Computing Cusp Forms Over Function Fields

Jonathan Love

Department of Mathematics and Statistics, McGill University
https://jonathanlove.info/

Explicit Methods for Modularity, April 2022

Initial comments

- Work done during my PhD studies[1] at Stanford University, supervised by Akshay Venkatesh, Ravil Vakil, and Dan Boneh.
- Write-up available in Chapter 4 of my thesis.
- Code available on Github.

[1] Funding from the Lebovitz Family Fellowship and NSF Award #1701567 (PI: Dan Boneh)

Outline

Definitions

Given a global field F, we have:

- The completion F_v for each place v of F
- the valuation ring $\mathcal{O}_v$ for each finite (non-archimedean) place v of F
- The ring of adeles $\mathbb{A} = \prod'_v F_v$ ($x_v \in \mathcal{O}_v$ for all but finitely many v)
- The ring of integral adeles $\widehat{\mathcal{O}} = \prod_{v \text{ finite}} \mathcal{O}_v$

F embeds as a discrete subgroup in $\mathbb{A}$ by

$$a \mapsto (a, a, a, \ldots).$$

Induces a discrete embedding $\mathrm{GL}_2(F) \to \mathrm{GL}_2(\mathbb{A})$.

Definitions

"Definition"

A *cusp form on* $\mathrm{GL}_2(\mathbb{A})$ is a function

$$\varphi : \mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/K \to \mathbb{C}$$

for some finite-index $K \subseteq \mathrm{GL}_2(\widehat{\mathcal{O}})$, such that for all $\tau \in \mathrm{GL}_2(\mathbb{A})$,

$$\int_{\mathbb{A}/F} \varphi\left(\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)\tau\right) dt = 0.$$

φ is *ramified at v* if $K_v \neq \mathrm{GL}_2(\mathcal{O}_v)$ (and *unramified* if $K = \mathrm{GL}_2(\widehat{\mathcal{O}})$).

This is missing a few conditions from the standard definition.

Comparison to $\mathbb{Q}$

Consider a classical cusp form $f : \mathbb{H} \to \mathbb{C}$, level 1, weight k:

- $f(\gamma \cdot z) = (cz+d)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (modularity)
- For all $z \in \mathbb{H}$, $\int_0^1 f(z+t)\,dt = 0$ (cuspidality)

Proposition

Given $\tau \in \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$, write $\tau = \gamma \tau_\infty r$, with $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, $\tau_\infty = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, and $r \in \mathrm{GL}_2(\widehat{\mathbb{Z}})$. Then

$$\varphi_f(\tau) := (\det \tau_\infty)^{k/2} (ci+d)^{-k} f\left(\tau_\infty \cdot i\right)$$

is a well-defined unramified cusp form on $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$.

Proof sketch: If $\tau'_\infty = \gamma \tau_\infty r$, then $\gamma = r^{-1}$ and $\gamma = \tau'_\infty \tau_\infty^{-1}$, so

$$\gamma \in \mathrm{GL}_2(\mathbb{Q}) \cap \mathrm{GL}_2(\widehat{\mathbb{Z}}) \cap \mathrm{GL}_2^+(\mathbb{R}) = \mathrm{SL}_2(\mathbb{Z}).$$

Modularity of f implies double-coset invariance of φ_f.

Comparison to $\mathbb{Q}$

Key feature of cusp forms φ over $\mathbb{A}_\mathbb{Q}$: **archimedean place.**

- Use analytic techniques over $\mathbb{R}$ to study φ.
- Properties of φ come from *topology* at $\mathbb{R}$.

Example: weight k of f appears as a *winding number* of φ_f:

$$\varphi_f(\tau) = (\det \tau_\infty)^{k/2}(ci+d)^{-k} f(\tau_\infty \cdot i)$$

$$r(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}_2(\mathbb{R}) \quad \Rightarrow \quad \varphi_f(\tau r(\theta)) = e^{ik\theta}\varphi_f(\tau).$$

Observation

φ_f is invariant under $\mathrm{GL}_2(\mathbb{Z}_p) \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$ for every p, but *not* invariant under $\mathrm{SO}_2(\mathbb{R}) \subseteq \mathrm{GL}_2(\mathbb{R})$. (No weight 0 cusp forms)

Cusp Forms over Function Fields

Let X be a smooth projective curve over $k = \mathbb{F}_q$, with function field $F = k(X)$. Let $\mathbb{A}$ be the adeles of F. No archimedean places.

Ramified places (nontrivial action of $\mathrm{GL}_2(\mathcal{O}_v)$) can be used as "substitutes" for archimedean places.

- Snowden and Tsimerman[2] show that certain ramified cusp forms on $\mathrm{GL}_2(\mathbb{A})$ correspond to **elliptic curves over an open subset of X.**

[2] Andrew Snowden and Jacob Tsimerman. "Constructing elliptic curves from Galois representations". In: *Compos. Math.* 154.10 (2018).

Cusp Forms over Function Fields

What about *unramified* cusp forms?

- Drinfeld[3] (geometric Langlands): irreducible 2-dim ℓ-adic **representations of** $\pi_1(X)$ correspond to unramified cusp forms on $\mathrm{GL}_2(\mathbb{A})$.
- Krishnamoorthy and Pál[4] conjecture that unramified cusp forms on $\mathrm{GL}_2(\mathbb{A})$ with certain properties should correspond to **abelian varieties** over X.

Not many known examples of unramified cusp forms to test!

---

[3] Drinfeld, V. G. *Two-dimensional ℓ-adic representations of the fundamental group of a curve over a finite field and automorphic forms on GL(2).* Am. J. Math. 105:85–114 (1983).

[4] Raju Krishnamoorthy and Ambrus Pál. "Rank 2 local systems and abelian varieties". In: *Sel. Math. New Ser.* 27, 51 (2021).

Cusp Forms over Function Fields

Let $\mathbb{A}$ be the adeles of the function field of a genus 2 curve X.

Goal

Compute the space of unramified cusp forms on $\mathrm{PGL}_2(\mathbb{A})$ (that is, the space of unramified cusp forms φ on $\mathrm{GL}_2(\mathbb{A})$ such that $\varphi(z\tau) = \varphi(\tau)$ for $z \in \mathbb{A}^\times$), together with the action of Hecke operators on this space.

Note: in this setting, the "Definition" of cusp forms above is correct (no additional conditions necessary).

Prior work:

- Lorscheid: Elliptic curves X.[5]

[5] Oliver Lorscheid. "Toroidal automorphic forms for function fields". PhD thesis. Utrecht University, 2008.

Outline

Outline of Algorithm

Inspired by an algorithm of Greenberg and Voight[6] for *algebraic modular forms* (G_∞ compact $\Rightarrow$ double-coset space is *finite*; no analytic conditions necessary).

If F is a function field, $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/(\mathbb{A}^\times \cdot \mathrm{GL}_2(\widehat{\mathcal{O}}))$ is not finite, but it is discrete.

Cusp forms supported on a finite subset.

[6] Matthew Greenberg and John Voight. "Lattice methods for algebraic modular forms on classical groups". In: *Computations with modular forms. Contrib. Math. Comput. Sci.* 6 (2014).

Outline of Algorithm

Step 1: Build Hecke graph

Let L be a list of elements of $\mathrm{GL}_2(\mathbb{A})$ (starting with $L = (1)$). Fix a place v of F, with uniformizer π_v. For each $\tau \in L$:

- Compute its *Hecke neighbors*

$$\left\{\tau\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi_v \end{smallmatrix}\right)\right\} \cup \left\{\tau\left(\begin{smallmatrix} \pi_v & i \\ 0 & 1 \end{smallmatrix}\right) : i \in k(v)\right\}.$$

- For each Hecke neighbor τ':
  - Determine whether τ' is in the same double coset as an existing $\mu \in L$. If so, add an edge $\tau \to \mu$.
  - If no equivalent μ is found, append τ' to L and add an edge $\tau \to \tau'$.

Outline of Algorithm

Step 2: Find simultaneous eigenvectors

- Using step 1, obtain adjacency matrices M_v for multiple places v of F.
- Compute simultaneous eigenspaces of all M_v.
- If a simultanous eigenspace is 1-dimensional, entries of the eigenvector are coefficients of a cusp form! (If not, compute more M_v).
- Continue until all eigenspaces are processed.

Only problem remaining: How to test if $\tau, \mu \in \mathrm{GL}_2(\mathbb{A})$ are in the same double-coset?

Outline of Algorithm

Testing for double-coset equivalence: classical

To determine whether $\tau, \mu \in \mathrm{GL}_n(\mathbb{R})$ are equivalent in $\mathrm{SL}_n(\mathbb{Z})\backslash \mathrm{GL}_n(\mathbb{R})/(\mathbb{R}_{>0} \cdot \mathrm{SO}_n(\mathbb{R}))$, use an algorithm by Plesken and Souvignier:[7]

- Associate τ, μ to lattices L_τ, L_μ.
- Lattice basis reduction (e.g. LLL).
- Find all vectors of length $\leq \lambda$ in L_τ and L_μ. Increase λ if necessary to ensure the found vectors span $\mathbb{R}^n$.
- Find all ways to match vectors from L_τ to vectors from L_μ with corresponding lengths. Check if these extend to a lattice isomorphism.

[7] W. Plesken and B. Souvignier. "Computing Isometries of Lattices". In: *Journal of Symbolic Computation*. 24.3 (1997).

Lattices vs Vector Bundles

$\tau \in \mathrm{GL}_2(\mathbb{R})$ defines a *lattice* L_τ *with basis* in $\mathbb{R}^2$. ($(x, y) \in \mathbb{R}^2$ is in L_τ if and only if $(x, y)\tau \in \mathbb{Z}^2$)	$\tau \in \mathrm{GL}_2(\mathbb{A})$ defines a *rank* 2 *vector bundle* V_τ on X. ($(f, h) \in F^2$ is a section of $V_\tau(U)$ if and only if $(f\ \ h)\tau_v \in \mathcal{O}_v^2$ for all places $v \in U$)
$t \in \mathbb{R}_{>0}$ determines a *scaling* $L_{t\tau} := \frac{1}{t} L_\tau$. Large $t \Rightarrow$ more vectors $(x, y) \in L_{t\tau}$ in the unit square ($\lvert x\rvert, \lvert y\rvert \leq 1$)	$t \in \mathbb{A}^\times$ determines a *twist* $V_{t\tau} := V_\tau \otimes \mathcal{O}(\mathrm{div}(t))$. Large $\deg(t) \Rightarrow$ more global sections $(f, h) \in V_\tau(X)$ ($\lvert f\rvert_v, \lvert h\rvert_v \leq 1$ for all v)
$\mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})^+/(\mathbb{R}_{>0} \cdot \mathrm{SO}_2(\mathbb{R}))$ classifies *lattices in* $\mathbb{R}^2$ *up to isometry and scaling.*	$\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/(\mathbb{A}^\times \cdot \mathrm{GL}_2(\widehat{\mathcal{O}}))$ classifies *vector bundles on* X *up to isomorphism and twisting by divisors.*

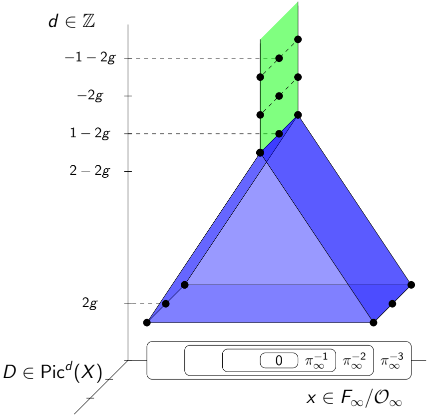
Outline of Algorithm

Testing for double-coset equivalence: function field

To determine whether $\tau, \mu \in \mathsf{GL}_2(\mathbb{A})$ are equivalent in $\mathsf{GL}_2(F)\backslash \mathsf{GL}_2(\mathbb{A})/(\mathbb{A}^\times \cdot \mathsf{GL}_2(\widehat{\mathcal{O}}))$:

- Associate τ, μ to vector bundles V_τ, V_μ.
- Reduce each to land in a Siegel set.

A Siegel Set for $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/(\mathbb{A}^\times \cdot \mathrm{GL}_2(\widehat{\mathcal{O}}))$



Every double coset has at least one representative

$$\left(\begin{pmatrix} 1 & x_v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pi_v^{D(v)} & 0 \\ 0 & 1 \end{pmatrix} \right)_v \in \mathrm{GL}_2(\mathbb{A})$$

parametrized by

$$d \leq 2g, \quad D \in \mathrm{Pic}^d(X),$$
$$x_\infty \in \pi_\infty^{-(d+2g-1)}\mathcal{O}_\infty/\mathcal{O}_\infty,$$
$$x_v = 0 \qquad \text{for all } v \neq \infty$$

Green: the cusp (infinite; easy to characterize, cusp forms vanish)
Blue: non-cusp (finite but large; need to check for isomorphisms)

Outline of Algorithm

Testing for double-coset equivalence: function field

To determine whether $\tau, \mu \in \mathrm{GL}_2(\mathbb{A})$ are equivalent in $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A})/(\mathbb{A}^\times \cdot \mathrm{GL}_2(\widehat{\mathcal{O}}))$:

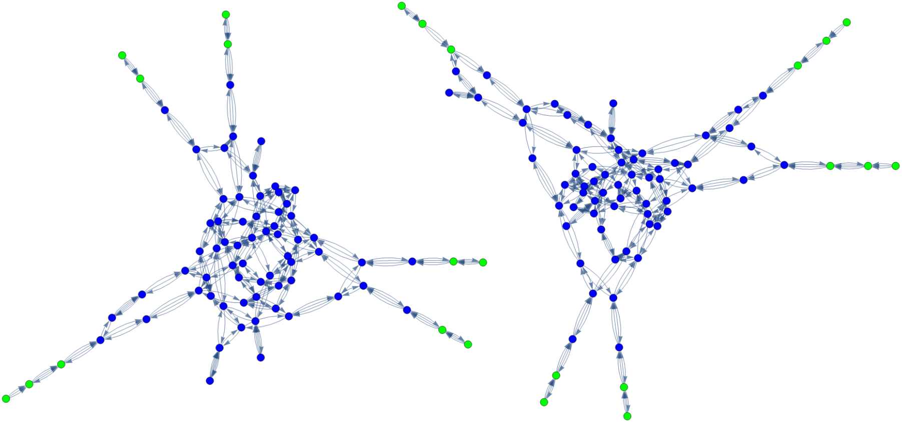
- Associate τ, μ to vector bundles V_τ, V_μ.
- Reduce each to land in a Siegel set.
- Compute global sections of V_τ and V_μ. Twist each by divisors if necessary until the F-span of the global sections is dim 2 over F.
- Find all ways to match global sections of V_τ with global sections of V_μ. Check if these extend to a vector bundle isomorphism.

Outline

Example: $y^2 = x^5 + 1$ over $\mathbb{F}_3$.

Vertices: double-cosets.

Edges: Neighbors according to Hecke operator at ∞.



Example: $y^2 = x^5 + 1$ over $\mathbb{F}_3$.

Computed Hecke action at $\infty, (0,1), (0,2), (2,0)$ ($|k_v| = 3$), as well as $(1+i, 1+i)$ ($|k_v| = 9$). Obtain a **76-dimensional basis of cusp forms**, in four Galois orbits. The corresponding Hecke eigenvalues are:

	Orbit 1	Orbit 2	Orbit 3	Orbit 4
$[K:\mathbb{Q}] \to$	2	2	12	60
∞	0	0	0	$\pm_1\sqrt{\beta}$
$(0,1)$	0	0	$\pm_1\alpha$	$\pm_1\sqrt{\beta}p(\beta)$
$(0,2)$	0	0	$\mp_1\alpha$	$\pm_1\sqrt{\beta}p(\beta)$
$(2,0)$	0	0	0	$(\pm_1\sqrt{\beta})(\pm_2\sqrt{r(\beta)})q(\beta)$
$(1+i, 1+i)$	$\frac{3\pm3\sqrt{5}}{2}$	$\frac{-3\pm3\sqrt{5}}{2}$	$\pm_2\sqrt{-\alpha^2+9\alpha-9}$	$\pm_2\sqrt{r(\beta)}$

- α satisfies $\alpha^3 - 13\alpha^2 + 48\alpha - 45 = 0$
- β satisfies $s(\beta) = 0$, for a degree 15 polynomial $s(x) \in \mathbb{Q}[x]$
- $p(x), q(x), r(x) \in \mathbb{Q}[x]$ have degree 14

What's next?

- Code is quite slow ($\sim$3 hours on a personal computer to process one curve); are there speed-ups?
- Complete database of unramified cusp forms over all genus 2 curves over $\mathbb{F}_3$ (there are 69 isomorphism classes;[8] Hecke graphs have been computed for nine).
- Can we find an unramified cusp form with Hecke eigenvalues in $\mathbb{Q}$? Ideal testing ground for Krishnamoorthy-Pál's conjecture (such a cusp form should correspond to a **fake elliptic curve**: abelian surface over X with endomorphism ring a quaternion order).

Thank you for your attention!

[8] Rose Steinberg. "Enumerating Curves of Genus 2 Over Finite Fields". PhD thesis. University of Vermont, 2018.