TWISTED MODULAR CURVES

MICHAEL D. FRIED

ABSTRACT. Frey and Kani put a particular modular space structure on the space of a space of modular curves that resembles a Hurwitz space structure. We follow up on this, simplifying the group theory so that properties of this space are clear. For the first, Prop. 2.4 shows it is simple to characterize the monodromy group of Frey-Kani covers of degree N (and that it is S_N). In anticipation of other problems bringing the appearance of Frey-Kani covers, a strengthened result puts them on par with our free characterization of covers whose branch cycles are four *dihedral involutions* (§1.1; such covers correspond to a point on the modular curve $X_0(N)$). Second: Prop. 3.7 shows the corresponding Hurwitz space is connected; it has one absolutely irreducible component over $\mathbb{Q}$. Lemma 2.3 is crucial for the first, much easier, part. A strengthened version of it concludes the proof of the second part.

1. STATEMENT OF THE RESULTS

Assume N is odd, and label a conjugacy class in S_N as of type 2^k if it is the conjugacy class of k disjoint 2-cycles. Let $\mathbf{C}_{3\cdot n,n-1,1}$ be the conjugacy classes of type $(2^n, 2^n, 2^n, 2^{n-1}, 2)$ in S_N with $n = (N-1)/2$. Recall also the Nielsen class notation $\boldsymbol{g} \in \mathbf{C}_{3\cdot n,n-1,1}$ to mean in some order the entries of $\boldsymbol{g} = (g_1, \dots, g_5)$ are in the respective conjugacy classes.

1.1. **Basic notation.** It is helpful to call an involution (element of order 2) that fixes exactly one integer of an odd degree representation a *dihedral involution*. The phrase *product one condition* applied to a branch cycle description $\boldsymbol{g}$ to mean the product $g_1 g_2 \cdots g_5$ is one. Let $N_{S_N}(\langle \boldsymbol{g} \rangle) = N_{\boldsymbol{g}}$ be the normalizer in S_N of the group $\langle \boldsymbol{g} \rangle$. Also, H_r is the Hurwitz monodromy group regarded as acting on r-tuples. The subgroup SH_r consisting of elements that fix the order of the conjugacy classes is also of interest.

1.2. **Nielsen classes of Frey-Kani covers.** The problem is to identify the bi-orbits of H_5 and $N_{\boldsymbol{g}}$ on those $\boldsymbol{g} \in \mathbf{C}_{3\cdot n,n-1,1}$ satisfying two conditions.

(1.1a) $\langle \boldsymbol{g} \rangle$ is transitive.
(1.1b) $\boldsymbol{g}$ satisfies the product one condition.

Denote the set of $\boldsymbol{g}$ satisfying 1.1 by $\mathrm{Ni}^*(\mathbf{C}_{3\cdot n,n-1,1})$. The isomorphism class of the group $\langle \boldsymbol{g} \rangle$ is an invariant of the H_5 action. A cover of the Riemann sphere $\mathbb{P}^1_z$ is in $\mathrm{Ni}^*(\mathbf{C}_{3\cdot n,n-1,1})$ if some (and therefore all) branch cycle descriptions from Riemann's Existence Theorem are in $\mathrm{Ni}^*(\mathbf{C}_{3\cdot n,n-1,1})$. Notice all such covers are of genus 0 by Riemann-Hurwitz.

Date: June 1, 2000.
1991 *Mathematics Subject Classification.* Primary 12F05; Secondary 14H40, 14D20, 14E20.
Key words and phrases. Moduli spaces of covers, permutation representations.
Support from NSF #DMS-9622928.

Call a cover $X \to \mathbb{P}^1_z$ (of degree t) a *cyclic isogeny* cover if there is a cyclic (degree t) isogeny $E \to E'$ of elliptic curves such that $X \to \mathbb{P}^1_z$ is equivalent (over $\mathbb{C}$) to the associated cover of Weierstrass normal forms $E/\langle \pm 1\rangle \to E'/\langle \pm 1\rangle$.

Let $\mathrm{Ni}(S_N, \mathbf{C}_{3\cdot n,n-1,1}) = \mathrm{Ni}_N$ be the Nielsen class of $\boldsymbol{g} \in \mathrm{Ni}^*(\mathbf{C}_{3\cdot n,n-1,1})$ with $\langle \boldsymbol{g}\rangle = S_N$: Frey-Kani branch cycles. Call covers in this Nielsen class Frey-Kani covers. §2 establishes that a cover in $\mathrm{Ni}^*(\mathbf{C}_{3\cdot n,n-1,1})$ has monodromy group S_N if and only if it doesn't factor through a nontrivial cyclic isogeny cover. This is simple. Yet, it establishes a principle for the §3 results: There is one $H_5 - S_N$ bi-orbit on Ni_N (Prop. 3.7).

2. Identifying when $\langle \boldsymbol{g}\rangle = S_N$

Consider $\boldsymbol{g}^* \in \mathrm{Ni}_N$. To know $\langle \boldsymbol{g}^*\rangle = S_N$ is equivalent to $\langle \boldsymbol{g}^*\rangle$ being a primitive subgroup of S_N, for it contains a 2-cycle. If N is a prime it is obviously primitive.

Now, suppose it is not primitive. Then, for a divisor t of N, you get a quotient monodromy group for another cover of $\mathbb{P}^1$ of degree t through the action of the branch cycles on a system of imprimitivity. Let $\boldsymbol{g} \in S_t$ be the result of applying $\boldsymbol{g}^*$ to the t elements in the system of imprimitivity.

Proposition 2.1. *The quotient monodromy group of degree t corresponds to a cover of $\mathbb{P}^1$ whose branch cycles are four dihedral involutions in S_t. There is one braid orbit on these absolute Nielsen classes. A representative of that orbit has the shape $(g_1, g_2, g_2^{-1}, g_1^{-1})$:*

$$g_1 = (1\,t{-}1)(2\,t{-}2)\dots(t{+}1)/2\,(t{+}1)/2), g_2 = (1\,t)(2\,t{-}1)(3\,t{-}2)\dots. \tag{2.1}$$

In particular, a cover $X \in \mathbb{P}^1_z$ in Ni_N whose monodromy group is not primitive factors through a cyclic isogeny cover of degree t.

2.1. **Two auxiliary lemmas.** Two lemmas contribute to this proposition. The first is in my Schur conjecture paper [Fri70].

Lemma 2.2. *Suppose $g_1, g_2 \in S_t$ are dihedral involutions and $\langle g_1, g_2\rangle$ is transitive (in S_t). Then, up to conjugation by an element of S_t, (g_1, g_2) are given in* (2.1).

Lemma 2.3. *Consider $g_1, \dots, g_4 \in S_t$ four dihedral involutions that generate a transitive subgroup of S_t and satisfy the product one condition. After applying an element of H_4 we may assume $\langle g_1, g_2\rangle$ is transitive. Further, $\langle g_1, \dots, g_4\rangle$ is the dihedral group of degree t. Any cover having such a branch cycle description is a cyclic isogeny cover.*

Proof. Assume not. Write $g_1 = g_1' a_1, g_2 = g_2' a_1$ where a_1 is the product of all disjoint cycles that repeat in g_1 and g_2. Then, Lem. 2.2 shows $g_1' g_2'$ is a product $\beta_1 \cdots \beta_u$ where β_i is a cycle on each full orbit of $\langle g_1', g_2'\rangle$. From the product one condition, $g_3 g_4$ is $\beta_u^{-1} \cdots \beta_1^{-1}$. Thus, $g_3 = g_3' a_3$ and $g_4 = g_4' a_3$, with a_3 the disjoint cycles repeated in g_3 and g_4. Also, the orbits of $\langle g_3', g_4'\rangle$ are the same as those of $\langle g_1', g_2'\rangle$. In particular, the orbits of $\langle a_1, a_3\rangle$ are disjoint from the orbits of $\langle g_1', g_2'\rangle$. So, there are only two possibilities, $\langle g_1', g_2'\rangle$ is transitive or $\langle a_1, a_3\rangle$ is transitive. Thus, by this argument the full group equals $\langle g_1, g_2\rangle$.

The transitivity of H_4 (actually of SH_4) and the identification of these covers with cyclic isogeny covers is in [Fri78] in support of finding all rational functions of prime degree having the Schur property. In outline: From the product one condition, the pair (g_3, g_4) is conjugation of the pair (g_2^1, g_1^{-1}) by some

power of the t-cycle $g_\infty = (1\,2\,\ldots t)$. We have only to braid $(g_1, g_2, g_2^{-1}, g_1^{-1})$ to $(g_1, g_2, (g_2')^{-1}, (g_1')^{-1})$ where (g_1', g_2') are conjugation of (g_1, g_2) by g_∞^j for some j. This is easy: Lemma 3.6. □

2.2. **Proof of Prop. 2.1.** Consider $\boldsymbol{g}^* \in \mathrm{Ni}_N$ and let $\boldsymbol{g}$ be its action on a system of imprimitivity. The previous lemmas give us the conclusion if $\boldsymbol{g}$ consists of four dihedral involutions. Factor a cover $X \to \mathbb{P}^1_z$ into $X \to Y \to \mathbb{P}^1_z$ with $Y \to \mathbb{P}^1_z$ corresponding to the system of imprimitivity. Let $z_1, \ldots, z_5 = \boldsymbol{z}$ be the branch cycles of $X \to \mathbb{P}^1_z$ corresponding to $\boldsymbol{g}^*$, relative to a set of appropriate paths on $\mathbb{P}^1_z \setminus \{\boldsymbol{z}\}$. So, $\boldsymbol{g}$ are the branch cycles corresponding to $Y \to \mathbb{P}^1_z$. Suppose z_5 corresponds to the 2-cycle. If $Y \to \mathbb{P}^1_z$ were ramified over z_5, then g_5 would have at least N/t disjoint 2-cycles, instead of just 1.

Consider any g^* from $g_1^*, \ldots, g_4^*$. We show g (its corresponding branch cycle for $Y \to \mathbb{P}^1_z$) is also a dihedral involution. It is of order 2, and so its index is at most $\frac{t-1}{2}$. This is true for each. Now apply Riemann-Hurwitz to the irreducible cover $Y \to \mathbb{P}^1_z$. The genus of Y is $g(Y)$ where

$$2(t + g(Y) - 1) = \sum_{i=1}^{4} \mathrm{ind}(g_i). \tag{2.2}$$

Since $g(Y) = 0$, this says that each of $\mathrm{ind}(g_i) = \frac{t-1}{2}$: These are, indeed, dihedral involutions.

2.3. **Producing Frey-Kani covers from cyclic isogenies.** Suppose $g_1, \ldots, g_4$ is a branch cycle description from a cyclic isogeny cover of degree N. Choose any 2-cycle β in g_4. Now separate g_4 into two pieces (g_4^*, β) where g_4^* consists of all the two cycles in g_4 excluding β. Consider: $\boldsymbol{g}^* = (g_1, g_2, g_3, g_4^*, \beta)$ and let G^* be $\langle \boldsymbol{g}^* \rangle$. For each divisor t of N there is a (unique) system of imprimitivity consisting of t elements. Then, it makes sense to ask if β permutes elements within one of these sets of imprimitivity; we say β preserves a set of imprimitivity. Here is the effect of the operation in going from $(\boldsymbol{g}, \beta)$ to $\boldsymbol{g}^*$ according to Prop. 2.1.

Proposition 2.4. *The group G^* is S_N if and only if β preserves no set of imprimitivity. More generally, let t be the smallest integer such that β preserves a set of imprimitivity. Then, G^* is the wreath product of $S_{N/t}$ by the dihedral group D_t acting through S_t.*

Proof. The first sentence is from Prop. 2.1. As in the discussion above, we have $X \to Y \to \mathbb{P}^1_z$ where $Y \to \mathbb{P}^1_z$ is a cyclic isogeny cover of degree t as given by the statement of the proposition, and $X \to Y$ factors through no cyclic isogeny cover. Further, we decipher the branch cycle type of the cover $X \to Y$ from the computations of §2.2; use the notation from that.

I explain why $X \to Y$ is a Frey-Kani cover (of degree N/t with group $S_{N/t}$). Let z' be any one of the points $z_1, \ldots, z_4$. The unique unramified point of Y lying over z' is the only branch point of $X \to Y$ lying over z'. Further, the unique ramified point of X lying over z_5 has image in Y the 5th branch point of $X \to Y$. Thus, Prop. 2.1 says $X \to Y$ is a Frey-Kani cover.

The geometric monodromy group G_X of $X \to \mathbb{P}^1_z$ is therefore a subgroup of the wreath product $S_{N/t} \wr D_t$ with these properties [Fri70, §3].

(2.3a) G_X maps surjectively to D_t.

(2.3b) The preimage H_X in G_X of the identity in D_t is a subgroup of $S_{N/t}^t$ whose projection on each factor is all of $S_{N/t}$.

To The whole wreath product follows if H_X contains $\overbrace{1 \times \cdots \times 1}^{t-1 \text{ times}} \times S_{N/t}$.

Take the branch cycle for z_5 (with no loss) as $\overbrace{1 \times \cdots \times 1}^{t-1 \text{ times}} \times \beta$ with β a 2-cycle. Also, H_X acts like $S_{N/t}$ on its restriction to the last set of imprimitivity. Thus, it conjugates β around to give $\overbrace{1 \times \cdots \times 1}^{t-1 \text{ times}} \times S_{N/t}$. □

3. H_5 orbits on Frey-Kani covers

This section establishes that there is one orbit of $H_5 - S_N$ on the Nielsen class Ni_N of branch cycle descriptions of Frey-Kani covers. The heart of the argument is simply a converse to the argument of §2.3. That is, given $\boldsymbol{g} \in \mathrm{Ni}_N$ we show there is a $Q \in H_5$ (very explicit) so that $Q(\boldsymbol{g}) = \boldsymbol{g}^*$ has the following properties.

(3.1a) g_1^*, g_2^*, g_3^* are all dihedral involutions.
(3.1b) $g_4^* g_5^*$ is also a dihedral involution.

Assume for notational simplicity that entries of $\boldsymbol{g}$ are in the conjugacy classes of $\mathbf{C}_{3\cdot n, n-1, 1}$ in the given order. This breaks into cases over the following criteria:

(3.2a) $\langle g_1, g_2 \rangle$ is or is not transitive.
(3.2b) g_5 has integers in common with the support of none, one or two disjoint 2-cycles of g_4.

To be a Frey-Kani cover requires the 2-cycle g_5^* does not map any subset of imprimitivity for $\langle g_1^*, g_2^*, g_3^*, g_4^* g_5^* \rangle = H$ into itself. Call $g_5^* = g$ *primitive relative to* H, a notion that makes sense for any transitive subgroup H of S_N: $\langle H, g \rangle$ is a primitive subgroup of S_N. A later argument uses the following obvious practical criterion for that. In the remainder of this section, $g_\infty = (1\,2\,\ldots\,N)$.

Lemma 3.1. *Let $g = (i\,j) \in S_N$. Then, g is primitive for $\langle g_\infty \rangle$ if and only if $(i - j, N) = 1$.*

3.1. **$\langle g_1, g_2 \rangle$ is transitive in (3.2).** Apply Lemma 2.2. Since $\langle g_1, g_2 \rangle$ is transitive, $g_1 g_2$ is an N-cycle, and therefore so is $g_3 g_4 g_5$. Further, we can braid $(g_1, g_2, g_3 g_4 g_5)$ to standard form. So, what we now want to show is that we can braid the 4-cycle $(g_1 g_2, g_3, g_4, g_5) = (g^*, g_3, g_4, g_5)$ to where the result has the 2-cycle g_5 having no common support with any 2-cycle of g_4. In that case, up to an obvious braiding, we can braid the 3-tuple $(g^*, g_3, g_4 g_5)$ to the normal form given by (2.1). That there is one braid orbit on Ni_N / S_N is then clear.

The alternatives appear in (3.2b). The case $n = 5$ appeared as a delicate diophantine problem in [DF99], the exceptional case for a general result about Hilbert's Irreducibility Theorem. It is instructive to have a listing here, for it shows the way to the result.

3.1.1. *Listing of* Ni_N/S_N *for* $N = 5$. The following list is of elements in Ni_5/S_5 having branch cycles in the fixed order given by $\mathbf{C}_{3\cdot 2,1,1}$.

$$\begin{array}{ll} \text{a) } ((2\,3)(4\,5),(1\,2),(1\,4)) & \text{b) } ((2\,3)(4\,5),(1\,4),(2\,4)) \\ \text{c) } ((2\,3)(4\,5),(2\,4),(1\,2)) & \text{d) } ((2\,5)(3\,4),(1\,2),(3\,5)) \\ \text{e) } ((2\,5)(3\,4),(3\,5),(1\,2)) \quad . & \end{array} \tag{3.3}$$

Consider any dihedral involution: Take it with no loss to be

$$g_2 = (1\,2)(3\,N)(4\,N-1)\dots(\frac{N+5}{2}\,\frac{N+1}{2}). \tag{3.4}$$

As in §2.3, form (g_1, g^*, β) with $\beta = (1\,2)$ and $g^* = g_2\beta$, the same as g_2 except for the removal of β and $g_1 = (2\,N)(3\,N-1)\dots(\frac{N+1}{2}\,\frac{N+3}{2})$. This agrees when $N = 5$ with (3.3e); with (3.3d) the case of removing the other 2-cycle. Note: All others from (3.3) have β with support in exactly one (there is only one!) 2-cycle of g_2.

3.1.2. *Outline of the approach.* The key calculation is the braid action B_3 on 3-tuples (g', h', β') with these properties:

(3.5a) (g', h', β') are conjugacy classes of type $(2^n, 2^{n-1}, 2)$ (in that order); and
(3.5b) $g'h'\beta' = g_\infty$.

The next lemma shows $g_\infty\beta'$ is a product of two disjoint cycles. These represent orbits for $\langle g', h'\rangle$ — of even and odd length — each tied to a standard Chebychev polynomial cover. The following lemma gives B_3 braiding between the branch cycles for different β' appearing in (3.5).

Lemma 3.2. *Let* (g', h', β') *be as in* (3.5). *Then,* $\langle g', h'\rangle = G_{\beta'}$ *has two orbits* S_1, S_2 *in its action on* $\{1, 2, \dots, N\}$. *Further, restricting* $(g', h', (g_\infty\beta')^{-1})$ *to each* S_i *gives a standard Chebychev branch cycle description, unique up to conjugation by some power of* g_∞ *restricted to* S_i, $i = 1, 2$. *Further,* $\langle g', h', \beta'\rangle = S_N$ *if and only if* β' *is primitive relative to* $G_{\beta'}$. *This last holds if and only if* $(|S_1|, |S_2|) = 1$.

Proof. Multiply an N-cycle and a 2-cycle together, as in $g_\infty\beta$, and you get two disjoint cycles: $(i\,i{+}1\dots j{-}1)(j\,j{+}1\dots i{-}1)$ if $\beta' = (i\,j)$. (There is an understanding here that one of those two disjoint cycles will cycle around N back to 1.) Clearly, $(g', h', (g_\infty\beta')^{-1})$ satisfies the product one condition and $G_{\beta'}$ has at most two orbits, those for $g_\infty\beta'$. Suppose $G_{\beta'}$ has exactly one orbit. Then, we can apply Riemann-Hurwitz and compute the genus g^* of the an irreducible cover of $\mathbb{P}^1_z$ with branch cycles $(g', h', (g_\infty\beta')^{-1})$ from the following formula: $2(N{+}g^*{-}1) = n{+}n{-}1{+}N{-}2$. Thus g^* would be negative: a contradiction.

Now restrict $(g', h', (g_\infty\beta')^{-1})$ to each of the orbits: ${}^i\boldsymbol{g}$ is the result on restriction to S_i, $i = 1, 2$. From [Fri70] (odd degree case; even, however, is similar) these are branch cycles for polynomial covers given by Chebychev polynomials, and given ${}^ig_3$ (g_∞ restricted to S_i), this determines $({}^ig_1, {}^ig_2)$ (on even degree orbit they are different conjugacy classes, so keep the given order of these conjugacy classes) up to conjugation by ${}^ig_3$.

The statement that $\langle g', h', \beta'\rangle = S_N$ if and only if β' is primitive relative to $G_{\beta'}$ is in Prop. 2.4. The proof of that was an application of Lemma 3.1. Now, $\beta' = (i\,j)$ preserves a set of imprimitivity for g_∞ if and only if $(i - j, N) > 1$. The lengths of the orbits S_1 and S_2 are exactly $i - j$ and $N - (i - j)$ (in some order). These two numbers are relatively prime if and only if $i - j$ and N are relatively prime. □

3.2. **Braiding among Lemma 3.2 elements.** Suppose $\boldsymbol{g} \in \mathrm{Ni}_N/S_N$ is a Frey-Kani branch cycle. Call $\boldsymbol{g}$ *dihedral transitive* if some two of the dihedral elements of $\boldsymbol{g}$ generate a transitive subgroup of S_N. In particular, this includes the condition that $\langle g_1, g_2\rangle$ is transitive in (3.2). Denote the collection of dihedral transitive elements in Ni_N by Ni_N^+. Further, denote the elements of Ni_N^+ that have entries in the conjugacy classes $\mathbf{C}_{3\cdot n,n-1,1}$ in the given order by SNi_N^+.

Proposition 3.3. *One H_5 orbit on Ni_N contains Ni_N^+.*

The proof apparently also shows one SH_5 orbit SNi_N contains SNi_N^+, though we are not careful about establishing that here.

3.2.1. *Preliminary lemmas for proving Prop. 3.3.* [BF82, Lemma 3.8] has the following observation. Recall: SB_r is the kernel of the standard representation $B_r \to S_r$ of the braid group.

Lemma 3.4 (Product One)**.** *Let $\mathrm{Ni}(G,\mathbf{C})$ be any Nielsen class with r conjugacy classes. Then, for any $h \in G$ and $\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})$ there exists $Q = Q_{h,\boldsymbol{g}} \in SB_r$ for which $(\boldsymbol{g})Q = h\boldsymbol{g}h^{-1}$.*

Lemma 3.5 (Blocks Lemma)**.** *Suppose $\boldsymbol{g} = (\boldsymbol{g}_1, \dots, \boldsymbol{g}_u)$ and $\boldsymbol{g}_i$ satisfies the product one condition, $i = 1, \dots, u$. Consider $\tau_i \in \langle \boldsymbol{g}_i\rangle$ for some i. For any $\pi \in S_u$, there exists $Q \in B_r$ with $(\boldsymbol{g})Q = (\boldsymbol{g}_{(1)\pi}, \dots, \boldsymbol{g}_{(u)\pi})$. Also, for any i and j, there exists $Q \in B_r$ with*

$$(\boldsymbol{g})Q = (\boldsymbol{g}_1, \dots, \boldsymbol{g}_{j-1}, \tau_i\boldsymbol{g}_j\tau_i^{-1}, \boldsymbol{g}_{j+1}, \dots, \boldsymbol{g}_u).$$

Proof. The case $u = 2$ suffices to show we can permute the appearance of the $\boldsymbol{g}_i$ s. For this, braid every entry of $\boldsymbol{g}_1$, in order from left to right, past every entry of $\boldsymbol{g}_2$. This gives the effect of

$$Q(\boldsymbol{g}_1, \boldsymbol{g}_2) = (\alpha\boldsymbol{g}_2\alpha^{-1}, \boldsymbol{g}_1), \alpha = \Pi(\boldsymbol{g}_1). \tag{3.6}$$

Since $\alpha = 1$, we are done.

The final conclusion reduces to the case $u = 2$. The essential two cases are $i = j = 1$ and $i = 1$, $j = 2$. For the first, apply the Products One Lemma to $\boldsymbol{g}_1$. For the second, the Products One Lemma produces $Q' \in B_r$ with $Q'(\boldsymbol{g}_1, \boldsymbol{g}_2) = (\tau_1\boldsymbol{g}_1\tau_1^{-1}, \tau_1\boldsymbol{g}_2\tau_1^{-1})$. Now apply the Products One Lemma to the first block to conjugate that by τ_1^{-1}. □

Lemma 3.6. *Let $\boldsymbol{g}_i$ be an r_i-tuple, $i = 1, 2$, with $(\boldsymbol{g}_1, \boldsymbol{g}_2)$ satisfying the product one condition. Denote the product (in order) of the entries of $\boldsymbol{g}_i$ by $\Pi(\boldsymbol{g}_i) = a_i$. Then, there exists $Q = Q_k \in B_{r_1+r_2}$ with $(\boldsymbol{g}_1, \boldsymbol{g}_2)Q = (\boldsymbol{g}_1, a_1^k\boldsymbol{g}_2a_1^{-k})$ for each integer k.*

Proof. This is an easy lemma based on producing two elements $Q_1, Q_2 \in B_{r_1+r_2}$ with the following properties:

(3.7a) $(\boldsymbol{g}_1, \boldsymbol{g}_2)Q_1 = (a_1\boldsymbol{g}_2a_1^{-1}, \boldsymbol{g}_1)$; and
(3.7b) $(\boldsymbol{g}_1, \boldsymbol{g}_2)Q_1 = (\boldsymbol{g}_2, \boldsymbol{g}_1)$.

The last of these uses the product one condition, in the form that you can braid from $(h, \boldsymbol{g})$ to $(\boldsymbol{g}, \Pi(\boldsymbol{g})^{-1}h\Pi(\boldsymbol{g}))$. The product one condition, however, implies

$$\Pi(\boldsymbol{g})^{-1}h\Pi(\boldsymbol{g}) = (h\Pi(\boldsymbol{g}))^{-1}h(h\Pi(\boldsymbol{g})) = h.$$

Now we note how these imply the lemma. First: Applying Q_1 and Q_2 shows it holds in the case $k = 1$. To iterate this k times requires only noting that $\Pi(a_1 \boldsymbol{g}_2 a_1^{-1}) = \Pi(\boldsymbol{g}_2)$. □

3.2.2. *Proof of Prop. 3.3.* It is trivial to use H_5 to permute the conjugacy classes of elements of Ni_N around. So we may assume with no loss that an H_5 orbit has a representative with the conjugacy classes in any desirable order. Given $\boldsymbol{g}$ in the form where (g_1, g_2) is transitive, apply Lemma 3.4 to assume $g_1 g_2 = (1 \ldots N) = g_\infty$. Apply Lemma 3.6 to replace either (g_1, g_2) (or (g_3, g_4, g_5)) by a conjugate of this tuple by any power of g_∞. Now consider where (g_1^*, g_2^*) are in standard form as in (2.1) (with N replacing t). Further, consider $(g_1^*, g_2^*, g_3^*, g_4^*, g_5^*) = \boldsymbol{g}^*$ with $(g_5^* g_4^*, g_3^*)$ in standard form (g_5 has been pulled from a primitive 2-cycle in g_4^*).

Completing the proof of transitivity of H_5 therefore requires only showing how to braid from $\boldsymbol{g}^*$ to a target of one of the standard forms for Lemma 3.2. Again, apply Lemma 3.6 to assume the target has this shape $(g_1^*, g_2^*, g_3, g_4, g_5)$ with g_5 a primitive 2-cycle and the following holds.

(3.8) $\langle g_3, g_4 \rangle$ has two orbits S_1, S_2, with restriction of the pair (g_4, g_3) to each in standard form (with $|S_1|$ odd).

With such explicit forms it is now easy to braid from $\boldsymbol{g}^*$ to the target.

3.3. $\langle g_1, g_2 \rangle$ **is not transitive.** The basic result will be complete if we show $\mathrm{Ni}_N^+ = \mathrm{Ni}_N$. That is, given any element of Ni_N there is a braid of it to an element that is dihedral transitive. Suppose $\boldsymbol{g} \in \mathrm{Ni}_N$ with the entries in $\mathbf{C}_N$ in standard order is not dihedral transitive. Consider the idea of Lemma 2.3. Write (g_1, g_2) as $(g_1' a_1, g_2' a_1)$ where $a_1 \neq 1$ is the maximal set of disjoint 2-cycles in common to g_1 and g_2. Then, $g_1 g_2 = g_1' g_2' = g'$ is a product of u disjoint cycles on the integers $\{1, \ldots, N'\}$, with each disjoint cycle representing an orbit of $\langle g_1', g_2' \rangle$. The remainder of the argument divides into subsections according to the relation between the support of g_5 and the orbits of $\langle g_1', g_2' \rangle$.

3.3.1. $g_1' = 1$. Then, $g_3 = (g_4 g_5)^{-1}$. Since g_3 is a dihedral involution, so is $g_4 g_5$; g_4 results from plucking a 2-cycle from a dihedral involution. In particular, $\langle g_1, \ldots, g_5 \rangle$ transitive implies $\langle g_1, g_3 \rangle$ is transitive, contrary to assumption.

3.3.2. *Assume $g_1' \neq 1$; support of g_5 is in $\{1, \ldots, N'\}$ or $\{N'+1, \ldots, N\}$.* Similarly, write $g_3 = g_3' a_2$ and $g_4 = g_4' a_2$ where a_2 is the maximal set of disjoint 2-cycles in common to g_3 and g_4. Then, $(g_5 g', g_3', g_4')$ satisfies the product one condition. There are several cases.

(3.9a) g_5 support is in just one of the $\langle g_1', g_2' \rangle$ orbits.
(3.9b) g_5 support joins two $\langle g_1', g_2' \rangle$ orbits.
(3.9c) g_5 support is outside $\{1, \ldots, N'\}$.

Consider (3.9a) and (3.9b). As in Lemma 2.3, these imply one of the following conditions. Either $\langle g_5, g_1', g_2', g_3', g_4' \rangle$ have orbits in $\{1, \ldots, N'\}$, and $\langle a_1, a_2 \rangle$ have orbits entirely outside $\{1, \ldots, N'\}$, or $a_1 = a_2 = 1$ and $\langle g_1, g_2 \rangle$ is transitive. The former is contrary to transitivity of $\boldsymbol{g}$. The latter is contrary to our assumption that $\langle g_1, g_2 \rangle$ is not transitive. A similar orbit argument excludes condition (3.9c).

3.3.3. *g_5 support joins a $\langle g_1', g_2'\rangle$ orbit to an integer outside $\{1,\dots,N'\}$.* For notational simplicity assume $g_5 = (1\,N'+1)$. Checking orbits now shows the following conditions hold.

(3.10a) $\langle g_1', g_2'\rangle$ has one orbit on $\{1,\dots,N'\}$.
(3.10b) $\langle g_3', g_4'\rangle$ has one orbit on $\{1,\dots,N'+1\}$.
(3.10c) The orbits of a_2 fall outside $\{1,\dots,N'+1\}$ and the orbits of a_1 fall outside $\{1,\dots,N'\}$.
(3.10d) $\langle a_1, a_2\rangle$ is transitive on $\{N'+1,\dots,N\}$.

Here, however, the product one condition implies that at least two elements from $\boldsymbol{g}$ must join the sets $\{1,\dots,N'\}$ and $\{N'+1,\dots N\}$.

Proposition 3.7. *There is one H_5 orbit for the action of* Ni_N.

Proof. The proof is done if we can braid (3.10) to a case where the 5-tuple contains two dihedral involutions generating a transitive group. Here is an instructive example of this occurring with $N'=5$, $N=9$:

$$(g_1', g_2', g_3', g_4')) = ((1\,5)(2\,4), (5\,2)(3\,4), (1\,5)(4\,6)(2\,3), (1\,4)(6\,3)).$$

$$\begin{array}{c}((1\,5)(2\,4)(6\,9)(7\,8), (5\,2)(3\,4)(6\,9)(7\,8),\\ (1\,5)(4\,6)(2\,3)(9\,7), (1\,4)(6\,3)(9\,7), (1\,6)).\end{array} \tag{3.11}$$

Here, however, we immediately see $\langle g_2, g_3\rangle$ is transitive. The general case works the same way. □

References

[BF82] R. Biggers and M. Fried, *Moduli spaces of covers and the Hurwitz monodromy group*, Crelles J. **335** (1982), 87–121.
[DF99] P. Dèbes and M. Fried, *Integral specialization of families of rational functions*, PJM (1999).
[Fri70] M.D. Fried, *On a conjecture of Schur*, Mich. Math. J. **17** (1970), 41–55.
[Fri78] M.D. Fried, *Galois groups and complex multiplication*, Trans.A.M.S. **235** (1978), 141–162.

UC Irvine, Irvine, CA 92697, USA
E-mail address: mfried@math.uci.edu