Hensel-lifting torsion points and Galois representations

Nicolas Mascot

American University of Beirut

Pari/GP workshop
IMB, Bordeaux
January 17th 2019

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Suppose we know a curve $C/\mathbb{Q}$ such that ρ is afforded by an $\mathbb{F}_\ell$-subspace $T \subset J[\ell]$, where $J = \mathrm{Jac}(C)$.

Goal

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ be a Galois representation.

Suppose we know a curve $C/\mathbb{Q}$ such that ρ is afforded by an $\mathbb{F}_\ell$-subspace $T \subset J[\ell]$, where $J = \mathrm{Jac}(C)$.

To isolate $T \subset J[\ell]$, we assume that for one good prime $p \neq \ell$, we know

$$\chi_\rho(x) = \det \left(x - \mathrm{Frob}_p \,|_T \right) \in \mathbb{F}_\ell[x]$$

and

$$L(x) = \det \left(x - \mathrm{Frob}_p \,|_J \right) \in \mathbb{Z}[x],$$

and that

$$\gcd(\chi_\rho, L/\chi_\rho) = 1 \in \mathbb{F}_\ell[x].$$

Strategy

1. Find $q = p^a$ such that $T \subset J(\mathbb{F}_q)[\ell]$,
2. Generate $\mathbb{F}_q$-points of T until we get an $\mathbb{F}_\ell$-basis,
3. Lift these points from $J(\mathbb{F}_q)$ to $J(\mathbb{Q}_q)$,
4. Form all linear combinations of these points in $J(\mathbb{Q}_q)[\ell]$,
5. $F(x) = \prod_{t \in T} \big(x - \alpha(t)\big)$, where $\alpha : J \dashrightarrow \mathbb{A}^1$,
6. Identify $F(x) \in \mathbb{Q}[x]$.

Strategy

1. Find $q = p^a$ such that $T \subset J(\mathbb{F}_q)[\ell]$,
2. Generate $\mathbb{F}_q$-points of T until we get ~~an $\mathbb{F}_\ell$-basis~~ an $\mathbb{F}_\ell[\mathrm{Frob}_p]$-generating set,
3. Lift these points from $J(\mathbb{F}_q)$ to $J(\mathbb{Q}_q)$,
4. Form ~~all~~ combinations of these points in $J(\mathbb{Q}_q)[\ell]$ representing all Frob_p-orbits,
5. $F(x) = \sout{\prod_{t \in T} (x - \alpha(t))} \prod_{t \in \mathrm{Frob}_p \backslash T} \operatorname{charpoly}(\alpha(t))$, where $\alpha : J \dashrightarrow \mathbb{A}^1$,
6. Identify $F(x) \in \mathbb{Q}[x]$.

Getting a basis of T

- $\# J(\mathbb{F}_q) = \operatorname{Res}\big(L(x), x^a - 1\big) = \ell^b M.$

$$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ [M]t \in J(\mathbb{F}_q)[\ell^\infty].$$

Getting a basis of T

- $\#J(\mathbb{F}_q) = \operatorname{Res}\big(L(x), x^a - 1\big) = \ell^b M.$

$$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ [M]t \in J(\mathbb{F}_q)[\ell^\infty].$$

- $L(x) = \chi_\rho(x)\psi(x) \in \mathbb{F}_\ell[x]$

$$\rightsquigarrow \forall t \in J(\mathbb{F}_q)[\ell],\ \psi(\operatorname{Frob}_p) \cdot t \in T.$$

Getting a basis of T

- $\#J(\mathbb{F}_q) = \operatorname{Res}\big(L(x), x^a - 1\big) = \ell^b M.$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q),\ [M]t \in J(\mathbb{F}_q)[\ell^\infty].$$

- $L(x) = \chi_\rho(x)\psi(x) \in \mathbb{F}_\ell[x]$

  $$\rightsquigarrow \forall t \in J(\mathbb{F}_q)[\ell],\ \psi(\operatorname{Frob}_p) \cdot t \in T.$$

☠ Not uniformly distributed!

Pairing

Use the Frey-Rück pairing

$$[\,\cdot\,,\,\cdot\,]_\ell : J(\mathbb{F}_q)[\ell] \times J(\mathbb{F}_q)/\ell J(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^\times / \mathbb{F}_q^{\times \ell}$$

to detect linear dependency in $J(\mathbb{F}_q)[\ell]$, and obtain a generating set of T.

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.
- A basis $v_1, v_2, \cdots$ of V can be represented by the matrix

$$\begin{pmatrix} v_1(P_1) & v_2(P_1) & \cdots \\ \vdots & \vdots & \\ v_1(P_n) & v_2(P_n) & \cdots \end{pmatrix}.$$

Makdisi's algorithms

- Fix $P_1, \cdots, P_n \in C(\mathbb{Q}_q)$ (where $n \gg_g 1$), and a divisor $D_0 \gg_g 0$. Let $V = \mathcal{L}(2D_0)$.
- A point $[D - D_0] \in J$ is represented by the subspace

$$W = \mathcal{L}(2D_0 - D) \subset V,$$

i.e. by the matrix

$$\begin{pmatrix} w_1(P_1) & w_2(P_1) & \cdots \\ \vdots & \vdots & \\ w_1(P_n) & w_2(P_n) & \cdots \end{pmatrix},$$

where $w_1, w_2, \cdots$ is a basis of W.

Membership test

Algorithm (Makdisi, 2004)

Let W be a matrix as above.

1. $w \leftarrow 1^{\text{st}}$ column of W
2. $W' \leftarrow \{v \in V \mid vW \subset wV\}$
3. $n \leftarrow \dim W'$
4. Return True if $n = \#W$, False if $n < \#W$.

Proof.

$W' = \mathcal{L}(2D_0 - D')$, where $(w) = -2D_0 + D + D'$ and D is the largest divisor such that $W \subset \mathcal{L}(2D_0 - D)$. □

Differentiation of linear algebra

Let ${}_rA_n$ have rank r.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n}\right)$,

where $S = \texttt{matsupplement}(A)$ so that $\widetilde{A}$ is invertible

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n} \right)$,

where $S = \texttt{matsupplement}(A)$ so that $\widetilde{A}$ is invertible,

and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n} \right)$,

where $S = \texttt{matsupplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array} \right)$$

so $K \stackrel{\text{def}}{=} \operatorname{Ker} A$.

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n}\right)$,

where $S = \texttt{matsupplement}(A)$ so that $\widetilde{A}$ is invertible, and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array}\right)$$

so $K \stackrel{\text{def}}{=} \operatorname{Ker} A$.

For ${}_rH_n$ small enough, $\widetilde{A+H} = \widetilde{A} + \left(\frac{H}{0}\right)$, so

$$\widetilde{A+H}^{-1} = \widetilde{A}^{-1} - \widetilde{A}^{-1}\left(\frac{H}{0}\right)\widetilde{A}^{-1} + O(H^2)$$

Differentiation of linear algebra

Let ${}_rA_n$ have rank r. Define $\widetilde{A} = \left(\frac{{}_rA_n}{{}_{n-r}S_n} \right)$,

where $S = \texttt{matsupplement}(A)$ so that $\widetilde{A}$ is invertible,

and split $\widetilde{A}^{-1} = ({}_nL_r \mid {}_nK_{n-r})$. Then

$$I_n = \widetilde{A}\widetilde{A}^{-1} = \left(\begin{array}{c|c} {}_rAL_r & {}_rAK_{n-r} \\ \hline {}_{n-r}SL_r & {}_{n-r}SK_{n-r} \end{array} \right)$$

so $K \stackrel{\text{def}}{=} \operatorname{Ker} A$.

For ${}_rH_n$ small enough, $\widetilde{A+H} = \widetilde{A} + \left(\frac{H}{0} \right)$, so

$$\widetilde{A+H}^{-1} = \widetilde{A}^{-1} - \widetilde{A}^{-1} \left(\frac{H}{0} \right) \widetilde{A}^{-1} + O(H^2)$$

$$\rightsquigarrow \operatorname{Ker}(A+H) = \operatorname{Ker}(A) - LH \operatorname{Ker}(A) + O(H^2).$$

Application (1/3)

Let S be the minimal regular model of the surface / $\mathbb{Q}$

$$z^2 = xy(x^2 - 1)(y^2 - 1)(x^2 - 2xy - y^2).$$

Application (1/3)

Let S be the minimal regular model of the surface / $\mathbb{Q}$

$$z^2 = xy(x^2-1)(y^2-1)(x^2-2xy-y^2).$$

Van Geemen & Top observed that there exists an eigenform u of level 2^7 over SL(3) such that $\forall \ell \in \mathbb{N}$, a twist of

$$\widetilde{\rho}_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{Q}_\ell(\sqrt{-1})\big)$$

is contained in $H^2(S, \mathbb{Q}_\ell)$.

For $p \notin \{2, \ell\}$, the characteristic polynomial of $\widetilde{\rho}_{u,\ell}$ is

$$x^3 - a_p x^2 + p\overline{a_p} x - p^3 \chi(p)$$

for some $\chi : (\mathbb{Z}/2^3\mathbb{Z})^\times \longrightarrow \mathbb{Q}(\sqrt{-1})^\times$, where $a_p \in \mathbb{Z}[\sqrt{-1}]$.

Application (2/3)

The fibres of

$$\begin{array}{cccc} \pi & : & S & \longrightarrow & \mathbb{P}^1 \\ & & (x,y,z) & \longmapsto & x/y \end{array}$$

are elliptic curves.

Application (2/3)

The fibres of

$$\begin{array}{rccc} \pi & : & S & \longrightarrow & \mathbb{P}^1 \\ & & (x,y,z) & \longmapsto & x/y \end{array}$$

are elliptic curves.

$\rightsquigarrow$ for each ℓ, we can find a curve C_ℓ / $\mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

Application (2/3)

$\rightsquigarrow$ for each ℓ, we can find a curve $C_\ell \ / \ \mathbb{Q}$ whose Jacobian contains

$$\rho_{u,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3\big(\mathbb{F}_\ell(\sqrt{-1})\big).$$

We find that the twist of

$$\rho_{u,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_3(\mathbb{F}_9)$$

by $\left(\frac{6}{\cdot}\right)$ cuts off the splitting field of

$$x^{28} - 12x^{27} + 60x^{26} - 132x^{25} - 30x^{24} + 624x^{23} + 420x^{22} - 7704x^{21} + 17118x^{20} - 9504x^{19} - 14424x^{18} + 10824x^{17} + 36492x^{16} - 64992x^{15} + 19488x^{14} + 56064x^{13} - 89604x^{12} + 109296x^{11} - 88368x^{10} - 11472x^{9} + 58488x^{8} - 130176x^{7} + 34224x^{6} - 58272x^{5} - 39960x^{4} + 32256x^{3} + 24480x^{2} - 352x - 1776$$

and has thus image $\mathrm{SU}_3(\mathbb{F}_3)$.

Application (3/3)

p	$\rho_{u,3}(\mathrm{Frob}_p)$	$a_p(u) \bmod 3\mathbb{Z}[i]$
$10^{1000}+453$	$+\begin{pmatrix} 1 & 0 & 0 \\ 0 & i-1 & i-1 \\ 0 & i+1 & -i-1 \end{pmatrix}$	-1
$10^{1000}+1357$	$-\begin{pmatrix} 0 & 0 & i \\ 0 & i & 0 \\ 1 & 0 & 0 \end{pmatrix}$	$-i$
$10^{1000}+2713$	$-\begin{pmatrix} 0 & 0 & -i \\ 0 & -i & 0 \\ 1 & 0 & 0 \end{pmatrix}$	i
$10^{1000}+4351$	$-\begin{pmatrix} 0 & i+1 & -i-1 \\ 0 & -i+1 & -i+1 \\ 1 & 0 & 0 \end{pmatrix}$	$i-1$
$10^{1000}+5733$	$+\begin{pmatrix} 0 & i+1 & -i+1 \\ 0 & -i-1 & -i+1 \\ 1 & 0 & 0 \end{pmatrix}$	$-i-1$

Any questions ?

Thank you !