It's hard to do better than rigidity

Béranger Seguin

November 15, 2023

Abstract. Let G be a finite group, K be a number field, n be an integer. In this short note, we prove that if C is an irreducible family of branched G-covers of $\mathbb{P}^1$ containing covers defined over C branched at each subset $S \subset K$ of size n, then a cover in C is determined by its branch points. In other words, any construction of regular G-extensions of $\mathbb{Q}(T)$ which works for all choices of branch points is doing something similar to the rigidity method. We use this result to show that there exist four rational numbers such that no regular realization of $\mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$ as a Galois group over $\mathbb{Q}(T)$ is ramified exactly at these four points.

Let G be a finite group, n be an integer, and $\mathcal{H}$ be the Hurwitz space classifying non-marked G-covers of $\mathbb{P}^1$ equipped with n distinct labeled points of $\mathbb{A}^1$ outside which the cover is unramified. The $\mathbb{Q}$-scheme $\mathcal{H}$ is a finite étale cover of the configuration space PConf_n of n distinct labeled points of $\mathbb{A}^1$, which is the open subscheme of $\mathbb{A}^n_{\mathbb{Q}}$ obtained by removing the "big diagonal" (the closed subscheme corresponding to any equality between two points). The study of rational points of $\mathcal{H}$ is central in inverse Galois theory: indeed, if K is a number field and the group G retracts on its center[1], K-points of $\mathcal{H}$ correspond to Galois extensions $F|K(T)$ of group G which are regular (i.e. $F \cap \bar{\mathbb{Q}} = K$) and have n ramified primes, all of degree 1. Moreover, these extensions may be specialized into G-extensions of K by Hilbert's irreducibility theorem. One of the key tools to find rational points on Hurwitz spaces is the rigidity criterion, introduced by Thompson to realize the Monster group as a Galois group over $\mathbb{Q}$.

Deterministic components. Let C be a geometrically connected component of $\mathcal{H}$. We say that C is *deterministic* if the étale cover $C \to (\mathrm{PConf}_n)_{\bar{\mathbb{Q}}}$ is of degree 1, i.e., for every $\underline{t} \in \mathrm{PConf}_n(\bar{\mathbb{Q}})$ there is a unique cover branched at $\underline{t}$ belonging to $C(\bar{\mathbb{Q}})$. If C is deterministic and defined over a number field K, then the unique point above any configuration $\underline{t} \in \mathrm{PConf}_n(K)$ is automatically K-rational, so that finding a deterministic component defined over K implies the existence of K-points in $\mathcal{H}$. We define the following set:

$$\Sigma = \left\{ (g_1, \dots, g_n) \in G^n \,\middle|\, g_1 \cdots g_n = 1 \text{ and } \langle g_1, \dots, g_n \rangle = G \right\}.$$

and we say that a tuple $(g_1, \dots, g_n) \in \Sigma$ is *deterministic* if it is conjugate to every tuple in its orbit under the Hurwitz action of the pure braid group PB_n; one only needs to check this for the $\binom{n}{2}$ standard generators of PB_n. Via the choice of distinguished generators of the fundamental group of the n-punctured sphere, we have a bijection between deterministic components of $\mathcal{H}$ and PB_n-orbits (equivalently, $\mathrm{Inn}(G)$-orbits) of deterministic tuples. Note that the "standard Hurwitz curve" obtained from a deterministic component by fixing all branch points except t_1 is isomorphic to $\mathbb{P}^1 \setminus \{t_2, \dots, t_n\}$, and therefore is of genus zero. Note also that deterministic components correspond to the case $U = \mathrm{PB}_n$ of the more general definition [MM99, III 5.1 (5.8)].

Relation with rigidity. Let $\underline{c} = (c_1, \dots, c_n)$ be a list of conjugacy classes of G. Let $\mathcal{H}_{\underline{c}}$ be the subscheme of $\mathcal{H}$ classifying covers with monodromy conjugacy classes at the branch locus $\underline{t} = (t_1, \dots, t_n)$ given by $(c_1, \dots, c_n)$. The list $\underline{c}$ is *rigid* if $\Sigma_{\underline{c}} = \Sigma \cap (c_1 \times \cdots \times c_n)$ is a single orbit

[1] i.e., the identity $Z(G) \to Z(G)$ extends to a morphism $G \to Z(G)$; equivalently, $Z(G)$ is a direct factor of G. Noteworthy examples are G centerless or abelian, e.g. G simple.

for the conjugacy action of G. This amounts to two simultaneous things, that we think are worth separating:

1. $\mathcal{H}_{\underline{c}}$ is geometrically connected, i.e. $\Sigma_{\underline{c}}$ consists of a single PB_n-orbit
2. Assuming 1., the geometrically connected component $\mathcal{H}_{\underline{c}}$ of $\mathcal{H}$ is deterministic.

These two hypotheses serve different goals: as we have seen, that a component is deterministic (point 2.) lets one find K-rational points when the component is defined over K. That $\mathcal{H}_{\underline{c}}$ is geometrically connected is used to obtain a component with a known field of definition: indeed, the smallest field of definition of $\mathcal{H}_{\underline{c}}$ is the smallest cyclotomic extension of $\mathbb{Q}$ over which the conjugacy classes $c_1, \ldots, c_n$ are all rational. In some ways, the usual rigidity criterion is rigid in two different ways: since there is a single component C in $\mathcal{H}_{\underline{c}}$, it can only be mapped onto itself by $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$ and therefore C is defined over K; and since there is a single point in C above any configuration $\underline{t} \in \mathrm{PConf}(K)$, this point can only be mapped onto itself by $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$ and therefore is K-rational.

Main result. Let K be a number field. A celebrated theorem of Thompson says: if G retracts on its center and if $(c_1, \ldots, c_n)$ is a rigid tuple of K-rational conjugacy classes of G, then for every $\underline{t} \in \mathrm{PConf}_n(K)$ there is a unique regular field extension of $K(T)$ with Galois group G unramified outside $\underline{t}$ whose monodromy conjugacy class at t_i is c_i. Our main result is a sort of converse:

THEOREM. — *Let C be a geometrically connected component of $\mathcal{H}$. If above every configuration $\underline{t} \in \mathrm{PConf}_n(\mathbb{Q})$ there is a K-point in the component C, then C is deterministic.*

Proof. Since C contains K-points, it is defined over K: we have a finite étale K-morphism p from C to the quasi-affine smooth scheme $(\mathrm{PConf}_n)_K$. By Hilbert's irreducibility theorem, there is a K-point $\underline{t} \in \mathrm{PConf}_n(\mathbb{Q})$ above which the fiber is irreducible over K, i.e. the elements of the finite set $C_{\underline{t}} = p^{-1}(\underline{t}) \subseteq C(\bar{\mathbb{Q}})$ are permuted transitively by $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$. By hypothesis, there is a K-point x in $C_{\underline{t}}$. The action of $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$ on $C_{\underline{t}}$ is transitive and has a fixed point x; this implies $C_{\underline{t}} = \{x\}$ and therefore p is a cover of degree 1. □

We also prove a variant using the language of thin sets:

THEOREM. — *Let K be a Hilbertian field (e.g. a number field), n be an integer. Assume that for every $S \in \mathrm{PConf}_n(K)$ there is a regular G-extension of $K(T)$ unramified outside S. There there is an n-tuple $(g_1, \ldots, g_n) \in \Sigma$ which is deterministic and such that the corresponding component of $\mathcal{H}$ is defined over K.*

Proof. Denote by p the étale map $\mathcal{H} \to \mathrm{PConf}_n$. Let $\mathcal{H}_1, \ldots, \mathcal{H}_r$ be the geometrically irreducible components of $\mathcal{H}$ defined over K. We have $\mathcal{H}(K) = \bigsqcup_{i=1}^r \mathcal{H}_i(K)$. Moreover, by the hypothesis, we have $p(\mathcal{H}(K)) = \mathrm{PConf}_n(K)$. Let $\Delta = \mathbb{A}^n(K) \setminus \mathrm{PConf}_n(K)$, which is a proper Zariski-closed subset of $\mathbb{A}^n(K)$. Then:

$$\mathbb{A}^n(K) = \Delta \cup \mathrm{PConf}_n(K) = \Delta \cup p(\mathcal{H}(K)) = \Delta \cup \bigcup_{i=1}^{r} p_i(\mathcal{H}_i(K))$$

where p_i denotes the restricted étale cover $\mathcal{H}_i \to \mathrm{PConf}_n$. Assume by contradiction that $\mathcal{H}$ has no deterministic component defined over K. Then, for every $i \in \{1, \ldots, r\}$, the cover p_i is of degree at least 2. By definition, $p_i(\mathcal{H}_i(K))$ is a thin set; as a finite union of thin sets, $\mathbb{A}^n(K)$ is a thin set, which is impossible since K is Hilbertian. □

A note on the $n = 3$ case. The theorem is of no use when $n = 3$, because

PROPOSITION. — *Every 3-tuple $(a, b, c) \in \Sigma$ is deterministic.*

Proof. The pure braids σ_1^2, σ_2^2 and $\sigma_1^{-1}\sigma_2^2\sigma_1$ generate PB_3. If $abc = 1$, then braid computations show that:

$$\begin{array}{rcl} \sigma_1^2.(a,b,c) & = & c^{-1}(a,b,c)c \\ \sigma_2^2.(a,b,c) & = & a^{-1}(a,b,c)a \\ (\sigma_1^{-1}\sigma_2^2\sigma_1).(a,b,c) & = & ac(a,b,c)c^{-1}a^{-1} \end{array}$$

Here is an amusing alternative "computation-free" proof: let C be the component of $\mathcal{H}_{\bar{\mathbb{Q}}}$ corresponding to (a,b,c). Take any point $x \in C(\bar{\mathbb{Q}})$ and let K be a number field over which x is K-rational. The action of $\mathrm{PSL}_2(K)$ on $\mathcal{H}(K)$ stabilizes $C(K)$ because $\mathrm{PSL}_2(\mathbb{C})$ is connected, so the $\mathrm{PSL}_2(K)$-orbit of x is included in $C(K)$. Since $\mathrm{PSL}_2(K)$ acts simply transitively on $\mathrm{PConf}_3(K)$, the $\mathrm{PSL}_2(K)$-orbit of x consists of a K-point of C above every K-point of PConf_3. By the theorem (proving its own uselessness!), C is deterministic. □

Computations in the case $n = 4$. Let $a,b,c,d \in G$ such that $abcd = 1$. As noted in [Hä22, Corollary 3.1], the action of PB_4 on (a,b,c,d) is entirely determined by the action of σ_1^2 and $\sigma_1^{-1}\sigma_2^2\sigma_1$. Using the notation $\bar{a} = a^{-1}, \bar{b} = b^{-1}$, etc., we have:

$$\begin{array}{rcccl} \sigma_1^2.(a,b,c,d) & = & (aba(ab)^{-1}, aba^{-1}, c, d) & = & ab(a,b,cdc\bar{d}\bar{c}, cd\bar{c})\bar{b}\bar{a} \\ \sigma_1^{-1}\sigma_2^2\sigma_1.(a,b,c,d) & = & (aca\bar{c}\bar{a}, ac\bar{a}\bar{c}bca\bar{c}\bar{a}, ac\bar{a}, d) & = & ac(a, \bar{a}\bar{c}bca, c, \bar{c}\bar{a}dac)\bar{c}\bar{a}. \end{array}$$

Therefore, (a,b,c,d) is deterministic if and only if, by denoting Z_a, Z_b, Z_c, Z_d the centralizers of a,b,c,d, the sets $Z_a \cap Z_b \cap cZ_d$ and $Z_a \cap Z_c \cap Z_d ac$ are both nonempty. Using the notation HH' for the product of two subgroups of G, this amounts to requiring that $c \in (Z_a \cap Z_b)Z_d$ and $ac \in Z_d(Z_a \cap Z_c)$.

Assume that $Z(G) = 1$. If G is generated by a and b (or a and c), then $Z_a \cap Z_b = 1$ (resp. $Z_a \cap Z_c = 1$); in that case, if (a,b,c,d) is deterministic then c and d commute (resp. ac and d commute). In particular, a 4-tuple of "Harbater-Mumford type" (x, x^{-1}, y, y^{-1}), with $G = \langle x, y \rangle$ a nontrivial centerless group, is never deterministic. This is unfortunate, as Harbater-Mumford components are among those whose fields of definition is best understood (see [DE06; Cau12; Seg23]).

Heuristically, the 4-tuples $\underline{g} \in \Sigma$ that have the best likelihood to be deterministic are those whose elements belong to small conjugacy classes (so that the centralizers are big) and such that no two elements suffice to generate G.

The case where $n = 4$ and $G = \mathtt{17T7}$. The non-trivial rational conjugacy classes of $\mathtt{17T7} = \mathrm{PSL}_2(\mathbb{F}_{16}) \rtimes \mathbb{Z}/2\mathbb{Z}$ are the classes labeled 2A, 2B, 3A, 4A, 6A. There are $\sum_{k=1}^{4} \binom{5}{k}\binom{4-1}{k-1} = 70$ unordered lists of four non-trivial rational conjugacy classes. An exhaustive computer search using GAP revealed that for all 4-tuples $\underline{c}$ of non-trivial rational classes of $\mathtt{17T7}$, there were no deterministic tuples in $\Sigma_{\underline{c}}$. By our main result, this implies:

Corollary. — *There exist subsets $S \subset \mathbb{Q}$ of size 4 such that no regular $\mathtt{17T7}$-extension of $\mathbb{Q}(T)$ is ramified exactly at S.*

Lifting invariants and deterministic-rigid pairs. Let K be a number field, $\underline{c} = (c_1, \ldots, c_n)$ be a list of K-rational conjugacy classes of G, and $c = \bigcup_i c_i$ One can prescribe more than the monodromy classes, namely the *lifting invariant* introduced by Fried and revisited by Ellenberg, Venkatesh and Westerland. We review this invariant, following [Woo21] closely.

Let $p : S \twoheadrightarrow G$ be a Schur cover of G. In particular, S is a central extension of G by $H_2(G,\mathbb{Z}) = \ker(p)$. Let Q_c be the normal subgroup of S generated by commutators $[a,b]$ of elements $a, b \in S$ such that $p(a), p(b) \in c$ and $p(ab) = p(ba)$. Note that Q_c is included in $H_2(G,\mathbb{Z})$. We let $H_2(G,c) = H_2(G,\mathbb{Z})/Q_c$. Choose for every conjugacy class c_i an element $x_i \in S$ such that $p(x_i) \in c_i$, and such that $x_i = x_j$ each time $c_i = c_j$. Now, if g is an element of c_i and γ is any element of S such that $g = p(\gamma x_i \gamma^{-1})$, the element $\gamma x_i \gamma^{-1}$ of S depends on the choice of γ only up to an element of Q_c; let $\hat{g}$ be its image in S/Q_c, which does not depend on γ.

If $(g_1, \ldots, g_n) \in \Sigma_{\underline{c}}$, we consider the element $\Pi(g_1, \ldots, g_n) = \hat{g}_1 \cdots \hat{g}_n \in S/Q_c$. This element has image $g_1 \cdots g_n = 1$ in G and therefore belongs to $H_2(G,\mathbb{Z})/Q_c = H_2(G,c)$. This is an invariant of the B_n-orbit of $(g_1, \dots, g_n)$, called its *lifting invariant*. Let K be a number field. The action of an automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}|K)$ on a component corresponds to a well-described action on its lifting invariant $\iota = \Pi(g_1, \dots, g_n)$:

$$\sigma.\iota = \iota^{\chi(\sigma)} \prod_{i=1}^{n} \left(x_i^{-\chi(\sigma)} \widehat{p(x_i)^{\chi(\sigma)}} \right).$$

If $\iota \in H_2(G, c)$, we say that the pair $(\underline{c}, \iota)$ is *K-rational* if $\underline{c}$ consists of K-rational conjugacy classes and ι is invariant under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$. We can then define:

$$\Sigma_{\underline{c},\iota} = \{ \underline{g} \in \Sigma_{\underline{c}} \mid \Pi(\underline{g}) = \iota \} \qquad\qquad \boldsymbol{\Sigma}_{\underline{c},\iota} = \{ \underline{g} \in \Sigma_{\underline{c},\iota} \mid \underline{g} \text{ is deterministic} \}.$$

Let $(\underline{c}, \iota)$ be a K-rational pair. If C is a deterministic geometrically irreducible component of $\mathcal{H}$ and $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}|K)$, then the component $\sigma.C$ is deterministic too. By choosing adequate generators of the fundamental group of the n-punctured sphere, this induces a Galois action of $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$ on $\boldsymbol{\Sigma}_{\underline{c},\iota}$. A fixed point of this action corresponds to a deterministic component of $\mathcal{H}_{\underline{c}}$ which has lifting invariant ι and is defined over K.

This approach leads to a criterion (generalized in several ways in [MM99]): we say that the pair $(\underline{c}, \iota)$ is *deterministic-rigid* if $\left|\boldsymbol{\Sigma}_{\underline{c},\iota}\right| = |\mathrm{Inn}(G)|$, i.e. if $\boldsymbol{\Sigma}_{\underline{c},\iota}$ consists of a single $\mathrm{Inn}(G)$-orbit, or equivalently of a single PB_n-orbit. If $(\underline{c}, \iota)$ is deterministic-rigid, then there is a unique deterministic component of $\mathcal{H}_{\underline{c}}$ with lifting invariant ι, and it is defined over K; if moreover G retracts on its center, then for any set S of n K-rational branch points, G is the Galois group of a regular extension of $K(T)$ unramified outside S. By the discussions above, this criterion is equivalent to usual rigidity criteria when $n = 3$, but is finer for larger n.

By a theorem of Conway and Parker and further improvements by Fried-Völklein/Ellenberg-Venkatesh-Westerland/Wood [Woo21, Theorem 3.1], there is a constant M such that if all conjugacy classes in the list $\underline{c} = (c_1, \dots, c_n)$ appear at least M times, then components of $\mathcal{H}_{\underline{c}}$ are determined by their lifting invariant. In this setting where branch points are numerous, one has a good understanding of the fields of definition of components; however, components with many branch points also tend to have a high degree: heuristically, the number of G-covers (including non-connected ones) branched at a configuration $\underline{t} \in \mathrm{PConf}_n$ is about $|G|^{n-2}$, whereas the number of components grows polynomially with n (see [Seg22]). Therefore, large tuples are rarely deterministic, but fields of definition of components associated to small tuples are not well-understood: this makes it hard to use deterministic components to find rational points in situations where we do not have rigidity.

Unordered branch loci and non-rational conjugacy classes. We have focused on regular extensions of $K(T)$ where the ramified primes were of degree 1, i.e. the branch loci are K-rational points of the configuration space of *ordered* configurations. This has led us to restrict our attention to K-rational conjugacy classes; this is also the reason why we were considering *pure* braids. The condition that the branch points be K-rational is restrictive; as was remarked in [DF94], as soon as K has a real embedding, only groups generated by involutions are realized by regular Galois extensions of $K(T)$.

Instead, we may look at *unordered* branch loci. Then, we need that the *set* of branch points be permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}|K)$, and that the list of conjugacy classes $(c_1, \dots, c_n)$ be invariant *up to permutation* under the exponentiation action of the image of the cyclotomic character $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}|K) \to (\mathbb{Z}/|G|\mathbb{Z})^\times$. The problem is that, in that context, components are rarely deterministic since any braid exchanging two branch points will yield a cover ramified at the same unordered configuration but often not isomorphic (e.g. if there are two non-equal conjugacy classes).

A solution, which is essentially the setting of [MM99, III 5.1], is to use a space of *colored* unordered configurations, where branch points are colored according to the monodromy class. If $(c_1, \dots, c_n)$ is a tuple of conjugacy classes, the topological fundamental group of that colored configuration space is the subgroup $\mathrm{B}_n^{\underline{c}}$ of B_n consisting of braids whose image in $\mathfrak{S}_n$ is a permutation which respects colors (i.e. it fixes the partition of $\{1, \dots, n\}$ induced by the equivalence relation "$i \sim j$ if $c_i = c_j$"). The correct generalization of deterministic components is then: a tuple $(g_1, \dots, g_n)$ is deterministic if it is conjugate to every tuple in its $\mathrm{B}_n^{\underline{c}}$-orbit. One can then reproduce the results of this note.

References

[Cau12] Orlando Cau. “Delta-composantes des espaces de modules de revêtements”. fr. In: *Journal de Théorie des Nombres de Bordeaux* 24.3 (2012), pp. 557–582. DOI: `10.5802/jtnb.811`. URL: `http://www.numdam.org/articles/10.5802/jtnb.811/`.

[DE06] Pierre Dèbes and Michel Emsalem. “Harbater-Mumford Components and Towers of Moduli Spaces”. In: *Journal of the Institute of Mathematics of Jussieu* 5 (2006), pp. 351 – 371.

[DF94] Pierre Dèbes and Michael D. Fried. “Nonrigid Constructions in Galois Theory”. In: *Pacific J. Math* 163.1 (1994), pp. 81–122.

[Hä22] Frank Häfner. *Braid orbits and the Mathieu group M_{23} as Galois group*. 2022. arXiv: `2202.08222 [math.NT]`.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory.* Springer Berlin, Heidelberg, 1999.

[Seg22] Béranger Seguin. *The Geometry of Rings of Components of Hurwitz Spaces.* 2022. arXiv: `2210.12793 [math.NT]`.

[Seg23] Béranger Seguin. *Fields of Definition of Components of Hurwitz Spaces.* 2023. arXiv: `2303.05903 [math.NT]`.

[Woo21] Melanie Wood. “An algebraic lifting invariant of Ellenberg, Venkatesh, and Westerland”. In: *Research in the Mathematical Sciences* 8 (June 2021). DOI: `10.1007/s40687-021-00259-2`. URL: `https://math.berkeley.edu/~mmwood/Publications/lifting.pdf`.