MOST HYPERELLIPTIC CURVES HAVE BIG MONODROMY

EMMANUEL KOWALSKI

Let $k/\mathbf{Q}$ be a number field and $\mathbf{Z}_k$ its ring of integers. Let $f \in \mathbf{Z}_k[X]$ be a monic squarefree polynomial of degree $n = 2g+2$ or $2g+1$ for some integer $g \geqslant 1$, and let C_f/k be the (smooth, projective) hyperelliptic curve of genus g with affine equation

$$C_f \,:\, y^2 = f(x),$$

and J_f its jacobian.

In [Ha], C. Hall shows that the image of the Galois representation

$$\rho_{f,\ell} \,:\, \mathrm{Gal}(\bar{k}/k) \rightarrow \mathrm{Aut}(J_f[\ell](\bar{k})) \simeq \mathrm{GL}_{2g}(\mathbf{F}_\ell)$$

on the ℓ-torsion points of J_f is as big as possible for almost all primes ℓ, if the following two (sufficient) conditions hold:

(1) the endomorphism ring of J_f is $\mathbf{Z}$;

(2) for some prime ideal $\mathfrak{p} \subset \mathbf{Z}_k$, the fiber over $\mathfrak{p}$ of the Néron model of C_f is a smooth curve except for a single ordinary double point.

These conditions can be translated concretely in terms of the polynomial f, and are implied by:

(1') the Galois group of the splitting field of f is the full symmetric group $\mathfrak{S}_n$ (this is due to a result of Zarhin [Z], which shows that this condition implies (1));

(2') for some prime ideal $\mathfrak{p} \subset \mathbf{Z}_k$, f factors in $\mathbf{F}_\mathfrak{p} = \mathbf{Z}_k/\mathfrak{p}\mathbf{Z}_k$ as $f = f_1 f_2$ where $f_i \in \mathbf{F}_\mathfrak{p}[X]$ are relatively prime polynomials such that $f_1 = (X-\alpha)^2$ for some $\alpha \in \mathbf{F}_\mathfrak{p}$ and f_2 is squarefree of degree $n-2$; indeed, this implies (2).

In this note, we show that, in some sense, "most" polynomials f satisfy these two conditions, hence "most" jacobians of hyperelliptic curves have maximal monodromy modulo all but finitely many primes (which may, a priori, depend on the polynomial, of course!).

More precisely, for k and $\mathbf{Z}_k$ as above, let us denote

$$\mathcal{F}_n = \{f \in \mathbf{Z}_k[X] \mid f \text{ is monic of degree } n\},$$

and let the height be defined on $\mathcal{F}_n$ by

$$H(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n) = \max_{0 \leqslant i \leqslant n-1} H(a_i),$$

where H is any reasonable height function on k, e.g., choose a $\mathbf{Z}$-basis $(\omega_i)_{1 \leqslant i \leqslant d}$ of $\mathbf{Z}_k$, where $d = [k : \mathbf{Q}]$, and let

$$H(\alpha_1\omega_1 + \cdots + \alpha_d\omega_d) = \max |\alpha_i|,$$

for all $(\alpha_i) \in \mathbf{Z}^d$.

Let $\mathcal{F}_n(T)$ denote the finite set

$$\mathcal{F}_n(T) = \{f \in \mathcal{F}_n \mid H(f) \leqslant T\}. \tag{1}$$

We have $|\mathcal{F}_n(T)| = N_k(T)^n$, where

$$N_k(T) = |\{x \in \mathbf{Z}_k \mid H(x) \leqslant T\}| \asymp T^d, \text{ where } d = [k : \mathbf{Q}].$$

Say that f has *big monodromy* if the Galois group of its splitting field is $\mathfrak{S}_n$. We will show:

Proposition 1. *Let k and $\mathbf{Z}_k$ be as above. Then*

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have big monodromy}\}| \ll N_k(T)^{n-1/2}(\log N_k(T)),$$

for all $T \geqslant 2$, where the implied constant depends on k and n.

Say that $f \in \mathcal{F}_n$ has *ordinary ramification* if it satisfies condition (2') above.

Proposition 2. *Let k and $\mathbf{Z}_k$ be as above, and assume $n \geqslant 2$. There exists a constant $c > 0$, depending on n and k, such that we have*

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have ordinary ramification}\}| \ll \frac{N_k(T)^n}{(\log N_k(T))^c}$$

for $T \geqslant 3$, where the implied constant depends on k and n.

Finally, say that J_f has *big monodromy* if the image of $\rho_{f,\ell}$ is as big as possible for almost all primes ℓ.

Corollary 3. *Assume that $n \geqslant 2$. Then we have*

$$\lim_{T\to+\infty} \frac{1}{|\mathcal{F}_n(T)|}|\{f \in \mathcal{F}_n(T) \mid J_f \text{ does not have big monodromy}\}| = 0.$$

Remark 4. Quantitatively, we have proved that the rate of decay of this probability is at least a small power of power of logarithm, because of Proposition 2. With more work, one should be able to get c equal or very close to 1, but it seems hard to do better with the current ideas (the problem being in part that we must avoid f for which the discriminant is a unit in $\mathbf{Z}_k$, which may well exist, and sieve can not detect them better than it does discriminants which generate prime ideals, the density of which could be expected to be about $(\log N_k(T))^{-1}$).

For both propositions, in the language of [K1], we consider a sieve with data

$$(\mathcal{F}_n, \{\text{prime ideals in } \mathbf{Z}_k\}, \{\text{reduction modulo } \mathfrak{p}\}), \quad (\mathcal{F}_n(T), \text{counting measure}),$$

and we claim that the "large sieve constant" Δ for the sifting range

$$\mathcal{L}^* = \{\mathfrak{p} \subset \mathbf{Z}_k \mid N\mathfrak{p} \leqslant L\}$$

satisfies

$$\Delta \ll N_k(T)^n + L^{2n},$$

where the implied constant depends only on k. Indeed, this follows from the work of Huxley [Hu], by combining in an obvious manner his Theorem 2 (which is the case $n = 1$, k arbitrary) with his Theorem 1 (which is the case $k = \mathbf{Q}$, n arbitrary).

Concretely, this implies that for arbitrary subsets $\Omega_\mathfrak{p}$ in the image of $\mathcal{F}_n$ under reduction modulo $\mathfrak{p}$ — the latter is simply the set of monic polynomials of degree n in $\mathbf{F}_\mathfrak{p}[X]$, and has cardinality $(N\mathfrak{p})^n$ — we have

(2)
$$|\{f \in \mathcal{F}(T) \mid f\,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_\mathfrak{p} \text{ for } N\mathfrak{p} \leqslant L\}| \ll (N_k(T)^n + L^{2n})\Big(\sideset{}{^\flat}\sum_{N\mathfrak{a}\leqslant L} \prod_{\mathfrak{p}|\mathfrak{a}} \frac{|\Omega_\mathfrak{p}|}{(N\mathfrak{p})^n - |\Omega_\mathfrak{p}|}\Big)^{-1},$$

where the sum is over squarefree ideals in $\mathbf{Z}_k$ with norm at most L, and therefore also

$$|\{f \in \mathcal{F}(T) \mid f\,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_{\mathfrak{p}} \text{ for } N\mathfrak{p} \leqslant L\} \ll (N_k(T)^n + L^{2n})\Big(\sum_{N\mathfrak{p}\leqslant L} \frac{|\Omega_{\mathfrak{p}}|}{(N\mathfrak{p})^n}\Big)^{-1}. \tag{3}$$

Proposition 1 is a result of S.D. Cohen [C]; it is also a simple application of the methods of Gallagher [G] (one only needs (3) here), the basic idea being that elements of the Galois group of the splitting field of a polynomial f are detected using the factorization of f modulo prime ideals. We recall that the first quantitative result of this type (for $k = \mathbf{Q}$) is due to van der Waerden [vdW], whose weaker result would be sufficient here (though the proof is not simpler than Gallagher's).

Proof of Proposition 2. Let $\mathfrak{p} \subset \mathbf{Z}_k$ be a prime ideal, and let $\Omega_{\mathfrak{p}}$ be the set of polynomials $f \in \mathbf{F}_{\mathfrak{p}}[X]$ which are monic of degree n and factor as described in Condition (2'). We claim that, for some constant $c > 0$, $c \leqslant 1$ (depending on k and n), we have

$$\frac{|\Omega_{\mathfrak{p}}|}{(N\mathfrak{p})^n} \geqslant \frac{c}{N\mathfrak{p}} \tag{4}$$

for all prime ideals with norm $N\mathfrak{p} \geqslant P_0$, for some P_0 depending on k and n.

Indeed, for $n \geqslant 4$, we have clearly

$$|\Omega_{\mathfrak{p}}| \geqslant (N\mathfrak{p}) \times |\{f \in \mathbf{F}_{\mathfrak{p}}[X] \mid \deg(f) = n-2,\ f \text{ monic irreducible}\}|;$$

for $n = 2$, this holds with the convention that 1 is irreducible of degree 0, and for $n = 3$, we must subtract 1 from the second factor on the right. If $n = 2$, we are done, otherwise it is well-known that

$$|\{f \in \mathbf{F}_q[X] \mid \deg(f) = n-2,\ f \text{ monic irreducible}\}| \sim \frac{q^{n-2}}{n-2}$$

as $q \to +\infty$, hence the lower bound (4) follows by combining these two facts (showing we can take for c any constant $< (n-2)^{-1}$ if P_0 is chosen large enough; using more complicated factorizations of the squarefree factor of degree $n-2$, one could get c arbitrarily close to 1).

Now we apply (3) with this choice of subsets for $\mathfrak{p}$ with norm $> P_0$, and with $\Omega_{\mathfrak{p}} = \emptyset$ for other $\mathfrak{p}$. We take $L = N_k(T)^{1/2}$, assuming that $L > P_0$, i.e., that T is large enough. Since, if $f \in \mathcal{F}_n(T)$ does not have ordinary ramification, we have by definition $f\,(\mathrm{mod}\,\mathfrak{p}) \notin \Omega_{\mathfrak{p}}$ for any $\mathfrak{p}$, it follows by simple computations that

$$|\{f \in \mathcal{F}_n(T) \mid f \text{ does not have ordinary ramification}\}| \ll N_k(T)^n H^{-1}$$

where the implied constant depends on k and

$$H = \sideset{}{^\flat}\sum_{N\mathfrak{a}\leqslant L} c^{\omega(\mathfrak{a})}(N\mathfrak{a})^{-1},$$

where now $\sum^\flat$ restricts the sum to squarefree ideals not divisible by a prime ideal of norm $\leqslant P_0$, and where $\omega(\mathfrak{a})$ is the number of prime ideals dividing $\mathfrak{a}$.

Writing

$$H = \sum_{n\leqslant L} \beta(n) n^{-1}$$

where

$$\beta(n) = \sum_{N\mathfrak{a}=n}^{\flat} c^{\omega(\mathfrak{a})},$$

it follows then from standard estimates about sums of multiplicative functions that

$$H \gg (\log L)^c$$

for L large enough, depending on P_0; recall that $0 < c \leqslant 1$. (E.g., one can easily check that Wirsing's Theorem cited in [K1, Th. G.1] is applicable to β with $\kappa = c$, by applying the Chebotarev density theorem to check the assumption of that result, and this leads even to an asymptotic formula; the idea is that the partial sum is comparable with that of the coefficients of $\zeta_k(s)^c$, where ζ_k is the Dedekind zeta function). This leads to the proposition, since L and $N_k(T)$ are comparable in logarithmic scale. □

References

[C] S.D. Cohen: *The distribution of the Galois groups of integral polynomials*, Illinois J. Math. 23 (1979), 135–152.

[G] P.X. Gallagher: *The large sieve and probabilistic Galois theory*, in Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc. (1973), 91–101.

[Ha] C.J. Hall: *Transvections and ℓ-torsion of abelian varieties*, preprint (2009).

[Hu] M.N. Huxley: *The large sieve inequality for algebraic number fields*, Mathematika 15 (1968) 178–187.

[K1] E. Kowalski: *The large sieve and its applications: arithmetic geometry, random walks, discrete groups*, Cambridge Univ. Tracts 175, C. U. P., 2008.

[vdW] B.L. van der Waerden: *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monath. Math. Phys. 43 (1936), 133–147.

[Z] Y.G. Zarhin: *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. 7 (2000), no. 1, 123–132.

ETH Zürich - DMATH, Rämistrasse 101, 8092 Zürich, Switzerland

E-mail address: kowalski@math.ethz.ch