THE DISTRIBUTION OF SELMER GROUPS IN QUADRATIC TWIST FAMILIES OVER FUNCTION FIELDS

AARON LANDESMAN

1. Background on Elliptic curves

Let $K = \mathbb{F}_q(t)$ of characteristic > 3. We can write elliptic curves E as $E : y^2 = x^3 + Ax + B$, for $A, B \in \mathbb{F}_q[t]$).

Theorem 1.1 (Mordell-Weil)**.** *The group of K-rational points $E(K) \simeq \mathbb{Z}^r \oplus T$ where T is a finite abelian group.*

The number r is the **rank** of E.

Question 1.2 (Motivating Question)**.** How often does E have finitely many solutions? More generally, what is the average value of r?

To make sense of average size, we'll need to work with a specific family of elliptic curves.

Definition 1.3. Given a fixed elliptic curve $E : y^2 = x^3 + Ax + B$, we can work with the *quadratic twist family*

$$\{E_f := f(t)y^2 = x^3 + A(t)xz^2 + B(t)z^3\}$$

for $f(t) \in \mathbb{F}_q[t]$ squarefree and prime to the discriminant of E. We define $\operatorname{ht} E_f := \deg f$ to be the *height* of the quadratic twist. (For convenience, we will restrict to f having even degree.)

Conjecture 1.4 (Minimalist Conjecture)**.** The average rank of elliptic curves in a quadratic twist family is $1/2$, and moreover, 50% of curves have rank 0, 50% have rank 1, and 0% have rank more than 1.

Remark 1.5. This is a greatly studied conjecture, with much work due to Heath-Brown, Swinnerton-Dyer, Kane, Mazur-Rubin-Klagbrun. Over number fields, many cases of the minimalist conjecture are known, due to breakthrough work of Alex Smith. In the universal family, Bhargava and collaborators have made progress toward this.

2. Main Results

More generally, we study Selmer groups, which sit in an exact sequence between the rank of the elliptic curve, and the Tate-Shafarevich group. Namely, the Selmer group $\mathrm{Sel}_\ell(E)$ sits in an exact sequence

$$0 \longrightarrow E(K)/\ell E(K) \longrightarrow \mathrm{Sel}_\ell(E) \longrightarrow Ш(E)[\ell] \longrightarrow 0 \tag{2.1}$$

Conjecture 2.1 (Bhargava–Shankar [BS13, Conjecture 4] and Poonen–Rains [PR12, Conjecture 1.4(b)])**.** When elliptic curves are ordered by height,

$$\lim_{n\to\infty} \mathbb{E}_{\deg f = n, f\in\mathbb{F}_q[t]}(\#\operatorname{Sel}_\ell(E_f)) = \ell + 1.$$

Remark 2.2. There is a growing literature on this. Over $\mathbb{Q}$ for $\ell \leq 5$, Bhargava and Shankar have verified this. Bhargava-Shankar-Swaminathan also computed the second moment of 2-Selmer groups. When $\ell = 3$ there is work of de Jong over function fields and when $\ell = 2$ Ho, Le Hung, and Ngo, and Achenjang. For quadratic twist families, there is work when $\ell = 2$ and powers of 2 by Smith, but little for odd ℓ.

Theorem 2.3. *Suppose E has a fiber of multiplicative reduction. For ℓ avoiding an explicit finite set of primes,*

$$\lim_{j\to\infty}\lim_{n\to\infty} \mathbb{E}_{\deg f = n, f\in\mathbb{F}_{q^j}[t]}(\#\operatorname{Sel}_\ell(E_f)) = \ell + 1.$$

The above conjecture was generalized to a conjecture regarding all moments of prime order Selmer groups, and then to a conjectural distribution for prime-order groups by Poonen-Rains. It was further conjecturally described for composite order Selmer groups by BKLPR.

Remark 2.4. In particular, one can deduce from this part of the minimalist conjecture: 100% of curves have rank at most 1. This follows from the fact that the average size is $\ell + 1$, while if the rank were ≥ 2, the size of the ℓ Selmer group would be ℓ^2. So this happens with probability roughly $1/\ell$. This goes to 0 as $\ell \to \infty$ and the rank is independent of ℓ.

Definition 2.5. Let O_{2r} denote an orthogonal group of rank $2r$ over the finite field $\mathbb{F}_\ell$ and define the BKLPR distribution, $\operatorname{Sel}_\ell^{BKLPR}$ by

$$\operatorname{Prob}(\dim \operatorname{Sel}_\ell^{BKLPR} = \alpha) = \lim_{r\to\infty} \operatorname{Prob}_{M\in O_{2r}}(\dim\ker(M - \mathrm{id}) = \alpha).$$

Remark 2.6. This distribution is motivated by the presence of actual Frobenius elements in an orthogonal group. Namely, if X is the minimal Weierstrass elliptic surface associated to E, Frobenius acts on $H^2(X_{\overline{\mathbb{F}}_q}, \mathbb{Z}/\ell\mathbb{Z})$ and this action factors through the orthogonal group. The 1-eigenspace of this action essentially recovers the Selmer group.

If we think of the Selmer group as a random element, Burnside's lemma identified the average size with the number of orbits of an orthognal group on its underlying vector space. There are $\ell + 1$ orbits (the ℓ level sets of the quadratic form and 0), which explains the above conjecture.

Theorem 2.7. *Suppose E has a place of multiplicative reduction and ℓ avoids an explicit finite set of primes depending on E.*

$$\lim_{j\to\infty}\limsup_{n\to\infty} \operatorname{Prob}_{\deg f = n, f\in\mathbb{F}_{q^j}[t]}(\dim \operatorname{Sel}_\ell(E_f) = \alpha) = \operatorname{Prob}(\operatorname{Sel}_\ell^{BKLPR} = \alpha).$$

Remark 2.8. The condition that E has a fiber of multiplicative reduction is necessary. For $E : y^2 = t(t-1)x(x-1)(x-t)$, and $q = 1 \bmod 4$ a prime, 100% of elliptic curves have even rank.

Remark 2.9. We prove the above result more generally

(1) over arbitrary global function fields of characteristic not 2

	Quadratic Twists	Universal Family	Class groups
Large q limit	Katz, Park-Wang	L, Feng-L-Rains	Achter, Yu
Large height limit	Ellenberg-L	???	Ellenberg-Venkatesh-Westerland

TABLE 1. Some prior work over function fields

(2) for higher dimensional abelian varieties,
(3) We also prove a natural generalization for composite integers in place of primes ℓ.

Remark 2.10. Previous results of Ellenberg Venkatesh Westerland prove results for torsion in class groups of quadratic fields. This can be viewed essentially as a special case of ours for the twist family associated to the "nodal elliptic curve" $y^2 = x^3 + x^2$.

3. SKETCH OF THE PROOF

The first key innovation is that we can think of Selmer elements as certain $\mathrm{ASL}_2(\mathbb{F}_\ell)$ covers over $\mathbb{P}^1$ where

$$0 \longrightarrow \mathbb{F}_\ell^2 \longrightarrow \mathrm{ASL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{SL}_2(\mathbb{F}_\ell) \longrightarrow 0 \tag{3.1}$$

(For experts, this is because the Galois representation for the ℓ torsion has image SL_2, and the affine part comes because Selmer elements are torsors for the ℓ-torsion.

There are then certain hurwitz spaces of these covers, X_n over $\mathbb{F}_q$ parameterizing these covers, living over the space of quadratic twists Qtwist_n. Let's say, as a first step, we want to compute the average size of the ℓ-Selmer group. Then we would want to compute,

$$\mathbb{E}_{\deg f=n, f\in\mathbb{F}_q[t]}(\#\mathrm{Sel}_\ell(E_f)) = \frac{\sum_{f,\deg f=n}\#\mathrm{Sel}_\ell(E_f)}{\sum_{f,\deg f=n}1} = \frac{\#X_n(\mathbb{F}_q)}{\sum_{f,\deg f=n}1}$$

So our goal is to compute $\#X_n(\mathbb{F}_q)$.

The key tool is the Grothendieck-Lefschetz trace formula, and Deligne's bounds, which tell us

$$X_n(\mathbb{F}_q) = \sum_{i=0}^{2\dim X_n}(-1)^i \operatorname{tr}(\mathrm{Frob_q}\,|H_c^i((X_n)_{\overline{\mathbb{F}}_q}, \mathbb{Q}_{\ell'})).$$

Remark 3.1. A monodromy computation shows the top cohomology group has dimension $\ell+1$, which gives the desired average size. In order to prove this is the number of $\mathbb{F}_q$ points, it is enough to control the other cohomology groups.

To compute the other cohomology groups, we prove the following homological stability theorem in topology.

Theorem 3.2. *There are constants A and B independent of i and n so that whenever $n > Ai + B$, there is an isomorphism $H_c^{2\dim X_n - i}(X_{n,\overline{\mathbb{F}}_q}) \simeq H_c^{2\dim X_{n+1}-i}(X_{n+1,\overline{\mathbb{F}}_q})$*

The rough idea is to tranfer to the complex numbers, and prove this homological stability theorem by using the highly connected arc complex.

Altogether, this allows us to compute the average size of $\mathrm{Sel}_\ell(E_f)$. Similar considerations let us compute the higher moments, the average size of $\mathrm{Sel}_\ell(E_f)^m$ for $m \geq 0$.

Goal 3.3. Use the moments to determine the distribution.

It turns out that the BKLPR distribution is not determined once we know the average value of $\mathrm{Sel}_\ell(E_f)^m$.

Example 3.4 (A distribution not determined by its moments)**.** Consider the distributions

$$\mathrm{Sel}_\ell^{\mathrm{BKLPR}},$$
$$(\mathrm{Sel}_\ell^{\mathrm{BKLPR}} | \dim \mathrm{Sel}_\ell^{\mathrm{BKLPR}} \equiv 0 \bmod 2)$$

with the latter distributions conditioning upon whether the dimension is even.

These distributions are clearly vastly different, because the dimensions have different parities. However, their moments in fact agree! This shows that the distribution of the Selmer group of an elliptic curve is not determined by its moments.

However, it is a theorem in probability, that once one does condition on the rank of the elliptic curve being even or odd, the moments do determine the distribution. Therefore, we only need one more piece of information, which shows equidistribution of the parity of the rank. Fortunately for us, there is a double cover $\pi_n : \mathrm{Rank}_n \to \mathrm{QTwist}_n$ so that $x \in \mathrm{QTwist}_n(\mathbb{F}_q)$ lies in the image of $\mathrm{Rank}_n(\mathbb{F}_q)$ if and only if x has rank of a specified parity.

Therefore, it is enough to show this double cover also satisfies good homological stability properties as we increase n. However, this double cover is not a Hurwitz space, so we prove a generalized homological stability theorem for "coefficient systems" which are more general than Hurwitz space, and include this rank double cover. After this, we then have enough moments, and can determine the whole distribution, as predicted.

4. Back to the minimalist conjecture

Now would be a good time to zone in, if you've been zoning out.

Let's explain how we can use the above to deduce the minimalist conjecture. We need to check two things:

(1) The parity of rank is equidistributed.
(2) 0% of elliptic curves have rank more than 2.

We saw the second one much earlier.

For the first, it is fairly well known that the parity of the rank is governed by root number. The spaces X_n described above are in fact local systems over QTwist_n, of rank r_n. Fortunately for us, there is a double cover $\pi_n : \mathrm{Rank}_n \to \mathrm{QTwist}_n$ so that $x \in \mathrm{QTwist}_n(\mathbb{F}_q)$ lies in the image of $\mathrm{Rank}_n(\mathbb{F}_q)$ if and only if x has rank with the same parity as r_n.

Proposition 4.1. *The Galois closure of the cover $X_n \to \mathrm{QTwist}_n$ has Galois group contained in $O_{r_n}(\mathbb{Z}/\ell\mathbb{Z})$, and so corresponds to a finite cover associated to the quotient $\pi_1(\mathrm{QTwist}_n) \to O_{r_n}(\mathbb{Z}/\ell\mathbb{Z})$. The rank double cover is then the double cover associated to the quotient $\pi_1(\mathrm{QTwist}_n) \to O_{r_n}(\mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{\det} \{\pm 1\}$. In particular, if the composition $\pi_1(x) \to \pi_1(\mathrm{QTwist}_n) \to O_{r_n}(\mathbb{Z}/\ell\mathbb{Z}) \xrightarrow{\det} \{\pm 1\}$ send Frob_x to $+1$, the elliptic curve has rank $r_n \bmod 2 \in \{0, 1\}$ with probability 1 and if it goes to -1, the elliptic curve has rank $1 - r_n \bmod 2$ with probability 1.*

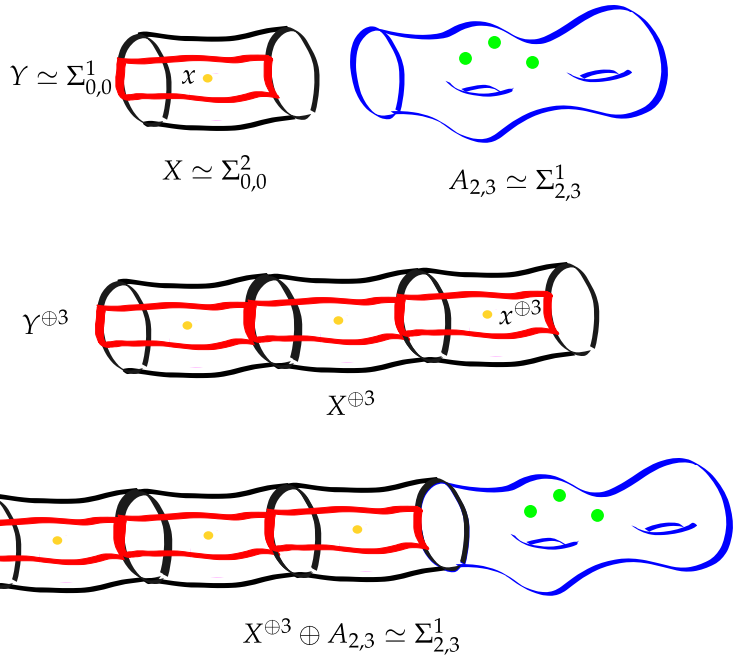

FIGURE 1. The blue surface with green punctures is a picture of $A_{2,3} \simeq \Sigma^1_{2,3}$ and the black surface is $X \simeq \Sigma^2_{0,0}$. The yellow circles correspond to the point x, the red rectangles are the subsurface Y with $x \in Y \subset X$. We also depict $X^{\oplus 3}$ and $X^{\oplus 3} \oplus A_{2,3}$.

5. TOPOLOGICAL RESULTS

Our main topological result will be a certain homological stability result for objects we call coefficient systems. We begin by introducing our main player, coefficient systems.

Let $A_{g,f} := \Sigma^1_{g,f}$, $X := \Sigma^2_{0,0}$ and $X^{\oplus n} \oplus A_{g,f}$ denote the surface given as in the diagram. Define $B^n_{g,f} := \pi_1(\mathrm{Conf}^n_{X^{\oplus n} \oplus A_{g,f}})$ denote the surface braid group parameterizing n points in $X^{\oplus n} \oplus A_{g,f}$. Fix finite dimensional vector spaces V_1, F_0 and define $V_i = V_1^{\otimes i}, F_i = F_0 \otimes V_1^{\otimes i}$. A *coefficient system* is the data of representations of $B^n_{0,0}$ on V_n and $B^n_{g,f}$ on F_n which are compatible in the sense that the composition $B^i_{g,f} \times B^{n-i}_{0,0} \to B^n_{g,f} \to \mathrm{Aut}(F_n)$ gives the representation $F_i \otimes V_{n-i}$ (and similarly $B^i_{0,0} \times B^{n-i}_{0,0} \to B^n_{0,0} \to \mathrm{Aut}(V_n)$ gives the representation $V_i \otimes V_{n-i}$).

Remark 5.1. We can think of F_n as local systems on $\mathrm{Conf}_n(\Sigma_{g,f})$ which are compatible upon restriction to smaller configuration spaces.

Hurwitz spaces give an example of coefficient systems.

Example 5.2. Fix $g, f \geq 0$ a finite group G and a conjugacy closed subset $c \subset G$. Let $T^0 := \mathrm{Hom}(\pi_1(A_{g,f}), G)$ and define $T^n := c^n \times T^0 \subset \mathrm{Hom}(\pi_1(X^{\oplus n} \oplus A_{g,f} - x^{\oplus n}), G)$ with the property that $T^n = c \times T^{n-1}$. Then take F_n to be the free vector space on T^n and V_n to be the free vector space on c^n. In this case, (F_n, V_n) yield a coefficient system, corresponding to a Hurwitz space of G covers of $\Sigma_{g,f}$ branched at n points, where the monodromy around each of these points lies in c.

Theorem 5.3. *Suppose V is a coefficient system for $\Sigma^1_{0,0}$ and $U \in \oplus_{i=0}^{\infty} H^0(B^i_{0,0}, V_i)$ is a homogeneous central element of positive degree whose kernel and cokernel have finite degree. If (F, V) is a coefficient system for $\Sigma^1_{g,f}$ there are constants $A(V), B(F)$ so U induces an isomorphism*

$$H_p(B^n_{g,f}, F_n) \xrightarrow{U} H_p(B^{n+\deg U}_{g,f}, F_{n+\deg U})$$

whenever $n > A(V)p + B(F)$.

Past work:

(1) EVW essentially proved the special case of this where $g = f = 0$ and the coefficient system comes from a Hurwitz space.
(2) Some notable examples where these techniques were developed further include Ellenberg-Tran-Westerland proving a version of Malle's conjecture,
(3) a "polynomial stability" version of homological stability in Bianchi-Miller
(4) One is able to replace $\deg U$ with a shift by 1 in Davis-Schlank
(5) Hoang proved a bound on ranks of homology groups of Hurwitz spaces when $g = 0$ (but f arbitrary).

REFERENCES

[BS13] Manjul Bhargava and Arul Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7. *arXiv preprint arXiv:1312.7333v1*, 2013.

[PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.