Function fields: Monodromy groups

Douglas Ulmer
University of Arizona

June 3, 2006

Let $f : X \to Y$ be a non-constant map of compact Riemann surfaces. Over some open set f is a covering space map $f^0 : X^0 \to Y^0$. Choose $y \in Y^0$ and look at the fiber over y:

$$(f^0)^{-1}(y) = \{x_1, \ldots, x_d\}$$

The fundamental group $\pi_1(Y^0, y)$ acts on the fiber by lifting of paths. So we get a homomorphism $\pi_1(Y^0, y) \to S_d$. The image of this homomorphism is the *monodromy group* of f. [picture]
(Fact for use later: the monodromy group can also be described as the Galois group of the Galois closure of $\mathbb{C}(X)$ over $\mathbb{C}(Y)$.)

$\pi_1(Y^0, y)$ is a quotient of $\mathrm{Gal}(\overline{K}/K)$ where $K = \mathbb{C}(Y)$, the function field of Y. So $\mathrm{Gal}(\overline{K}/K)$ also acts on $(f^0)^{-1}(y)$ and the monodromy group is also the image of $\mathrm{Gal}(\overline{K}/K) \to S_d$.

Similar remarks apply when $X \to Y$ is some other algebraic object where the fibers are, say, vector spaces and the fundamental group acts by linear transformations.

So, quite generally, a monodromy group is the image of the action of π_1 or Galois on some family of sets or vector spaces, a so-called "local system."

Fix q and let $F_n = \mathbb{F}_{q^n}(t)$ and $R_n = \mathbb{F}_{q^n}[t]$. Quadratic extensions of F_n look like $K = F_n(\sqrt{h})$ where $h \in R_n$ is square free. For simplicity, we'll assume h is monic. Fix a degree d and look at monic h of degree d:

$$h = t^d + a_1 t^{d-1} + \cdots + a_d \qquad a_i \in \mathbb{F}_{q^n}$$

Varying h amounts to varying the coefficients a_i and so the set of all h (monic of degree d) is in bijection with $(\mathbb{F}_{q^n})^d = \mathbb{A}^d(\mathbb{F}_{q^n})$. The subset of h which are square free is a Zariski open subset of $\mathbb{A}^n$, namely the complement of the zero set of the discriminant. Write $U \subset \mathbb{A}^n$ for this set (or rather variety).

For each $h \in U(\mathbb{F}_{q^n})$ we get a quadratic extension $K = F_n(\sqrt{h})$, an L-function $L(\chi_h, s)$, and a symplectic matrix $A_{n,h}$ such that $L(\chi_h, s)$ is the characteristic polynomial of $q^{1/2-s}A_{n,h}$. (Recall that $A_{n,h}$ is symplectic because of the pairing on $H^1(\sigma_f)$.) Studying the variation of $L(\chi_h, s)$ as h varies through U is the same as studying the variation of $A_{n,h}$.

The same technology that gave us the vector space $H^1(\sigma_h)$ with Fr_{q^n} action that calculates $L(\chi_h, s)$ for an individual h gives us a single vector space H on which $\pi_1(U)$ acts. Moreover, for each n and each $h \in U(\mathbb{F}_{q^n})$, there is a Frobenius element $Fr_{n,h} \in \pi_1(U)$. We have

$$\det(1 - q^{1/2-s} Fr_{n,h} | H) = \det(1 - q^{1/2-s} Fr_{q^n} | H(\sigma_h))$$

Define

$$G^{\mathrm{arith}} = \overline{Im\left(\pi_1(U) \to \mathrm{GL}(H) \cong \mathrm{GL}_N(\mathbb{Q}_\ell)\right)}$$

where the bar denotes Zariski closure. I.e., G^{arith} is the smallest subgroup of $\mathrm{GL}_N(\mathbb{Q}_\ell)$ defined by polynomials which contains the image.
(Technical point: One also considers

$$G^{\mathrm{geom}} = \overline{Im\left(\pi_1(U \times \overline{\mathbb{F}_q}) \to \mathrm{GL}(H) \cong \mathrm{GL}_N(\mathbb{Q}_\ell)\right)}.$$

A priori $G^{\mathrm{geom}} \subset G^{\mathrm{arith}}$ and in many cases they coincide. For convenience we assume they coincide and denote both by G.)

G is an algebraic group defined over $\mathbb{Q}_\ell$. There is a corresponding complex algebraic group and a maximal compact subgroup K inside it.

3 key examples:

- $G = GL_{N/\mathbb{Q}_\ell}$ $\quad K = U_N$
- $G = O_{N/\mathbb{Q}_\ell}$ $\quad K = O_N(\mathbb{R})$
- $G = Sp_{N/\mathbb{Q}_\ell}$ $\quad K = USp_N$

Given a matrix in G with algebraic eigenvalues (e.g., some $A_{n,h}$) there is a well defined conjugacy class of elements in K with the same eigenvalues. Call it $\theta_{n,h}$.

The main equidistribution result for the $L(\chi_h, s)$ is that

1. $G = Sp_N$
2. As $n \to \infty$, the set of matrices $\{\theta_{n,h} | h \in U(\mathbb{F}_{q^n})\}$ becomes equidistributed in $K = USp_N$ with respect to Haar measure. More precisely, if ϕ is any continuous, conjugation invariant function on K, we have

$$\lim_{n\to\infty} \frac{1}{\# U(\mathbb{F}_{q^n})} \sum_{h \in U(\mathbb{F}_{q^n})} \phi(\theta_{n,h}) = \int_{USp_N} \phi$$

The second part of the main result can be thought of as a black box that comes from Deligne's proof of the Weil conjectures: his work shows that whatever G happens to be, the Frobenius matrices are equidistributed in the corresponding K.
So what is needed to establish the main equidistribution result is to check part 1, namely to compute the monodromy group G and see that it is Sp_N.

Let's warm up with a simple monodromy/Galois group calculation.

Let $F = \mathbb{F}_q(t)$ (or $\mathbb{C}(t)$). Let $K = F(x)$ where

$$h(x) = x^d + x^{d-1} + t = 0.$$

We assume $(q, d) = (q, d-1) = 1$. We want to compute the monodromy group of the extension K/F, or what is the same, the Galois group of the Galois closure of K over F.

We'll see in a minute that the ramification of K/F is all tame. This implies that the monodromy group is generated by the action of a generator of the inertia groups at the ramified points and that these inertia groups are generated by one element each. (Roughly speaking, when the ramification is tame, the picture is just like over $\mathbb{C}$.) [picture]

Computing the discriminant of h, we see that h has distinct roots for all values of t except $t = 0$, $t = a := ((1-d)/d)^d$, and $t = \infty$.

- At $t = 0$, h has a simple root and another root of multiplicity $d - 1$.
- At $t = a$, h has a double root and $d - 2$ simple roots.
- At $t = \infty$ h has one root of multiplicity d.

Since q is prime to d and $d - 1$, this shows that the ramification is tame.

Also, with suitable labels on the fiber, the generator of inertia at 0 acts by the $(d-1)$-cycle $(23 \cdots d)$ and the generator of inertia at a acts by the transposition (12).

The monodromy group is *a priori* a subgroup of S_d. But S_d is already generated by (12) and $(23 \cdots d)$, and so the monodromy group is as large as possible, namely S_d.

Here is what we needed to know to carry out this calculation:

- The structure of the tame fundamental group of $\mathbb{P}^1$ minus a finite set of points: it is generated by generators of inertia at each missing point, and these inertia groups are generated by one element each.
- Action of these generators is determined by ramification information.
- A global fact about S_d, namely it is generated by (12) and $(23 \cdots d)$.

Many calculations of fancier monodromy groups have similar ingredients.

We consider the family of L-functions corresponding to quadratic extensions $K = F_n(\sqrt{h})$ with $F_n = \mathbb{F}_{q^n}(t)$ and h varying through monic square free polynomials of degree d

$$h = t^d + a_1 t^{d-1} + \cdots + a_d \qquad a_i \in \mathbb{F}_{q^n}.$$

We know *a priori* that the monodromy group is contained in Sp_N ($N = d - 1$ or $d - 2$) and we'll show it is actually equal to Sp_N. It will suffice to see that the restriction of this family to polynomials h of the form $t^d + t^{d-1} + a$ with $a \in \mathbb{F}_{q^n}$ already has monodromy Sp_N. (If $V \subset U$ is the subvariety $\{(1, 0, \ldots, a)\}$, then $\pi_1(V) \to \pi_1(U)$ so $Im(\pi_1(V) \to \mathrm{GL}_N) \subset Im(\pi_1(U) \to \mathrm{GL}_N)$.)

The Galois group calculation for the polynomial

$$h = x^d + x^{d-1} + t$$

shows that the ramification in our family is tame. (Details omitted.)

Our monodromy group G is given as a subgroup of GL_N, i.e.,comes equipped with an N-dimensional representation V. We want to know that this representation is irreducible.
By Schur's lemma, V is irreducible iff $\dim End_G(V) = 1$. Katz, using the Weil conjectures, gave a diophantine way to calculate $\dim End_G(V)$. One has to estimate a sum like this:

$$\sum_{a \in \mathbb{F}_{q^n}} (\#C_a(\mathbb{F}_{q^n}) - (q^n + 1))^2$$

and show that it is $q^{2n} + O(q^{3n/2})$ as $n \to \infty$ where $\#C_a$ is the number of solutions to $y^2 = x^d + x^{d-1} + a$.
This estimation can be carried out with character sums, the Weil bound, and the Galois group calculation above.

Some classical algebraic geometry (the Picard-Lefschetz formula) shows that the generator of inertia at the place $a = ((1-d)/d)^d$ acts via a "unipotent pseudoreflection" namely a matrix like this:

$$\begin{pmatrix} 1 & 1 & 0 & \cdots \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \\ \vdots & & & \ddots \end{pmatrix}$$

The next step is to show that G acts "Lie irreducibly," i.e., every finite index subgroup of G acts irreducibly. Equivalently, G acts irreducibly and G is connected.

One shows this using the irreducibility, the existence of a unipotent pseudoreflection in G, and some more analysis of the ramification at $a = 0$ or $a = \infty$. (If not, there is a short list of possible reasons why some finite index subgroup of G could act reducibly, and one rules them out case by case.)

Finally, a general theorem about Lie groups (Kazhdan-Margulis) implies that an algebraic subgroup $G \subset Sp_N \subset GL_N$ which acts Lie irreducibly and contains a unipotent pseudoreflection is in fact equal to Sp_N.

The calculations look daunting, but there is one reassuring fact: it seems to almost always be the case that unless the monodromy has some reason to be small, it is in fact as large as possible (namely is GL_N, O_N or SO_N, or Sp_N). So it is usually possible to guess the monodromy group just from sign considerations on the input data.