The relative class number one problem for function fields, II

Kiran S. Kedlaya

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu

These slides can be downloaded from https://kskedlaya.org/slides/.
Jupyter notebooks available from https://github.com/kedlaya/same-class-number.

Arithmetic, Geometry, Cryptography, and Coding Theory (AGC^{2}T)
Centre International de Rencontres Mathématiques (CIRM), Luminy
June 5, 2023

Supported by NSF (grant DMS-2053473) and UC San Diego (Warschawski Professorship).

I acknowledge that my workplace occupies unceded ancestral land of the Kumeyaay Nation.

The problem

Let F'/F be a finite extension of function fields associated to a cover $C' \to C$ of curves over finite fields. Let g, g' be the genera of F and F'. Let q, q' be the cardinalities of the base fields[1] of F, F'.

Let h, h' be the class numbers[2] of F and F'. The ratio h'/h equals $\#A(\mathbb{F}_q)$ for A the **Prym (abelian) variety** of C'/C, and hence an integer. Following Leitzel–Madan (1976), we ask: in what cases does $h'/h = 1$?

To make this a potentially finite problem, we only specify the isomorphism classes of F and F', not the inclusion (this only makes a difference when $g \leq 1$). We also ignore the trivial cases:

- $F' \cong F$;
- $g = g' = 0$.

[1] By "base field" I mean the integral closure of the prime subfield.

[2] That is, $h = \#J(C)(\mathbb{F}_q)$ and $h' = \#J(C')(\mathbb{F}_{q'})$.

Where was I? (ANTS-XV, Bristol, August 2022)

At ANTS-XV, I reported progress on this problem. This borrows[3] from the study of the maximum number of points on a genus-g curve over $\mathbb{F}_q$.

- **Solved** when F'/F is **constant** (i.e., $F' = F \cdot \mathbb{F}_{q'}$). We thus need only treat the case where F'/F is **geometric** (i.e., $q' = q$).
- **Solved** when $q > 2$, i.e.,[4] $q \in \{3, 4\}$. Assume hereafter $q = 2$.
- **Solved**[5] when $g \leq 1$ (we get $g' \leq 6$). Assume hereafter $g \geq 2$, so that $d := [F' : F] \leq \frac{g'-1}{g-1}$ by Riemann–Hurwitz.
- **Reduced to a finite computation**: the zeta functions $\zeta_F, \zeta_{F'}$ of F, F' form one of 208 known pairs. In all cases, $g \leq 7, g' \leq 13$.
- **Solved** when $g \leq 5$ and F'/F is a **cyclic** extension, by a table lookup for F (Howe, Xarles, Dragutinović) plus explicit CFT.

[3] Special thanks to the AGC^{2}T community for its work to type/publish Serre's 1985 Harvard lecture notes. Without these efforts my work would surely not have happened!

[4] By the Weil bound, $h'/h = \#A(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2\dim(A)} > 1$ if $q \geq 5$.

[5] Modulo one step which we indicate later.

Where am I now? Where do I go next?

In this talk, I focus on the following statement.

Theorem

Let F'/F be a finite geometric extension of function fields with $q = 2, g > 1, h'/h = 1$. Then F'/F is cyclic.

A useful slogan here is

the most radical [extreme] **covers are radical** [cyclic]:

the class number condition puts severe pressure on point counts and splitting behavior in the extension, and cyclic covers are better able to withstand this pressure.

The proof will make free use of the zeta function constraint from the ANTS-XV work, cited hereafter as ANTS.

Where do I go next? (LuCaNT, July 2023)

This will leave unsettled the cases where $g = 6, 7$ and F'/F is unramified of degree 2, as in these cases we do not have complete tables of genus-g curves over $\mathbb{F}_2$ with which to perform a table lookup by zeta function.

We are thus forced to exhaust over all curves ourselves using Mukai's explicit descriptions of canonical curves of these genera. This will be discussed at LuCaNT (ICERM, Providence, July 2023).

The state of play

We need to check that certain pairs $\zeta_F, \zeta_{F'}$ (specified by ANTS) cannot occur for a noncyclic cover of curves of some degree $d \geq 3$ over $\mathbb{F}_2$. By Riemann–Hurwitz plus ANTS, $d \leq 7$ and $g \leq 4$.

In this range, **in principle** it is possible to:

- find (by table lookup) all F with a particular ζ_F;[6]
- find all F'/F of degree d, e.g., using Bhargava's orbit parametrizations for $d \leq 5$;
- compute $\zeta_{F'}$ and confirm that the only extensions consistent with ANTS are cyclic.

However, it is not straightforward at present to make this practical. In particular orbit parametrizations have not been implemented for $d = 4, 5$, and do not exist at all for $d > 5$.

[6] We cannot do this for F' at present, as g' can be as large as 10 and such tables do not yet exist, although the methods of my LuCaNT talk could conceivably reach that far.

A paradigm for $d \leq 6$

For $3 \leq d \leq 6$, we instead execute the following strategy.

- Given $\zeta_F, \zeta_{F'}$, identify the combinatorial options[7] for the splitting types of the low-degree places of F. E.g., there is **always** a degree-1 place of F that is inert in F'.
- Let F''/F be the Galois closure of F'/F. For each noncyclic candidate for $G = \mathrm{Gal}(F''/F) \subseteq S_d$, use the character theory of G to find other subfields of F''/F **and** compute how the various places of F split in these subfields. One important example is the **quadratic resolvent**, i.e., the fixed field of $G \cap A_d$.
- Identify isogeny factors of Jacobians for which we read off some Frobenius traces, then exhaust over Weil polynomials to obtain a contradiction.

This can be done uniformly using some simple SAGE code, but individual cases can also be analyzed by hand.

[7] These options differ slightly when the cover is ramified, but the strategy persists.

The case $d = 7$

By ANTS, there is **one** possible pair $(\zeta_F, \zeta_{F'})$ with $(d, g, g') = (7, 2, 8)$. This does occur for a cyclic cover.

In principle one could execute the previous paradigm for $d = 7$. However, this requires working with the character tables of S_7 and its transitive subgroups (like $\mathrm{PSL}(2, 7)$), which seems infeasible.

Luckily, a method of Howe shows (in **very** special cases) that a curve whose zeta function “suggests an automorphism” actually has one.

This method also covers one missing step from ANTS: every curve $C/\mathbb{F}_2$ of genus 6 with $(\#C(\mathbb{F}_{2^i}))_{i=1}^{6} = (0, 0, 0, 20, 15, 90)$ is a cyclic étale degree-5 cover of $y^2 + y = x^5$.

Plan for this part of the talk

Here we illustrate the implementation of the paradigm, spelling out details only in a few cases. The goal is to make the case that

- all of the analysis **could** be done by hand,
- but **should** be automated for reliability.

Reminders: A is the Prym variety of C'/C and F''/F is the Galois closure of F'/F. Write C'' for the curve with function field F''.

The case $d = 3$ (part 1)

For $d = 3$, we have to rule out $G = S_3$. Since F has a degree-1 place which is inert in F', the quadratic resolvent C''/A_3 is a geometric cover of C; let B be the Prym variety and $T_{B,q}$ its q-Frobenius trace.

Useful fact: if $\#C'(\mathbb{F}_q) = 0$, then $\#C''(\mathbb{F}_q) = 0$ and[8]

$$\begin{aligned} T_{A,q} &= T_{J(C'),q} - T_{J(C),q} = \#C(\mathbb{F}_q) \\ T_{B,q} &= T_{J(C''),q} - T_{J(C),q} - 2T_{A,q} = -\#C(\mathbb{F}_q). \end{aligned}$$

If F'/F is ramified, then by ANTS,

$$(g, g') = (2, 6); \quad \#C(\mathbb{F}_2) \geq 3; \quad \#C'(\mathbb{F}_2) = 0; \quad \#C'(\mathbb{F}_4) = 2.$$

$C' \to C$ ramifies at 1 or 2 points of $C'(\overline{\mathbb{F}}_2)$. Since $\#C'(\mathbb{F}_2) = 0$, $C' \to C$ must have a triple point at the unique degree-2 place of C'; hence the quadratic resolvent is **étale**, so $\dim(B) = 1$ and $T_{B,2} \leq -3$, $\Rightarrow\Leftarrow$.

[8] By decomposing the ℓ-adic Tate module of $J(C'')$ as an S_3-representation.

The case $d = 3$ (part 2)

If F'/F is unramified, then $\dim(B) = g - 1$. By ANTS, $(g, g') \in \{(2,4), (3,7), (4,10)\}$.

- If $g = 2$, by ANTS, $T_{B,2} = -\#C(\mathbb{F}_2) = -3$, $\Rightarrow\Leftarrow$.
- If $g = 4$, by ANTS, $T_{B,2} \leq -7$ or $T_{B,2} = T_{B,4} = -6$, $\Rightarrow\Leftarrow$.
- If $g = 3$ and $\#C'(\mathbb{F}_2) > 1$, then by ANTS, there are not enough places of F' of degree ≤ 3 to cover the degree-1 places of F.
- If $g = 3$ and $\#C'(\mathbb{F}_2) = 1$, then the unique degree-1 place of C' occurs in a fiber with a degree-2 place, so $\#C'(\mathbb{F}_4) \geq 3$. By ANTS, $\#C(\mathbb{F}_2) = 5, \#C(\mathbb{F}_4) = 9, \#C'(\mathbb{F}_4) = 3$ and the **splitting sequence**[9] begins $\{3(\times 4), 2+1\}, \{3(\times 2)\}$; so $(T_{B,2}, T_{B,4}) = (-3, -9)$, $\Rightarrow\Leftarrow$.
- If $g = 3$, $\#C'(\mathbb{F}_2) = 0$, and $\#C'(\mathbb{F}_4) > 0$, then (details omitted).
- If $g = 3$ and $\#C'(\mathbb{F}_2) = \#C'(\mathbb{F}_4) = 0$, then (details omitted).

[9] How to read this notation: of the degree-1 places of F, four lift to degree-3 places of F' and one to a degree-2 place plus a degree-1 place; and of the degree-2 places of F, both lift to degree-6 places of F'.

The case $d = 4$

For $d = 4$, we must rule out $G = D_4, S_4$. If $G = D_4$, we have a tower of geometric quadratic extensions $F'/E/F$ of relative class number 1, which we exclude using ANTS except for one case that arises as a cyclic cover.[10]

If $G = S_4$, we split into cases based on the quadratic resolvent.

- If the quadratic resolvent is constant, then the splittings of odd-degree places of F' must include only even indices. Combining with ANTS, we easily get $\Rightarrow\Leftarrow$.
- If the quadratic resolvent is geometric, we can make arguments as for $d = 3$ (details omitted).

[10] We can distinguish C_4 from D_4 using the Deuring–Shafarevich formula for p-ranks in cyclic p-covers in characteristic p: in this case E' admits a **unique** unramified quadratic extension.

The case $d = 5$

For $d = 5$, by ANTS, $g = 2$. We rule out $G = D_5, S_5$ using the quadratic resolvent (which must be geometric because F has a degree-1 place which is inert in F').

For $G = A_5$, we have abelian varieties B_1, B_2 of dimensions[11] 5,6 with

$$\begin{aligned}\#(C''/D_5)(\mathbb{F}_q) &= \#C(\mathbb{F}_q) - T_{B_1,q} \\ \#(C''/A_3)(\mathbb{F}_q) &= \#C(\mathbb{F}_q) - 2T_{A,q} - T_{B_1,q} - T_{B_2,q}.\end{aligned}$$

Using ANTS to compute possible splitting sequences and then $T_{B_1,2^i}, T_{B_2,2^i}$ for $i = 1, \ldots, 7$ (!!)[12], we get $\Rightarrow\Leftarrow$.

[11] These are dimensions of certain irreducible **rational** A_5-representations. Over $\mathbb{C}$, there is a pair of 3-dimensional irreducible representations that do not descend to $\mathbb{Q}$.

[12] Here we are using that we know all Weil polynomials of genus ≤ 6 over $\mathbb{F}_2$; this list can be reproduced easily in Sage.

The case $d = 6$

For $d = 6$, by ANTS, $g = 2$. We again use ANTS to rule out the possibility that F'/F has an intermediate subfield.

This leaves the cases $G = S_6$ and $G = \mathrm{PGL}(2,5) \cong S_5$. We also split into cases based on whether the quadratic resolvent is constant or geometric.

In the case $G = S_6$, we look at the Prym B for $C''/\mathrm{PGL}(2,5)$ over C; then $\dim(B) = 5$.

In the case $G = \mathrm{PGL}(2,5)$, $C''/\mathrm{PGL}(2,5)$ splits as a copy of C plus another cover; we look at the Prym B of the latter, so $\dim(B) = 4$.

In all cases, we use ANTS to compute splitting sequences and then $T_{B,2^i}$ for $i \leq 6$, then $\Rightarrow\Leftarrow$.

Further thoughts

The method of ANTS can (probably) be used to derive effective upper bounds for the relative class number m problem for any $m > 1$. However, we got lucky for $m = 1$ in (at least) three ways that may fail for $m > 1$.

- We only had to compute splittings in relatively small degrees, where the number did not explode.
- There may be cases that do not occur but which are not ruled out by Weil polynomials.
- For $m > 1$ there probably do exist some noncyclic covers, so we need more sensitive arguments that can accommodate this possibility.