pi_1(G, v)/\langle w = 1\rangle$.
- By standard results, as $G = \bigvee_{i=1}^{2g} S^1$: $\pi_1(G, v) = \langle e_1, \dots, e_{2g}\rangle$.

Putting everything together :

$$\Gamma \simeq \langle e_1, \dots, e_{2g} | w = 1\rangle$$

which is the one-word presentation.

General case

Dévissage of Γ

When Γ has signature $(g, \nu_1, \ldots, \nu_f) \to$ remove elliptic points Y in $\mathfrak{h}$, then Γ acts totally discontinuously on $\mathfrak{h} - Y$ and by covering space theory :

- $\Gamma = \Gamma(p)$ where $p\colon \mathfrak{h} - Y \to \Gamma\backslash(\mathfrak{h} - Y)$ is the covering map and $\Gamma(p)$ the automorphism group of p.
- There is a short exact sequence

$$1 \to \pi_1(\mathfrak{h} - Y, v) \to \pi_1(\Gamma\backslash(\mathfrak{h} - Y), \Gamma.v) \to \Gamma(p) \to 1$$

  where the last map is given by monodromy : in practice, the side pairing.

Main computation : $\pi_1(\Gamma\backslash(\mathfrak{h} - Y), \Gamma.v)$.

Small problems for applying Van Kampen directly :

- The graph $\Gamma\backslash\partial P$ may not have a single vertex $\to$ edges are not loops.
- Elliptic points lie at vertices of $P \to$ the embedding $G - V(G) \hookrightarrow \Gamma\backslash(\mathfrak{h} - V(G))$ is not combinatorial anymore.

Solving problem 1

(Use groupoids)

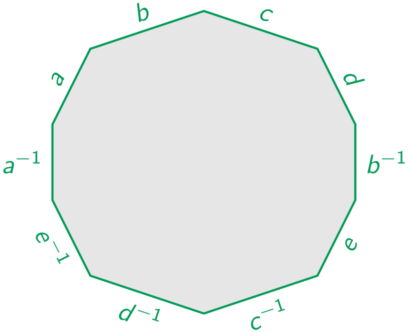
Work with the short exact sequence of groupoids :

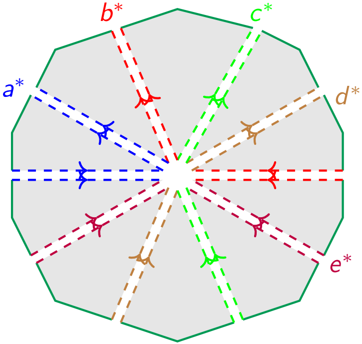
$$\Gamma.V \to \pi_1(\mathfrak{h} - Y, \Gamma.V) \to \pi_1(\Gamma\backslash(\mathfrak{h} - Y), V) \to \Gamma(p) \to 1$$

for a vertex set V. The map on the right will then exactly be generated by a side pairing of the form (σ_1, φ).

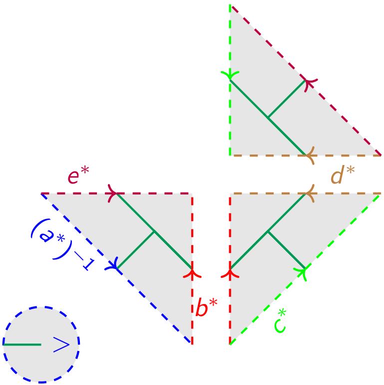
Solving problem 2

Have a new set of polygons with centers vertices of G as follows, first cut along dashed lines





Then glue along σ_1 and call G^* the new quotient graph $(\sqcup_{i=1}^{f} P_i)/\sigma_1$:



Remark :

The gluing can be done using the Γ action but the polygons don't form a fundamental domain anymore.

Defining $\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) \to \Gamma$ with (σ_1^*, φ^*)

New side pairing :

For x in E, x^* and x are both mapped to $\varphi(x)$ through

$$\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) \to \Gamma$$

Indeed $\varphi(x)$ is determined by its action on $\{x(1/2), x^{-1}(1/2), v\}$ where v is the center of P.

This means that the new side pairing (σ_1^*, φ^*) is just (σ_1, φ).

- Now see that polygons are represented by the words

$$a^*,\ e^*b^*(a^*)^{-1},\ (b^*)^{-1}(d^*)^{-1}c^*,\ d^*(c^*)^{-1}(e^*)^{-1}$$

which are exactly the predicted by the main structure theorem.

Defining $\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) \to \Gamma$ with (σ_1^*, φ^*)

New side pairing :

For x in E, x^* and x are both mapped to $\varphi(x)$ through

$$\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) \to \Gamma$$

Indeed $\varphi(x)$ is determined by its action on $\{x(1/2), x^{-1}(1/2), v\}$ where v is the center of P.

This means that the new side pairing (σ_1^*, φ^*) is just (σ_1, φ).

- Now see that polygons are represented by the words

$$a^*,\ e^*b^*(a^*)^{-1},\ (b^*)^{-1}(d^*)^{-1}c^*,\ d^*(c^*)^{-1}(e^*)^{-1}$$

which are exactly the predicted by the main structure theorem.

Retrieving the basic presentation of Γ

Using (groupoid-theoritic)) Van Kampen on the new cell decomposition of $\Gamma\backslash\mathfrak{h} - V(G)$, with $\{c_v\}_{v\in V(G)}$ being the cycles of $\sigma_1\sigma_2^{-1}$ and γ_v being the counter clock-wise loops c_v^{-1} we get

$$\pi_1(\Gamma\backslash\mathfrak{h} - V(G), V(G^*)) = \langle E(G^*) | c_v\gamma_v = 1;\ v\rangle$$

Further $\pi_1(\mathfrak{h} - \Gamma.V(G), \Gamma.V(G^*))$ is generated for each $v \in V(G^*)$ by the images $g.\gamma_v$ for a small loop γ_v around v for each $g \in \Gamma$. Each $g.\gamma_v$ maps to $\gamma_v^{\nu_v}$. So that we get

$$\Gamma \simeq \langle E(G^*) | c_v^{\nu_v} = 1\rangle$$

Retrieving the basic presentation of Γ

Using (groupoid-theoritic)) Van Kampen on the new cell decomposition of $\Gamma\backslash\mathfrak{h} - V(G)$, with $\{c_v\}_{v\in V(G)}$ being the cycles of $\sigma_1\sigma_2^{-1}$ and γ_v being the counter clock-wise loops c_v^{-1} we get

$$\pi_1(\Gamma\backslash\mathfrak{h} - V(G), V(G^*)) = \langle E(G^*) | c_v\gamma_v = 1;\ v\rangle$$

Further $\pi_1(\mathfrak{h} - \Gamma.V(G), \Gamma.V(G^*))$ is generated for each $v \in V(G^*)$ by the images $g.\gamma_v$ for a small loop γ_v around v for each $g \in \Gamma$. Each $g.\gamma_v$ maps to $\gamma_v^{\nu_v}$. So that we get

$$\Gamma \simeq \langle E(G^*) | c_v^{\nu_v} = 1\rangle$$

Retrieving the basic presentation of Γ

Using (groupoid-theoritic)) Van Kampen on the new cell decomposition of $\Gamma\backslash\mathfrak{h} - V(G)$, with $\{c_v\}_{v\in V(G)}$ being the cycles of $\sigma_1\sigma_2^{-1}$ and γ_v being the counter clock-wise loops c_v^{-1} we get

$$\pi_1(\Gamma\backslash\mathfrak{h} - V(G), V(G^*)) = \langle E(G^*) | c_v\gamma_v = 1;\ v\rangle$$

Further $\pi_1(\mathfrak{h} - \Gamma.V(G), \Gamma.V(G^*))$ is generated for each $v \in V(G^*)$ by the images $g.\gamma_v$ for a small loop γ_v around v for each $g \in \Gamma$. Each $g.\gamma_v$ maps to $\gamma_v^{\nu_v}$. So that we get

$$\Gamma \simeq \langle E(G^*) | c_v^{\nu_v} = 1\rangle$$

Improving the presentation

From the map $\mathfrak{h} - V(G) \to \mathfrak{h}$ there is a surjective morphism of groupoids

$$\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) \to \pi_1(\Gamma\backslash\mathfrak{h}, V(G^*))$$

and studying its kernel shows that it is made of loops around vertices of $V(G)$.

Goal :

Use the one polygon presentation of the compact surface $\Gamma\backslash\mathfrak{h}$ to compute $\pi_1(\Gamma\backslash\mathfrak{h}, v)$ and pull it back.

To do so :

- Find a covering tree in the graph made of polygons (cycles of σ_2) and edges those x such that x and x^{-1} lie in different polygons.
- Glue the polygons along the tree $\to$ get 1 polygon.
- Pull it back to $\pi_1(\Gamma(\mathfrak{h} - V(G)), V(G))$.

Improving the presentation

From the map $\mathfrak{h} - V(G) \to \mathfrak{h}$ there is a surjective morphism of groupoids

$$\pi_1(\Gamma \backslash (\mathfrak{h} - V(G)), V(G^*)) \to \pi_1(\Gamma \backslash \mathfrak{h}, V(G^*))$$

and studying its kernel shows that it is made of loops around vertices of $V(G)$.

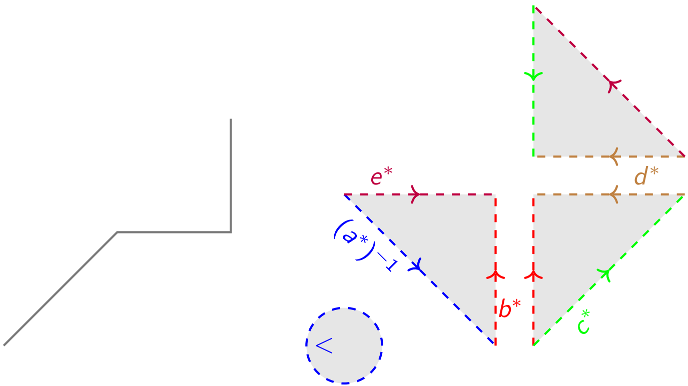
Goal :

Use the one polygon presentation of the compact surface $\Gamma \backslash \mathfrak{h}$ to compute $\pi_1(\Gamma \backslash \mathfrak{h}, v)$ and pull it back.

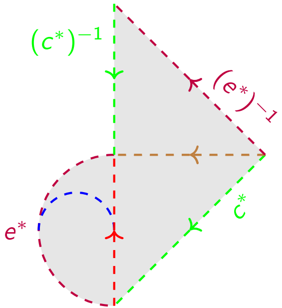
To do so :

- Find a covering tree in the graph made of polygons (cycles of σ_2) and edges those x such that x and x^{-1} lie in different polygons.
- Glue the polygons along the tree $\to$ get 1 polygon.
- Pull it back to $\pi_1(\Gamma(\mathfrak{h} - V(G)), V(G))$.

In practice :

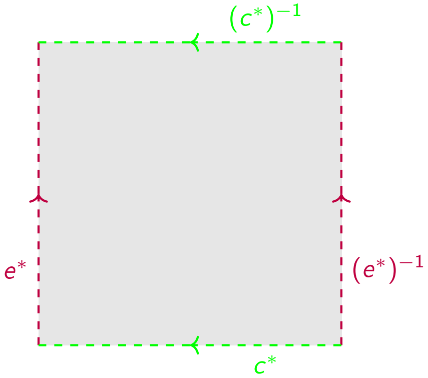


Post-gluing



Post-flattening

We see that $\Gamma\backslash\mathfrak{h}$ is just a torus.



Call P' the new glued polygon and γ be the boundary loop $\partial P'$ in counter-clockwise orientation.

Recover a presentation for Γ

- γ lies in $\pi_1(\Gamma(\mathfrak{h} - V(G)), V(G^*))$ we can write it as a product $\gamma = \gamma_1\gamma_2 e^*\gamma_3\gamma_4\bar{e}^*$.
- A last application of Van Kampen on $P' - V(G)$ shows that

$$\begin{aligned}\pi_1(\Gamma\backslash(\mathfrak{h} - V(G)), V(G^*)) &= \langle E(\Gamma\backslash P'), \gamma_1, \ldots, \gamma_f | w\gamma = 1,\ \gamma_i^{\nu_i} = 1\rangle \\ &= \langle e^*, c^*, \gamma_1, \gamma_2, \gamma_3, \gamma_4 | [e^*, c^*]\gamma_1\gamma_2 e^*\gamma_3\gamma_4(e^*)^{-1} = 1\end{aligned}$$

Quotienting by $\pi_1(\mathfrak{h} - \Gamma.V(G), V(G^*))$ we get

$$\Gamma = \langle e^*, c^*, \gamma_1, \gamma_2, \gamma_3, \gamma_4 | [e^*, c^*]\gamma_1\gamma_2 e^*\gamma_3\gamma_4(e^*)^{-1} = 1,\ (a^*)^3 = 1\rangle$$

which is the one-word (even geometric) presentation.

Work in progress

For a covering $\Gamma_1\backslash\mathfrak{h} \to \Gamma_2\backslash\mathfrak{h}$ given as a permutation representation $\Gamma_1 \to S_n$. Compute one-word, m-handles and geometric presentations for Γ_2 from that of Γ_1 expected in $\tilde{O}(n)$ time. Permits increasing the level of $S_k(\eta)$.

Thanks!