Regular realizations of p-projective quotients and modular curve-like towers

M. D. Fried

Abstract. This exposition on Modular Towers (**MT** s) shows how the Regular Inverse Galois Problem (RIGP) generalizes modular curves by considering all Frattini extensions of a given p-perfect finite group G. The result is towers of spaces generalizing modular curve towers — minus their cusps : $\{Y_1(p^{k+1})\}_{k=0}^{\infty}$ is a case with $G = D_p$ (p odd).

The Main Conjecture on **MT** s is that there are no rational points at high levels [LUM]. If true the difficulty in the RIGP is because the context generalizes the Mazur-Merel results. More so, A. Cadoret has shown the Strong Torsion Conjecture (STC) implies the Main Conjecture [STMT]. Though the STC is known only for dim. 1, there has been serious progress on the Main Conjecture. Ingredients include a theory of cusp types on a **MT**. We understand those projective systems of tower components that have properties resembling modular curves through two tools:

- The Fried-Serre lifting invariant generalizing an invariant for the spin covers of alternating groups [AGLI]; and
- a result of T. Weigel that explains towers levels through a group extension problem applied to a p-Poincaré duality group [We].

Here is a list of the sections.

1. Use of conjugacy classes
2. Is the RIGP really so hard?
3. The RIGP realm using virtually pro-p groups
4. Cusps on curve components ($r = 4$)
5. Compare modular curve cusps with **MT** cusps
6. Where is the Main Conjecture with $r = 4$?

The following were not in the talk, but are an addition to the pdf talk file [WS].

7. What happens in real **MT** levels!
8. Generalizing Serre's OIT and the g-p' conjecture

App. A: Fried-Serre Formula for Spin-Lift Invariant
App. B: **sh**-incidence Matrix for $(A_4, \mathbf{C}_{\pm 3^2})$

The I(nverse)G(alois)P(roblem) for G: Is finite group G the Galois group of an extension of every number field?

The R(egular)IGP for G: Is there one Galois extension $L_G/\mathbb{Q}(z)$ with group G containing only $\mathbb{Q}$ for constants? From Hilbert's irreducibility Theorem, RIGP (for G) $\implies$ IGP (for G). Further, beyond the solvable case, the RIGP has provided most all the successes through the *braid monodromy method.*

1. Use of conjugacy classes

We say $\boldsymbol{g} \stackrel{\text{def}}{=} (g_1, \dots, g_r) \in G^r$ *generates* with product-one if

$$\langle g_1, \dots, g_r \rangle = G \text{ and } \prod g_1 \cdots g_r \stackrel{\text{def}}{=} \Pi(\boldsymbol{g}) = 1.$$

Also, $\boldsymbol{g}$ defines a set $\mathbf{C}$ of conjugacy classes in G. Given $\mathbf{C}$, $\boldsymbol{g} \in \mathbf{C}$ means $\boldsymbol{g}$ defines $\mathbf{C}$. Such $\boldsymbol{g}$ form the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ of $(G, \mathbf{C})$.

In $\mathbf{C} = \{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ some classes may appear several times: multiplicity counts; order does not.

1.1. **R(iemann's)E(xistence)T(hm).** A regular realization $L_G/\mathbb{Q}(z)$ has $r \geq 2$ branch points $= \{z_1, \dots, z_r\}$ (z over which are less than $[L_G : \mathbb{Q}(z)]$ places): $z_i \mapsto$ conjugacy class C_i of inertia gen. from a clockwise small circle around z_i.

RET: $G(L_G/\mathbb{Q}(z)) = G \implies$ some $\boldsymbol{g} \in \mathbf{C}$ generates G with product-one.

Since the realization is over $\mathbb{Q}$, $\mathbf{C}$ is a rational union (its union is closed under putting all elements in it to powers prime to orders of elements in $\mathbf{C}$).

1.2. **An addition to** [FrV, Main Thm.]

Theorem 1.1 (Branch-Generation Thm.)**.** *Assume G is centerless and $\mathbf{C}^*$ is a distinct set of (nonidentity) classes in G. An infinite set $I_{G,\mathbf{C}^*}$ indexes distinct absolutely irreducible $\mathbb{Q}$ varieties $\mathcal{R}_{G,\mathbf{C}^*} \stackrel{\text{def}}{=} \mathcal{R}_{G,\mathbf{C}^*,\mathbb{Q}} = \{\mathcal{H}_i\}_{i \in I_{G,\mathbf{C}^*}}$ with:*

- *$i \in I_{G,\mathbf{C}^*} \mapsto {}_i\mathbf{C}$, a rational union of r_i conjugacy classes in G with support in $\mathbf{C}^*$.*
- *The RIGP holds for G with conjugacy classes $\mathbf{C}$ supported in $\mathbf{C}^* \Leftrightarrow i \in I_{G,\mathbf{C}^*}$ with $\mathbf{C} = {}_i\mathbf{C}$ and $\mathcal{H}_i$ has a $\mathbb{Q}$ point.*

1.3. **Using Nielsen classes.** Realizations come from augmenting existence of $\mathcal{R}_{G,\mathbf{C}^*}$ with info on $\mathcal{H}_i$, $i \in I_{G,\mathbf{C}^*}$.

The reduced space $\mathcal{H}_i^{\mathrm{rd}}$: Equivalence field extensions under change of variables $z \mapsto \alpha(z)$, $\alpha \in \mathrm{PGL}_2(\mathbb{C})$. Dimension of $\mathcal{H}_i^{\mathrm{rd}}$ is $r_i - 3$.

1.4. **D_p and A_n cases.** $G = D_{p^{k+1}}$, p odd, $\mathbf{C}^* = \{\mathrm{C}_2\}$ (class of involution): Then $i \mapsto \mathbf{C}_{2^{r_i}}$ is one-one and onto $r_i \geq 4$ even. Also, H_i^{rd} identifies with the space of cyclic p^{k+1} covers of hyperelliptic jacobians of genus $\frac{r_i - 2}{2}$.

(Fried-Serre) $G = A_n$ with $\mathbf{C}^* = \{\mathrm{C}_3\}$, class of 3-cycles: Then $i \mapsto \mathbf{C}_{3^{r_i}}$ with $r_i \geq n$ is two-one. Denote indices mapping to r by $i_r^{\pm}$. Covers in $\mathcal{H}_{i_r^{\pm}}$ are Galois closures of degree n covers $\phi : X \to \mathbb{P}_z^1$ with 3-cycles for local monodromy. Write divisor $(d\phi)$ of differential of ϕ as $2D_\phi$. Then, $\phi \in \mathcal{H}_{i_r^+}$ (resp. $\mathcal{H}_{i_r^-}$) if the linear system of D_ϕ has even (resp. odd) dim.; even (resp. odd) θ characteristic. For $r_i = n-1$, $i \mapsto \mathbf{C}_{3^{r_i}}$ is one-one.

2. Is the RIGP really so hard?

Dividing RIGP techniques into three cases shows how $i \in I_{G,\mathbf{C}^*}$ on ${}_i\mathbf{C}$ affects complexity of computation. Yet, it is diophantine reasons more than group theory complexity that makes the RIGP hard.

1. When $r_i = 3$, $\mathcal{H}_i^{\mathrm{rd}}$ is a finite collection of ($\mathbb{Q}$) points.
2. When $r_i = 4$, $\mathcal{H}_i^{\mathrm{rd}}$ is naturally an upper half-plane quotient and a cover of the j-line, with meaningful cusp types.
3. No matter what is r_i, $\mathcal{H}_i$ is a cover of U_{r_i}, projective r_i space minus its discriminant locus; can compare this with the (Galois) Noether cover $U^{r_i} \to U_{r_i}$ (with group S_{r_i}).

2.1. **Using #1.** *Rigidity* is an effective sufficiency test for finding $i \in I$ with $r_i = 3$. It requires only the character table of G to conclude the RIGP for G.

Problem: Rarely does this hold. Even for Chevalley groups, the method achieved only special rank 1 groups over prime finite fields (Belyi) and some other special simple groups by Matzat and Thompson.

2.2. **Using #3.** For many families of simple groups Thompson and Völklein found $\mathbf{C}^*$ and used specific $i \in I_{G,\mathbf{C}^*}$ (Thompson-tuples). Their $\mathcal{H}_i \to U_{r_i}$ covers were *almost* subcovers of $U^{r_i} \to U_{r_i}$. This gave many examples of simple G satisfying RIGP.

Problem: This required much luck and great expertise on simple group series.

2.3. **Virtues of using #2.**

- $\mathcal{H}_i^{\text{rd}}$ is a curve with *useful cusps* from the moduli problem to compactify it. Gives precise statements about these spaces.
- More groups (like all simple groups and all their Frattini covers) have conjugacy classes producing this case than holds for #1.
- Combinatorial techniques allow computing the genus of these spaces, and to *identify the part of the Nielsen class they come from*.

3. The RIGP realm using virtually pro-p groups

We use the virtually pro-p *universal p-Frattini* cover ${}_p\tilde{G}$ of G, for any prime $p||G|$ to see how the RIGP generalizes classical results for modular curves. If G is centerless and *p-perfect* (no surjective $G \to \mathbb{Z}/p$), then ${}_p\tilde{G} = \lim_{\infty \leftarrow k} G_k$, with:

- G_k also p-perfect and centerless; and
- $G_k \to G$ versal for all extensions $\psi : H \to G$ with $\ker(\psi)$ a p-group of exponent at most p^k.

3.1. **Add a restriction on Ramification.** From Schur-Zassenhaus, if a conjugacy class is p', then it has a unique lifts to a p' class in G_k. So, if $\mathbf{C}$ consists of p' classes, denote those lifted classes to G_k by the same notation. Here is a *restrict ramification condition* depending on $r_0 \geq 3$:

Ram_{r_0}: For $k \geq 0$, use covers in $\text{Ni}(G_k, \mathbf{C}_k)$ with at most r_0 classes in $\mathbf{C}_k$.

Question 3.1 (RIGP(G,p,r_0) Question)**.** Is there an r_0 so all G_ks satisfy the RIGP from covers in Ram_{r_0}?

3.2. **How the Main Conjecture Arises.**

Theorem 3.2 (Fried-Kopeliovic, 1997)**.** *If the conclusion of Quest. 3.1 is affirmative (for (G, p, r_0)), then there are p' conjugacy classes $\mathbf{C}$ (no more than r_0) in G, and a projective system $\{\mathcal{H}'_k \in \mathcal{R}_{G_k,\mathbf{C}}\}_{k=0}^{\infty}$ each having a $\mathbb{Q}$ point.*

We call $\{\mathcal{H}'_k\}_{k=0}^{\infty}$ a *M(odular) T(ower) component branch* (over $\mathbb{Q}$).

Conjecture 3.3 (Main Conjecture)**.** Given any **MT** component branch, and any number field K, for $k >> 0$, ${\mathcal{H}'}_k^{\text{rd}}(K) = \emptyset$.

4. Cusps on curve components ($r = 4$)

Twist action of $H_4 = \langle q_1, q_2, q_3 \rangle$ generators on $\boldsymbol{g} \in \mathrm{Ni}(G_k, \mathbf{C})/G \stackrel{\text{def}}{=} \mathrm{Ni}(G_k, \mathbf{C})^{\text{in}}$. Ex.: $q_2 : \boldsymbol{g} \mapsto (g_1, g_2 g_3 g_2^{-1}, g_2, g_4)$.

Level k Cusps: $\mathrm{Cu}_4 \stackrel{\text{def}}{=} \langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2, q_2 \rangle$ orbits on $\mathrm{Ni}(G_k, \mathbf{C})^{\text{in}}$. Denote $\langle q_1 q_3^{-1}, (q_1 q_2 q_3)^2 \rangle$ by $\mathcal{Q}''$.

4.1. Why $\bar{M}_4 \stackrel{\text{def}}{=} H_4/\mathcal{Q}''$ is $\mathrm{PSL}_2(\mathbb{Z})$.

- $q_2 \mapsto \gamma_\infty$;
- $q_1 q_2 q_3$ (shift) $\mapsto \gamma_1$ (order 2).
- $q_1 q_2 \mapsto \gamma_0$ has order 3, from braid relation $q_1 q_2 q_1 = q_2 q_1 q_2 \mod \mathrm{Cu}_4$ and Hurwitz relation $1 = q_1 q_2 q_3 q_3 q_2 q_1$:

$$= q_1 q_2 q_1 q_1 q_2 q_1 = q_1 q_2 q_1 q_2 q_1 q_2 = (q_1 q_2)^3.$$

4.2. From a component branch, what to compute.

- Nature of cusps and their widths (length of $\mathrm{Cu}_4 \mod \mathcal{Q}''$ orbits).
- How they fall in $\bar{M}_4$ orbits and of what genera (Riemann-Hurwitz).

5. Compare modular curve cusps with **MT** cusps

When $r = 4$, **MT** levels ($k \geq 0$) are j-line covers, but rarely modular curves. The following description of cusps is from [LUM, §3.2].

With $r = 4$, $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^{\text{in}}$, denote:

$$\langle g_2, g_3 \rangle = H_{2,3}(\boldsymbol{g}) \text{ and } \langle g_1, g_4 \rangle = H_{1,4}(\boldsymbol{g}).$$

$(\boldsymbol{g})\mathrm{Cu}_4$ is a *g-p' cusp*: $H_{2,3}(\boldsymbol{g})$ and $H_{1,4}(\boldsymbol{g})$ are p' groups. Ex: H(arbater)-M(umford) cusps have $g_2 = g_1^{-1}$.

p cusps: Those with $p|\mathrm{ord}(g_2 g_3)$.

o(nly)-p': Cusps neither p nor g-p'.

Modular curve $X_1(p^{k+1})$ has H-M cusps, many p cusps of different cusps widths, all growing in width by p as k increases, but no o-p' cusps.

5.1. Apply R-H to MT components. Ni' is a $\bar{M}_4$ orbit on a reduced Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\text{abs}}/\mathcal{Q}''$ (or $\mathrm{Ni}(G, \mathbf{C})^{\text{in}}/\mathcal{Q}''$). Denote action of $(\gamma_0, \gamma_1, \gamma_\infty)$ (§4.1) on Ni' by $(\gamma_0', \gamma_1', \gamma_\infty')$: Branch cycles for a cover $\overline{\mathcal{H}}' \to \mathbb{P}^1_j$,

R-H gives genus, $g_{\overline{\mathcal{H}}'}$: $2(\deg(\overline{\mathcal{H}}'/\mathbb{P}^1_j) + g' - 1) = \mathrm{ind}(\gamma_0') + \mathrm{ind}(\gamma_1') + \mathrm{ind}(\gamma_\infty')$.

5.2. Answer these questions to compute genera of MT components.

- What are the components $\overline{\mathcal{H}}_k'$ of $\overline{\mathcal{H}}_k$ ($\bar{M}_4$ orbits Ni_k' on $\mathrm{Ni}_k^{\text{rd}}$)?
- What are ram. orders over ∞ (orbit lengths of γ_∞' on Ni_k')?
- What points ramify in each component over elliptic points $j = 0$ or 1; length 3 (resp. 2) orbits of γ_0' (resp. γ_1') on Ni_k'?

6. Where is the Main Conjecture with $r = 4$?

[LUM] has three Frattini Principles. We use here Frattini Princ. 1: If $g \in G_k$ is exactly divisible by p^u, $u > 0$, it has above it in G_{k+1} only elements of order exactly divisible by p^{u+1}. [LUM] shows Main Conj. 3.3 for G a general p-perfect group reduces to the case the p part of the center is trivial. This allows the following conclusion: A level $k+1$ cusp over a p cusp at level k is ramified (of order p).

6.1. **Reductions from** [LUM]**.** Let $B' = \{\mathcal{H}'_k\}_{k=0}^{\infty}$ be an infinite component branch. Main Conj. contradictions:

(6.1a) $g_{\overline{\mathcal{H}}'_k} = 0$ for all $0 \le k < \infty$ (B' has genus 0; $g_{B'}$ consists of 0's); or
(6.1b) For k large, $g_{\overline{\mathcal{H}}'_k} = 1$ (B' has genus 1; almost all of $g_{B'}$ is 1's).

Usage: From R-H, for $k >> 0$, (6.1b) implies $\overline{\mathcal{H}}'_{k+1} \to \overline{\mathcal{H}}'_k$ doesn't ramify. So, FP1 says: For no k does $\overline{\mathcal{H}}'_k$ have a p cusp or a Main Conj. exception satisfies (6.1a).

6.2. **Possible exceptional cases! [LUM, §5].** Assume $\boldsymbol{p}'_k \in \overline{\mathcal{H}}'_k$ is a p cusp (some k). Denote: $\deg(\overline{\mathcal{H}}'_{k+1}/\overline{\mathcal{H}}'_k) = \nu_k$ and $|\boldsymbol{p}_{k+1} \in \overline{\mathcal{H}}'_{k+1}$ over $\boldsymbol{p}'_k| = u_k$.

Theorem 6.1. *Then, the Main Conj. is true unless for $k >> 0$, $\nu_k = p$, $u_k = 1$ and $\overline{\mathcal{H}}'_{k+1}/\overline{\mathcal{H}}'_k$ is equivalent (as a cover over K) to either:*

- ($\mathrm{P}^{\mathrm{oly}}$ M) *a degree p polynomial map; or*
- ($\mathrm{R}^{\mathrm{edi}}$M) *a degree p rational function p order ramification over two points.*

Corollary 6.2. *If neither* ($\mathrm{P}^{\mathrm{oly}}$M) *nor* ($\mathrm{R}^{\mathrm{edi}}$M) *hold for the component branch B', then high levels of B' have no K points.*

For B' with full elliptic ramification (includes when B' has fine reduced moduli) for $k >> 0$, the Main Conj. holds unless ($\mathrm{R}^{\mathrm{edi}}$ M) *holds.*

References

[STMT] A. Cadoret, *Modular Towers and Torsion on Abelian Varieties*, preprint May, 2006.

[FrV] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800.

[AGLI] Alternating groups and lifting invariants, Out for refereeing (2006), 1–36.

[LUM] M.D. Fried, *The Main Conjecture of Modular Towers and its higher rank generalization*, in Groupes de Galois arithmetiques et differentiels (Luminy 2004; eds. D. Bertrand and P. Dèbes), Seminaires et Congres, **13**, 2006.

[WS] M.D. Fried, *Regular realizations of p-projective quotients and modular curve-like towers*, this is the talk I gave on May 26 at Oberwolfach, augmented by other topics. Access at www.math.uci.edu/conffiles_rims/exp-profgeom.html in the list in the scientific part of the homepage of the conference "Profinite Arithmetic Geometry and Their Associated Moduli Spaces," at RIMS, Kyoto October 23 - 29, 2006.

[We] T. Weigel, *Maximal l-Frattini quotients of l-Poincaré duality groups of dimension* 2, Arch. Math. (Basel) **85** (2005), no. 1, 55–69.

Reporter: Benjamin Klopsch (Düsseldorf)