

The relative class number one problem for function fields


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>.

Number Theory Seminar
Massachusetts Institute of Technology
September 15, 2022

Based on arXiv:2202.08382, 2206.02084, 2208.11277.

Supported by  (grants DMS-2053473 and prior) and [UC San Diego](#) (Warschawski Professorship).

The UC San Diego campus sits on unceded ancestral land of the [Kumeyaay Nation](#).

The problem

Let F'/F be a finite extension of function fields of curves over finite fields. Let $g_F, g_{F'}$ be the genera of F and F' . Let $q_F, q_{F'}$ be the cardinalities of the base fields* of F, F' .

Let $h_F, h_{F'}$ be the class numbers of F and F' . The ratio $h_{F'/F} := h_{F'}/h_F$ is always an integer (more on this shortly). Following Leitzel–Madan (1976), we ask: in what cases does $h_{F'/F} = 1$?

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 $g_F \leq 1$). We also ignore the trivial cases:

- $F' \cong F$ (e.g., F'/F corresponds to an isogeny of elliptic curves);
- $g_F = g_{F'} = 0$.

*By “base field” I mean the integral closure of the prime subfield.

Contrast with the number field case

In the number field setting, class number 1 is much more common, because class groups are always “incomplete”. The product

$$\text{class number} \times \text{unit regulator}$$

behaves much more predictably, and can be interpreted as the volume of a natural compact topological group defined using adèles.

For relative class number 1, one can only hope for a finiteness result for (nontrivial) extensions which preserve the unit rank, i.e., CM fields.[†] For **normal** CM fields, using Odlyzko’s discriminant bounds (under GRH) the full classification was given by Lee–Kwon and Hoffman–Sircana.

By contrast, the full Picard group of a function field looks like $\mathbb{Z} \times (\text{finite})$ and removing one point always takes out \mathbb{Z} .

[†]A **CM field** is a totally imaginary quadratic extension of a totally real field.

Constant vs. geometric extensions

We say that:

- F'/F is **constant** if $F' = F \cdot \mathbb{F}_{q_{F'}}$;
- F'/F is **purely geometric** (hereafter **geometric**) if $q_F = q_{F'}$.

Let E be the compositum $F \cdot \mathbb{F}_{q_{F'}}$; then E/F is constant and F'/E is geometric. Since the relative class number is always an integer, $h_{F'/F} = 1$ if and only if $h_{E/F} = h_{F'/E} = 1$.

The relative class number one problem thus reduces to the constant and geometric cases. The constant case is relatively easy,[‡] so most of the work will occur in the geometric case, particularly when $q_F = 2$ (see below).

[‡]One ingredient to be highlighted here is the $\overline{\mathbb{F}}_2$ -decomposition of simple abelian varieties over \mathbb{F}_2 of order 1, joint with D'Nelly-Warady.

Weil polynomials

Assume F'/F is geometric and put $q := q_F$. Let C, C' be the curves with function fields F, F' . Let P, P' be the **Weil polynomials** of these curves (the charpoly of Frobenius on the ℓ -adic Tate module for any prime ℓ which is nonzero in \mathbb{F}_{q_F}).

- P and P' are monic polynomials over \mathbb{Z} whose \mathbb{C} -roots all have absolute value \sqrt{q} .
- P' is divisible by P . More precisely, we have[§]

$$J(C') \cong J(C) \times A$$

for some abelian variety A over \mathbb{F}_q (the **Prym variety**) and P'/P is the Weil polynomial of A .

- We have $h_F = P(1)$, $h_{F'} = P'(1)$ and hence $h_{F'/F} = (P'/P)(1)$.

[§]This holds even if F'/F is not geometric, as long as we replace $J(C')$ with its Weil restriction from $\mathbb{F}_{q_{F'}}$ to \mathbb{F}_{q_F} . This explains why $h_{F'/F} \in \mathbb{Z}$.

The Prym variety has order 1

If $F' \neq F$ and $h_{F'/F} = 1$, then the Prym variety A satisfies $\dim(A) > 0$ and $\#A(\mathbb{F}_q) = 1$. Hence:

- we have $q \leq 4$ by the Weil bounds (i.e., the restriction on the absolute value of the roots of the Weil polynomial);
- for $q = 3, 4$, A is isogenous to a product of the unique elliptic curve E over \mathbb{F}_q with $\#E(\mathbb{F}_q) = 1$;
- for $q = 2$, A is isogenous to a product of simple factors classified by Madan–Pal–Robinson in 1977.

Summary of the results, part 1

See the appendix of [arXiv:2202.08382](https://arxiv.org/abs/2202.08382) for tables listing the options for F and F' in the following results.

Theorem

Assume F'/F is constant and $g_F > 0$. Then (q_F, d, g_F) is one of

$$(2, 2, 1), (2, 2, 2), (2, 2, 2), (2, 2, 3), (2, 3, 1), (2, 3, 1), (3, 2, 1), (4, 2, 1)$$

and all options for F are known.

Theorem

Assume F'/F is geometric, $g_F \leq 1$, and $g_{F'} > g_F$. Then

$$(q_F, g_F, g_{F'}) \in \{(2, 0, 1), (2, 0, 2), (2, 0, 3), (2, 0, 4), (2, 1, 2), (2, 1, 3), (2, 1, 4), (2, 1, 5), (2, 1, 6), (3, 0, 1), (3, 1, 2), (3, 1, 3), (4, 0, 1), (4, 1, 2)\}$$

and all options for (F, F') are known.

Summary of the results, part 2

Theorem

Assume F'/F is geometric, $g_{F'} > g_F > 1$, and $q_F > 2$. Then

$$(q_F, d, g_F, g_{F'}) \in \{(3, 2, 2, 3), (3, 2, 2, 4), \\ (3, 2, 3, 5), (3, 3, 2, 4), (4, 2, 2, 3), (4, 3, 2, 4)\}$$

and all options for F'/F are known **and cyclic**.

Theorem

Assume F'/F is geometric, $g_{F'} > g_F > 1$, $q_F = 2$, and $d > 2$. Then

$$(d, g_F, g_{F'}) \in \{(3, 2, 4), (3, 2, 6), (3, 3, 7), \\ (3, 4, 10), (4, 2, 5), (5, 2, 6), (7, 2, 8)\}$$

and all options for F'/F are known **and cyclic**.

Summary of the results, part 3

Theorem

Assume F'/F is geometric, $g_{F'} > g_F > 1$, $q_F = 2$, and $d = 2$. Then

$$(g_F, g_{F'}) \in \{(2, 3), (2, 4), (2, 5), (3, 5), \\ (3, 6), (4, 7), (4, 8), (5, 9), (6, 11), (7, 13)\}$$

and all options for F'/F are known.

Outline of the proof

Hereafter, assume F'/F is geometric and write

$$q := q_F = q_{F'}, \quad g := g_F, \quad g' := g_{F'}.$$

- Use the class number 1 hypothesis to derive lower bounds on $\#C(\mathbb{F}_{q^i})$, then compare with “linear programming” upper bounds on $\#C(\mathbb{F}_{q^i})$ to obtain upper bounds on $g_F, g_{F'}$.
- For each remaining pair $(g_F, g_{F'})$, exhaust over candidate Weil polynomials and impose constraints coming from the geometry of the cover $C' \rightarrow C$. When $g_F > 1$, we separately consider each value of $d := [F'/F]$ compatible with Riemann–Hurwitz.
- When $g_F \leq 1$, look in tables to find F, F' with suitable Weil polys.
- When $g_F > 1$, look in tables to find F . For each F , compute degree- d cyclic extensions F'/F and check $h_{F'/F}$.
- Rule out noncyclic covers with $d > 2$. More on this later.

A lower bound on point counts

Let T_{A,q^n} be the trace of the q^n -power Frobenius on A ; then

$$\#C(\mathbb{F}_{q^n}) = \#C'(\mathbb{F}_{q^n}) + T_{A,q^n} \geq T_{A,q^n}.$$

For $q = 3, 4$, we have $1 = \#E(\mathbb{F}_q) = q + 1 - T_{E,q}$ and so[¶]

$$\#C(\mathbb{F}_q) \geq T_{A,q} = q \dim(A) = q(g' - g) \geq q(g - 1).$$

For $q = 2$, we can have $T_{A,q} = 0$, so there is no useful bound on $\#C(\mathbb{F}_2)$. But using the Madan–Pal–Robinson classification, data from LMFDB for $\dim(A) \leq 6$, and a bit of linear programming, we get

$$\begin{aligned} &1.3366 T_{A,2} + 0.3366 T_{A,4} + 0.1137(T_{A,8} - T_{A,2}) \\ &\quad + 0.0537(T_{A,16} - T_{A,4}) \geq 1.5612 \dim(A) \implies \\ &1.3366 \#C(\mathbb{F}_2) + 0.3366 \#C(\mathbb{F}_4) + 0.1137(\#C(\mathbb{F}_8) - \#C(\mathbb{F}_2)) \\ &\quad + 0.0537(\#C(\mathbb{F}_{16}) - \#C(\mathbb{F}_4)) \geq 1.5612(g' - g) \geq 1.5612(g - 1). \end{aligned}$$

[¶]The estimate $g' - g \geq g - 1$ follows from Riemann–Hurwitz.

Comparison with upper bounds on point counts

We now compare with effective “linear programming” upper bounds on $\#C(\mathbb{F}_{q^n})$ (Ihara, Drinfeld–Vlăduț, Oesterlé, Serre).

$$q = 4 : \quad \#C(\mathbb{F}_q) \leq 1.435g + 21.75$$

$$q = 3 : \quad \#C(\mathbb{F}_q) \leq 1.153g + 11.67.$$

For $q = 2$, let a_i be the number of degree- i closed points on C ; then

$$a_1 + 0.3366(2a_2) + 0.1382(3a_3) + 0.0537(4a_4) \leq 0.8042g + 5.619.$$

For each q , combining this slide with the previous one limits (g, g') to an explicit finite list. With some care, the bounds can be brought down to a reasonable size; for instance, for $q = 2$ the worst case that survives is $(g, g') = (9, 17)$.

Inverting the Weil polynomial by exhaustion

We need to solve various instances of the following problem: given a Weil polynomial P potentially coming from a genus- g curves over \mathbb{F}_q with $g \leq 7$, find all such curves. In the following cases, this can be done by lookup into a table of **all** genus- g curves over \mathbb{F}_q :

$g \leq 3$, $q \leq 4$ (Howe). All such curves are either hyperelliptic or plane quartic.

$g = 4$, $q = 2$ (Xarles). All such curves are hyperelliptic, trigonal, or a complete intersection of type $(2, 3)$ in \mathbf{P}^3 .

$g = 5$, $q = 2$ (Dragutinović). All such curves are hyperelliptic, trigonal, or a complete intersection of type $(2, 2, 2)$ in \mathbf{P}^4 .

Inverting the Weil polynomial without exhaustion

We also need some cases with $g \in \{6, 7\}$, $q = 2$. One has a similar description of all genus- g curves (Mukai), with the generic case being a complete intersection in a certain homogenous space.

In principle it should be possible to make a full enumeration using Mukai's description. Instead, we short-circuit by imposing constraints coming from our set of Weil polynomials. For instance, for $g = 7$ we know that $\#C(\mathbb{F}_2) \in \{6, 7\}$. (We have about 40 polynomials to handle in all.)

We find two examples of relative class number 1 with $g = 6, g' = 11$. The curves C are generic (not hyperelliptic, trigonal, bielliptic, or plane quintic).

We find one example of relative class number 1 with $g = 7, g' = 13$. The curve C is bielliptic.

Noncyclic covers: scope of the problem

Given an explicit function field F , it is easy using MAGMA to compute its abelian extensions with prescribed ramification (explicit class field theory). This makes it easy to find **cyclic** extensions with relative class number 1, without even using any constraints on the Weil polynomial of F' .

For $d = 2$, there is nothing more to do. However, we must also consider cases with $d \in \{3, \dots, 7\}$, for which it is hard to enumerate noncyclic extensions (more on this later).

Instead, we try to show that there are **no** noncyclic extensions giving rise to the pairs of Weil polynomials that we found. Luckily this succeeds!

The paradigm for $d = 3, 4, 5, 6$

For $d = 3, 4, 5, 6$ we are able to execute a strategy of the following form.

- ① Enumerate options for the splitting of the places of F of low degree that are consistent with the Weil polynomials of F and F' and the possible ramification types of the covering.
- ② Let F''/F be the Galois closure of F'/F . For each of these options and each option $G \subseteq S_d$ for $\text{Gal}(F''/F)$, compute point counts for the other subfields of F'' .
- ③ Using the character table of G , translate the point counts into Frobenius traces for the various isogeny factors of $J(C'')$.
- ④ Enumerate Weil polynomials consistent with these Frobenius traces. Ideally there are none; otherwise, go back to the beginning and enlarge the degree cutoff.

What about $d = 7$?

For $d = 7$, this strategy seems to be infeasible and we did not attempt it. Fortunately, we only have one case to handle, which **does** occur for a cyclic cover.

Luckily, this case is well-suited^{||} to methods of Howe, which can be used to show that the cover has to admit an order-7 automorphism.

^{||}Elision from earlier: such methods are also needed to settle two cases with $g = 1, g' = 6$. In one of them, C' is forced to admit an order-5 automorphism.

What about larger relative class numbers?

In principle, one can use similar techniques to solve the relative class number m problem** for any fixed $m > 1$, with two caveats.

- It is probably hopeless to classify abelian varieties A over \mathbb{F}_2 with $\#A(\mathbb{F}_2) = m$. However, it should be possible to make a direct linear programming argument to establish a useful lower bound on some linear combination of traces of A .
- We cannot hope to exclude noncyclic extensions. One alternative might be a good method to enumerate degree- d extensions of a fixed function field; for $d = 3, 4, 5$ this should be doable†† using Bhargava's parametrizations.

** Again, when the base field has genus 0 or 1, one can only hope to describe the isomorphism classes of the two fields and not the morphism.

†† In the number field setting, this was done by Belabas for $d = 3$.