BIG SYMPLECTIC MONODROMY: A THEOREM OF C. HALL

E. KOWALSKI (D'APRÈS C. HALL)

For "The large sieve, monodromy and zeta functions of curves", it is important to have criteria to show that, for a family of sheaves of $\mathbf{F}_\ell$-vector spaces with symplectic monodromy, the geometric monodromy groups are maximal for ℓ large enough.

A particular case used in loc. cit. is:

Theorem 1 (J-K. Yu)**.** *Let q be an odd power of a prime p, $f \in \mathbf{F}_q[T]$ a monic squarefree polynomial of degree $2g$. Let $U/\mathbf{F}_q$ be the open subset of the affine line which is the complement of the closed subset of zeros of f, and let $C \xrightarrow{\pi} U$ be the family of hyperelliptic curves*

$$C : y^2 = f(x)(x-t)$$

with $C \to U$ being given by t. For $\ell \neq p$, let $\mathcal{F}_\ell = R^1\pi_!\mathbf{F}_\ell$. Then for $\ell \nmid 2p$, the geometric monodromy group of $\mathcal{F}_\ell$ is the whole symplectic group $\mathrm{Sp}(2g, \mathbf{F}_\ell)$.

Yu's proof, working by lifting to characteristic zero, is still unpublished.

Recently, C. Hall found new techniques to prove that certain monodromy groups modulo ℓ are large. Those were first stated for the case (more difficult) of orthogonal monodromy, but he also quickly found the following symplectic version which suffices to recover the theorem above.

Theorem 2 (C. Hall)**.** *Let $\ell \neq 2$ be a prime number, V a $2g$-dimensional vector space over $\mathbf{F}_\ell$ with a non-degenerate alternating pairing $\langle \cdot, \cdot, \rangle$. Let $G \subset \mathrm{Sp}(V)$ be a subgroup of the corresponding symplectic group. Assume that:*

– G is irreducible, i.e., the only $\mathbf{F}_\ell$-subspaces $W \subset V$ which are invariant under G are $W = 0$ and $W = V$.

– there is some $r \geqslant 1$ and a set of generators $S \subset G$ with all elements $\gamma \in S$ of drop $\mathrm{drop}(\gamma) \leqslant r$.

– G contains one element of drop 1, i.e., G contains a transvection.

Then, denoting by S_0 the subset of S of elements with order divisible by some prime $\ell \leqslant r+1$, we have either

– $G = \mathrm{Sp}(V)$, *or*

– $\dim(V) < 2(r+1)|S_0|$.

In this statement, recall that the *drop* of an endomorphism A of a vector space V over a field k is defined as the codimension of the invariant subspace $V^A = \{v \mid Av = v\}$. An element of drop 1 with determinant 1 is a *transvection*. If A is symplectic for some pairing on V, the orthogonal $(V^A)^\perp$ is equal to $\mathrm{Im}(A-1)$ and is of dimension 1. If r_A is a non-zero generator of this space, it is called a *root* of A. One can write

$$Av = v + \alpha\langle v, r_A\rangle r_A$$

for some $\alpha \in k$. (Note that $r_A \in V^A$ because the pairing is alternating!)

Proof of Th. 1 from Th. 2. We will apply Th.2 with set of generators S given by the local monodromy operators around the finite singularities of U, i.e., the zeros of f. Each of these will turn out to be a transvection, so that one can take $r = 1$ in Th. 2, and because symplectic transvections (over fields of characteristic $\neq 2$) are not of order 2, we have $S_0 = 0$, and therefore the conclusion must be that $G = \mathrm{Sp}(V)$. (In fact, the proof of Th. 2 for an irreducibly group G generated by a set S of transvections is much quicker: one can directly apply the theorem of Zalesskiĭ and Serežkin in the last step (13) below)...

The transvectional nature of local monodromy in this case follows from 3.3.6 of "Rigid local systems" by Katz (knowing that the theory of middle convolution which is developped there for

$\bar{\mathbf{Q}}_\ell$-sheaves works identically for $\bar{\mathbf{F}}_\ell$-sheaves), or by Katz-Sarnak, Lemma 10.1.13 (which works with the $\bar{\mathbf{Q}}_\ell$-sheaf also, but in ways that do not affect the argument for the reduction modulo ℓ, i.e., for our sheaf $\mathcal{F}_\ell$).

The irreducibility of the action of the geometric monodromy group on $\mathcal{F}_\ell$ is more tricky. For *almost all* ℓ, this follows from Lemma 10.1.15 of Katz-Sarnak, since the action is irreducible at the $\bar{\mathbf{Q}}_\ell$ level. For all ℓ, it seems one must refer to 3.3.6 of "Rigid local systems". □

Proof of Th. 2. The proof is divided in many small steps.

– (1) Let $H \subset G$ be a normal subgroup, $W \subset V$ a non-trivial irreducible H-subspace. If $\dim W \geqslant r+1$, then $W = V$.

◇ Indeed, notice that for any $\gamma \in S$, we have $V^\gamma \cap W \neq 0$ because $\mathrm{drop}(\gamma) \leqslant r$. Let $w_0 \in V^\gamma \cap W$, $w_0 \neq 0$. Any $w \in W$ can be expressed as combination of the vectors hw_0 for $h \in H$, since W is H-irreducible. But $w_0 \in V^\gamma$ and H normal in G imply

$$\gamma h w_0 = \gamma h \gamma^{-1} w_0 = h' w_0 \text{ with } h' \in H$$

so $\gamma(hw_0) \in W$ for all h, and therefore $\gamma W \subset W$. As $\{\gamma\} = S$ generates G, it follows that W is a G-subrepresentation, hence irreducibility again gives $W = V$.

Let H and W be as above with $\dim W \leqslant r$. Assume that there is a decomposition in direct sum

$$W = \bigoplus_i g_i W \tag{1}$$

where $\{g_i W\}$ runs over the set X of translates of W by G (i.e., if $H \neq G$, assume that G is *imprimitive*, induced by H acting on W).

– (2) Any subset Y of X containing at least $(r+1)(\dim W)^{-1}$ elements contains at least one γ-orbit (i.e., one orbit of the subgroup generated by γ) for every $\gamma \in S$.

◇ Indeed, we have a direct sum

$$W' = \bigoplus_{L \in Y} L \subset W$$

with $\dim W' \geqslant r+1$, hence again $W' \cap V^\gamma \neq 0$. A non-zero vector in $W' \cap V^\gamma$, when decomposed according to (1), has only non-zero components at some of the elements in Y, say at $Y' \subset Y$. The action of γ sends the non-zero components of v to those of γv; since $\gamma v = v$, this means γ permutes the non-zero components in Y', hence Y' is γ-stable, and in particular contains at least one orbit.

– (3) If $\gamma \notin S_0$, i.e. if the order of γ is not divisible by a prime $\leqslant r+1$, then γ acts trivially on the set X of translates of W.

◇ Indeed, under this assumption any γ-orbit which is not reduced to a single subspace must contain at least $r+2$ elements; but then taking any (proper) subset of $r+1$ elements in this orbit, since $\dim W \geqslant 1$ we would be able to apply step (2) to deduce that this subset contains a γ-orbit, which is a contradiction.

– (4) If there exists a translate $gW \in X$ which is not contained in any γ-orbit for some $\gamma \in S_0$ which does not act trivially on X, then $W = V$.

◇ Indeed, if $W' = gW \in X$ is as stated, we must have $\gamma W' = W'$ for any $\gamma \in S_0$. Since it follows first from (3) that W' is stable by $\gamma \in S - S_0$, we conclude that W' is stable under the action of S, hence under the action of G. By irreducibility, this means $W' = V$ and $W = V$ also.

– (5) If $\gamma \in S_0$, then

$$\sum_i (e_i - 1) < \frac{r+1}{\dim W}$$

where i runs over the γ-orbits in X, and each orbit has e_i elements.

$\diamond$ Let Y be a subset of X constructed by removing one element from each γ-orbit; then Y has $\sum(e_i-1)$ elements and doesn't contain any γ-orbit, so by (2) we must have $|Y| < (r+1)(\dim W)^{-1}$.

– (6) The number N of elements in X which are in γ-orbits containing at least two elements for some $\gamma \in S_0$ is $< 2(r+1)|S_0|(\dim W)^{-1}$.

$\diamond$ For given $\gamma \in S_0$, we have $e_i - 1 \geqslant 1$ for all orbits with at least two elements, hence the number $n(\gamma)$ of those orbits satisfies

$$n(\gamma) \leqslant \sum_i (e_i - 1) < \frac{r+1}{\dim W}$$

by (5). Then again by (5) we get that the total number $N(\gamma)$ of elements of X in the union of those γ-orbits satisfies

$$N(\gamma) = \sum_i e_i = \sum_i (e_i - 1) + n(\gamma) < \frac{2(r+1)}{\dim W}.$$

Finally

$$N = \sum_{\gamma \in S_0} N(\gamma) < \frac{2(r+1)|S_0|}{\dim W}.$$

– (7) If $\dim V \geqslant 2(r+1)|S_0|$, then $W = V$.

$\diamond$ Indeed, if such is the case, the dimension of the space

$$\bigoplus_L L,$$

where L runs over those translates of X counted in (6), is $< \dim V$, hence this space is distinct from V, so the Assumption of (4) holds, and it follows that $W = V$.

Here we summarize what we have found by (1), (4) and (7): either $\dim V < 2(r+1)|S_0|$ or W is primitive, i.e., a decomposition such as (1) does not exist for any normal subgroup $H \subset G$.

Now assume that $\dim V \geqslant 2(r+1)|S_0|$. Let $R \subset G$ denote the subgroup of G generated by the transvections in G.

– (8) R is a non-trivial normal subgroup of G.

$\diamond$ Indeed, G contains at least one transvection by assumption, so R is non-trivial, and the conjugate of a transvection is still one, so that all conjugates of R are contained in R.

– (9) Let $W \subset V$ be a non-zero R-irreducible subspace. Then $W^R = 0$.

$\diamond$ Indeed, the subspace $W^R \subset V$ is a G-subrepresentation because R is normal in G:

$$g \in G,\ r \in R,\ w \in W^R \text{ implies } r(gw) = g(g^{-1}rg)w = g(r'w) = gw,\ \text{i.e., } gw \in W^R.$$

So either $W^R = 0$ or $W^R = V$ by irreducibility, but since R is non-trivial, the second case is impossible.

– (10) The roots of elements of R which lie in W span W.

$\diamond$ Notice first that if $\gamma \in R$ is a transvection, then either γ acts trivially on W, or its roots lie in W: indeed, the space $\mathrm{Im}(\gamma - 1) \cap W$ is either 0 or one-dimensional. In the first case, γ acts trivially (since $\gamma w - w \in \mathrm{Im}(\gamma - 1) \cap W$), and in the second case, the roots (i.e., non-zero elements of $\mathrm{Im}(\gamma - 1)$) are in W. Let S_1 denote the set of transvections in R of the second type, and let $r_\gamma \in W$ denote one root of $\gamma \in S_1$. We have $S_1 \neq \emptyset$, because otherwise all transvections (and hence R itself) act trivially on W, contrary to (9).

Now let W' be the space spanned by the roots r_γ. Then W' is an R-subrepresentation of W: indeed, for $h \in R$, it is easy to see that $hr_\gamma \in W$ is a root of $h^{-1}\gamma h \in R$, which is still a transvection. Since $W' \neq 0$ ($S_1 \neq \emptyset$) we have $W' = W$.

– (11) For any $g \in G$ such that $gW \neq W$, we have $gW \cap W = 0$ and $gW \perp W$.

$\diamond$ Indeed, R normal in G implies that $gW \cap W$ is an R-subrepresentation (because $hgw = g(g^{-1}hg)w$ for $h \in R$, $w \in W$), hence is 0 if $gW \neq W$. Then for any transvection γ with a root in W, γ acts trivially on gW since $gW \cap W = 0$, and this means that the roots of γ are in $(gW)^{\perp}$. Therefore by (10), we have in fact $gW \perp W$.

– (12) The space V is a direct orthogonal sum of the distinct translates of W, i.e., we have a decomposition (1).

$\diamond$ Let $\{gW\}$ be a maximal set of translates of W which are in orthogonal direct sum, and let V' be their direct sum. By G-irreducibility of V, if $V' \neq V$ there exists some other translate g_0W such that g_0W is not contained in V'. In particular for any g (parameterizing the set of translates), we can apply (11) to gW and $g_0g^{-1}(gW)$ in place of W and gW, and conclude that $g_0W \perp gW$, $g_0W \cap gW = 0$. So $g_0W \perp V'$, and moreover $g_0W \cap V'$ is an R-subrepresentation of g_0W, and is therefore either 0 or equal to g_0W. The latter being impossible by assumption (g_0W is not contained in V'), we have $g_0W \cap V' = 0$. All in all, we have constructed a set $\{gW, g_0W\}$ contradicting the stated maximality of $\{gW\}$. So it must have been that $V' = W$ as desired.

– (13) Conclusion: the theorem holds.

$\diamond$ If $\dim V \geqslant 2(r+1)|S_0|$, we have obtained in (12) a decomposition of type (1) for $H = R$ (which is normal in G) and W a non-trivial R-subspace. By (7), this means that $W = V$, i.e., this means that V is an irreducible R-space. Now the group R is generated by symplectic transvections and acts irreducibly on V, and a theorem of Zalesskiĭ and Serežkin implies that $R = \mathrm{Sp}(V)$. As $G \supset R$, we have $G = \mathrm{Sp}(V)$ also. $\square$