Algorithmes pour la topologie des variétés arithmétiques compactes et les opr de Hecke

(I)

jw/ Michael Lipnowski

§1 Intro

Un groupe arithmétique est un groupe $\Gamma = \mathbb{G}(\mathbb{Z})$ où $\mathbb{G} \subseteq SL_n$ est un groupe algébrique. (semisimple)

ex: $\Gamma = SL_n(\mathbb{Z})$, $SO(Q, \mathbb{Z})$ ← forme quadratique / $\mathbb{Q}$.

Γ généralement infini, mais de présentation finie (Borel, Harish-Chandra)

$\Gamma \curvearrowright X = \mathbb{G}(\mathbb{R})/K$ $K \subseteq \mathbb{G}(\mathbb{R})$ compact maximal

← contractile : "espace symétrique"

variété arithmétique $\Gamma \backslash X$ → ≈ variété compacte ; → $\pi_1 \approx \Gamma$

opérateurs de Hecke $\curvearrowright H^i(\Gamma \backslash X)$ → retrouve formes modulaires classiques $\Gamma \subseteq SL_2(\mathbb{Z})$, $X = \mathcal{H}$

→ formes automorphes, → torsion } ⟷ représentations Galoisiennes (ℓ-adiques / mod ℓ)

Q: Étant donné $\mathbb{G}$, peut-on calculer ces objets ? À quelle vitesse ? Mesure de complexité : $V = vol(\Gamma \backslash X)$.

Thm (Grunewald-Segal '80) Il existe un algorithme qui, étant donné $\mathbb{G}$, calcule une présentation pour Γ.

Complexité ?

Thm (Lipnowski – P.)

Il existe un algorithme qui, étant donné G tq

- $\Gamma\backslash X$ est une variété compacte,

calcule

- un complexe simplicial $S \simeq \Gamma\backslash X$ (équiv. d'homotopie) avec $O_{dim}(V)$ simplexes
- un isomorphisme explicite $\pi_1(S) \longrightarrow \Gamma$

Cet algorithme termine en temps $O_{dim}(V^2)$.

De plus, il existe un algorithme qui, étant donnés une chaîne $\sigma \in C^\circ(S)$ et un opérateur de Hecke T, calcule une chaîne dans $C^\circ(S)$ qui est homologue à $\underbrace{T\sigma}_{\in C^\circ(S)}$, en temps $O_{dim}(V \cdot \deg T)$

degré, mesure de complexité d'un opérateur de Hecke

Remarque : le nombre de simplexes est essentiellement optimal.

§2 – Méthodes précédentes

dim 0 $\quad Q$ forme quadratique définie positive sur $\mathbb{Q}^n$.

$L_1 \subseteq \mathbb{Q}^n$ réseau.

$G = SO(Q)$

$\rho : G(\mathbb{Q}) \longrightarrow \mathrm{Aut}(W)$ représentations de dim finie "poids".

$\widetilde{X} = \text{genre}(L_1) = \{ L \subseteq \mathbb{Q}^n \text{ réseau tel que } (L,Q) \underset{\mathbb{Z}_p}{\cong} (L_1, Q) \ \forall p \}$

$M(W) := \{ f : \widetilde{X} \to W \text{ tq } f(gx) = \rho(g) f(x) \ \forall g \in G(\mathbb{Q}), x \in \widetilde{X} \}$

Thm $\quad G(\mathbb{Q}) \backslash \widetilde{X}$ est fini (variété arithmétique de dimension 0)

$$G(\mathbb{Q}) \backslash \widetilde{X} = \{ [L_1], [L_2], \dots, [L_v] \}$$

$$\Longrightarrow M(W) \cong \bigoplus_{i=1}^{v} \underbrace{H^0(\Gamma_i, W)}_{= W^{\Gamma_i}} \qquad \Gamma_i = SO(Q, L_i) \ \text{(fini)}$$

Problème Comment calculer $G(\mathbb{Q}) \backslash \widetilde{X}$?

$x, x' \in \widetilde{X}$, $[x] = [x']$?

L, L' réseaux $\quad \exists g \in G(\mathbb{Q}) \quad gL = L'$?

Algorithme (Plesken-Souvignier)

- $b_1, \dots, b_n$ base de L
- Q définie-positive $\Longrightarrow$ $gb_i \in$ ensemble fini calculable
- $\to$ énumération

Voisins $\quad p \nmid 2\,\mathrm{disc}(L_1, Q)$

L, L' sont <u>p-voisins</u> si $L/_{L \cap L'} \cong L'/_{L\cap L'} \cong \mathbb{Z}/_{p\mathbb{Z}}$

$\rightsquigarrow \widetilde{X}$ devient un graphe $\widetilde{X}_p$

<u>Thm</u> (Kneser) $\quad \mathbb{G}(\mathbb{Q}) \backslash \widetilde{X}_p$ est connexe.

<u>Algorithme</u> Explorer $\widetilde{X}_p$ en partant de L_1.

À chaque étape tester l'équivalence avec les sommets précédents.

Complexité $O_{\dim}(V^2)$

Opérateurs de Hecke

$$f \in M(W)$$

$$T_p f(L) = \sum_{L' \in \mathrm{Vois}_p(L)} f(L') \qquad \deg T_p = \# \mathrm{Vois}_p(L)$$

Algo évident, complexité $O_{\dim}(V \cdot \deg T_p)$ par point.

$\dim > 0$

1) Information géométrique sur $\Gamma \backslash X$
2) Complexe de dimension finie calculant $H^\circ(\Gamma\backslash X)$ $\quad \cancel{\circlearrowleft}$ Hecke
4) $\uparrow\downarrow$
3) Complexe de dimension infinie calculant $H^\circ(\Gamma \backslash X)$ $\circlearrowleft$ Hecke

Oralement : symboles modulaires, H^1, Voronoï & sharblies.

III – Méthode par recouvrement

Cohomologie de $\Gamma\backslash X$?

<u>Idée</u> : Imiter les méthodes en dim 0, approximer $\Gamma\backslash X$ par un ensemble fini.

~~Trouver $F \subseteq \Gamma\backslash X$ tq~~

• ~~$\bigcup_{x\in F} B_R(x) = \Gamma\backslash X$~~ ~~$R$-dense~~

<u>Def</u> $F \subseteq Y$ espace métrique, $R>0$

- F <u>R-dense</u> si $Y = \bigcup_{x\in F} B_R(x)$
- F <u>R-séparée</u> si $d(x,y) \geq R \quad \forall x \neq y \in F$

<u>Rq</u> $F \subseteq Y$ R-~~indépendante~~ séparée maximale $\Rightarrow$ F R-dense.

<u>Def</u> F espace métrique, $R>0$

<u>Complexe de Čech</u> $\mathcal{C}_R(F)$:

- sommets : points de F
- $\{x_0, \dots, x_k\}$ k-simplexe $\Leftrightarrow \bigcap_i B_R(x_i) \neq \emptyset$

<u>Thm</u> (~~...~~

Y variété Riemannienne compacte.

$F \subseteq Y$ R-dense avec $R \ll 1$.

Alors $\mathcal{C}_R(F) \simeq Y$ (équivalence d'homotopie)

<u>Étapes</u> 1) <u>Géométrie</u> : F fini R-dense + graphe de $2R$-adjacence

2) Complexe fini : $\mathcal{C}_R(F)$

3) Complexe infini : $\mathcal{C}_R(\Gamma\backslash X) \circlearrowleft$ Hecke.

4) Equivalence : $\mathcal{C}_R(\Gamma\backslash X) \longrightarrow \mathcal{C}_{R'}(F) \supseteq \mathcal{C}_R(F)$.

Algorithme ?

1) Rendre remarque effective.
2) Calcul dans le quotient

1) On veut une partie dense mais pas trop grosse.
F' Partie $R/2$ - dense $\longrightarrow$ enlever des éléments ?
Solution : $F \subseteq F'$ $R/2$ - séparée maximale

$$\Longrightarrow F \quad R/2\text{- dense dans } F'$$

$$\Longrightarrow F \quad R\text{- dense dans } \Gamma\backslash X.$$

Procédé d'expansion pour toujours garder F de taille raisonnable.

2) $x, y \in X$, $\quad \exists \gamma \in \Gamma$ tq $d(x, \gamma y) \leq R$?

<u>exemple</u> $G = SL_n$ $\quad X = \left\{ \begin{array}{l} \text{formes quadratiques définie-positives} \\ \text{sur } \mathbb{R}^n \end{array} \right\}$

$Q, Q' \in X$.
Observation : $\forall x \in \mathbb{R}^n \setminus 0$,

$$|\log Q(x) - \log Q'(x)| \leq d(Q, Q')$$

Si $\gamma \in G(\mathbb{Z})$ et $d(Q, \gamma Q') \leq R$ alors $\forall x \in \mathbb{Q}^n$

$$Q'(x)\, e^{-R} \leq Q(\gamma x) \leq Q'(x)\, e^{R}$$

ie $\gamma : (\mathbb{Z}^n, Q) \longrightarrow (\mathbb{Z}^n, Q')$ e^R-quasi-isométrie.

$\rightsquigarrow$ nombre fini de possibilités, énumération à la Plesken-Souvignier.

ex :

dim X	nb pts finaux	nb pts intermédiaires	tps
2	4	304	0.25 s.
3	9	11952	26 s.
4	21	180 600	1175 s.