RANK AND BIAS IN FAMILIES OF HYPERELLIPTIC CURVES VIA NAGAO'S CONJECTURE

TRAJAN HAMMONDS, SEOYOUNG KIM, BENJAMIN LOGSDON, ÁLVARO LOZANO-ROBLEDO, AND STEVEN J. MILLER

ABSTRACT. Let $\mathcal{X} : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}(T)$ of genus $g \geq 1$. Assume that the jacobian of $\mathcal{X}$ over $\mathbb{Q}(T)$ has no subvariety defined over $\mathbb{Q}$. Denote by $\mathcal{X}_t$ the specialization of $\mathcal{X}$ to an integer $T = t$, let $a_{\mathcal{X}_t}(p)$ be its trace of Frobenius, and let $A_{\mathcal{X},r}(p) = \frac{1}{p} \sum_{t=1}^{p} a_{\mathcal{X}_t}(p)^r$ be its r-th moment. The first moment is related to the rank of the jacobian $J_{\mathcal{X}}(\mathbb{Q}(T))$ by a generalization of a conjecture of Nagao:

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \leq X} -A_{\mathcal{X},1}(p) \log p = \operatorname{rank} J_{\mathcal{X}}(\mathbb{Q}(T)).$$

Generalizing a result of S. Arms, Á. Lozano-Robledo, and S.J. Miller, we compute first moments for various families resulting in infinitely many hyperelliptic curves over $\mathbb{Q}(T)$ having jacobian of moderately large rank $4g + 2$, where g is the genus; by Silverman's specialization theorem, this yields hyperelliptic curves over $\mathbb{Q}$ with large rank jacobian. Note that Shioda has the better record in this direction: he constructed hyperelliptic curves of genus g with jacobian of rank $4g + 7$. In the case when $\mathcal{X}$ is an elliptic curve, Michel proved $p \cdot A_{\mathcal{X},2} = p^2 + O\left(p^{3/2}\right)$. For the families studied, we observe the same second moment expansion. Furthermore, we observe the largest lower order term that does not average to zero is on average negative, a bias first noted by S.J. Miller in the elliptic curve case. We prove this bias for a number of families of hyperelliptic curves.

1. INTRODUCTION

Given an elliptic curve $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ with A and B integers, the Mordell–Weil theorem shows that the set of rational solutions $E(\mathbb{Q})$ forms a finitely generated abelian group. Mazur [Maz1, Maz2] proved there are only fifteen possibilities for the torsion subgroup, all of which occur for infinitely many non-isomorphic elliptic curves over $\mathbb{Q}$. However, much less is known about the rank. Recent breakthroughs, such as [Bh, BhSh1, BhSh2], have shown that the average rank among all elliptic curves over $\mathbb{Q}$ is bounded by 7/6, and that a positive percentage of curves are rank 0, but it is still unknown if the rank is unbounded as we vary over all curves. The largest known rank is at least 28, due to Noam Elkies [E], and some recent models (see [PPVW]) suggest that the rank may in fact be bounded (interestingly, their prediction for the largest rank is very close to the largest observed!).

If the Birch and Swinnerton-Dyer conjecture [BSD1, BSD2] holds, then the order of vanishing of the Hasse–Weil L-function $L(E/\mathbb{Q}, s)$ at the central point (the analytic rank) equals the number of generators of the Mordell–Weil group (the algebraic rank). Conjecturally, however, there are other relations between the traces of Frobenius at each prime p and the algebraic rank. Nagao posited that the first moment sums in a one-parameter family of elliptic curves determine the rank of the elliptic surface. More concretely, let

$$(1.1) \qquad \mathcal{E} : y^2 = x^2 + A(T)x + B(T)$$

be an elliptic curve over $\mathbb{Q}(T)$ and, for an integer $t \in \mathbb{Z}$, let

$$(1.2) \qquad a_{\mathcal{E}_t}(p) \;=\; p + 1 - \#\mathcal{E}_t(\mathbb{F}_p),$$

where $\#\mathcal{E}_t(\mathbb{F}_p)$ is the number of points over $\mathbb{F}_p$ on the specialization of $\mathcal{E}$ at $T = t$. Also, for each $r \geq 1$, we define the rth moment of the traces of Frobenius by

$$(1.3) \qquad A_{\mathcal{E},r}(p) \;=\; \frac{1}{p} \sum_{t=0}^{p-1} a_{\mathcal{E}_t}(p)^r.$$

Then, Nagao [Na3] conjectured that

$$(1.4) \qquad \lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} -A_{\mathcal{E},1}(p) \log p \;=\; \operatorname{rank} \mathcal{E}(\mathbb{Q}(T)).$$

Rosen and Silverman [RS] have proved that Nagao's conjecture holds for surfaces where Tate's conjecture holds, which includes rational surfaces[1]. The second author [Kim] has shown that the Sato-Tate conjecture implies Nagao's conjecture for certain twist families of elliptic curves, and also in a generalized form for hyperelliptic curves, that we shall describe below.

There has been a long history of attempts to construct either individual elliptic curves with large rank, or families with large rank. Many of these were found by looking for curves where these associated sums are large and then analyzing these curves carefully; however, the work of Nagao, Rosen and Silverman presents another approach. If one can find a family of elliptic curves so that the sum $A_{\mathcal{E},1}(p)$ is computable, then we would conjecturally have computed (unconditionally if Tate's conjecture is true for the surface) the rank of the family. Thus, the challenge is to find choices of $A(T)$ and $B(T)$ so that the resulting moments $A_{\mathcal{E},1}(p)$ can be computed and are negative, and large in absolute value. This was first done by Arms, Lozano-Robledo and Miller [ALM, Mil1, Mil2], where elliptic curves over $\mathbb{Q}(T)$ of rank up to 8 were constructed[2], and then generalized in [MMRSY] to function fields over number fields. In this paper, we are interested in constructing jacobians of hyperelliptic curves over $\mathbb{Q}$ with high rank, conditional on the following generalization of Nagao's conjecture.

Conjecture 1.1. *Let $\mathcal{X}$ be a hyperelliptic curve defined over $\mathbb{Q}(T)$. Assume that the jacobian of $\mathcal{X}$ over $\mathbb{Q}(T)$ has no subvariety defined over $\mathbb{Q}$. For an integer $t \in \mathbb{Z}$, let $\#\mathcal{X}_t(\mathbb{F}_p)$ be the number of points over $\mathbb{F}_p$ on the specialization of $\mathcal{X}$ at $T = t$, and for each prime $p \geq 2$, we define $a_{\mathcal{X}_t}(p) = p + 1 - \#\mathcal{X}_t(\mathbb{F}_p)$, and $A_{\mathcal{X},1}(p) = \frac{1}{p} \sum_{t=0}^{p-1} a_{\mathcal{X}_t}(p)$. Then, we have*

$$(1.5) \qquad \lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} -A_{\mathcal{X},1}(p) \log p \;=\; \operatorname{rank} J_{\mathcal{X}}(\mathbb{Q}(T)).$$

We recall here that the Chow $\mathbb{Q}(T)/\mathbb{Q}$ trace of an abelian variety $A/\mathbb{Q}(T)$ is a pair $(\tau, B/\mathbb{Q})$, where B is an abelian variety over $\mathbb{Q}$, and $\tau\colon B \to A$ is a homomorphism of abelian varieties defined over $\mathbb{Q}(T)$, with the universal mapping property that, given any such pair (τ', B'), the map $\tau'\colon B' \to A$ should factor through τ (see [C] for more details on Chow traces). In particular, we note that if $A/\mathbb{Q}(T)$ has no subvariety defined over $\mathbb{Q}$, then its Chow trace is necessarily trivial.

Hindry and Pacheco [HP] have given a more general version of Nagao's conjecture for a projective surface with a fibration onto a curve. We shall discuss below the relation between their conjecture and Conjecture 1.1.

In our main theorem, and for each fixed genus $g \geq 1$, we construct a hyperelliptic curve $\mathcal{X} : y^2 = f_g(x, T)$ such that Nagao's limit is computable, and if we assume Conjecture 1.1, then its jacobian has rank $4g + 2$. We note that preliminary data of hyperelliptic curves ordered by

---

[1]The elliptic surface is rational iff one of the following is true: (1) $0 < \max\{3\deg A, 2\deg B\} < 12$; (2) $3\deg A = 2\deg B = 12$ and $\operatorname{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0$. See [RS], pages $46-47$ for more details.

[2]Up to rank 6 the constructions gave rational surfaces and the results were unconditional; for the larger rank the surfaces were not rational, but one can isolate candidate points from the method, and then directly show that these are linearly independent. The rank 8 case would correspond in this setting to rank 4g+4, but we do not pursue this in this paper.

discriminant up to size 10^6 and 10^7, due to Sutherland [Su], show that 95.68% of genus 2 curves (resp. 92.52% of genus 3 curves) have analytic rank 0, 1, or 2 (resp. 0,1,2, or 3). Thus, a rank of 10 (resp. 14) in a hyperelliptic jacobian of genus 2 (resp. genus 3) is well above the average rank one would expect.

Theorem 1.2. *Let $g \geq 1$ be fixed, and assume that the jacobian of $\mathcal{X}$ over $\mathbb{Q}(T)$ has no subvariety defined over $\mathbb{Q}$ in its factorization. Then, Conjecture 1.1 implies that the jacobian of $\mathcal{X}$ has rank $4g + 2$ over $\mathbb{Q}(T)$.*

Each specialization of T to an integer t gives a hyperelliptic curve $\mathcal{X}_t$ over $\mathbb{Q}$ of genus g. By the specialization theorem of Néron, Silverman, and Tate we produce examples of hyperelliptic jacobians over $\mathbb{Q}$ with moderate rank.

Corollary 1.3. *Let $g \geq 1$ be fixed, and assume the conditions from Theorem 1.2. Then, there are infinitely many hyperelliptic curves over $\mathbb{Q}$ of genus g with rank at least $4g + 2$.*

We remark here that Shioda [Sh1] has produced examples of hyperelliptic jacobians over $\mathbb{Q}$ with rank $4g + 7$. Our approach, however, is different from that of Shioda because we do not need to exhibit points in the jacobian $J_\mathcal{X}$ in order to (conjecturally) deduce its rank. Note also when $g = 1$ we recover the result in [ALM] and, in that case, the result is unconditional since Nagao's conjecture is known for rational surfaces.

Example 1.4. *When $g = 2$, our construction (see Sections 4.3 and 4.4) yields, for instance, the following hyperelliptic curve over $\mathbb{Q}(T)$ of genus 2, with trivial Chow trace (see below), and conjectural rank 10:*

$$
\begin{aligned}
\mathcal{X} : y^2 = f(x, T) = {} & 624764679274960436330496000000000 x^5 T^2 \\
& + 1249529358549920872660992000000000 x^5 T \\
& - 329080786084534587317408441482126295040000000 x^5 \\
& - 780771244568520743299045501636880021299200000 x^4 T \\
& + 126688294930102536253784468113282127199787008000 x^4 \\
& - 123371083167607662332725955346616811520000000 x^3 T \\
& + 243931316579178829424195314754396457957219840205596481 21 x^3 \\
& + 977809477912386424285879709825236992000000000 x^2 T \\
& + 771061216671488509646569562558331367512145294273931520 00 x^2 \\
& - 254999391610370282637413063055114240000000000000 xT \\
& - 107885191824305149307223906345415330631958573883392000 0 x \\
& + 3290807860845408349642011910864896000000000000 T \\
& + 1524014810925296267945145551729277974339657041182720000 000.
\end{aligned}
$$

When evaluating at $T = 1$, we obtain a hyperelliptic curve over $\mathbb{Q}$ of genus 2 and rank ≥ 10:

$$
\begin{aligned}
C : y^2 = f(x) = {} & -329080786084515844377030192669036380160000000 0 x^5 \\
& + 126680487217656851046351477658265758399574016 0000 x^4 \\
& + 2439313165779451185925192381310691984037536720 9039648121 x^3 \\
& + 771061216672466319124481948982617247221970531 26593152000 x^2 \\
& - 1078851920793045409175941889828283936870728138 833920000 x \\
& + 15240148109285870758059909600789199862505219371 82720000000.
\end{aligned}
$$

First, we note that the quintic polynomial $f(x) = f(x, 1)$ has Galois group S_5 (verified using Magma). Hence, the polynomial $f(x, T)$ must have generic Galois group S_5 as well. A theorem of Zarhin (Theorem 3.2) now shows that $J_\mathcal{X}(\mathbb{Q}(T))$ must be an absolutely simple abelian variety. In particular, its Chow trace must be trivial.

In order to verify that the rank of the jacobian $J_C/\mathbb{Q}$ of C is ≥ 10, we have found 10 rational points $P_{\mathcal{X},i}$ on $\mathcal{X}(\mathbb{Q}(T))$, given by:

$$P_{\mathcal{X},1} = (1, 7904205711360000T + 4030428281951822662650591373 9),$$
$$P_{\mathcal{X},2} = (4, 252934582763520000T - 656852958963092283737847540 88),$$
$$P_{\mathcal{X},3} = (9, 1920721987860480000T - 159820218040209384630193418504 7),$$
$$P_{\mathcal{X},4} = (16, 8093906648432640000T - 3480808342520943564187101607 04),$$
$$P_{\mathcal{X},5} = (25, 24700642848000000000T - 65637757003820653671375137462 5),$$
$$P_{\mathcal{X},6} = (36, 61463103611535360000T - 111332950618790961825250887237 6),$$
$$P_{\mathcal{X},7} = (49, 132845985390827520000T - 174826681870029778880328477152 3),$$
$$P_{\mathcal{X},8} = (64, 259005012749844480000T - 259071659377494958432768474163 2),$$
$$P_{\mathcal{X},9} = (81, 466735443050096640000T - 367027018546299819729991656426 9),$$
$$P_{\mathcal{X},10} = (100, 790420571136000000000T - 50165429116498937900583124370 00).$$

We evaluated $P_{\mathcal{X},i}$ at $T = 1$ to obtain points P_i on $C(\mathbb{Q})$, and finally we defined points $(P_i) - (\mathcal{O})$ on the jacobian J_C, where $\mathcal{O}$ is the unique point at infinity. Here are the points:

$P_1 = (1, 4030428281952613083221727373 9), P_2 = (4, 6568529589605629379102123408 8),$

$P_3 = (9, 1598202180401731243140737050 47), P_4 = (16, 3480808342440004497702775207 04),$

$P_5 = (25 : 6563775700135058938657513746 25 : 1), P_6 = (36 : 1113329506126446514640973512 376 : 1),$

$P_7 = (49 : 1748266818567451803412457251 523 : 1), P_8 = (64 : 2590716593515944571577840261 632 : 1),$

$P_9 = (81 : 3670270184996262754249819924 269 : 1), P_{10} = (100 : 5016542910859473218922312437 000 : 1).$

Further, we have computed the canonical height matrix for these 10 points, and its determinant, which equals $1131062371638072163.8139\ldots \neq 0$. Thus, the points $\{(P_i) - (\mathcal{O})\}$ are independent and the rank of $J_C(\mathbb{Q})$ is at least 10. Further, since these points come from evaluating points on $J_{\mathcal{X}}(\mathbb{Q}(T))$, we conclude that the points $\{(P_{\mathcal{X},i}) - (\mathcal{O})\}$ on $J_{\mathcal{X}}$ must be independent also, and so the rank of $J_{\mathcal{X}}$ must be ≥ 10 as well, in agreement with the generalized Nagao's Conjecture 1.1.

Note that Shioda [Sh1] has constructed a curve of genus g defined over $\mathbb{Q}(t_1, t_2, \ldots, t_n)$ of rank $4g + 7$ for any $g > 1$. In a private communication, Elkies has pointed out that methods using K3 surfaces one can construct genus 2 jacobians with rank about 20.

1.1. **Results on higher moments.** So far we have just focused on the first moments; however, the second moments are also interesting and play a key role in several problems. For one-parameter families of elliptic curves, Michel [Mi] proved that if $j(T)$ is non-constant then

(1.6) $$pA_{\mathcal{E},2}(p) \;=\; p^2 + O\left(p^{3/2}\right)$$

(we have multiplied the second moment by p to match the quantity he studied); there are cohomological interpretations of the lower order terms, and Miller [Mil3] showed that the bound is sharp by exhibiting a family with a term of that size. While early investigations of the second moment was for the purpose of bounding the average rank in families, these are also key ingredients in understanding the behavior of zeros of the L-functions near the central point. According to the Katz-Sarnak theory [KS1, KS2], in the limit as the conductors tend to infinity the behavior of zeros near the central point behave similarly with the scaling limit of a subgroup of unitary matrices as their sizes tend to infinity (this is true for far more than just families of elliptic curves; see for example the survey article [MMRTW]).

Interestingly, the main terms for the n-level densities of the low-lying zeros of families of elliptic curves depend only very weakly on the different values of the moments $A_{\mathcal{E},r}(p)$. The first two moments contribute to the main term; if the first moment is k then there is a contribution equal to what one would expect if there were k zeros at the central point, providing evidence in support of the Birch and Swinnerton-Dyer Conjecture (for more on this see [GM]). The second moment's universality (of p^2 for families with non-constant $j(T)$, and $2p^2$ half the time and 0 half the time for $j(T)$ constant) is similar to the universality of the second moments of Satake

parameters in the work of Rudnick and Sarnak [RuSa], which was responsible for the universal behavior in the n-level correlations. If $r \geq 3$ then these terms never contribute to the main term. It is also similar to the Central Limit Theorem, where the universality is due to our ability to standardize any nice density to have mean zero and variance one (i.e., fix the first two moments), and the higher moments only surface in controlling the rate of convergence.

While the main term in the behavior of low-lying zeros is independent of the finer properties of the arithmetic of the curve, the higher moments ($r \geq 3$) and the lower order terms in the first and second moments *are* observable in lower order corrections (i.e., in the rate of convergence). In particular, the lower order terms in the second moment have applications towards understanding the observed excess rank in many families of elliptic curves (see [Mil3]), while the higher moments allow us to distinguish different families of elliptic curves in fine properties of the behavior of zeros near the central point (see [Mil4]).

In this paper we concentrate on the first two moments. As has been remarked above, the first moment can be used to construct families with rank. The second moment is related to finer questions about the distribution of zeros. Interestingly, in all families of elliptic curves investigated to date, the first lower order term in the second moment $A_{\mathcal{E},2}(p)$ which does not average to zero always averages to a negative value; see [A–, MMRW] for results for families of elliptic curves, as well as generalizations to other families of L-functions. In our study of families of hyperelliptic curves, we observe this same bias.

Our results are as follows. Let $g \geq 1$ be arbitrary, put $n = 2g+1$, and let $0 \leq k < n$. We shall consider the family $\mathcal{X}_{n,h,k} : y^2 = x^n + x^h T^k$. We show the following (the proof can be found in Section 5):

Theorem 1.5. *Suppose* $\gcd(k, n-h, p-1) = 1$. *Then*

$$(1.7) \quad p \cdot A_{\mathcal{X}_{n,h,1},2}(p) = \begin{cases} (\gcd(p-1, n-h) - 1)(p^2 - p) & \text{if } h \text{ even,} \\ \gcd(n-h, p-1)(p^2 - p) & \text{if } h \text{ odd and } \nu_2(p-1) > \nu_2(n-h), \\ 0 & \text{otherwise.} \end{cases}$$

The paper is organized as follows. In Section 2 we recall the Hindry–Pacheco generalized version of Nagao's conjecture for surfaces and compare it to our version Conjecture 1.1. In Section 3 we give some related results and some preliminary lemmas about computations with Legendre symbols. In Section 4 we give constructions of hyperelliptic jacobians of rank $2g$, $2g+1$, and finally $4g + 2$, in Sections 4.1, 4.2, and 4.3, respectively, and in Section 4.4 we specialize our $4g + 2$ construction in the case of $g = 2$ and rank 10. Finally, in Section 5, we compute the second moments in a family of hyperelliptic curves of arbitrary genus.

2. Generalized Nagao's conjecture for surfaces

In this section, we recall Hindry and Pacheco's [HP] generalized Nagao's conjecture for a projective surface with a fibration onto a curve. Let $\mathcal{X}$ be a projective smooth irreducible surface over $\mathbb{Q}$ with a proper flat fibration $f : \mathcal{X} \to \mathbb{P}^1$ which allows us to have (arithmetic) curves of genus $g \geq 1$ for each fiber. Moreover, this implies that the generic fiber X is a smooth irreducible curve over the function field of $\mathbb{P}^1$, i.e., $\mathbb{Q}(T)$. Denote by $J_{\mathcal{X}}$ the jacobian variety of X and (τ, B) the $\mathbb{Q}(T)/\mathbb{Q}$-Chow trace of $J_{\mathcal{X}}$. The following theorem of Lang and Néron shows a Mordell–Weil analogue for a jacobian variety over function field.

Theorem 2.1. *The quotients $J_{\mathcal{X}}(\mathbb{Q}(T))/\tau(B(\mathbb{Q}))$ and $J_{\mathcal{X}}(\bar{\mathbb{Q}}(T))/\tau(B(\bar{\mathbb{Q}}))$ are both finitely generated groups.*

Hindry and Pacheco generalized Nagao's conjecture to compute the rank of $J_{\mathcal{X}}(\mathbb{Q}(T))/\tau(B(\mathbb{Q}))$. We describe Hindry and Pacheco's work next (over $\mathbb{Q}$ for simplicity, but they work over a number field).

Let $\mathcal{X}$ be a smooth irreducible projective surface over $\mathbb{Q}$ and let C be a smooth irreducible projective curve over $\mathbb{Q}$ which allows a proper flat morphism $f : \mathcal{X} \to C$ so that the fibers are curves of (arithmetic) genus $g \geq 1$. Let $J_{\mathcal{X}}$ be the jacobian of $\mathcal{X}/\mathbb{Q}(C)$, and let (τ, B) be the $\mathbb{Q}(C)/\mathbb{Q}$-Chow trace of $J_{\mathcal{X}}$. For a prime p, we can consider the reduction $\tilde{f} : \tilde{\mathcal{X}} \to \tilde{C}$ of f. Define

a finite set of primes S which satisfies the following conditions: for all $p \notin S$, the surface $\mathcal{X}$ and the curve C have good reduction and the reduced morphism $\tilde{f}: \tilde{\mathcal{X}} \to \tilde{C}$ is proper and flat. And, the fibers are curves with arithmetic genus g over the residue field $\mathbb{F}_p$.

Denote $\tilde{\mathcal{X}}_t = \tilde{f}^{-1}(t)$, i.e., the fiber of $\tilde{f}$ at $t \in \tilde{C}(\mathbb{F}_p)$. Denote $\overline{\mathcal{X}}_t = \mathcal{X}_t \times_{\mathbb{Q}} \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$. Let $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ be a Frobenius element and $I_p \subset G_{\mathbb{Q}}$ be the inertia group at p. Also, define the discriminant of the fibration f by $\Delta_f = \{t \in C : \tilde{\mathcal{X}}_t \text{ is singular}\}$. By enlarging the set S if necessary, we can make the discriminant of $\tilde{f}$ be the same as the discriminant of f modulo p outside of S.

Let $\overline{\mathrm{Frob}}_p$ be the Frobenius automorphism on $H^1_{\text{ét}}(\overline{\mathcal{X}}_t, \mathbb{Q}_\ell)$. Define the trace of Frobenius using cohomology as

$$a_{\mathcal{X}_t}(p) = \mathrm{Tr}(\overline{\mathrm{Frob}}_p | H^1_{\text{ét}}(\overline{\mathcal{X}}_t, \mathbb{Q}_\ell)),$$

where we consider ℓ-adic cohomology with compact support if $t \in \tilde{\Delta}_f(\mathbb{F}_p)$, that is to say,

$$(2.1) \qquad a_{\mathcal{X}_t}(p) = \mathrm{Tr}(\overline{\mathrm{Frob}}_p | H^1_{\mathrm{c}}(\overline{\mathcal{X}}_t, \mathbb{Q}_\ell)).$$

Also define a trace of Frobenius for the Chow trace B by

$$a_B(p) = \mathrm{Tr}(\overline{\mathrm{Frob}}_p | H^1_{\text{ét}}(\overline{B}, \mathbb{Q}_\ell)^{I_p}),$$

where $\overline{B} = B \times_{\mathbb{Q}} \overline{\mathbb{Q}}$. By enlarging the set S if necessary, we can assume that B has good reduction for primes $p \notin S$, i.e.,

$$a_B(p) = \mathrm{Tr}(\overline{\mathrm{Frob}}_p | H^1_{\text{ét}}(\overline{B}, \mathbb{Q}_\ell)).$$

Now we are ready to state Hindry and Pacheco's version of [Na3].

Conjecture 2.2 (Hindry–Pacheco, [HP]). *Let $\mathcal{X}$, C, and f be as above, and define*

$$A_{\mathcal{X},1}(p) = \frac{1}{p} \sum_{t \in C(\mathbb{F}_p)} a_{\mathcal{X}_t}(p), \text{ and } A^*_{\mathcal{X}}(p) = A_{\mathcal{X},1}(p) - a_B(p).$$

Then:

$$(2.2) \qquad \lim_{P \to \infty} \frac{1}{P} \sum_{\substack{p \notin S \\ p \leq P}} -A^*_{\mathcal{X}}(p) \cdot \log p = \mathrm{rank}\left(\frac{J_{\mathcal{X}}(\mathbb{Q}(C))}{\tau(B(\mathbb{Q}))}\right).$$

Under the hypothesis that the surface satisfies Tate's conjecture, they show the following.

Theorem 2.3 (Hindry–Pacheco, [HP], Thm. 1.3). *Suppose that the surface $\mathcal{X}$ satisfies Tate's conjecture. Then,*

$$\mathop{\mathrm{res}}_{s=1}\left(\sum_{p \notin S} -A^*_{\mathcal{X}}(p) \cdot \frac{\log p}{p^s}\right) = \mathrm{rank}\left(\frac{J_{\mathcal{X}}(\mathbb{Q}(C))}{\tau(B(\mathbb{Q}))}\right).$$

If in addition the L function $L_2(\mathcal{X}/\mathbb{Q}, s)$ associated to $H^2_{\text{ét}}(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ has an analytic continuation on $\Re(s) = 2$, and does not have zeros on this line, then Conjecture 2.2 holds.

In order to compare Conjecture 1.1 with the Hindry–Pacheco version, we quote the following lemma from [HP, Lemme 3.2] (see also [RS, Lemma 1.7.]).

Lemma 2.4. *Let $\mathcal{X}/\mathbb{Q}$ be a surface as above, with $C = \mathbb{P}^1$. Let $p \notin S$, and $t \in \mathbb{F}_p$. Denote by $m_{t,p}$ the number of $\mathbb{F}_p$-rational components of the reduced fiber $\tilde{\mathcal{X}}_t$ modulo p. We denote by $\#\mathcal{X}_t(\mathbb{F}_p)$ the number of solutions on the reduced fiber $\tilde{\mathcal{X}}_t$ over $\mathbb{F}_p$. Let $a_{\mathcal{X}_t}(p)$ be the trace of Frobenius defined by Equation (2.1). Then*

$$(2.3) \qquad a_{\mathcal{X}_t}(p) = p \cdot m_{t,p} + 1 - \#\mathcal{X}_t(\mathbb{F}_p).$$

In particular, when $\mathcal{X}_t$ has good reduction at $p \notin S$, we get $m_{t,p} = 1$ and therefore the definitions of $a_{\mathcal{X}_t}(p)$ in Equation (2.1) and Conjecture 1.1 coincide.

3. PRELIMINARIES AND AUXILIARY LEMMAS

First, we cite a result of Nagao, about the convergence of the limits that appear in the conjectures. Below, $\pi(x)$ is the prime counting function.

Lemma 3.1 (Nagao, [Na3], Lemmas 2.1 and 2.2). *Let $\{c_p\}_p$ be a bounded sequence of non-negative numbers indexed by prime numbers. If one of the sequences of numbers*

$$\left\{\frac{1}{\pi(N)}\sum_{p \leq N} c_p\right\}_N \quad \text{and} \quad \left\{\frac{1}{N}\sum_{p \leq N} c_p \cdot \log p\right\}_N$$

converges, then both of them converge to a common limit. In particular, $\{\frac{1}{N}\sum_{p \leq N}\log p\}_N$ is a convergent sequence, and the limit is 1.

Next we cite work of Zarhin [Za1, Za2, Za3] that we shall use in order to prove that a Chow trace is trivial.

Theorem 3.2 (Zarhin). *Let K be a field of characteristic different from 2, and suppose that $f \in K[x]$ is a polynomial of degree n without multiple roots, such that $\mathrm{Gal}(f)$ is either S_n or A_n. Let $C : y^2 = f(x)$ and let $J(C_f)$ be its jacobian. Assume also that either $\mathrm{char}(K) \neq 3$ or $n \geq 7$. Then, $\mathrm{End}(J(C_f)) = \mathbb{Z}$. In particular, $J(C_f)$ is an absolutely simple abelian variety.*

Let $C : y^2 = f(x)$ be a hyperelliptic curve, with $f(x)$ of odd degree, and let p be a prime number. Since the degree of f is odd, there is a unique point $\mathcal{O}$ at infinity. Then, one can count the (affine) points on $C^*(\mathbb{F}_p) = C(\mathbb{F}_p) - \{\mathcal{O}\}$ via Legendre symbols, by

$$\#C^*(\mathbb{F}_p) = \sum_{\substack{x(p) \\ f(x)\equiv 0 \bmod p}} 1 + \sum_{\substack{x(p) \\ f(x)\not\equiv 0 \bmod p}} \left(1 + \left(\frac{f(x)}{p}\right)\right) = p + \sum_{x(p)}\left(\frac{f(x)}{p}\right),$$

where $x(p) = \{x : 0 \leq x \leq p - 1\}$. Thus,

$$a_C(p) = p + 1 - \#C(\mathbb{F}_p) = p + 1 - \left(1 + p + \sum_{x(p)}\left(\frac{f(x)}{p}\right)\right) = -\sum_{x(p)}\left(\frac{f(x)}{p}\right),$$

Thus, if $\mathcal{X} : y^2 = f(x, T)$ is a hyperelliptic surface, then

$$A_{\mathcal{X},1}(p) = \frac{1}{p}\sum_{t(p)} a_{\mathcal{X}_t}(p) = -\frac{1}{p}\sum_{t,x(p)}\left(\frac{f(x,t)}{p}\right),$$

where $t, x(p)$ means that both t and x range in the interval $0, \ldots, p - 1$. In the remainder of this section, we show a number of lemmas about sums of Legendre symbols that we will use in the next sections. First, we reproduce [ALM, Lemma A.2] that shall be used in computing first and second moments.

Lemma 3.3. *Assume a and b are not both zero $\bmod p$ and $p > 2$. Then*

$$(3.1) \qquad \sum_{t=0}^{p-1}\left(\frac{at^2 + bt + c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2 - 4ac, \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases}$$

Lemma 3.4. *For any $p > 2$, we have $\sum_{t(p)}\left(\frac{at+b}{p}\right) = 0$, for any integers $a, b \in \mathbb{Z}$ with $a \not\equiv 0 \bmod p$.*

Proof. As t runs over all elements of $\mathbb{F}_p$, the quantity $at + b$ also runs over all elements of $\mathbb{F}_p$. There are $(p-1)/2$ quadratic residues, and $(p-1)/2$ quadratic non-residues, so the sum cancels out. $\qquad\square$

Lemma 3.5. *Fix $n \geq 1$ and a prime number p. Then, the number of solutions (x, y) to the congruence $x^n \equiv y^n \bmod p$ is given by $\gcd(p - 1, n) \cdot (p - 1) + 1$.*

7

Proof. First note that $x \equiv y \equiv 0 \bmod p$ is a solution. Otherwise, let x, y be non-zero mod p, with $x^n \equiv y^n \bmod p$. Let g be a generator of $\mathbb{F}_p^\times$, and write $x \equiv g^a$ and $y \equiv g^b \bmod p$ for some a and b. Hence we have $g^{an} \equiv g^{bn} \bmod p$ and so $g^{an-bn} \equiv 1 \bmod p$. Since the order of g is $p - 1$, by Lagrange's theorem, we have

$$an - bn \equiv n(a - b) \equiv 0 \bmod p - 1.$$

The congruence $nX \equiv 0 \bmod p - 1$ has $\gcd(n, p - 1)$ solutions for X and each solution for X yields $p - 1$ solutions (a, b). Hence, there are $\gcd(n, p - 1) \cdot (p - 1) + 1$ solutions to the original congruence. $\qed$

Lemma 3.6. *Let $h \geq 2$ be even. Let $S_h(p) := \displaystyle\sum_{\substack{x,y(p) \\ x^h \equiv y^h \bmod p}} \left(\dfrac{xy}{p}\right)$. Furthermore, let ν_2 be the usual 2-adic valuation. Then,*

$$(3.2) \qquad S_h(p) = \begin{cases} \gcd(h, p-1)(p-1) & \text{if } \nu_2(p-1) > \nu_2(h), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We proceed by passing from the multiplicative group $\mathbb{F}_p^\times$ to the cyclic additive group $\mathbb{Z}/(p-1)\mathbb{Z}$ (by implicitly fixing a primitive root). In $\mathbb{Z}/(p-1)$, we use $\langle a \rangle$ to denote the subgroup generated by a.

$$(3.3) \qquad S_h(p) := \sum_{\substack{a,b(p) \\ a^h \equiv b^h \bmod p}} \left(\frac{ab}{p}\right) = \sum_{\substack{x,y(p-1) \\ ha \equiv hb \bmod p-1}} \left(\begin{cases} 1 & a + b \in \langle 2 \rangle \\ -1 & \text{otherwise} \end{cases} \right).$$

We know that $h(y - x) \equiv 0 \bmod p$ iff $y - x \in \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle$ iff $y \in x + \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle$. Furthermore, $x + y \in \langle 2 \rangle$ iff $x + y - 2x \in \langle 2 \rangle$ iff $y \in x + \langle 2 \rangle$. Thus, we have

$$(3.4) \qquad = \sum_{\substack{x,y(p-1) \\ y \in \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle}} \left(\begin{cases} 1 & y \in x + \langle 2 \rangle \\ -1 & \text{otherwise} \end{cases} \right) = \sum_{x(p-1)} \sum_{\substack{y(p-1) \\ y \in x + \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle}} \left(2 \cdot \mathbf{1}_{y \in x + \langle 2 \rangle} - 1 \right)$$

$$(3.5) \qquad = \sum_{x(p-1)} \left(2 \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \cap \langle 2 \rangle \right| - \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \right| \right).$$

If $\frac{p-1}{\gcd(h,p-1)} \in \langle 2 \rangle$, then this is

$$(3.6) \qquad = \sum_{x(p-1)} \left(2 \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \right| - \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \right| \right) = (p-1)\gcd(h, p-1).$$

If $\frac{p-1}{\gcd(h,p-1)} \notin \langle 2 \rangle$, then this is

$$(3.7) \qquad = \sum_{x(p-1)} \left(2 \cdot \frac{1}{2} \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \right| - \left| \left\langle \frac{p-1}{\gcd(h,p-1)} \right\rangle \right| \right) = 0.$$

Since $\frac{p-1}{\gcd(h,p-1)} \in \langle 2 \rangle$ precisely when $\nu_2(p-1) > \nu_2(h)$, this completes the proof. $\qed$

Lemma 3.7. *Let k, n_1, and n_2 be integers. If $\gcd(k, n_1, n_2) = 1$, then there exists an m such that $\gcd(m, n_1) = 1$ and $m \equiv k \bmod n_2$.*

Proof. By Dirichlet's theorem on primes in arithmetic progressions, one can choose a prime $m \equiv k \bmod n_2$ such that $m > n_1$. $\qed$

4. Jacobians of Hyperelliptic Curves with Positive Rank Over $\mathbb{Q}(T)$

In this section we will show a number of constructions that yield hyperelliptic curves $\mathcal{X}/\mathbb{Q}(T)$ such that their jacobians have positive rank.

4.1. Rank $2g$. In [Na3, Proposition 3.2.], Nagao considers the elliptic curve

$$\mathcal{E}/\mathbb{Q}(T) : y^2 = f(x) + T^2,$$

where $f(x) \in \mathbb{Z}[x]$ is a monic cubic polynomial without double roots, and computed $A_{\mathcal{E},1}(p)$ for this family. In particular, he showed

(4.1)
$$- A_{\mathcal{E},1}(p) = \begin{cases} 2p & \text{if } f(x) \bmod p \text{ factors completely,} \\ -p & \text{if } f(x) \bmod p \text{ is irreducible,} \\ 0 & \text{if otherwise.} \end{cases}$$

We now present an analogous construction for curves of genus g and compute their corresponding Legendre sums. Let $g \geq 1$ be fixed, and let

$$\mathcal{X}/\mathbb{Q}(T) : y^2 = f(x) + T^2,$$

where $f(x)$ is a monic degree $2g+1$ polynomial without double roots. Note that the discriminant in t of $f(x) + t^2$ is $-4f(x)$, and so if $p > 2$, then the condition that $p \mid -4f(x)$ is equivalent to $p \mid f(x)$. Hence, using Lemma 3.3, we have

$$
\begin{aligned}
-p \cdot A_{\mathcal{X},1}(p) &= \sum_{t,x(p)} \left(\frac{f(x) + t^2}{p} \right) \\
&= \sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} (p-1) \left(\frac{1}{p} \right) - \sum_{\substack{x(p) \\ f(x) \not\equiv 0 \bmod p}} \left(\frac{1}{p} \right) \\
&= \sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} p \left(\frac{1}{p} \right) - \sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} \left(\frac{1}{p} \right) - \sum_{\substack{x(p) \\ f(x) \not\equiv 0 \bmod p}} \left(\frac{1}{p} \right) \\
&= \sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} p - \sum_{x(p)} \left(\frac{1}{p} \right) = p \# \{x \in \mathbb{Z}/p\mathbb{Z} \mid f(x) \equiv 0 \bmod p\} - p.
\end{aligned}
$$
(4.2)

Let $\tilde{f}(x)$ denote $f(x) \bmod p$ and write L_f for the number of distinct linear factors in the factorization of $\tilde{f}(x)$. Then

(4.3)
$$- p \cdot A_{\mathcal{X},1}(p) = (L_f - 1) \cdot p,$$

and in particular, if $\tilde{f}(x)$ factors completely, then $L_f = 2g + 1$ and $-p \cdot A_{\mathcal{X},1}(p) = 2gp$. If we choose $f(x)$ so that it splits completely over $\mathbb{Q}$, then we have $-p \cdot A_{\mathcal{X},1}(p) = 2gp$ for all sufficiently large p. Thus, Lemma 3.1 implies that

$$\lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} -A_{\mathcal{X},1}(p) \cdot \log p = \lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} 2g \cdot \log p = 2g.$$

Further, if $f(x)$ is a Morse function, then the Galois group of $f(x) + T^2$ over $\mathbb{Q}(T)$ is S_n, by [Se, Theorem 4.4.5]. Hence, Zarhin's Theorem 3.2 shows that, under these conditions, $J_{\mathcal{X}}(\mathbb{Q}(T))$ is an absolutely simple abelian variety, and therefore the $\mathbb{Q}(T)/\mathbb{Q}$-Chow trace of $\mathcal{X}$ is trivial. Thus, Conjecture 1.1 implies that rank $J_{\mathcal{X}}(\mathbb{Q}(T)) = 2g$.

In this case, Shioda [Sh2] has shown that $J_{\mathcal{X}}(\mathbb{Q}(T))$ has rank $2g$ by exhibiting $2g$ independent points. Moreover, Hindry and Pacheco [HP, Exemple 5.6] show that $\mathcal{X}$ is a rational surface, and therefore Tate's conjecture and Conjecture 2.2 hold for this surface, showing again that rank $J_{\mathcal{X}}(\mathbb{Q}(T)) = 2g$.

Example 4.1. *Let $f(x) = (x-1)(x-2) \cdots (x-7)$ and let $\mathcal{X} : y^2 = f(x) + T^2$. Specializing at $T = 2$ we obtain the hyperelliptic curve of genus 3 given by*

$$\mathcal{X}_2 : y^2 = x^7 - 28x^6 + 322x^5 - 1960x^4 + 6769x^3 - 13132x^2 + 13068x - 5036,$$

which Magma shows to be of rank $2g = 6$. In fact, one can check that the points $(P_i) - (\mathcal{O})$ given by $P_i = (i, T)$, for $T = 2$, are independent in $J_{\mathcal{X}_2}(\mathbb{Q})$. Hence, the same points are independent

9

in $J_{\mathcal{X}}$ over $\mathbb{Q}(T)$. Magma also verifies that the Galois group of $f(x) + 4$ is S_7, and therefore the Galois group of $f(x) + T^2$ over $\mathbb{Q}(T)$ is S_7 as well. Thus, $J_{\mathcal{X}}(\mathbb{Q}(T))$ is a simple hyperelliptic jacobian of rank 6.

If we put $f(x) = (x-1)(x-2)\cdots(x-8)(x-9)$ and let $\mathcal{X} : y^2 = f(x) + T^2$, then Magma verifies that the specialization at $T = 2$ yields a curve of genus 4 given by

$$y^2 = x^9 - 45x^8 + 870x^7 - 9450x^6 + 63273x^5 - 269325x^4 + 723680x^3 - 1172700x^2 + 1026576x - 362876$$

with rank 9. Note that here $J_{\mathcal{X}}(\mathbb{Q}(T))$ is of rank $2g = 8$, but the specialization at $T = 2$ has higher rank equal to 9.

4.2. Rank $2g + 1$. We consider the family $\mathcal{X} : y^2 = f(x)T + 1$, where $f(x)$ is a polynomial of degree $2g + 1$ that splits completely, with no double roots. We compute the first moment of $\mathcal{X}$ as follows:

$$(4.4) \qquad -p \cdot A_{1,\mathcal{X}} = -\sum_{t(p)}\sum_{x(p)} \left(\frac{f(x)t + 1}{p}\right)$$

$$(4.5) \qquad = -\sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} \sum_{t(p)} \left(\frac{1}{p}\right) - \sum_{\substack{x(p) \\ f(x) \not\equiv 0 \bmod p}} \sum_{t(p)} \left(\frac{f(x)t + 1}{p}\right)$$

$$(4.6) \qquad = -p \sum_{\substack{x(p) \\ f(x) \equiv 0 \bmod p}} 1 + 0 = -L_f \cdot p,$$

where we have used Lemma 3.4, and L_f is the number of linear factors in the factorization of $\tilde{f}(x)$ modulo p, as before. Since $f(x)$ factors completely over $\mathbb{Q}$, it follows that $L_f = 2g + 1$ for all sufficiently large p. Thus, $-A_{\mathcal{X},1}(p) = 2g + 1$, and Lemma 3.1 implies that

$$\lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} -A_{\mathcal{X},1}(p) \cdot \log p = 2g + 1.$$

Thus, if we assume that $f(x)$ is chosen so that the $\mathbb{Q}(T)/\mathbb{Q}$-Chow trace of $\mathcal{X}$ is trivial, then Conjecture 1.1 implies that the rank of $J_{\mathcal{X}}(\mathbb{Q}(T))$ is $2g + 1$.

Example 4.2. Let $f(x) = (x-1)(x-2)\cdots(x-7)$ and let $\mathcal{X} : y^2 = f(x)T + 1$. Specializing at $T = 2$ we obtain the hyperelliptic curve of genus 3 given by

$$\mathcal{X}_2 : y^2 = 2x^7 - 56x^6 + 644x^5 - 3920x^4 + 13538x^3 - 26264x^2 + 26136x - 10079,$$

which Magma shows to be of rank $2g+1 = 7$. In fact, one can check that the points $(P_i)-(\mathcal{O})$ given by $P_i = (i, 1)$, for $T = 2$, are independent in $J_{\mathcal{X}_2}(\mathbb{Q})$. Hence, the same points are independent in $J_{\mathcal{X}}$ over $\mathbb{Q}(T)$. Magma also verifies that the Galois group of $2f(x) + 1$ is S_7, and therefore the Galois group of $f(x)T + 1$ over $\mathbb{Q}(T)$ is S_7 as well. Thus, $J_{\mathcal{X}}(\mathbb{Q}(T))$ is a simple hyperelliptic jacobian of rank 7.

4.3. Rank $4g + 2$. Consider the following genus g curve:

$$(4.7) \qquad\qquad \mathcal{X} : y^2 = f(x, T) = x^{2g+1}T^2 + 2q(x)T - h(x)$$

where $q(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degree $2g+1$ to be chosen at a later time. We will imitate the construction in [ALM] for $g = 1$, and choose $q(x)$ and $h(x)$ such that $\text{rank}(\mathcal{X}) = 4g+2$. In order to do so, we define $D_T(x)$ as a fourth of the discriminant of $f(x, T)$ as a polynomial in the variable T.

Lemma 4.3. Suppose that $D_T(x)$ has distinct integer roots $r_i = \rho_i^2$ for $1 \leq i \leq 4g + 2$. Then, the first moment of the surface $\mathcal{X}$ satisfies $-p \cdot A_{\mathcal{X},1}(p) = (4g + 2)p$, for all sufficiently large p.

10

Proof. We use Lemma 3.3 to compute

$$(4.8) \qquad -p \cdot A_{\mathcal{X},1}(p) = \sum_{t(p)} \sum_{x(p)} \left(\frac{f(x,t)}{p} \right) = \sum_{t(p)} \sum_{x(p)} \left(\frac{x^{2g+1}T^2 + 2q(x)T - h(x)}{p} \right)$$

$$(4.9) \qquad = \sum_{\substack{x(p) \\ D_t(x) \equiv 0 \bmod p}} (p-1) \left(\frac{x^{2g+1}}{p} \right) - \sum_{\substack{x(p) \\ D_t(x) \not\equiv 0 \bmod p}} \left(\frac{x^{2g+1}}{p} \right)$$

$$(4.10) \qquad = \sum_{\substack{x(p) \\ D_t(x) \equiv 0 \bmod p}} p \left(\frac{x}{p} \right) - \sum_{x(p)} \left(\frac{x}{p} \right) = p \cdot \left(\sum_{\substack{x(p) \\ D_t(x) \equiv 0 \bmod p}} \left(\frac{x}{p} \right) \right).$$

Since $D_T(x)$ has $4g+2$ distinct integer roots, for large enough p these will also be distinct modulo p, and therefore $-p \cdot A_{\mathcal{X},1}(p) = (4g+2)p$, as claimed. $\qquad\square$

Lemma 4.4. *For any choice of distinct integers $\rho_1, \ldots, \rho_{4g+2}$, there exists polynomials*

$$q(x) = x^{2g+1} + \sum_{i=0}^{2g} a_i x^i, \text{ and } h(x) = (A-1)x^{2g+1} + \sum_{i=0}^{2g} A_i x^i,$$

in $\mathbb{Z}[x]$ so that $D_T(x) = q(x)^2 + x^{2g+1}h(x)$ has $4g+2$ distinct roots $r_i = \rho_i^2$.

Proof. We want to choose a_i and A_i such that

$$D_T(x) = q(x)^2 + x^{2g+1}h(x)$$
$$= Ax^{4g+2} + (A_{2g} + 2a_{2g})x^{4g+1} + \left(A_{2g-1} + a_{2g}^2 + 2a_{2g-1} \right)x^{4g} + \cdots + (2a_0a_1)x + a_0^2$$
$$= A \left(x^{4g+2} + R_{4g+1}x^{4g+1} + R_{4g}x^{4g} + \cdots + R_1 x + R_0 \right)$$
$$= A(x - \rho_1^2)(x - \rho_2^2) \cdots (x - \rho_{4g+1}^2)(x - \rho_{4g+2}^2).$$

The only nontrivial equality here is between the second and third lines. We choose a_i and A_i by equating coefficients between those two lines. Thus, we have $4g+1$ equations in $4g+3$ variables. In particular, the equation of the kth coefficient is the following (where $(\cdot)_k$ denotes the coefficient of x^k):

$$R_k A = (D_T(x))_k,$$

for $0 \le k \le 4g+2$. Note that $R_{4g+2} = 1$. Furthermore, we have

$$(D_T(x))_k = (q(x)^2)_k + (h(x)x^{2g+1})_k$$
$$= (h(x)x^{2g+1})_k + \sum_{\substack{i+j=k \\ 0 \le i,j \le k}} (q(x))_i (q(x))_j$$
$$= A_{k-(2g+1)} + \sum_{\substack{i+j=k \\ 0 \le i,j \le k}} a_i a_j,$$

where $A_i = 0$ by convention if $i < 0$. Therefore, it suffices to solve for the variable $R_k A$ via

$$(4.11) \qquad R_k A = A_{k-(2g+1)} + \sum_{\substack{i+j=k \\ 0 \le i,j \le k}} a_i a_j$$

for $0 \le k \le 4g+2$. For consistency, we require $A_{2g+1} = A$ and $a_{2g+1} = 1$. Recall that R_k are fixed for $0 \le k \le 4g+2$. First of all, for $2g+1 \le k \le 4g+2$, we can choose the adequate coefficients of $h(x)$ to satisfy (4.11). Thus, if we list these equations for $0 \le k \le 2g$ as k increases, we should determine the coefficients of $q(x)$. In the $k = 0$ case, the equation is $R_0 A = a_0^2$. Thus, if we allow rational solutions and choose A such that $R_0 A$ is a square in $\mathbb{Z}$, then these equations have solutions.

This yields $h, q \in \mathbb{Q}[x]$ such that the roots of $D_T(x)$ meet the stated condition. However, we require $h, q \in \mathbb{Z}[x]$. To move h and g into $\mathbb{Z}[x]$ without changing the roots of $D_T(x) =$

11

$q(x)^2 + h(x)x^{2g+1}$, we replace $q(x)$ with $L \cdot q(x)$ and $h(x)$ with $L^2 \cdot h(x)$ where L is the least common multiple of the denominators of the coefficients of h and q. $\qquad\square$

We are now ready to restate and prove our main Theorem 1.2.

Theorem 4.5. *Let $g \geq 1$ be fixed, and let $\rho_1, \dots, \rho_{4g+2}$ be distinct integers. Let $h(x)$ and $q(x)$ be chosen as in Lemma 4.4, and let*

$$\mathcal{X} : y^2 = x^{2g+1}T^2 + 2q(x)T - h(x).$$

Assume that the jacobian of $\mathcal{X}$ over $\mathbb{Q}(T)$ has no subvariety defined over $\mathbb{Q}$ in its factorization. Then, Conjecture 1.1 implies that the jacobian of $\mathcal{X}$ has rank $4g + 2$ over $\mathbb{Q}(T)$.

Proof. Let $g \geq 1$ be fixed, and let $\rho_1, \dots, \rho_{4g+2}$ be distinct integers. By Lemma 4.4, we can find polynomials $h(x)$ and $q(x)$ such that $D_T(x) = (q(x))^2 + x^{2g+1}h(x) = A(x - \rho_1^2) \cdots (x - \rho_{4g+2}^2)$. If we define $\mathcal{X}$ as in the statement, then Lemma 4.3 shows that $-p \cdot A_{\mathcal{X},1}(p) = (4g + 2)p$ for all sufficiently large primes p. Therefore, Lemma 3.1 shows that

$$\lim_{P \to \infty} \frac{1}{P} \sum_{p \leq P} -A_{\mathcal{X},1}(p) \log p \; = 4g + 2.$$

Moreover, if we assume that $J_{\mathcal{X}}$ has no subvariety defined over $\mathbb{Q}$, then its Chow trace must be trivial. Thus, Conjecture 1.1 implies that the rank of $J_{\mathcal{X}}(\mathbb{Q}(T))$ is $4g + 2$, as claimed. $\qquad\square$

Remark 4.6. *If desired, we can change variables so that $\mathcal{X}$ is given in the form $y^2 = F(x, T)$ with $F(x, T)$ monic in the variable x. Indeed, we replace $y^2 = f(x, T)$ by the form $y^2 = F(x, T)$ with a monic polynomial $F(x, T)$ by changing the basis*

$$y \to \frac{y}{(T^2 + 2T - A + 1)^2}, \;\; x \to \frac{x}{T^2 + 2T - A + 1}.$$

Then we have

$$y^2 = f(x, T)$$
$$= x^5 T^2 + 2(x^5 + ax^4 + bx^3 + cx^2 + dx + e)T - (A - 1)x^5 - Bx^4 - Cx^3 - Dx^2 - Ex - F$$
$$= (T^2 + 2T - A + 1)x^5 + (2aT - B)x^4 + (2bT - C)x^3 + (2cT - D)x^2 + (2dT - E)x + (2eT - F)$$
$$y^2 = F(x, T)$$
$$= x^5 + (2aT - B)x^4 + (2bT - C)(T^2 + 2T - A + 1)x^3 + (2cT - D)(T^2 + 2T - A + 1)^2 x^2$$
$$+ (2dT - E)(T^2 + 2T - A + 1)^3 x + (2eT - F)(T^2 + 2T - A + 1)^4.$$

4.4. **An example in genus** 2 **and rank** 10**.** In this section, we follow the recipe of Theorem 4.5 to construct a hyperelliptic curve $\mathcal{X}/\mathbb{Q}(T)$ with jacobian of rank 10, which is how we found the curve in Example 1.4 of the introduction. Let $\rho_1, \dots, \rho_{10}$ be distinct integers. We need to find polynomials

$$q(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e \text{ and } h(x) = (A - 1)x^5 + Bx^4 + Cx^3 + Dx^2 + Ex + F,$$

such that

(4.12)
$$D(x) = q(x)^2 + x^5 h(x)$$
$$= Ax^{10} + (B + 2a)x^9 + (C + a^2 + 2b)x^8 + (D + 2ab + 2c)x^7$$
$$+ (E + 2d + 2ac + b^2)x^6 + (F + 2e + 2ad + 2bc)x^5$$
$$+ (2ae + 2bd + c^2)x^4 + (2be + 2cd)x^3 + (2ce + d^2)x^2 + (2de)x + e^2.$$
$$= A(x^{10} + R_9 x^9 + R_8 x^8 + R_7 x^7 + R_6 x^6 + R_5 x^5 + R_4 x^4 + R_3 x^3 + R_2 x^2 + R_1 x + R_0)$$
$$= A(x - \rho_1^2)(x - \rho_2^2)(x - \rho_3^2)(x - \rho_4^2)(x - \rho_5^2)(x - \rho_6^2)(x - \rho_7^2)(x - \rho_8^2)(x - \rho_9^2)(x - \rho_{10}^2).$$

Now we will explicitly describe how to determine coefficients of $q(x)$ and $h(x)$ for given R_i, $i = 0, 1, \dots, 9$. Since we can adjust the integer values of $B, C, D, E,$ and F, solving the following

12

simultaneous equations from (4.12) is equivalent to give $q(x), h(x) \in \mathbb{Z}[x]$ for any given distinct roots of $D_T(x)$.

$$2ae + 2bd + c^2 = R_4 A,$$
$$2be + 2cd = R_3 A,$$
$$2ce + d^2 = R_2 A,$$
$$2de = R_1 A,$$
$$e^2 = R_0 A.$$

For simplifying the procedure, let $A = 2e$. Then, we can find the values for the rest of the constants recursively as follows:

(4.13)

$$e = 2R_0, \ d = R_1, \ c = (2eR_2 - d^2)/2e, \ b = (2eR_3 - 2cd)/2e, \ a = (2eR_4 - c^2 - 2bd)/2e,$$

$$F = R_5 A - 2e - 2ad - 2bc, \ E = R_6 A - 2d - 2ac - b^2, \ D = R_7 A - 2ab - 2c,$$

$$C = R_8 A - a^2 - 2b, \ B = R_9 A - 2a, \ A = 4R_0 = 2e.$$

Note: these coefficients are not in $\mathbb{Z}$ but later it is easy to find an integral model for $\mathcal{X}$.

Example 4.7. *For simplicity, let $\rho_i = i$, for $i = 1, \ldots, 10$. Then we get*

$$R_0 = 13168189440000, \ R_1 = -20407635072000, \ R_2 = 8689315795776,$$

$$R_3 = -1593719752240, \ R_4 = 151847872396, \ R_5 = -8261931405,$$

(4.14) $$R_6 = 268880381, \ R_7 = -5293970, \ R_8 = 61446, \ R_9 = -385.$$

From Eq. (4.13), we obtain the coefficients $a, \ldots, e$, and then $A, \ldots, F$, and we build a hyperelliptic curve:

$$\mathcal{X} : y^2 = 6247646792749604363304960000000000x^5 T^2$$
$$+ 12495293585499208726609920000000000x^5 T$$
$$- 3290807860845345873174084414821262950400000000x^5$$
$$- 7807712445685207432990455016368800212992000000x^4 T$$
$$+ 1266882949301025362537844681132821271997870080000x^4$$
$$- 12337108316760766233272595534661681152000000000x^3 T$$
$$+ 2439313165791788294241953147543964579572198402055 9648121x^3$$
$$+ 977809477912386424285879709825236992000000000x^2 T$$
$$+ 7710612166714885096465695625583313675121452942739 3152000x^2$$
$$- 254999391610370282637413063055114240000000000000xT$$
$$- 10788519182430514930722390634541533063195857388339 20000x$$
$$+ 32908078608454083496420119108648960000000000000T$$
$$+ 15240148109252962679451455517292779743396570411827 20000000.$$

Then, we can proceed as in Example 1.4 to show that rank $J_{\mathcal{X}}(\mathbb{Q}(T)) = 10$, *unconditionally, and therefore verifying Conjecture 1.1 in this case.*

5. THE SECOND MOMENTS

In this section we compute the second moments in a family of hyperelliptic curves of the form

$$\mathcal{X}_{n,h,k} : y^2 = x^n + x^h T^k$$

where $n = 2g + 1$, and g is the genus of $\mathcal{X}$, and $0 \le k < n$.

We first write a formula for $A_{\mathcal{X},2}(p) = \frac{1}{p}\sum_{t(p)} a_{\mathcal{X}_t}(p)^2$ in a useful way. For convenience, let c be 2 if h is even and 1 if h is odd. Then we have

$$
p \cdot A_{\mathcal{X}_{n,h,k},2}(p) = \sum_{t(p)} a_{\mathcal{X}_t}(p)^2 = \sum_{t(p)}\left(-\sum_{x(p)}\left(\frac{x^n + x^h t^k}{p}\right)\right)^2
$$

$$
= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)
$$

(5.1)
$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^n + x^h t^k}{p}\right)\left(\frac{y^n + y^h t^k}{p}\right)
$$

$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^h y^h}{p}\right)\left(\frac{x^{n-h} + t^k}{p}\right)\left(\frac{y^{n-h} + t^k}{p}\right)
$$

$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)^c\left(\frac{x^{n-h} + t^k}{p}\right)\left(\frac{y^{n-h} + t^k}{p}\right).
$$

where we have used Lemma 3.4 to remove $t = 0$ from the summations. This formula is effectively casewise on the parity of h: if h is odd, there is an $\left(\frac{xy}{p}\right)$ term, and if h is even, there is not an $\left(\frac{xy}{p}\right)$ term. We first use this formula to prove a k-periodicity result:

$$
p \cdot A_{\mathcal{X}_{n,h,k},2}(p) = \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)^c\left(\frac{x^{n-h} + t^k}{p}\right)\left(\frac{y^{n-h} + t^k}{p}\right)
$$

(5.2)
$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{(t^{-1}x)(t^{-1}y)}{p}\right)^c\left(\frac{t^{h-n}x^{n-h} + t^k}{p}\right)\left(\frac{t^{h-n}y^{n-h} + t^k}{p}\right)
$$

$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)^c\left(\frac{x^{n-h} + t^{k+(n-h)}}{p}\right)\left(\frac{y^{n-h} + t^{k+(n-h)}}{p}\right)
$$

$$
= p \cdot A_{\mathcal{X}_{n,h,k+(n-h)},2}(p).
$$

Next, we prove a lemma that greatly simplifies the calculation.

Lemma 5.1. *Suppose* $\gcd(k, n-h, p-1) = 1$. *Then,* $A_{\mathcal{X}_{n,h,k},2}(p) = A_{\mathcal{X}_{n,h,1},2}(p)$.

Proof. By Lemma 3.7, there exists an m such that $\gcd(m, p-1) = 1$ and $m \equiv k \bmod (n-h)$. Thus

$$
p \cdot A_{\mathcal{X}_{n,h,k},2}(p) = p \cdot A_{\mathcal{X}_{n,h,m},2}(p)
$$

$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)^c\left(\frac{x^{n-h} + t^m}{p}\right)\left(\frac{y^{n-h} + t^m}{p}\right)
$$

(5.3)
$$
= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)^c\left(\frac{x^{n-h} + t}{p}\right)\left(\frac{y^{n-h} + t}{p}\right)
$$

$$
= p \cdot A_{\mathcal{X}_{n,h,1},2}(p).
$$

$\square$

Finally, it remains to compute $A_{\mathcal{X}_{n,h,1},2}(p)$. We now turn our attention to this.

Theorem 5.2. *Suppose* $\gcd(k, n - h, p - 1) = 1$. *Then*

$$(5.4) \quad p \cdot A_{\mathcal{X}_{n,h,1},2}(p) = \begin{cases} (\gcd(p-1, n-h) - 1)(p^2 - p) & \text{if } h \text{ even} \\ \gcd(n-h, p-1)(p^2 - p) & \text{if } h \text{ odd and } \nu_2(p-1) > \nu_2(n-h) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned}
p \cdot A_{\mathcal{X}_{n,h,1},2}(p) &= \sum_{t=1}^{p-1} \sum_{x(p)} \sum_{y(p)} \left(\frac{xy}{p}\right)^c \left(\frac{x^{n-h} + t}{p}\right) \left(\frac{y^{n-h} + t}{p}\right) \\
&= \sum_{x,y(p)} \left(\frac{xy}{p}\right)^c \sum_{t(p)} \left(\frac{x^{n-h} + t}{p}\right) \left(\frac{y^{n-h} + t}{p}\right) \\
&= \sum_{\substack{x,y(p) \\ x^{n-h} \equiv y^{n-h} \bmod p}} \left(\frac{xy}{p}\right)^c (p-1) - \sum_{\substack{x,y(p) \\ x^{n-h} \not\equiv y^{n-h} \bmod p}} \left(\frac{xy}{p}\right)^c \\
&= p \sum_{\substack{x,y(p) \\ x^{n-h} \equiv y^{n-h} \bmod p}} \left(\frac{xy}{p}\right)^c - \sum_{x,y(p)} \left(\frac{xy}{p}\right)^c
\end{aligned}$$

(5.5)

First, suppose that $c = 2$. Then, by Lemma 3.5, we have

$$\begin{aligned}
p \cdot A_{\mathcal{X}_{n,h,1},2}(p) &= p N_p(x^{n-h} \equiv y^{n-h}) - p^2 \\
&= p(\gcd(p-1, n-h)(p-1) + 1)) - p^2 \\
&= (\gcd(p-1, n-h) - 1)(p^2 - p).
\end{aligned}$$

(5.6)

Second, suppose that $c = 1$. Then Lemma 3.6 yields

$$\begin{aligned}
p \cdot A_{\mathcal{X}_{n,h,1},2}(p) &= p \sum_{\substack{x,y(p) \\ x^{n-h} \equiv y^{n-h} \bmod p}} \left(\frac{xy}{p}\right) \\
&= \begin{cases} \gcd(n-h, p-1)(p^2 - p) & \nu_2(p-1) > \nu_2(n-h) \\ 0 & \text{otherwise,} \end{cases}
\end{aligned}$$

(5.7)

as desired. $\square$

REFERENCES

[ALM]   S. Arms, Á. Lozano-Robledo and S. J. Miller, *Constructing one-parameter families of elliptic curves over* $\mathbb{Q}(T)$ *with moderate rank*, Journal of Number Theory **123** (2007), no. 2, 388–402.

[A–]   M. Asada, R. Chen, E. Fourakis, Y. Kim, A. Kwon, J. Lichtman, B. Mackall, S. J. Miller, E. Winsor, K. Winsor, J. Yang and K. Yang, *Lower-Order Biases Second Moments of Fourier Coefficients in Families of L-Functions*, preprint. https://arxiv.org/abs/1808.06056.

[Bh]   M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063.

[BhSh1]   M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. **181** (2015), no. 1, 191–242.

[BhSh2]   M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. **181** (2015), no. 2, 587–621.

[BSD1]   B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212** (1963), 7–25.

[BSD2]   B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218** (1965), 79–108.

[C]   B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*, Enseign. Math. **52** (2006), 37–108.

[E]   N. Elkies, $\mathbb{Z}^{28}$ **in** $E(\mathbb{Q})$**, etc.**, Number Theory Listserver, Wednesday 3 May 2006. See also https://web.math.pmf.unizg.hr/~duje/tors/rk28.html.

[GM]   J. Goes and S. J. Miller, *Towards an 'average' version of the Birch and Swinnerton-Dyer Conjecture*, Journal of Number Theory **130** (2010), no. 10, 2341–2358.

[HP]   M. Hindry, A. Pacheco, *Sur le rang des jacobiennes sur un corps de fonctions.*, Bulletin de la Société Mathématique de France **133** (2005), no. 2, 275–295.

[KS1]   N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.

[Kim]   S. Kim, *The Sato-Tate conjecture and Nagao's conjecture*, preprint, https://arxiv.org/abs/1712.02775.

[KS2]   N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36** (1999), 1–26.

[MMRTW]   B. Mackall, S. J. Miller, C. Rapti, C. Turnage-Butterbaugh and K. Winsor (with and an appendix with M. Asada, E. Fourakis and K. Yang), *Some Results in the Theory of Low-lying Zeros*, in Families of Automorphic Forms and the Trace Formula (Werner Müller, Sug Woo Shin and Nicolas Templier, editors), Simons Symposia series, Springer-Verlag, 2016.

[MMRW]   B. Mackall, S. J. Miller, C. Rapti and K. Winsor, *Lower-Order Biases in Elliptic Curve Fourier Coefficients in Families*, Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures (David Kohel and Igor Shparlinski, editors), Contemporary Mathematics **663**, AMS, Providence, RI 2016.

[Maz1]   B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques de l'IHÉS **47** (1977), no. 1, 33–186.

[Maz2]   B. Mazur (with appendix by Dorian Goldfeld), *Rational isogenies of prime degree*, Inventiones Mathematicae **44** (1978), no. 2, 129–162.

[MMRSY]   S. J. Miller, D. Mehrle, T. Reiter, J. Stahl and D. Yott, *Constructing families of moderate-rank elliptic curves over number fields*, Minnesota Journal of Undergraduate Mathematics **2** (2016–2017), 11 pages.

[Mi]   P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120** (1995), 127–136.

[Mil1]   S. J. Miller, *1- and 2-Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, P.H.D. Thesis, Princeton University, 2002. http://www.williams.edu/Mathematics/sjmiller/public_html/math/thesis/SJMthesis_Rev2005.pdf.

[Mil2]   S. J. Miller, *1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), 952–992.

[Mil3]   S. J. Miller, *Variation in the number of points on elliptic curves and applications to excess rank*, C. R. Math. Rep. Acad. Sci. Canada **27** (2005), no. 4, 111–120.

[Mil4]   S. J. Miller, *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98.

[Na1]   K. Nagao, *On the rank of elliptic curve $y^2 = x^3 - kx$*, Kobe J. Math. **11** (1994), 205–210.

[Na2]   K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, (1994), 211-2-19.

[Na3]   K. Nagao, *$\mathbb{Q}(t)$-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92** (1997), 13–32.

[PPVW]   J. Park, B. Poonen, J. Voight and M. M. Wood, *A Heuristic For Boundedness of Ranks of Elliptic Curves*, preprint. http://www-math.mit.edu/~poonen/papers/bounded-ranks.pdf.

[RS]   M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), 43–67.

[RuSa]   Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Journal of Math. **81** (1996), 269–322.

[Se]   J-P. Serre, *Topics in Galois Theory* (Research Notes in Mathematics), A K Peters/CRC Press; 2 edition (November 2, 2007).

[Sh1]   T. Shioda, *Constructing Curves with High Rank via Symmetry*, American Journal of Mathematics. **120** (1998), 551–556.

[Sh2]   T. Shioda, *Mordell–Weil lattices for higher genus fibration over a curve*, in New Trends in Algebraic Geometry, London Math. Soc. Lecture Notes, vol. 264, Cambridge University Press, 1999, pp. 359-373.

[Si1]   J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2]   J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Su]   A. Sutherland, *Computing L-functions of hyperelliptic curves*, Presented at ICTP Workshop on the Arithmetic of Hyperelliptic curves, 2017.

[Za1]   Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication.* Math. Res. Letters 7 (2000), 123-132.

[Za2]   Yu. G. Zarhin, *Very simple 2-adic representations and hyperelliptic jacobians.* Moscow Math. J. 2 (2002), 403-431.

[Za3]   Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians.* Bull. Soc. Math. France 132 (2004), 617-634.

E-mail address: thammond@andrew.cmu.edu

DEPARTMENT OF MATHEMATICAL SCIENCES, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA 15213

E-mail address: sk206@queensu.ca

Department of Mathematics, Brown University, Providence, RI 02912

Current address: Department of Mathematics and Statistics, Queen's University, Kingston, ON, Canada K7L 3N6

E-mail address: bcl5@williams.edu

Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267

E-mail address: alvaro.lozano-robledo@uconn.edu

Department of Mathematics, University of Connecticut, Storrs, CT 06269

E-mail address: sjm1@williams.edu

Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267