The relative class number one problem for function fields, III

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.

LMFDB, Computation, and Number Theory (LuCaNT)
ICERM, Providence, RI
July 13, 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.

Contents

The relative class number one problem

Let F'/F be an extension of degree d of function fields associated to a cover $C' \to C$ of curves[1] over finite fields. Let g, g' be the genera of F and F'. Let q, q' be the cardinalities of the base fields[2] of F, F'.

Let h, h' be the class numbers[3] 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 where $\dim(A) = 0$:

- $g = g' = 0$;
- $q = q'$ and $1 \leq g = g'$.

[1] All curves are smooth, projective, and geometrically irreducible (a/k/a "nice").
[2] By "base field" I mean the integral closure of the prime subfield.
[3] That is, $h = \#J(C)(\mathbb{F}_q)$ and $h' = \#J(C')(\mathbb{F}_{q'})$.

A heuristic for finiteness

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

The condition $h'/h = 1$ means $\#A(\mathbb{F}_q)$ is abnormally **small**. This implies (roughly) that the Frobenius trace $T_{A,q}$ of A is abnormally **large**. Since

$$\begin{aligned} T_{A,q} &= T_{C',q} - T_{C,q}, \\ T_{C',q} &= q + 1 - \#C'(\mathbb{F}_q) \leq q + 1, \\ T_{C,q} &= q + 1 - \#C(\mathbb{F}_q), \end{aligned}$$

this means $T_{C,q}$ is abnormally **small** and so $\#C(\mathbb{F}_q)$ is abnormally **large**.

Using "linear programming" bounds on $\#C(\mathbb{F}_q)$ in terms of g, one can establish an effective finiteness result. By also accounting for d (Riemann–Hurwitz, Deuring–Shafarevich, splitting behavior), one can make this bound practical.

An answer, part I

I reported some partial results at ANTS-XV (Bristol, June 2022).

- **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., $q \in \{3, 4\}$. Assume hereafter $q = 2$.
- **Solved** when $g \leq 1$ (we get $g' \leq 6$).[4] 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[5] $\zeta_F, \zeta_{F'}$ 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 plus explicit class field theory (Magma).

For the last step, LMFDB includes a complete census of genus-g curves over $\mathbb{F}_2$ for $g \leq 3$ (Sutherland), $g = 4$ (Xarles), and $g = 5$ (Dragutinović).

[4] The case $g = 0$ was handled by Mercuri–Stirpe and Shen–Shi; we get $g' \leq 4$.

[5] Reminder: the data of ζ_F and $(\#C(\mathbb{F}_{q^i}))_{i=1}^{g}$ are equivalent.

An answer, part II

I reported another partial result at AGC^{2}T (Luminy, June 2023).

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.

The proof strategy: for each pair $(\zeta_F, \zeta_{F'})$ with $3 \leq d \leq 7$ listed in the ANTS-XV data, check that the noncyclic options for the Galois group lead to abelian varieties[6] with untenable point counts.

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 of places, and cyclic covers are most resistant to this pressure.

[6] These are certain isogeny factors of the Jacobian of the Galois closure. Compare Paulhus's ANTS-X paper.

Contents

Where am I now? (part 1 of 2)

The only remaining cases of the relative class number one problem are $q = 2$, $g \in \{6, 7\}$, and F'/F is unramified of degree 2. Again it will suffice to find all F with a given ζ_F, then use MAGMA to find F' and h'/h.

If $g = 6$ then $\#C(\mathbb{F}_2), \dots, \#C(\mathbb{F}_{2^6})$ appears in this list:

4, 14, 16, 18, 14, 92	5, 11, 11, 31, 40, 53	6, 10, 9, 38, 11, 79
4, 14, 16, 18, 24, 68	5, 11, 11, 31, 40, 65	6, 10, 9, 38, 21, 67
4, 14, 16, 26, 14, 68	5, 11, 11, 39, 20, 53	6, 10, 9, 38, 31, 55
4, 16, 16, 20, 9, 64	5, 11, 11, 39, 20, 65	6, 14, 6, 26, 26, 68
5, 11, 11, 31, 20, 65	5, 13, 14, 25, 15, 70	6, 14, 6, 26, 26, 80
5, 11, 11, 31, 20, 77	5, 13, 14, 25, 15, 82	6, 14, 6, 26, 36, 56
5, 11, 11, 31, 20, 89	5, 13, 14, 25, 15, 94	6, 14, 6, 34, 16, 56
5, 11, 11, 31, 30, 53	5, 13, 14, 25, 25, 46	6, 14, 6, 34, 26, 44
5, 11, 11, 31, 30, 65	5, 13, 14, 25, 25, 58	6, 14, 12, 26, 6, 44
5, 11, 11, 31, 30, 77	5, 13, 14, 25, 25, 70	6, 14, 12, 26, 6, 56
5, 11, 11, 31, 30, 89	5, 15, 5, 35, 20, 45	6, 14, 12, 26, 6, 66

Where am I now? (part 2 of 2)

If $g = 7$ then $\#C(\mathbb{F}_2), \dots, \#C(\mathbb{F}_{2^7})$ appears in this list:

6, 18, 12, 18, 6, 60, 174
6, 18, 12, 18, 6, 72, 132
6, 18, 12, 18, 6, 84, 90
7, 15, 7, 31, 12, 69, 126
7, 15, 7, 31, 22, 45, 112
7, 15, 7, 31, 22, 57, 70
7, 15, 7, 31, 22, 57, 84

Note that $\#C(\mathbb{F}_2)$ is "large" (in particular nonzero) but not "extremely large": for $g \in \{6, 7\}$, the maximum number of points on a genus-g curve over $\mathbb{F}_2$ is 10. Hence we **do** expect to find some curves C, so methods based on ruling out curves cannot cover the entire range.

An iteration over curves

We instead construct an iteration over a (possibly redundant) set of isomorphism representatives for genus-g curves over $\mathbb{F}_2$.

Previous calculations of this sort (e.g., in the work of Faber[7]–Grantham on the gonality of curves over finite fields) use singular plane models. Here, we instead use Mukai's descriptions of canonically embedded genus-g curves in terms of linear sections of homogeneous varieties, with some extra effort paid to descending special linear systems to finite base fields.

[7] This is Xander, not Carel.

Contents

Special linear systems

Let C be a curve of genus g over a finite field k. A g^r_d is a line bundle of degree d whose space of global sections has dimension $r+1$; if such a bundle is basepoint-free, then it defines a degree-d map to $\mathbf{P}^r_k$. For example, the canonical bundle is a g^r_d for $r = g-1, d = 2g-2$.

Since k is finite, every Galois-invariant divisor class on C contains a k-rational divisor. In particular, if $C_{\overline{k}}$ admits a **unique** g^r_d for some r, d, then so does C.[8]

For example, the Castelnuovo–Severi inequality implies that if $g > (d-1)^2$, then $C_{\overline{k}}$ can have at most one g^1_d. We say C is **hyperelliptic** if it admits a unique g^1_2 and **trigonal** if it is not hyperelliptic but admits a unique g^1_3.

[8] By contrast, over $\mathbb{Q}$, when $g > 2$ it is possible for a curve to be "geometrically hyperelliptic" by being a double cover of a pointless genus-0 curve.

The canonical embedding

The canonical system defines a map $\iota : C \to \mathbf{P}_k^{g-1}$ which is an embedding **unless** C is hyperelliptic (then ι is a 2-1 cover of a rational normal curve).

By Petri's theorem[9], $\iota(C)$ is cut out (schematically) by quadrics **unless**

- C is trigonal, or
- $g = 6$ and C is a smooth plane quintic.

This implies that the usual classification of curves of genus up to 5 remains valid when k is finite:[10]

- If $g = 2$, then C is hyperelliptic.
- If $g = 3$, then C is hyperelliptic or a CI[11] of type (4) in $\mathbf{P}_k^2$.
- If $g = 4$, then C is hyperelliptic or a CI of type $(2) \cap (3)$ in $\mathbf{P}_k^3$.
- If $g = 5$, then C is hyperelliptic, trigonal, or a CI of type $(2) \cap (2) \cap (2)$ in $\mathbf{P}_k^4$.

[9] More precisely, by Saint-Donat's version valid in any characteristic.

[10] For k perfect, we must insert "geometrically" before "hyperelliptic/trigonal".

[11] complete intersection

The Maroni invariant of a trigonal curve

For C trigonal, the quadrics vanishing on $\iota(C)$ cut out a Hirzebruch surface

$$\mathbf{F}_n = \mathbf{Proj}_{\mathbf{P}^1_k}(\mathcal{O}_{\mathbf{P}^1_k} \oplus \mathcal{O}(n)_{\mathbf{P}^1_k})$$

embedded in $\mathbf{P}^{g-1}$ by $|b + (n+1+i)f|$ for some $i \geq 0$ where f is a fiber of $\mathbf{F}_n \to \mathbf{P}^1_k$ and b is the unique irreducible curve with $b^2 = -n$.

We call n the **Maroni invariant** of C. We have $b \cdot C = \frac{g-3n+2}{2}$, so so $n \in \{0, \dots, \frac{g+2}{3}\}$ and $n \equiv g \pmod 2$.

For $n = 0$, $\mathbf{F}_{0,\overline{k}} \cong \mathbf{P}^1_{\overline{k}} \times \mathbf{P}^1_{\overline{k}}$ and $C_{\overline{k}}$ is a $(3, \frac{g+2}{2})$-hypersurface. Since $\frac{g+2}{2} \neq 3$ for $g \geq 5$, this description descends to k.

For $n > 0$, $\mathbf{F}_n$ is an $(n, 1)$-hypersurface in $\mathbf{P}^1_k \times \mathbf{P}^2_k$. Blowing down along b yields the weighted projective space $\mathbf{P}(1 : 1 : n)_k$.

Contents

The Brill-Noether stratification for $g = 6$

From a corresponding result of Mukai over $\overline{k}$, we deduce that for $g = 6$, C has one of the following forms.

- Hyperelliptic.
- Trigonal of Maroni invariant 2: CI of type $(2,1) \cap (1,3)$ in $\mathbf{P}^1_k \times \mathbf{P}^2_k$.
- Trigonal of Maroni invariant 0: CI of type $(3,4)$ in $\mathbf{P}^1_k \times \mathbf{P}^1_k$.
- **Bielliptic**:[12] double cover of a genus 1 curve.
- Smooth quintic: CI of type (5) in $\mathbf{P}^2_k$.
- A CI of type $(1)^4 \cap (2)$ in the Grassmannian $\mathrm{Gr}(2,5) \subset \mathbf{P}^9_k$ in its Plücker embedding.

[12] Again by Castelnuovo–Severi, this cover is unique for $g > 5$, and so descends to k.

The Brill-Noether stratification for $g = 7$

By Mukai again, for $g = 7$, C has one of the following forms.

- Hyperelliptic.
- Trigonal of Maroni invariant 3: CI of type (9) in $\mathbf{P}(1:1:3)_k$.
- Trigonal of Maroni invariant 1: CI of type $(1,1) \cap (3,3)$ in $\mathbf{P}^1_k \times \mathbf{P}^2_k$.
- Bielliptic.
- Not bielliptic but admits a self-adjoint g^2_6: CI of type $(3) \cap (4)$ in $\mathbf{P}(1:1:1:2)_k$.
- Admits two distinct g^2_6's over k: CI of type $(1,1) \cap (1,1) \cap (2,2)$ in $\mathbf{P}^2_k \times \mathbf{P}^2_k$.
- Admits two distinct g^2_6's only over $\overline{k}$: CI of type $(1,1) \cap (1,1) \cap (2,2)$ in the quadratic twist of $\mathbf{P}^2_k \times \mathbf{P}^2_k$.
- **Tetragonal** (admits a g^1_4 but not a g^1_3 or g^2_6): CI of type $(1,1) \cap (1,2) \cap (1,2)$ in $\mathbf{P}^1_k \times \mathbf{P}^3_k$.
- None of the above, see below.

Generic canonical curves of genus 7

Let V be the vector space k^{10} equipped with the quadratic form[13] $\sum_{i=1}^{5} x_i x_{5+i}$. Let $\mathrm{SO}(V)$ be the index-2 subgroup of the orthogonal group of V on which the **Dickson invariant** is trivial.

The 10-dimensional **orthogonal Grassmannian** OG parametrizes Lagrangian (maximal isotropic) subspaces of V. It admits a canonical **spinor embedding** $\mathrm{OG} \hookrightarrow \mathbf{P}^{15}_k$ on which $\mathrm{SO}(V)$ acts transitively.

There are two connected components of OG, stabilized by $\mathrm{SO}(V)$. Given $L_0 \in \mathrm{OG}(k)$, we may characterize the component OG^+ containing L_0 as parametrizing L with $\dim_k(L \cap L_0) \equiv 1 \pmod 2$.

Theorem (after Mukai)

Every canonical genus-7 curve over k arises as a CI of type $(1)^9$ in OG^+.

[13] For k finite, there is a second form with no Lagrangian subspaces defined over k; but the fact that curves always have points over large **odd**-degree extensions means we don't need to worry about the second form.

Contents

Review of point count conditions

For $g = 6$, we are looking for C for which $\#C(\mathbb{F}_2), \dots, \#C(\mathbb{F}_{2^6})$ appears in:

4, 14, 16, 18, 14, 92	5, 11, 11, 31, 40, 53	6, 10, 9, 38, 11, 79
4, 14, 16, 18, 24, 68	5, 11, 11, 31, 40, 65	6, 10, 9, 38, 21, 67
4, 14, 16, 26, 14, 68	5, 11, 11, 39, 20, 53	6, 10, 9, 38, 31, 55
4, 16, 16, 20, 9, 64	5, 11, 11, 39, 20, 65	6, 14, 6, 26, 26, 68
5, 11, 11, 31, 20, 65	5, 13, 14, 25, 15, 70	6, 14, 6, 26, 26, 80
5, 11, 11, 31, 20, 77	5, 13, 14, 25, 15, 82	6, 14, 6, 26, 36, 56
5, 11, 11, 31, 20, 89	5, 13, 14, 25, 15, 94	6, 14, 6, 34, 16, 56
5, 11, 11, 31, 30, 53	5, 13, 14, 25, 25, 46	6, 14, 6, 34, 26, 44
5, 11, 11, 31, 30, 65	5, 13, 14, 25, 25, 58	6, 14, 12, 26, 6, 44
5, 11, 11, 31, 30, 77	5, 13, 14, 25, 25, 70	6, 14, 12, 26, 6, 56
5, 11, 11, 31, 30, 89	5, 15, 5, 35, 20, 45	6, 14, 12, 26, 6, 66

For $g = 7$, we are looking for C for which $\#C(\mathbb{F}_2), \dots, \#C(\mathbb{F}_{2^7})$ appears in:

6, 18, 12, 18, 6, 60, 174	7, 15, 7, 31, 12, 69, 126	7, 15, 7, 31, 22, 57, 70
6, 18, 12, 18, 6, 72, 132	7, 15, 7, 31, 22, 45, 112	7, 15, 7, 31, 22, 57, 84
6, 18, 12, 18, 6, 84, 90		

Initial cases

- If $g = 6$, then C cannot be hyperelliptic: we have $\#C(\mathbb{F}_4) > 10 = 2\#\mathbf{P}^1(\mathbb{F}_4)$ except in three cases where $\#C(\mathbb{F}_{16}) = 38 > 34 = 2\#\mathbf{P}^1(\mathbb{F}_{16})$.
- If $g = 7$, then C cannot be hyperelliptic: we have $\#C(\mathbb{F}_4) \geq 15 > 10 = 2\#\mathbf{P}^1(\mathbb{F}_4)$.
- If $g = 7$ and $\#C(\mathbb{F}_2) = 6$, then C cannot be trigonal: we have $\#C(\mathbb{F}_4) = 18 > 15 = 3\#\mathbf{P}^1(\mathbb{F}_4)$.
- If $g = 7$ and $\#C(\mathbb{F}_2) = 7$, then C cannot be trigonal of Maroni invariant 3: we have $\#C(\mathbb{F}_2) = 7$ which exceeds the number of *smooth* points of $\mathbf{P}(1:1:3)(\mathbb{F}_2)$.

Also, for C bielliptic, we can identify options for the genus-1 curve, then use $\textsc{Magma}$ to compute all double covers of the right genus.

A paradigm for the remaining cases

In each remaining case, we are looking for certain complete intersections $X_1 \cap \cdots \cap X_m$ inside some homogeneous variety X over $\mathbb{F}_2$.

- Compute $S := X(\mathbb{F}_2)$ and $G := \mathrm{Aut}(X)(\mathbb{F}_2)$.
- Compute orbit representatives for the G-action on subsets of S of size at most g. More on this below.[14]
- For each representative subset of size in $\{4, 5, 6\}$ (if $g = 6$) or $\{6, 7\}$ (if $g = 7$), use linear algebra to find all tuples of hypersurfaces $X_1, \dots, X_{m-1}$ of the desired degrees containing these $\mathbb{F}_2$-points.
- For each choice, impose linear conditions on X_m to ensure that $X_1 \cap \cdots \cap X_m$ has *exactly* the specified set of $\mathbb{F}_2$-rational points. This crucially exploits the fact that the base field is $\mathbb{F}_2$; a similar strategy is used by Faber–Grantham.

[14] For $g = 7, X = \mathrm{OG}^+$, we use a slightly different setup that requires only the action on 6-element subsets.

Group actions on subsets

Let G be a finite group acting on a finite set S. We need to compute orbit representatives for the action of G on k-element subsets of S **without** instantiating in memory the full list of k-element subsets.

For this we use an inductive combinatorial construction called an **orbit lookup tree**. It answers the question: given a sequence $x_1, \dots, x_k$, find a permutation π of $\{1, \dots, k\}$ and an element $g \in G$ such that for each i, $\{g(x_{\pi(1)}), \dots, g(x_{\pi(i)})\}$ is an orbit representative for i-element subsets.

In some cases, a strategy introduced by Auel–Kulkarni–Petok–Weinbaum based on decomposing $k[G]$-modules may be superior.

Summary of the computation

Type of C	Dim	$\#C$	$\#C'$	Time[15]
$g = 6$, hyperelliptic	11	0	0	—
$g = 6$, trigonal, Maroni 2	12	9	0	10m
$g = 6$, trigonal, Maroni 0	13	9	0	2m
$g = 6$, bielliptic	10	0	0	—
$g = 6$, plane quintic	12	1	0	1m
$g = 6$, generic	15	38	2	4h
$g = 7$, hyperelliptic	13	0	0	—
$g = 7$, trigonal, Maroni 3	13	0	0	—
$g = 7$, trigonal, Maroni 1	15	0	0	5m
$g = 7$, bielliptic	12	2	1	5m
$g = 7$, self-adjoint g^2_6	15	0	0	5m
$g = 7$, rational g^2_6	16	0	0	30m
$g = 7$, irrational g^2_6	16	0	0	45m
$g = 7$, tetragonal, no g^2_6	17	1	0	2h
$g = 7$, generic	18	1	0	1h

[15] These are wall times on a laptop. Don't take them too seriously; there are many confounding factors at work.

The final results

Theorem

(a) *There are two isomorphism classes of curves C of genus 6 over $\mathbb{F}_2$ admitting an étale double covering $C' \to C$ such that $\#J(C')(\mathbb{F}_2) = \#J(C)(\mathbb{F}_2)$. The curves C are Brill–Noether general with automorphism groups C_3 and C_5.*

(b) *There is a unique isomorphism class of curves C of genus 7 over $\mathbb{F}_2$ admitting an étale double covering $C' \to C$ such that $\#J(C')(\mathbb{F}_2) = \#J(C)(\mathbb{F}_2)$. The curve C is bielliptic with automorphism group D_6.*

In the latter case, C admits the affine model

$$\operatorname{Spec} \frac{\mathbb{F}_2[x,y,z]}{(y^2 + (x^3 + x^2 + 1)y + x^2(x^2 + x + 1), z^2 + z + x^2(x + 1)y)}.$$

Contents

A full census of genus-6 and genus-7 curves

It would be desirable to have a full census of genus-g curves over $\mathbb{F}_2$ for $g = 6, 7$. This would provide a valuable consistency check, and also serve as a rich resource for future investigation (ideally as part of LMFDB).

A further consistency check[16] would be provided by computing[17] $\# M_g(\mathbb{F}_2)$ using explicit generators/relations for the Chow ring. For $g = 6$, this has been achieved using very recent work of Canning–H. Larson.[18]

It should be possible to upgrade our existing code to remove the filtering on zeta functions to achieve a full census. For $g = 6$, this is work in progress with Jun Bo Lau, but extra help would be welcome.

[16] Such a count can even be used to **certify** the validity of a census: it is easy to compute automorphism groups and check pairwise nonisomorphism for an explicit list of curves, this providing a concrete lower bound on stacky $\# M_g(\mathbb{F}_2)$.

[17] This point count is **stacky**: the isomorphism class of a curve C has weight $\frac{1}{\# \mathrm{Aut}(C)}$.

[18] Odd coincidence: Hannah is also lecturing in Providence at this hour!

Into the wild: beyond genus 7

Since M_g has dimension $3g-3$, we expect $\#M_g(\mathbb{F}_2)$ to be roughly 2^{3g-3}. So it might be feasible to compile a census[19] of genus-g curves over $\mathbb{F}_2$ for $g = 8, 9, 10$.

Conveniently, Mukai also has similar descriptions of canonical curves in these genera. For example, a general canonical genus-8 curve is a linear section of $\mathrm{Gr}(2,6) \subset \mathbf{P}^{14}_k$.

However, it will take significant implementation skill to keep the complexity down to a manageable level.

[19] Faber-Grantham encountered a single zeta function that they had to show did not occur in genus 9. Fortunately they were able to do this by "pure thought".