Average size of 2-Selmer groups of elliptic curves over function fields

Q.P. Hồ, V.B. Lê Hùng, B.C. Ngô

October 27, 2014

Abstract

Employing a geometric setting inspired by the proof of the Fundamental Lemma, we study some counting problems related to the average size of 2-Selmer groups and hence obtain an estimate for it.

1 Introduction

By the Mordell-Weil theorem, for every elliptic curve E over a global field K, the group $E(K)$ of K-rational points of E is a finitely generated abelian group. The rank of $E(K)$, called the Mordell-Weil rank, is a fascinating invariant as revealed by the Birch and Swinnerton-Dyer conjecture. It remains nevertheless very mysterious. For instance, it is not known if the Mordell-Weil rank of elliptic curves defined over a given number field is bounded. Over function fields, according to Ulmer [Ulm02], the Mordel-Weil rank is known to be unbounded.

In the ground breaking papers [BS10a] and [BS10b], Bhargava and Shankar were able to prove an upper bound for the average rank of $E(\mathbb{Q})$, when E ranges over the set of elliptic curves defined over $\mathbb{Q}$.

An attractive feature of their work is its rather elementary nature. Bhargava and Shankar bound the average rank by estimating the average size of the 2-Selmer groups $\mathrm{Sel}_2(E)$ of E. This computation is then carried out as the solution of a problem in geometry of numbers which involves counting integral points in a certain fundamental domain built out of the action of PGL_2 on the space of binary quartic polynomials.

The aim of this work is to introduce certain moduli spaces, also built out of the action of PGL_2 on binary quartics, which should be viewed as the geometric analog of this problem in geometry of numbers in the case of global fields of rational functions on a curve defined over a finite field. Counting points on these moduli spaces, which is roughly counting torsors for suitable quasi-finite group schemes over the curve, will then help to estimate the average size

of 2-Selmer groups, and hence the average rank of elliptic curves. This gives a (weakened) function field analog of the main result of [BS10a], valid for all functions fields with very mild restrictions.

Theorem. *Let K be a global function field over a finite field $\mathbb{F}_q$ with $q > 32$ and $\mathrm{char}\,\mathbb{F}_q > 3$. Then the average size of 2-Selmer groups of elliptic curves over K when ordered by height, is bounded above and below by explicit functions $3 + F(q)$ and $3 - G(q)$. Furthermore $F(q)$, $G(q)$ tend to 0 as $q \to \infty$.*

More precise statements of our result are given in subsection 2.2. We also remark that the results of [dJ02] give upper bounds for the size of 3-Selmer groups of a similar nature for the case $K = k(\mathbb{P}^1) = \mathbb{F}_q(t)$. After the completion of this paper, we learned from J. Ellenberg that Y. Zhao in [Zha13] has also obtained results in the case of cubic polynomials using an argument which is in part similar to ours. It seems that our methods may be applicable to more general coregular representations, for example the ones studied in [Jac13], and we hope to return to this in future work.

Acknowledgement

This work is partially supported by the NSF grant DMS-1302819 and a Simons investigator's grant of B.C. Ngô. The work started during a summer seminar on the work [BS10a], organized by B.C. Ngô at the Vietnam Institute for Advanced Studies in Mathematics (VIASM). V.B. Lê Hùng and Q. Hồ would like to thank the VIASM for its hospitality. V.B. Lê Hùng would like to thank the University of Chicago for its support and hospitality during a visit where part of this work was done. We thank the referees for their careful reading of our manuscript.

Notations: $k = \mathbb{F}_q$ with $\mathrm{char}\,k \neq 2, 3$, $\overline{k}$ its algebraic closure, C is a smooth, complete, geometrically connected curve over k such that $C(k) \neq \emptyset$, $K = k(C)$, the field of rational functions on C, and $G = \mathrm{PGL}_2$.

2 Elliptic curves over K

We will need to specify an ordering on the infinite set of isomorphism classes of elliptic curves over $K = k(C)$ in order to make sense of the notion of average. This can be done via the notion of height, which in turn relies on the theory of minimal Weierstrass models of elliptic curves.

2.1 Height and minimal Weierstrass model

We will recall the statements of the necessary results of the theory of Weierstrass model, and refer the readers to the literature for the proofs.

Definition 2.1.1. *A family of Weierstrass curves over a scheme S is a flat family of arithmetic genus one curves $\pi : E \to S$ with integral geometric fibers, equipped with a section $e : S \to E$ not passing through the cusps or nodes of any fiber.*

A family of Weierstrass curves admits a simple presentation, which justifies its name.

Proposition 2.1.2. *Let (E, e) be a family of Weierstrass curves over a scheme S. Then, there exists a triple $(\mathscr{L}, a, b)$ with $\mathscr{L}$ a line bundle over S, $a \in H^0(C, \mathscr{L}^{\otimes 4})$ and $b \in H^0(C, \mathscr{L}^{\otimes 6})$ such that the pair (E, e) is isomorphic to the closed subscheme of $\mathbb{P}(\mathscr{L}^{\otimes -2} \oplus \mathscr{L}^{\otimes -3} \oplus \mathscr{O}_C)$ defined by the equation*

$$yz^2 = x^3 + axz^2 + bz^3,$$

and the section $e : S \to E$ is given by $(0, 1, 0)$.

Moreover, $(\mathscr{L}, a, b)$ is unique up to the following identification: $(\mathscr{L}, a, b) \sim (\mathscr{L}', a', b')$ when $\mathscr{L} \cong \mathscr{L}'$ and $(a, b) = (c^4 a, c^6 b)$ for some $c \in k^\times$. In particular, (E, e) completely determines $\mathscr{L}$, and in fact, $\mathscr{L} = \pi_*(\mathscr{O}_E(e)/\mathscr{O}_E)^{-1}$.

Proof. See [Mir81, theorem 2.1] and [SM70]. □

Remark 2.1.3. Proposition 2.1.2 allows us to construct the moduli stack of Weierstrass curves as the stack quotient $[\mathbb{A}^2/\mathbb{G}_m]$, with $\mathbb{G}_m$ acting on $\mathbb{A}^2$ by the formula $c \cdot (a, b) = (c^4 a, c^6 b)$. The universal family is the closed subscheme of $\mathbb{P}(\mathscr{L}_{uni}^{\otimes -2} \oplus \mathscr{L}_{uni}^{\otimes -3} \oplus \mathscr{O}_C)$ cut out by the equation $yz^2 = x^3 + axz^2 + bz^3$, with $\mathscr{L}_{uni}$ being the pullback of the universal line bundle on $B\mathbb{G}_m$, and the section $e : S \to E$ given by $(0, 1, 0)$.

Theorem 2.1.4. *Let (E_K, e_K) be an elliptic curve over K. Then, we can extend (E_K, e_K) to a family of Weierstrass curves (E, e) over C. Moreover, the extension is unique up to isomorphism if we demand that the line bundle $\mathscr{L} = \pi_*(\mathscr{O}_E(e)/\mathscr{O}_E)^{-1}$ (see proposition 2.1.2) is of minimal degree.*

Proof. See [Liu06, section 9.4]. □

Definition 2.1.5. *The height of an elliptic curve E_K defined over K is defined to be the minimal* $\deg \mathscr{L}$ *in the theorem above.*

Using proposition 2.1.2 and remark 2.1.3, theorem 2.1.4 can now be reformulated in a slightly different way. Every elliptic (E_K, e_K) over the generic point $\mathrm{Spec}(K)$ of C can be extended as a family of Weierstrass curves (E, e) over C, and hence gives rise to a morphism $h_E : C \to [\mathbb{A}^2/\mathbb{G}_m]$. The extension is unique if $\deg h_E^* \mathscr{L}_{uni}$ is minimal.

Let (E, e) be a family of Weierstrass curves over C. Then the fiber E_v over a point $v \in C$ is singular if and only if v lies in the zero divisor of the discriminant

$$\Delta(a, b) = -(4a^3 + 27b^2) \in \Gamma(C, \mathscr{L}^{\otimes 12}).$$

We will sometimes use the notation $\Delta(E_K)$ to denote the discriminant of the minimal Weierstrass model.

Definition 2.1.6. *A morphism $\alpha : C \to [\mathbb{A}^2/\mathbb{G}_m]$ is said to be transversal to the discriminant locus if the zero divisor of $\alpha^*\Delta = 4a^3 + 27b^2 \in \Gamma(C, \mathscr{L}^{\otimes 12})$ is multiplicity free.*

2.2 Statements of the main theorems

We recall that for each elliptic curve E defined over K, the 2-Selmer group of E is defined as the kernel of the homomorphism:

$$\mathrm{Sel}_2(E) = \ker(H^1(K, E[2]) \to \prod_{v \in |C|} H^1(K_v, E)).$$

We will now state the main results of the paper. First, we introduce the following notation:

$$\mathrm{AS}(d) = \frac{\displaystyle\sum_{h(E_K) \leq d} \frac{|\mathrm{Sel}_2(E_K)|}{|\mathrm{Aut}(E_K)|}}{\displaystyle\sum_{h(E_K) \leq d} \frac{1}{|\mathrm{Aut}(E_K)|}} \quad \text{and} \quad \mathrm{AR}(d) = \frac{\displaystyle\sum_{h(E_K) \leq d} \frac{|\mathrm{Rank}(E_K)|}{|\mathrm{Aut}(E_K)|}}{\displaystyle\sum_{h(E_K) \leq d} \frac{1}{|\mathrm{Aut}(E_K)|}}. \tag{2.2.1}$$

Similarly, we denote $\mathrm{AS}(\mathscr{L})$ and $\mathrm{AR}(\mathscr{L})$ to be similar to $\mathrm{AS}(d)$ and $\mathrm{AR}(d)$ except that we restrict ourselves to those elliptic curves whose minimal models are given by a fixed line bundle $\mathscr{L}$ (see theorem 2.1.4). Note that it makes sense to talk about AS and AR since the number of isomorphism classes of elliptic curves over K with bounded height is finite.

In all the results below, we make the assumption that the base field k has more than 32 elements. The source of this restriction will be explained in subsection 6.2.

Theorem 2.2.2. *We have the following bounds for $\mathrm{AS}(\mathscr{L})$:*

$$\limsup_{\deg \mathscr{L} \to \infty} \mathrm{AS}(\mathscr{L}) \leq 3 + \frac{T}{(q-1)^2},$$

and

$$\liminf_{\deg \mathscr{L} \to \infty} \mathrm{AS}(\mathscr{L}) \geq 3\zeta_C(10)^{-1},$$

where T is a constant depending only on C, and ζ_C is the zeta function associated to C.

From this theorem, we derive the following corollaries.

Corollary 2.2.3. *If we order elliptic curves over K by height, then we have*

$$\limsup_{d\to\infty} \mathrm{AS}(d) \leq 3 + \frac{T}{(q-1)^2},$$

and

$$\liminf_{d\to\infty} \mathrm{AS}(d) \geq 3\zeta_C(10)^{-1}.$$

In particular,

$$\lim_{q\to\infty} \limsup_{d\to\infty} \mathrm{AS}(d) \leq 3,$$

and

$$\lim_{q\to\infty} \liminf_{d\to\infty} \mathrm{AS}(d) \geq 3.$$

Proof. This is clear from theorem 2.2.2, noticing that $\lim_{n\to\infty} \zeta_{C\otimes\mathbb{F}_{q^n}}(10) = 1$. □

Corollary 2.2.4. *We have the following bounds for the average rank:*

$$\limsup_{d\to\infty} \mathrm{AR}(d) \leq \frac{3}{2} + \frac{T}{2(q-1)^2}.$$

In particular,

$$\lim_{q\to\infty} \limsup_{d\to\infty} \mathrm{AR}(d) \leq \frac{3}{2},$$

Proof. This is a direct consequence of corollary 2.2.3. □

If we restrict ourselves to the case where $\Delta(E_K)$ square-free, then we get a better estimate for the average size of the 2-Selmer groups, and hence, also for the average rank. For the sake of brevity, we add the superscript sf to $\mathrm{AS}^{sf}(d)$, $\mathrm{AR}^{sf}(d)$, $\mathrm{AS}^{sf}(\mathscr{L})$ and $\mathrm{AR}^{sf}(\mathscr{L})$ to mean that we restrict the range to the cases where $\Delta(E_K)$ is square-free.

Theorem 2.2.5. *When we restrict ourselves to the square-free range, then*

$$\lim_{\deg\mathscr{L}\to\infty} \mathrm{AS}^{sf}(\mathscr{L}) = 3,$$

and hence

$$\lim_{d\to\infty} \mathrm{AS}^{sf}(d) = 3,$$

and

$$\lim_{d\to\infty} \mathrm{AR}^{sf}(d) \leq \frac{3}{2}.$$

The rest of the paper will be devoted to the proofs of theorems 2.2.2 and 2.2.5. The main strategy to our counting problem is the introduction of a morphism of stacks $\mathscr{M}_{\mathscr{L}} \to \mathscr{A}_{\mathscr{L}}$ parametrized by line bundles $\mathscr{L}$ on C, and calculate the limit of the ratio of masses

$$|\mathscr{M}_{\mathscr{L}}(k)|/|\mathscr{A}_{\mathscr{L}}(k)|$$

as $\deg(\mathscr{L}) \to \infty$. This geometric situation will be set up in subsection 4.4 after some necessary preparations.

3 Invariant theory of binary quartic forms

3.1 Invariants

Let $V = \operatorname{Spec} k[c_0, c_1, c_2, c_3, c_4]$ be the space of binary quartic forms with coefficients c_0, c_1, c_2, c_3, c_4, i.e. a point $f \in V(k)$ can be written as

$$f(x, y) = c_0 x^4 + c_1 x^3 y + c_2 x^2 y^2 + c_3 x y^3 + c_4 y^4.$$

We can view V as a representation of GL_2 by identifying V with $\mathrm{Sym}^4 \mathrm{std} \otimes \det^{-2}$, where std stands for the standard representation of GL_2. The center of GL_2 acts trivially on V, which makes this into a representation of $G = \mathrm{PGL}_2$. From the classical theory of invariants, we know that the GIT quotient $V/\!\!/G$ of V is isomorphic to $S = \operatorname{Spec} k[a, b]$, where

$$\begin{aligned} a &= -\frac{1}{3}(12c_0c_4 - 3c_1c_3 + c_2^2), \\ b &= -\frac{1}{27}(72c_0c_2c_4 + 9c_2c_3c_4 - 27c_0c_3^2 - 27c_4c_1^2 - 2c_2^3), \end{aligned}$$

and we denote $\pi : V \to S$ the quotient map. The discriminant

$$\Delta(f) = -(4a^3 + 27b^2)$$

defines regular functions on V and S.

We also have a linear action of $\mathbb{G}_m$ on V and S compatible with π and with the G-action defined as follows

$$c \cdot f = c^2 f \qquad \text{and} \qquad c \cdot (a, b) = (c^4 a, c^6 b). \tag{3.1.1}$$

These relations induce a natural morphism of quotient stacks $\pi : [V/G \times \mathbb{G}_m] \to [S/\mathbb{G}_m]$. We also have the relation:

$$c \cdot \Delta = c^{12} \Delta$$

which implies that Δ defines a divisor on $[S/\mathbb{G}_m]$.

The quotient map π admits a section s given by

$$s(a,b) = y(x^3 + axy^2 + by^3), \tag{3.1.2}$$

which we will call the Weierstrass section. In fact, this section can be extended to a map $S \times \mathbb{G}_m \to V \times G \times \mathbb{G}_m$ compatible with all the actions involved

$$s((a,b),c) = \left(y(x^3 + axy^2 + by^3), \begin{pmatrix} 1 & 0 \\ 0 & c^2 \end{pmatrix}, c \right).$$

This section induces a section on the level of quotient stacks:

$$[S/\mathbb{G}_m] \to [V/G \times \mathbb{G}_m]$$

also to be called the Weierstrass section.

3.2 Stable orbits

We will now investigate the orbits and stabilizers of the action of G on the space of binary quartic forms. A non-zero binary quartic form $f \in V(\overline{k})$ can be written in the following form:

$$f(x,y) = \prod_{i=1}^{4} (a_i x + b_i y), \qquad a_i, b_i \in \overline{k}.$$

Based on multiplicity of its zeros, a non-zero binary quartic form f can be assigned one of the following types:

$$(1,1,1,1), \quad (1,1,2), \quad (1,3), \quad (2,2), \quad (4).$$

For instance, type $(1,1,1,1)$ includes those binary quartic forms with no multiple root, while type $(1,1,2)$ includes those with exactly one double root, and so on. It is clear that if two geometric points $f, g \in V(\overline{k}) - \{0\}$ are conjugate, then they have the same type and also have the same invariants a and b. The converse is also true.

Proposition 3.2.1. *In each geometric fiber of $\pi : V \to S$, G acts transitively on the set of geometric points of a given type. In other words, if $f, g \in V(\overline{k}) - \{0\}$ have the same invariants a and b, and are of the same type, then there exists an element of $h \in G(\overline{k})$ such that $hf = g$.*

Let $(a,b) \in \bar{k}^2$ be a geometric point of S. Then the geometric fiber $V_{(a,b)} = \pi^{-1}(a,b)$ has the following descriptions:

- *(i) If $\Delta(a,b) \neq 0$, $V_{(a,b)}$ has precisely one orbit, and it is of type $(1,1,1,1)$.*
- *(ii) If $\Delta(a,b) = 0$ but $(a,b) \neq (0,0)$, $V_{(a,b)}$ has two orbits, which are of types $(1,1,2)$ and $(2,2)$.*

(iii) Finally, $V_{(0,0)}$ has three orbits, which are of types $(1,3),(4)$ and $f=0$.

A non-zero binary quartic form $f \in V(\bar{k})$ is said to be *stable* if it has at least one single zero, or in other words if it is of one of the types $(1,1,1,1),(1,1,2)$ or $(1,3)$. We will first treat the stable case.

Proposition 3.2.2. *Let $f \in V(\bar{k})$ be a stable binary quartic form. Then there exists $h \in G(\bar{k})$ such that*

$$hf = y(x^3 + axy^2 + by^3)$$

where $a = a(f)$ and $b = b(f)$.

Proof. Let $\mathbb{P}^1$ be the projective line with projective coordinate $[x : y]$, where ∞ is defined by the equation $y = 0$. By conjugation, we can assume that f has a single zero at ∞. In other words, it has the form

$$f = y(c_0x^3 + c_1x^2y + c_2xy^2 + c_3y^3)$$

with $c_0 \in \bar{k}^\times$ and $c_1, c_2, c_3 \in \bar{k}$. The subgroup of upper triangular matrix in G stabilizes $\infty \in \mathbb{P}^1$. Its action allows us to bring the cubic factor into the form $x^3 + axy^2 + by^3$ provided that $\operatorname{char} k \neq 3$. We can then check that $a = a(f)$ and $b = b(f)$ on the form $y(x^3 + axy^2 + by^3)$. □

Proof. (of proposition 3.2.1) The case of stable orbits is already settled by proposition 3.2.2. Indeed, since any stable binary quartic form f of invariant (a,b) is conjugate to the polynomial $y(x^3 + axy^2 + by^3)$, two stable binary quartic forms of the same invariant (a,b) are conjugate. Also $\Delta(a,b) \neq 0$ if and only if the cubic polynomial $x^3 + ax^2 + b$ have three distinct zeros. If $\Delta(a,b) = 0$, it has at least a double zero, and furthermore, it has a triple zero if and only if $(a,b) = (0,0)$.

We next consider the case of a quartic form f type $(2,2)$. By using the action of G we can assume that f has double zeros at 0 and ∞. In other words, f is of the form $f = cx^2y^2$ with $c \neq 0$. We observe that in this case, the invariants $a(f) = -c^2/3$ and $b(f) = 2c^3/27$ completely determine c, and hence f, assuming that the characteristic of k is not 2 nor 3.

We finally consider the case of a quartic form f of type (4). By using the action of G we can assume that f has quadruple zero at ∞. In other words, f is of the form $f = cy^4$ with $c \neq 0$. It is then easy to exhibit a diagonal two by two matrix h such that $hf = y^4$. □

Let I be the universal stabilizer of the action of G on V, that is

$$I = (G \times_S V) \times_{V \times_S V} V, \tag{3.2.3}$$

where $G \times_S V \to V \times_S V$ is defined by $(g,v) \mapsto (v, gv)$ and $V \to V \times_S V$ is the diagonal map. This is a group scheme over V whose Lie algebra can be described as follows.

Proposition 3.2.4. *The infinitesimal stabilizers of the action of* $\mathfrak{g} = \mathrm{Lie}(G)$ *on* V *are as follows:*

(i) Trivial for points of stable types $(1,1,1,1)$*,* $(1,1,2)$ *and* $(1,3)$*,*
(ii) One-dimensional for points of types $(2,2)$ *and* (4)*,*
(iii) All of $\mathfrak{g}$ *for the point* $f = 0$*.*

Proof. The action of $\mathfrak{g} = \mathrm{Lie}(G)$ on V can be identified with the representation $\mathrm{Sym}^4\mathrm{std}$ of $\mathfrak{sl}_2$. Let us consider a pair $(X, f) \in \mathfrak{sl}_2 \times V$ with $X \neq 0$, $f \neq 0$ but $Xf = 0$. Since $X \neq 0$, it is either regular semi-simple or regular nilpotent.

If X is regular semi-simple, after conjugation by an element $h \in G$, it has the form

$$X = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

In this case, f has to be a multiple of x^2y^2. In other words, f is of type $(2,2)$. Conversely, if f is of type $(2,2)$, it is conjugate to a quartic polynomial of the type cx^2y^2 with $c \neq 0$ whose infinitesimal centralizer is the space of diagonal matrices in $\mathfrak{sl}_2$.

If X is regular nilpotent, after conjugation by an element $h \in G$, it has the form

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{3.2.5}$$

The space of f annihilated by X is generated by y^4. In other words, f is of type (4). Conversely, if f is of type (4), it is conjugate to y^4. Its infinitesimal centralizer is a one-dimensional space of matrices generated by a non-zero nilpotent matrix (3.2.5). □

We can compute explicitly the geometric stabilizers in stable orbits. Since there is no infinitessimal stabilizer by proposition 3.2.4, it suffices to determine the $\overline{k}$-points of I_f for a given stable binary quartic form.

Proposition 3.2.6. *If* $f \in V(\overline{k})$ *is of type* $(1,1,1,1)$*,* $(1,1,2)$ *and* $(1,3)$*, then* I_f *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z}$ *and* 0*, respectively.*

Proof. The case where f is of type $(1,1,1,1)$ is postponed to proposition 4.2.1.

If f is of type $(1,1,2)$, by the action of G, we can assume that $f = cxy(x-y)^2$. Thus, each element in the stabilizer of f must stabilize the multiset $\{0, \infty, 1^{(2)}\}$. If $h \in I_f$ then either it stabilizes all three points $\{0, 1, \infty\}$, or it exchanges $0, \infty$ and stabilizes 1. Since an element of G is completely determined by its action on three distinct points on $\mathbb{P}^1$, the stabilizer in this case is at most $\mathbb{Z}/2$. A direct calculation shows that it is equal to $\mathbb{Z}/2\mathbb{Z}$.

For type $(1,3)$, as above, we can assume that $f = cx^3y$. Each element in the stabilizer of f must stabilize the multiset $\{0^{(3)}, \infty\}$, which means it stabilizes both 0 and ∞. An element of G fixing both points 0 and ∞ has to lie in the diagonal torus. Now the diagonal torus acts on x^3y by scalar multiplication, and only scalar matrices stabilizes x^3y. □

Proposition 3.2.7. *The union of orbits of stable types* $(1,1,1,1),(1,1,2)$ *and* $(1,3)$ *is a dense open subset* V^{reg} *of* V*, which contains the image of the Weierstrass section* $s : S \to V$*. The restriction of* $\pi : V \to S$ *to* V^{reg} *is smooth. Moreover, the restriction of the stabilizer group scheme* I *to* V^{reg} *is étale.*

Proof. The first two assertions follow directly from proposition 3.2.4 and 3.2.2 above. We derive from 3.2.4, that the morphism $m : G \times S \to V$, defined by restricting the action morphism to the Weierstrass section, is étale. By proposition 3.2.1, the image of this map is V^{reg}. We infer that the restriction of π to V^{reg} is smooth. Moreover, the morphism $G_S \times_S V^{\mathrm{reg}} \to V^{\mathrm{reg}} \times_S V^{\mathrm{reg}}$ defined by $(g, v) \mapsto (v, gv)$ is étale, and in particular, the restriction of I to V^{reg} is an étale group scheme. □

Corollary 3.2.8. *There exists a unique group scheme* I_S *over* S *equipped with a* G*-equivariant isomorphism* $\pi^* I_S \to I$ *over* V^{reg}*. There is a* $\mathbb{G}_m$*-equivariant isomorphism* $[BI_S] = [V^{\mathrm{reg}}/G]$ *where* BI_S *is the relative classifying stack of* I_S *over* S*.*

Proof. The group scheme I_S is obtained by descending I along $\pi|_{V^{\mathrm{reg}}}$. The descent datum is obtained using the conjugating action of G on I and the fact that I is abelian. The rest of the corollary is a formal consequence of what we have established so far. □

4 Elliptic curves

The relation between elliptic curves and invariant geometry of binary quartic forms has been discovered since 19th century by Cayley and Hermite, and later stated with precision by Weil [Wei54].

4.1 Jacobian of genus one curves

Let D_V be the family of arithmetic genus one curves defined over V by the equation $z^2 = f(x, y)$ where f varies over all binary quartic forms. It is constructed by the following cartesian diagram:

$$\begin{array}{ccc} D_V & \longrightarrow & \mathscr{O}_{\mathbb{P}^1_V}(2) \\ \downarrow & \overset{f}{\curvearrowright} & \downarrow{\scriptstyle (-)^2} \\ \mathbb{P}^1_V & \longleftarrow & \mathscr{O}_{\mathbb{P}^1_V}(4) \\ \downarrow & & \\ V & & \end{array} \tag{4.1.1}$$

where f is the universal binary quartic form, and $(-)^2 : \mathscr{O}_{\mathbb{P}^1_V}(2) \to \mathscr{O}_{\mathbb{P}^1_V}(4)$ is the squaring map.

Lemma 4.1.2. *If $f \in V(\bar{k}) - \{0\}$, D_f is reduced. If $f \in V^{\mathrm{reg}}(\bar{k})$, D_f is integral.*

Proof. For every $f \in V$, the curve D_f is defined on the ruled surface $\mathscr{O}_{\mathbb{P}^1_V}(2)$ by one single equation. For $f \neq 0$, it is generically reduced and thus reduced. If moreover $f \in V^{\mathrm{reg}}(\bar{k})$, the restriction of D_f over the formal completion of $\mathbb{P}^1$ at a simple zero of f is an irreducible covering of this formal disc. We deduce that D_f is irreducible for every $f \in V^{\mathrm{reg}}(\bar{k})$. Since D_f is reduced and irreducible, it is integral. □

Let D^{reg} be the restriction of D to V^{reg}. We can now apply the representability of the relative Picard functor and obtain the scheme $\mathrm{Pic}_{D^{\mathrm{reg}}/V^{\mathrm{reg}}}$ locally of finite type over V^{reg}. The Jacobian $E_{V^{\mathrm{reg}}} = \mathrm{Pic}^0_{D^{\mathrm{reg}}/V^{\mathrm{reg}}}$ over V^{reg} is defined to be the component classifying line bundles of degree 0. The smooth locus D^{sm} of $D^{\mathrm{reg}} \to V^{\mathrm{reg}}$ can be identified with $\mathrm{Pic}^1_{D^{\mathrm{reg}}/V^{\mathrm{reg}}}$, which is the component classifying line bundles of degree 1. In particular, D^{sm} is an E-torsor over V^{reg}.

One can easily check that if $f \in V^{\mathrm{reg}}(\bar{k})$ is a binary quartic form of one of the types $(1,1,1,1)$, $(1,1,2)$ and $(1,3)$, then E_f is an elliptic curve, $\mathbb{G}_m$ and $\mathbb{G}_a$ respectively. In the first case, D_f is a smooth genus one curve acted on simply transitively by the elliptic curve E_f. In the two latter cases, D_f is a rational curve, with nodal or cuspidal singularity respectively, acted on by E_f.

Over S, the universal Weierstrass curve E_S is defined to be the closed subscheme of $\mathbb{P}^2_S$ given by the equation:

$$z^2 y = x^3 + axy^2 + by^3.$$

Following Cayley and Hermite, Weil proved in [Wei54] that for every binary quartic form $f \in V^{\mathrm{reg}}(\bar{k})$ of type $(1,1,1,1)$ of invariant $(a,b) \in S(\bar{k})$, there is a canonical isomorphism $E_f = E_{a,b}$. His proof can be extended to the regular locus so that we have a canonical isomorphism

$$E_{V^{\mathrm{reg}}} \to E_S \times_S V^{\mathrm{reg}}. \tag{4.1.3}$$

We remark that this isomorphism can be made naturally $G \times \mathbb{G}_m$-equivariant compatible with the action of $G \times \mathbb{G}_m$ on V given by the formula (3.1.1).

4.2 Centralizer and 2-torsion of elliptic curves

In this subsection, we will present what we see as an important link between the arithmetic of elliptic curves and invariant geometry of binary quartic forms. Recall that over S, formula (3.2.3) defines the stabilizer group scheme I, which is quasi-finite and étale over V^{reg}.

Proposition 4.2.1. *Over V^{reg}, there is a canonical isomorphism*

$$I|_{V^{\mathrm{reg}}} \cong E[2]|_{V^{\mathrm{reg}}}.$$

Proof. By construction (4.1.1), G acts on the family of arithmetic genus one curve D over V^{reg}. This induces an action of G on the Jacobian E of D. For every $f \in V^{\mathrm{reg}}$, the stabilizer I_f acts on the genus one curve D_f and its Jacobian E_v. It follows from the Cayley-Hermite-Weil theorem (4.1.3) that I_f acts trivially on E_f.

As our construction is functorial, if $h \in I_f$, $d \in D_f^{\mathrm{sm}}$ and $e \in E_f$, we have

$$h(ed) = h(e)h(d)$$

where ed denotes the action of E_f on D_f^{sm}. Since I_f acts trivially on E_f, the above equality implies that the action of I_f and E_f on D_f^{sm} commute. As D_f^{sm} is a torsor under the action of E_f, this gives rise to a homomorphism

$$I_f \to E_f \tag{4.2.2}$$

through which the action of I_f on D_f^{sm} factors.

We will first prove that the homomorphism (4.2.2) factors through the subgroup $E_f[2]$ of 2-torsions of E_f. It suffices to prove this for f of type $(1,1,1,1)$, since the general case follows by flatness. Let R_f denote the ramification locus of D_f over $\mathbb{P}^1$. One can check that $E_f[2]$ acts simply transitively on R_f and this action commutes with the action of I_f. This gives rise to a homomorphism $I_f \to E_f[2]$ through which (4.2.2) factors.

For both I and $E[2]$ are étale group schemes over V^{reg}, in order to prove that $I \to E[2]$ is an isomorphism, it is enough to check that it induces a bijection on geometric points over each $f \in V^{\mathrm{reg}}(\bar{k})$.

Let $f \in V^{\mathrm{reg}}(\bar{k})$ be of type $(1,1,1,1)$. Let $h \in I_f$ be an element with trivial image in $E_f[2]$. In this case, f fixes all the four ramifications points of D_f. In other words, it fixes the four zeros of f, which implies that $h = 1$ since PGL_2 acts sharply 3-transitive on the projective line. It follows that the homomorphism $I_f \to E_f[2]$ is injective. It must also be surjective, for both groups I_f and $E_f[2]$ have 4 elements.

For type $(1,1,2)$, this is an explicit calculation for nodal rational curve as in proposition 3.2.6. Finally, for type $(1,3)$, there is nothing to be proved, since both groups I_f and $E_f[2]$ are trivial. □

The isomorphism $I \to E[2]$ over V^{reg} is by construction G-equivariant. It descends to an isomorphism of group schemes $I_S \to E_S[2]$ over S, where I_S is defined in proposition 3.2.8 and E_S in (4.1.3). It follows from proposition (3.2.8) that there exists a $\mathbb{G}_m$-equivariant isomorphism

$$BE_S[2] = [V^{\mathrm{reg}}/G]. \tag{4.2.3}$$

4.3 Link to 2-Selmer groups

Recall that C is a smooth, projective and geometrically connected curve over k. We will denote $K = k(C)$ the field of rational functions of C and K_v its completion at a closed point $v \in |C|$.

For each morphism $\alpha : C \to [S/\mathbb{G}_m]$ we have a family of Weierstrass curve $E_\alpha = \alpha^* E_S$. The groupoid of maps $\beta : C \to [BI_S/\mathbb{G}_m]$ over α is by definition the groupoid of I_α-torsors over E where $I_\alpha = \alpha^* I_S$. We will show in this section that there is a closed connection between this groupoid and the 2-Selmer group of the generic fiber $E_{\alpha,K}$ of E_α. We recall that for each elliptic curve E defined over K, the 2-Selmer group of E is defined as the kernel of the homomorphism:

$$\mathrm{Sel}_2(E) = \ker(H^1(K, E[2]) \to \prod_{v \in |C|} H^1(K_v, E)).$$

We will write $\mathrm{Sel}_2(E_\alpha)$ instead of $\mathrm{Sel}_2(E_{\alpha,K})$ as this shorthand doesn't cause any confusion.

The étale cohomology group $H^1(C, I_\alpha)$ is naturally identified with the group of isomorphism classes of I_α-torsors over E. By restriction to the generic fiber of C, we obtain a homomorphism

$$H^1(C, I_\alpha) \to H^1(K, I_\alpha) = H^1(K, E_\alpha[2]). \tag{4.3.1}$$

Proposition 4.3.2. *The homomorphism* (4.3.1) *factors through the 2-Selmer group* $\mathrm{Sel}_2(E_\alpha)$.

Proof. We have the following commutative diagram for each $v \in |C|$:

$$\begin{array}{ccc} H^1(C, I_\alpha) & \longrightarrow & H^1(K, I_\alpha) \\ \downarrow & & \downarrow \\ H^1(\mathrm{Spec}\, \mathcal{O}_v, I_\alpha) & \longrightarrow & H^1(K_v, I_\alpha) \\ \downarrow & & \downarrow \\ H^1(\mathrm{Spec}\, \mathcal{O}_v, E_\alpha) & \longrightarrow & H^1(K_v, E_\alpha). \end{array}$$

But by Lang's theorem, we know that $H^1(\mathrm{Spec}\, \mathcal{O}_v, E_\alpha) = 0$ since E_S has connected fibers. It follows that the composition map

$$H^1(C, I_\alpha) \to H^1(K_v, E_\alpha)$$

is trivial for all $v \in |C|$. The lemma follows. □

As a corollary, we obtain a natural map

$$\rho_\alpha : H^1(C, I_\alpha) = H^1(C, E_\alpha[2]) \to \mathrm{Sel}_2(E_\alpha) \tag{4.3.3}$$

for all maps $\alpha : C \to [S/\mathbb{G}_m]$ whose image is not contained in the discriminant locus.

Proposition 4.3.4. *If $\alpha : C \to [S/\mathbb{G}_m]$ is transversal to the discriminant locus in the sense of 2.1.6, then the homomorphism $\rho_\alpha : H^1(C, H^1(C, E_\alpha[2])) \to \mathrm{Sel}_2(E_\alpha)$ is an isomorphism.*

Proof. The assumption $\alpha : C \to [S/\mathbb{G}_m]$ is transversal to the discriminant locus implies that E_α/C is a smooth group scheme with elliptic or multiplicative fibers, which is the global Néron model of its generic fiber.

Let v be a geometric point of C such that $c(v)$ lies in the discriminant locus. We denote C_v the completion of $C \otimes_k \bar{k}$ at v, $\mathrm{Spec}(K_v)$ the generic point of C_v, and $I_v = \mathrm{Gal}(K_v)$. The transversality implies that Δ vanishes at v to order 1. Using the description of the Tate curve, we know that

$$(E_\alpha(K_v)[2])^{I_v} = \mathbb{Z}/2\mathbb{Z}.$$

Geometrically, this means that over C_v, the étale group scheme $E_\alpha[2]$ is exactly the étale locus in its normalization over C_v. We deduce that globally, $E_\alpha[2]$ is exactly the étale locus in its normalization over C.

This observation will allow us to prove the injectivity of the map

$$H^1(C, E_\alpha[2]) \to H^1(K, E_\alpha[2]).$$

Indeed, let T be an $E_\alpha[2]$-torsor over C. We will prove that T is uniquely determined by its generic fiber. We observe that for every geometric point v of C, the restriction of T to the formal disc C_v is isomorphic to the restriction of $E_\alpha[2]$. As $E_\alpha[2]$, T restricted to C_v is exactly the étale locus of its normalization over C_v. Hence, globally, T can also be identified with the étale locus of its normalization over C. This means that we can reconstruct T by removing the ramification locus from the normalization of its generic fiber. This proves the injectivity of ρ_α.

We will now prove that ρ_α is surjective. Let T_K be an $E_\alpha[2]$-torsor over K whose isomorphism class lies in $\mathrm{Sel}_2(E_\alpha)$. We will show that the Selmer condition implies that T can be extended as an I-torsor over C. We first spread T to a $E_\alpha[2]$-torsor defined over some nonempty open subset U of C. After that, we only need to prove that T can be extended to a $E_\alpha[2]$-torsor over the formal discs C_v around the remaining points, and thus we are reduced to a local problem.

The Selmer condition at v implies that the class of T in $H^1(K_v, E_\alpha[2])$ lies in the image of $E_\alpha(K_v)/2E_\alpha(K_v)$. There exists a point $x \in E_\alpha(K_v)$ such that the torsor T_{K_v} fits in a cartesian diagram:

$$\begin{array}{ccc} T_{K_v} & \longrightarrow & E_{\alpha,K_v} \\ \downarrow & & \downarrow{\scriptstyle \cdot 2} \\ \mathrm{Spec}\, K_v & \xrightarrow{x} & E_{\alpha,K_v} \end{array}$$

Since E_{α,C_v} is the Néron model of E_{α,K_v}, the K_v-point x of E_α can be extended as a C_v-point

$\tilde{x}$. We can now extend the E_{K_v}-torsor T_{K_v} to a E_{C_v}-torsor by forming the cartesian diagram

$$\begin{array}{ccc} T_{C_v} & \longrightarrow & E_{\alpha,C_v} \\ \downarrow & & \downarrow{\scriptstyle \cdot 2} \\ C_v & \xrightarrow{x} & E_{\alpha,C_v} \end{array}$$

This completes the proof of surjectivity of ρ_α. □

In the case where α is not transversal to the discriminant locus, it can happen that the homomorphism ρ_α is neither surjective nor injective. Nevertheless, we can compare sizes of $\mathrm{Sel}_2(E_\alpha)$ and $H^1(C, I_\alpha)$.

Proposition 4.3.5. *Let $\alpha : C \to [S/\mathbb{G}_m]$ and suppose that the generic fiber of E_α is an elliptic curve. Then*

$$\begin{cases} |\mathrm{Sel}_2(E_\alpha)| \leq |H^1(C, I_\alpha)|, & \text{when } E_\alpha[2](K) = 0, \\ |\mathrm{Sel}_2(E_\alpha)| \leq 4|H^1(C, I_\alpha)|, & \text{otherwise.} \end{cases}$$

Proof. From the proof of proposition 4.3.4, we always have

$$|\mathrm{Sel}_2(E_\alpha)| \leq |H^1(C, \mathscr{E}[2])|,$$

where $\mathscr{E}$ is the Néron model of the generic fiber of E_α over C, since we can always lift a Selmer class to a torsor of $\mathscr{E}[2]$ over C. Note that in the proof of proposition 4.3.4, we lift the Selmer class to an $E[2]$-torsor over C, exploiting the isomorphism $E \cong \mathscr{E}$ in the transversal situation.

From the short exact sequence of group schemes over C

$$0 \longrightarrow E_\alpha[2] \longrightarrow \mathscr{E}[2] \longrightarrow Q \longrightarrow 0,$$

where Q is a skyscraper sheaf, we have the following long exact sequence

$$0 \longrightarrow H^0(E_\alpha[2]) \longrightarrow H^0(\mathscr{E}[2]) \longrightarrow H^0(Q) \longrightarrow H^1(E_\alpha[2]) \longrightarrow H^1(\mathscr{E}[2]) \longrightarrow H^1(Q) \longrightarrow L \longrightarrow 0.$$

where L is the kernel of the map $H^2(E_\alpha[2]) \to H^2(\mathscr{E}[2])$.

Since Q is a skyscraper sheaf, its cohomology groups are direct sums of Galois cohomology groups of finite fields. It follows that

$$|H^0(Q)| = |H^1(Q)|.$$

Using multiplicative Euler characteristic, combined with the fact that

$$|H^0(E_\alpha[2])| = |H^0(\mathscr{E}[2])| = 1$$

under the assumption $E_\alpha[2](K) = 0$, or

$$|H^0(\mathscr{E}[2])|/|H^0(E_\alpha[2])| \leq 4,$$

without this assumption, we get the desired inequality. □

4.4 The geometric setup

We can now define the moduli spaces $\mathscr{M}_{\mathscr{L}}$ and $\mathscr{A}_{\mathscr{L}}$ promised at the end of section 2. First, we denote

$$\mathscr{M} = \mathrm{Hom}(C, [BI_S/\mathbb{G}_m])$$
$$\mathscr{A} = \mathrm{Hom}(C, [S/\mathbb{G}_m]).$$

We clearly have a map $\mathscr{M} \to \mathscr{A}$, compatible with the natural map to $\mathrm{Bun}_{\mathbb{G}_m} = \mathrm{Hom}(C, B\mathbb{G}_m)$.

For a given line bundle $\mathscr{L} \in \mathrm{Bun}_{\mathbb{G}_m}(k)$ over C, we denote $\mathscr{M}_{\mathscr{L}}$ and $\mathscr{A}_{\mathscr{L}}$ the fiber of $\mathscr{M}$ and $\mathscr{A}$ over $\mathscr{L}$. The space $\mathscr{A}_{\mathscr{L}}$ classifies family of Weierstrass curves of Hodge bundle $\mathscr{L}$. For a given $\alpha : C \to [S/\mathbb{G}_m]$, we denote $E_\alpha = \alpha^* E$ the induced family of Weierstrass elliptic curves and $E_\alpha[2]$ its 2-torsion subgroup. The fiber of $\mathscr{M} \to \mathscr{A}$ over α, classifying $E_\alpha[2]$-torsor over C is our replacement for the Selmer group $\mathrm{Sel}_2(E_\alpha)$, for as shown in proposition 4.3.4, there is a canonical isomorphism $H^1(C, E_\alpha[2]) \to \mathrm{Sel}_2(E_\alpha)$ in case α is transversal to the discriminant locus, anh otherwise we have the inequality in proposition 4.3.5.

Even though it is not easy to count points on $\mathrm{Hom}(C, [BI_S/\mathbb{G}_m])$ directly, the invariant theory of binary quartic forms allows us to represent $\mathscr{M}$ by yet another way. Namely, (4.2.3) induces an isomorphism:

$$\mathscr{M} = \mathrm{Hom}(C, [V^{\mathrm{reg}}/G \times \mathbb{G}_m]).$$

By definition, a k-point of $\mathscr{M}$ consists of a triple $(\mathscr{E}, \mathscr{L}, \alpha)$, where $\mathscr{E}$ is a G-torsor, $\mathscr{L}$ a line bundle, and α a section of $V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}} = (V^{\mathrm{reg}} \times^G \mathscr{E}) \otimes \mathscr{L}^{\otimes 2}$. This new presentation is thus very convenient for counting points, since we are essentially counting sections of the vector bundle $V(\mathscr{E}, \mathscr{L}) = (V \times^G \mathscr{E}) \otimes \mathscr{L}^{\otimes 2}$ satisfying some condition.

This suggests that instead of counting points on $\mathscr{M}$, we should count points on

$$\mathscr{M}' = \mathrm{Hom}(C, [V/G \times \mathbb{G}_m]).$$

and study the ratio between the two numbers. The k-points on $\mathscr{M}'$ are of course those triples $(\mathscr{E}, \mathscr{L}, \alpha)$ where $\mathscr{E}, \mathscr{L}$ are as above, and α is a section of $V(\mathscr{E}, \mathscr{L})$.

However, one needs to pay attention to the fact that for any line bundle $\mathscr{L}$, the number of k-points on $\mathscr{M}'_{\mathscr{L}}$ is infinite. In order to make sense of the ratio, one fix a G-bundle $\mathscr{E}$, and calculate the ratio

$$\frac{|\mathscr{M}_{\mathscr{E},\mathscr{L}}(k)|}{|\mathscr{M}'_{\mathscr{E},\mathscr{L}}(k)|}$$

as $\deg(\mathscr{L}) \to \infty$ while $\mathscr{E}$ being fixed. This ratio calculation will be performed in the next section following some ideas of Poonen.

5 On density

5.1 Poonen's results

In this section, we will prove a density result that allows us to compute the difference between the number of sections to the regular part and the number of all sections. As the main ideas are already presented in [Poo03], we will only indicate necessary modifications in the proof.

Proposition 5.1.1. *Let C be a smooth projective curve over $\mathbb{F}_q$, $\mathscr{E}$ a vector bundle over C of rank n. Let $X \subset \mathscr{E}$ be a locally closed $\mathbb{G}_m$-stable subscheme of codimension at least 2 whose fiber at every point $v \in C$, $X_v \subset \mathscr{E}_v$ is also of codimension at least 2. Then the ratio*

$$\mu(X, \mathscr{L}) = \frac{|\{s \in \Gamma(C, \mathscr{E} \otimes \mathscr{L}) : s \text{ avoids } X \otimes \mathscr{L}\}|}{|\Gamma(C, \mathscr{E} \otimes \mathscr{L})|}$$

as $\deg(\mathscr{L}) \to \infty$, tends to the limit

$$\mu(X) := \lim_{\deg \mathscr{L} \to \infty} \mu(X, \mathscr{L}) = \prod_{v \in |C|} \left(1 - \frac{c_v}{|k(v)|^n}\right),$$

where $c_v = |X_v(k(v))|$, with $k(v)$ denoting the residue field at v.

The main point of this result is that the density can be computed as the product of local densities, which are the factors in the product on the RHS of the formula above. Before starting the proof, we first prove the following lemma.

Lemma 5.1.2. *Let C be a smooth projective curve over k. There exists a finite set $S \subset |C|$ and a number n such that for all line bundles $\mathscr{L}$ with $\deg \mathscr{L} > n$, there exists an effective divisor D supported on S such that $\mathscr{L} \cong \mathscr{O}_C(D)$. Moreover, we can choose $D_{\mathscr{L}} = \sum_{v \in S} a_v(\mathscr{L})v$ for each $\mathscr{L}$ such that as $\deg \mathscr{L}$ goes to ∞, so does $a_v(\mathscr{L})$ for each $v \in S$.*

Proof. We start with m distinct points $Q_1, \ldots, Q_m \in |C|$ with m being a big enough integer such that $\mathscr{L}(\sum_{j=1}^m Q_j)$ has non zero global sections for all line bundles $\mathscr{L} \in \mathrm{Pic}^0_{C/\mathbb{F}_q}(\mathbb{F}_q)$. It follows that every line bundle $\mathscr{L} \in \mathrm{Pic}^0_{C/\mathbb{F}_q}(\mathbb{F}_q)$ can be written as

$$\mathscr{L} = \mathscr{O}_C\left(\sum_i P_i - \sum_{j=1}^m Q_j\right). \tag{5.1.3}$$

Since $\mathrm{Pic}^0_{C/\mathbb{F}_q}(\mathbb{F}_q)$ is a finite set, there are finitely many points P_i that may appear in (5.1.3). We let S be the union of all the Q_j and P_i appearing above.

We also suppose that the points $Q_1, \dots, Q_m$ have been chosen such that their degrees are relatively prime. It that case the monoid generated by $\deg(Q_1), \dots, \deg(Q_m)$ will contain all integers d big enough. That is, there exists N such that for all $d > N$, we can write $d = \sum_{j=1}^{m} d_i \deg(Q_i)$ with d_i being positive integers. We can also choose the integers d_j in such a way that each $d_j \to \infty$ as $d \to \infty$.

Let $\mathscr{L} \in \mathrm{Pic}^d_{C/\mathbb{F}_q}(\mathbb{F}_q)$. If $d > N$, then we can write

$$\mathscr{L} \cong \mathscr{O}\left(\sum_{j=1}^{m} d_i Q_i\right) \otimes \mathscr{L}',$$

and $\deg \mathscr{L}' = 0$. Then by using (5.1.3), we have

$$\mathscr{L} \cong \mathscr{O}\left(\sum P_i + \sum_{j=1}^{m} (d_j - 1) Q_j\right),$$

where $P_i, Q_i \in S$.

The last part of the lemma can be proved by an obvious modification of the argument above. □

Remark 5.1.4. From the proof of the lemma, we see at once that the set S can always be made arbitrarily large.

Following [Poo03, theorem 3.1], we will prove proposition 5.1.1 by showing that we can compute the density as the limit of a finite product of densities over closed points where the sizes of the residue fields are bounded. The following lemma enables us to do so.

Lemma 5.1.5. *Let $C, \mathscr{E}$ and X be as in proposition 5.1.1. For each $M > 0$ we define*

$$\mathscr{Q}_{M,\mathscr{L}} = \{s \in \Gamma(X, \mathscr{E} \otimes \mathscr{L}) : \exists v \in |C|, |k(v)| \geq M \text{ and } s_x \in X_x\}.$$

Then

$$\lim_{M \to \infty} \limsup_{\deg \mathscr{L} \to \infty} \frac{|\mathscr{Q}_{M,\mathscr{L}}|}{|\Gamma(X, \mathscr{E} \otimes \mathscr{L})|} = 0.$$

Proof. This statement is more or less a restatement of what is already proved in the first part of the proof of [Poo03, theorem 8.1] (see also [Poo03, lemma 5.1]). We will thus only indicate why this is the case.

Since we are only interested in the case where $M \gg 0$, we can throw away as many points of C as we want. We can therefore replace C by any open affine subscheme C' such that $\mathscr{E}$ is free over C'. Now, lemma 5.1.2 implies that we can choose C' such that our limit has the same form as the limit defined in [Poo03, theorem 8.1].

Observe that Poonen proves his limit for the case where $X|_{C'}$ is defined by 2 equations that are generically relative primes. But now, we can conclude by noting that since X is of codimension at least 2, we can find such f, g that both vanish on X (see the proof of [Poo03, lemma 5.1]). □

Proof of 5.1.1. The proof of 5.1.1 can be carried word for word from the proof of [Poo03, theorem 3.1], where lemma 5.1.5 plays the role of [Poo03, lemma 5.1]. Indeed, if we denote

$$\mu(X_M) = \lim_{\deg \mathscr{L} \to \infty} \frac{|\{s \in \Gamma(C, \mathscr{E} \otimes \mathscr{L}) : s \text{ avoids } X \otimes \mathscr{L} \text{ at all } v \in |C|, |k(v)| < M\}|}{|\Gamma(C, \mathscr{E} \otimes \mathscr{L})|},$$

then lemma 5.1.5 implies that

$$\mu(X) = \lim_{M \to \infty} \mu(X_M).$$

Note that the linear map

$$\Gamma(C, \mathscr{E} \otimes \mathscr{L}) \to \prod_{\substack{v \in |C| \\ |k(v)| < M}} \mathscr{E} \otimes \mathscr{L} \otimes k(v) \cong \prod_{\substack{v \in |C| \\ |k(v)| < M}} \mathscr{E} \otimes k(v)$$

is surjective when $\deg \mathscr{L} \gg 0$ due to the vanishing of

$$H^1\left(C, \mathscr{E} \otimes \mathscr{L}\left(-\sum_{\substack{v \in |C| \\ |k(v)| < M}} v\right)\right)$$

when $\deg \mathscr{L} \gg 0$. Thus, we have

$$\mu(X_M) = \prod_{\substack{v \in |C| \\ |k(v)| < M}} \left(1 - \frac{c_v}{|k(v)|^n}\right),$$

where c_v is defined as in proposition 5.1.1. □

Using a similar argument, we have the following result also.

Proposition 5.1.6. *Let $C, \mathscr{E}, X$ as above, and $D \subset \mathscr{E}$ be a subscheme defined by the vanishing of an equation $d : \mathscr{E} \to \mathscr{L}'$, where $\mathscr{L}'$ is a line bundle over C. Suppose that d is generically square-free, then*

$$\lim_{\deg \mathscr{L} \to \infty} \frac{|\{s \in \Gamma(C, \mathscr{E} \otimes \mathscr{L}) : s \in \mathscr{E} \setminus X \text{ and } s \text{ intersects } D \text{ transversally}\}|}{|\Gamma(C, \mathscr{E} \otimes \mathscr{L})|} = \prod_{v \in |C|} \left(1 - \frac{c_v}{|k(v)|^{2n}}\right),$$

where c_v is the number of elements s in $\mathscr{E} \otimes \mathscr{O}_{C,v}/\mathfrak{m}_v^2$ such that s lies in $X \otimes \mathscr{O}_{C,v}/\mathfrak{m}_v^2$ or $d(s) = 0$ in $\mathscr{O}_{C,v}/\mathfrak{m}_v^2$.

Proof. The proof of this proposition is almost identical to the one above. As we have seen, all we need to do is to prove the analog of lemma 5.1.5 for this case. Observe also that we only need to prove such a lemma for a suitable open affine sub-curve C' which can be chosen such that $\mathscr{E}|_{C'}$ and $\mathscr{L}|_{C'}$ are free. In this case, d is just a generically square-free polynomial with coefficient in $\Gamma(C', \mathscr{O}_{C'})$.

If X is an empty scheme, this is already done in [Poo03, theorem 8.1]. When X is not empty then we see that the error term is bounded above by the sum of the error term in the case where X is empty and the error term given in 5.1.5 above. But since both go to zero as M goes to infinity, we are done. □

5.2 Some density computations

In this subsection, for brevity's sake, we will use $V(\mathscr{E})$ and $V(\mathscr{E})^{\mathrm{reg}}$ to denote $V(\mathscr{E}, \mathscr{O}_C)$ and $V(\mathscr{E}, \mathscr{O}_C)^{\mathrm{reg}}$ respectively (see the notation in subsection 4.4), where $\mathscr{E}$ denotes an arbitrary fixed G-torsor.

Proposition 5.2.1. *The density of $V(\mathscr{E})^{\mathrm{reg}}$ inside $V(\mathscr{E})$ is $\zeta_C(2)^{-1}$.*

Proof. By proposition 5.1.1, it suffices to show that the local density at a point $v \in |C|$ of the regular part is $1 - |k(v)|^{-2}$. For this, we first count the number of points in the non-regular part. By the classification of different orbits on V, we know that a point f in the non-regular part must be of type $(2,2)$ or (4) or 0. Thus, we see at once that up to a scalar multiple, f is a square of a quadratic polynomial.

Note that the squaring map (from quadratic to quartic polynomials) is a two to one map, except at the 0 polynomial. The image of the map is not surjective on the non-regular part, and the missing points are precisely those which are a scale of a point in the image by a non-square element in $k(v)^\times$. Thus, the number of points in the non-regular part is

$$\frac{|\{\text{non-zero binary quadratic polynomials}\}|}{2}|k(v)^\times/k(v)^{\times 2}| + 1 = \frac{|k(v)|^3 - 1}{2}2 + 1 = |k(v)|^3.$$

Thus, the local density of the regular part is

$$\frac{|k(v)|^5 - |k(v)|^3}{|k(v)|^5} = 1 - |k(v)|^{-2}.$$

□

Proposition 5.2.2. *The density of $(a,b) \in \Gamma(C, \mathscr{L}^{\otimes 4} \oplus \mathscr{L}^{\otimes 6})$ transversal to the discriminant locus among all pairs (a,b) is*

$$\prod_{v \in |C|} (1 - 2|k(v)|^{-2} + |k(v)|^{-3}).$$

Proof. By proposition 5.1.6, it suffices to show that the local density at a point $v \in |C|$ of the transversal part is $1 - 2|k(v)|^{-2} + |k(v)|^{-3}$.

Let denote $R = k(v)[\varepsilon]/(\varepsilon^2)$. We observe that $(a, b) \in S(R) = R^2$ is in the transversal part if and only if $\Delta(a, b) \neq 0$ in R. If $(a, b) \in S(R)$, then we denote $(\overline{a}, \overline{b}) \in S(k(v))$ the associated $k(v)$-point, by reduction. Observe that $\Delta : \mathbb{A}^2 \to \mathbb{A}^1$ is smooth on $S - \{(0,0)\}$. In particular, when $(a, b) \in S(R)$ such that $(\overline{a}, \overline{b}) \neq (0, 0)$, then the fiber of $T_{(\overline{a},\overline{b})}S \to T_{\Delta(\overline{a},\overline{b})}$ has dimension exactly one. Thus, the number of non-transversal pairs $(a, b) \in S(R)$ is

$$\begin{aligned}\sum_{\substack{(\overline{a},\overline{b})\neq(0,0)\\ \Delta(\overline{a},\overline{b})=0}} |k(v)| + \sum_{(\overline{a},\overline{b})=(0,0)} |k(v)|^2 &= |k(v)|(|\mathbb{G}_a(k(v))| - 1) + |k(v)|^2 \\ &= |k(v)|(|k(v)| - 1) + |k(v)|^2 \\ &= 2|k(v)|^2 - |k(v)|.\end{aligned}$$

Thus, the local density of transversal pairs is

$$\frac{|k(v)|^4 - 2|k(v)|^2 + |k(v)|}{|k(v)|^4} = 1 - 2|k(v)|^{-2} + |k(v)|^{-3},$$

where we have used $|R|^2 = |k(v)|^4$. □

Proposition 5.2.3. *The density of sections in $V(\mathscr{E})$ that are in $V(\mathscr{E})^{\mathrm{reg}}$ whose associated pair (a, b) is transversal to the discriminant is*

$$\prod_{v\in|C|}(1 - |k(v)|^{-2})(1 - 2|k(v)|^{-2} + |k(v)|^{-3}).$$

Proof. The strategy is similar to what we have done above. Here, we also compute the complement of the described condition on $V(\mathscr{E})$. As in the previous lemma, we let $v \in |C|$ and $R = k(v)[\varepsilon]/(\varepsilon^2)$. In this computation, for brevity's sake, we denote $k = \mathbb{F}_q = k(v)$, and hence, $q = |k(v)|$. The number of points that fail the described condition is

$$\begin{aligned}&|V^{\text{non-reg}}(R)| + |V^{\text{reg,non-transversal}}(R)| \\ &= \sum_{f\in V^{\text{non-reg}}(k)} |T_{V,f}(k)| + \sum_{\substack{f\in V^{\mathrm{reg}}(k)\\ \Delta(f)=0}} |\ker d\Delta_f(k)| \\ &= q^3q^5 + \sum_{\substack{f\in V^{\mathrm{reg}}(k)\\ a(f)\neq0, b(f)\neq0\\ \Delta(f)=0}} |\ker d\Delta_f(k)| + \sum_{\substack{f\in V^{\mathrm{reg}}(k)\\ a(f)=b(f)=0}} |\ker d\Delta_f(k)|, \qquad (5.2.4)\end{aligned}$$

where q^3 comes from the computation made in proposition 5.2.1 above.

Observe that if $f \in V^{\mathrm{reg}}(k)$, then geometrically, namely, over $\overline{\mathbb{F}_q}$, f is in the same orbit as $y(x^3 + a(f)xy^2 + b(f)y^3)$. The condition $\Delta(f) = 0$, then implies that f can only be of type $(1,1,2)$ or $(1,3)$. We see easily that type $(1,1,2)$ and type $(1,3)$ can only occur in the second and third summands, respectively, of (5.2.4).

We will now compute the number of $f \in V(k)$ of type $(2,1,1)$. We see at once that the double root must be rational and hence, over k, we have $f = c(x - ay)^2(x^2 + uxy + vy^2)$. Thus, the number of such f can be computed as

$$|\mathbb{G}_m(k)||\mathbb{P}^1(k)||\mathrm{Sym}^2\mathbb{A}^1(k) - \mathrm{diagonal}(k)| = (q-1)(q+1)(q^2-q) = q(q^2-1)(q-1).$$

Similarly, the number of f of type $(1,3)$ can be computed as

$$|\mathbb{G}_m(k)||\mathbb{P}^1(k)||\mathbb{A}^1(k)| = (q-1)(q+1)q = q(q^2-1).$$

To compute the $|\ker d\Delta_f|$ factors, we note that the map $V^{\mathrm{reg}} \to S$ is smooth by corollary 3.2.7, and the smooth locus of $\Delta : S \to \mathbb{A}^1$ is precisely $S - \{(0,0)\}$. This enables us to compute the dimension of $\ker d\Delta_f$, and hence its size, at some point $f \in V^{\mathrm{reg}}(k)$. Indeed, for type $(1,1,2)$ and $(1,3)$, $|\ker d\Delta_f(k)|$ is $q^3 q = q^4$ and $q^3 q^2 = q^5$ respectively.

Gathering all the results above, we have

$$(5.2.4) = q^8 + q^5(q^2-1)(q-1) + q^6(q-1)(q+1) = 3q^8 - q^7 - 2q^6 + q^5.$$

Thus, the number of transversal and regular points in $V(R)$ is

$$q^{10} - 3q^8 + q^7 + 2q^6 - q^5 = q^5(q^2-1)(q^3-2q+1).$$

The local density is thus

$$(1-q^{-2})(1-2q^{-2}+q^{-3}).$$

as stated. □

A similar computations and arguments as above will give us the following results.

Proposition 5.2.5. *The density of sections in S that are minimal is $\zeta_C(10)^{-1}$.*

Proposition 5.2.6. *The density of sections in $V(\mathscr{E})$ that are in $V(\mathscr{E})^{\mathrm{reg}}$ and whose associated invariant (a,b) is minimal, is $\zeta_C(2)^{-1}\zeta_C(10)^{-1}$.*

6 Counting

6.1 The Harder-Narasimhan polygon

We will first compute the average number of I-torsors, i.e. we want to estimate the following

$$\lim_{d\to\infty} \frac{|\mathscr{M}_{\mathscr{L}}(k)|}{|\mathscr{A}_{\mathscr{L}}(k)|}.$$

Let $d = \deg(\mathscr{L})$. Since we are only interested in the behavior of this quotient when $d \to \infty$, when we do the computation below, we assume that $d \gg 0$. Note also that when $d \gg 0$, $|\mathscr{A}_{\mathscr{L}}(k)|$ is easy to compute using Riemann-Roch, since it is just the number of sections to $\mathscr{L}^{\otimes 4} \oplus \mathscr{L}^{\otimes 6}$. Indeed, we have

$$|\mathscr{A}_{\mathscr{L}}(k)| = |H^0(C, \mathscr{L}^{\otimes 4} \oplus \mathscr{L}^{\otimes 6})| = q^{10d+2(1-g)}, \qquad \text{when } d \gg 0.$$

We will count $|\mathscr{M}_{\mathscr{L}}(k)|$ by using the map

$$\mathscr{M}_{\mathscr{L}} \to \mathrm{Bun}_G$$

and a partition of $\mathrm{Bun}_G(k)$ according to the Harder-Narasimhan polygon. Note that since $H^2(C, \mathbb{G}_m) = 0$ (see [Mil80, p. 109]) every G-bundle $\mathscr{E}$ over C can be lifted to a vector bundle $\mathscr{F}$ of rank 2 which is well defined up to tensor twist by a line bundle. If $\mathscr{F}$ is not semi-stable, then there is a unique tensor twist so that its Harder-Narasimhan filtration has the form

$$0 \longrightarrow \mathscr{L}' \longrightarrow \mathscr{F} \longrightarrow \mathscr{O}_C \longrightarrow 0, \tag{6.1.1}$$

with $\deg \mathscr{L}' > 0$. Note that after such normalization, $\mathscr{F}$ is determined uniquely by the associated G-bundle $\mathscr{E}$, and we will call $n = \deg \mathscr{L}'$ the unstable degree of $\mathscr{E}$. It is not difficult to determine the size of the automorphism group of a G-bundle $\mathscr{E}$ of unstable degree n large enough compared to the genus g

$$|\mathrm{Aut}_G(\mathscr{E})| = (q-1)q^{n+1-g}. \tag{6.1.2}$$

Let $\mathscr{E}$ be a G-torsor of unstable degree $n > 0$; it can be lifted to a rank two vector bundle $\mathscr{F}$ fitting in the exact sequence (6.1.1). We then have an associated 5-dimensional vector bundle $V(\mathscr{E}, \mathscr{L})$:

$$V(\mathscr{E}, \mathscr{L}) = (V \times^G \mathscr{E}) \otimes \mathscr{L}^{\otimes 2} = V(\mathscr{E}) \otimes \mathscr{L}^{\otimes 2} \cong \mathrm{Sym}^4 \mathscr{F} \otimes \det{}^{-2} \mathscr{F} \otimes \mathscr{L}^{\otimes 2}$$

and $V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}}$ the regular part of $V(\mathscr{E}, \mathscr{L})$. The filtration (6.1.1) on $\mathscr{F}$ induces an obvious filtration on $V(\mathscr{E}, \mathscr{L})$

$$0 \subset \mathscr{F}_0 \subset \mathscr{F}_1 \subset \mathscr{F}_2 \subset \mathscr{F}_3 \subset \mathscr{F}_4 = V(\mathscr{E}, \mathscr{L}),$$

where $\mathscr{F}_i / \mathscr{F}_{i-1} \cong \mathscr{L}'^{\otimes(2-i)} \otimes \mathscr{L}^{\otimes 2}$.

We will calculate the mass of the groupoid $\mathscr{M}_{\mathscr{L}}(k)$ in different ranges according to the integers n and d:

Case 1: $n > 2d$. When d is sufficiently large, the exact sequence (6.1.1) splits, and we have $F \cong \mathscr{L}' \oplus \mathscr{O}_C$, which implies that

$$V(\mathscr{E},\mathscr{L}) \cong (\mathscr{L}'^{\otimes 2} \otimes \mathscr{L}^{\otimes 2}) \oplus (\mathscr{L}' \otimes \mathscr{L}^{\otimes 2}) \oplus \mathscr{L}^{\otimes 2} \oplus (\mathscr{L}'^{\otimes -1} \otimes \mathscr{L}^{\otimes 2}) \oplus (\mathscr{L}'^{\otimes -2} \oplus \mathscr{L}^{\otimes 2}). \quad (6.1.3)$$

Because $n > 2d$, there is no non zero sections to of last 2 summands. Thus, any section f to $V(\mathscr{E},\mathscr{L})$ will have the form

$$f = c_0 x^4 + c_1 x^3 y + c_2 x^2 y^2 = x^2(c_0 x^2 + c_1 xy + c_2 y^2),$$

where c_0, c_1, c_2 are sections of the first three summands in (6.1.3). Observe that

$$c_1^2 - 4c_0 c_2 \in H^0(C, \mathscr{L}'^{\otimes 2} \otimes \mathscr{L}^{\otimes 4})$$

necessarily vanishes somewhere, and at that point, f is of type $(2,2)$, which is not in the regular part. Thus the subset of $\mathscr{M}_{\mathscr{L}}(k)$ with $n > 2d$ is empty, and the contribution to the average is precisely 0.

Case 2: $n = 2d$. If $\mathscr{L}'^{-1} \otimes \mathscr{L}^{\otimes 2}$ is not trivial, then since $\deg \mathscr{L}'^{-1} \otimes \mathscr{L}^{\otimes 2} = 0$, we have $H^0(C, \mathscr{L}'^{-1} \otimes \mathscr{L}^{\otimes 2}) = 0$. Thus, similar to the first case, there is no regular section. Hence, we need only to consider the case where $\mathscr{L}' \cong \mathscr{L}^{\otimes 2}$. In this case, when d is sufficiently large, then $\mathscr{F} \cong \mathscr{L} \oplus \mathscr{O}$, and hence, $V(\mathscr{E},\mathscr{L}) \cong \mathscr{L}^{\otimes 6} \oplus \mathscr{L}^{\otimes 4} \oplus \mathscr{L}^{\otimes 2} \oplus \mathscr{O}_C \oplus \mathscr{L}^{\otimes -2}$. Therefore, any section f to $V(\mathscr{E},\mathscr{L})^{\mathrm{reg}}$ must have the form $(c_0, c_1, c_2, c_3, 0)$ with $c_3 \neq 0$, or in a different notation

$$f = c_0 x^4 + c_1 x^3 y + c_2 x^2 y^2 + c_3 x y^3,$$

since $H^0(C, \mathscr{L}^{\otimes -2}) = 0$. But now, we can bring this section to the form $y(x^3 + axy^2 + by^3)$ via the automorphism

$$\begin{pmatrix} 1 & 0 \\ -c_2/3 & 1 \end{pmatrix} \begin{pmatrix} c_3^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad c_3 \neq 0.$$

We have thus shown that all regular sections in this case actually factor through the Weierstrass section. Thus, the contribution to the average of this case is precisely 1.

Case 3: $d < n < 2d$. As above, where d is sufficiently large, the exact sequence (6.1.1) splits, and we have $\mathscr{F} \cong \mathscr{L}' \oplus \mathscr{O}$. This also splits $V(\mathscr{E},\mathscr{L})$ into a direct sum of $\mathscr{L}'^{\otimes(2-i)} \oplus \mathscr{L}^{\otimes 2}$ as in (6.1.3). Using (6.1.2) and Riemann-Roch for the first three summands, we see that the mass of $\mathscr{M}_{\mathscr{L}}$ in this range is majorized by

$$\sum_{n=d+1}^{2d-1} \sum_{\deg \mathscr{L}'=n} \frac{q^{6d+3n+3(1-g)} |H^0(C, \mathscr{L}'^{-1} \otimes \mathscr{L}^{\otimes 2})|}{(q-1)q^{n+1-g}}$$

$$
\begin{aligned}
&= \sum_{n=d+1}^{2d-1} \frac{q^{6d+2n+2(1-g)} |\mathrm{Sym}_C^{2d-n}(\mathbb{F}_q)|}{q-1} \\
&\leq \sum_{n=d+1}^{2d-1} \frac{T q^{8d+n+2(1-g)}}{q-1} && \text{(where } T \text{ is some constant)} \\
&= \frac{T q^{8d+2(1-g)}}{q-1} \sum_{n=d+1}^{2d-1} q^n \\
&\leq \frac{T q^{10d+2(1-g)}}{q-1} \frac{1}{q-1}.
\end{aligned}
$$

Thus, the contribution to the average is bounded above by

$$\frac{T q^{10d+2(1-g)}}{(q-1)^2 q^{10d+2(1-g)}} = \frac{T}{(q-1)^2}.$$

We also note that the implied constant T only depends on the genus of C.

Case 4: $d-g-1 \leq n \leq d$. Similar to the above, when d is sufficiently large, $\mathscr{F} \cong \mathscr{L}' \oplus \mathscr{O}_C$, which induces a splitting of the filtration on $V(\mathscr{E}, \mathscr{L})$. We then see that

$$\dim H^0(C, V(\mathscr{E}, \mathscr{L})) = \sum_{i=0}^{4} \dim H^0(C, \mathscr{L}'^{\otimes(2-1)} \otimes \mathscr{L}^{\otimes 2}) \leq 10d+5.$$

Thus, if we let $A = |\mathrm{Pic}^0_{C/\mathbb{F}_q}(\mathbb{F}_q)| = |\mathrm{Pic}^i_{C/\mathbb{F}_q}(\mathbb{F}_q)|, \forall i$ (they are all equal since we assume that C has an $\mathbb{F}_q$-rational point), then the mass of $\mathscr{M}_{\mathscr{L}}$ in this range is majorized by

$$\sum_{n=d-g-1}^{d} \frac{A q^{10d+5}}{(q-1)q^{n+1-g}} = \frac{A q^{10d+5}}{(q-1)q^{1-g}} \sum_{n=d-g-1}^{d} \frac{1}{q^n}.$$

The contribution to the average is therefore

$$\frac{1}{q^{10d+2(1-g)}} \frac{A q^{10d+5}}{(q-1)q^{n+1-g}} \sum_{n=d-g-1}^{d} \frac{1}{q^n} = \frac{A q^{2+3g}}{q-1} \sum_{n=d-g-1}^{d} \frac{1}{q^n}.$$

But this goes to 0 as d goes to infinity, which means that there is no contribution to the average from this case.

Case 5: $0 < n < d - g - 1$ or $\mathscr{F}$ is semi-stable. By Riemann-Roch, we see that when d is large enough,

$$\dim H^0(C, V(\mathscr{E}, \mathscr{L})) = \sum_{i=0}^{4} \dim H^0(C, \mathscr{L}'^{\otimes(2-i)} \otimes \mathscr{L}^{\otimes 2}) = 10d + 5(1-g).$$

Thus, when $0 < n < d - g - 1$ or $\mathscr{F}$ is semi-stable, we always have

$$|H^0(C, V(\mathscr{E}, \mathscr{L}))| = q^{10d+5(1-g)}.$$

To complete the computation in this case, we need one extra ingredient.

Proposition 6.1.4. *We have,*

$$|\mathrm{Bun}_G(\mathbb{F}_q)| = 2q^{3(g-1)}\zeta_C(2).$$

Proof. This comes from the fact that the Tamagawa number of G is 2. □

The contribution of this part to the average can now be computed as follows (here, the measure on $\mathrm{Bun}_G(\mathbb{F}_q)$ is just the counting measure, weighted by the sizes of the automorphism groups):

$$\begin{aligned}
&\lim_{d\to\infty} \frac{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}})| d\mu}{|H^0(C, S \times^{\mathbb{G}_m} \mathscr{L})|} \\
&= \lim_{d\to\infty} \frac{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}}) \, d\mu}{|H^0(C, \mathscr{L}^{\otimes 4})||H^0(C, \mathscr{L}^{\otimes 6})|} \\
&= \lim_{d\to\infty} \frac{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}})| \, d\mu}{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L}))| \, d\mu} \frac{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L}))| \, d\mu}{q^{10d+2(1-g)}} \\
&= \lim_{d\to\infty} \frac{\displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} |H^0(C, V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}})| \, d\mu}{|\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)||H^0(C, V(\mathscr{E}, \mathscr{L}))|} \frac{|\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)||H^0(C, V(\mathscr{E}, \mathscr{L}))|}{q^{10d+2(1-g)}} \\
&= \lim_{d\to\infty} \frac{q^{10d+5(1-g)} \displaystyle\int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} \frac{|H^0(C, V(\mathscr{E}, \mathscr{L})^{\mathrm{reg}})|}{|H^0(C, V(\mathscr{E}, \mathscr{L}))|} \, d\mu}{q^{10d+2(1-g)}}
\end{aligned}$$

$$= \lim_{d\to\infty} q^{3(1-g)} \int_{\mathrm{Bun}_G^{<d-g-1}(\mathbb{F}_q)} \zeta_C(2)^{-1}\, d\mu \tag{6.1.5}$$

$$= |\mathrm{Bun}_G(\mathbb{F}_q)| q^{3(1-g)} \zeta_C(2)^{-1}$$

$$= 2q^{3(g-1)}\zeta_C(2) q^{3(1-g)} \zeta_C(2)^{-1} \tag{6.1.6}$$

$$= 2.$$

The equality at (6.1.5) is due to the dominated convergent theorem, the fact that the integrand is bounded by 1, and the actual value of the limit given by proposition 5.2.1. The equality at (6.1.6) is due to proposition 6.1.4.

Altogether, we have

$$\limsup_{d\to\infty} \frac{|\mathscr{M}_{\mathscr{L}}(k)|}{|\mathscr{A}_{\mathscr{L}}(k)|} \leq 3 + \frac{T}{(q-1)^2}.$$

6.2 The case $E[2](C)$ is non-trivial

We have estimated the average number of I-torsors. Proposition 4.3.5 shows that we have a weaker link between the number of I-torsors and the size of the 2-Selmer groups when $E[2](C)$ is non-trivial. This subsection shows that the stronger inequality dominates our estimate of the average size of the 2-Selmer groups. In other words, we will show that the contribution from the case where $E[2](C)$ is non-trivial is 0.

When $E[2](C)$ is non-trivial, where E is given by $(\mathscr{L}, a, b)$, then we see that $x^3 + axz^2 + bz^3$ can be written in the form $(x + cz)(x^2 - cxz + vz^2)$, where $c \in H^0(C, \mathscr{L}^{\otimes 2})$ and $v \in H^0(C, \mathscr{L}^{\otimes 4})$. In other words, (a, b) is in the image of

$$H^0(C, \mathscr{L}^{\otimes 2}) \times H^0(C, \mathscr{L}^{\otimes 4}) \to H^0(C, \mathscr{L}^{\otimes 4}) \times H^0(C, \mathscr{L}^{\otimes 6})$$
$$(c, v) \mapsto (v - c^2, cv).$$

When $d = \deg \mathscr{L}$ is sufficiently large, then we can use Riemann-Roch to compute the size of all the spaces involved and see that the number of all such pairs (a, b) is bounded by $q^{6d+2(1-g)}$.

We know that the number of points on C, where the fiber of E fails to be smooth is bounded by $\deg \Delta(a, b) = 10d$. Let C' be the complement of these points in C, then from an argument similar to that of proposition 4.3.5, we know that $|\mathrm{Sel}_2(E_{k(C)})| \leq |H^1(C', E[2])|$. Observe that we have the following map

$$H^1(C', E[2]) \to \{\text{tame étale covers of } C' \text{ of degree } 4\},$$

where we know that the image lands in the tame part since the characteristic of our base field is at least 5 and the cover is of degree 4.

Note that the number of topological generators of $\pi_1^{\text{tame}}(C')$ is bounded by $2g + 10d$, since it is the profinite completion of the usual fundamental group of a lifting of C' to $\mathbb{C}$. The right hand side is therefore bounded by $m4^{10d}$ where m is some constant. Thus, to bound the size of $H^1(C', E[2])$, it suffices to bound the sizes of the fibers of this map.

Suppose T is a degree 4 étale cover of C', then giving T the structure of an $E[2]$-torsor is the same as giving a map $E[2] \times_{C'} T \to T$ compatible with the structure maps to C' satisfying certain properties. Since everything involved is proper and flat over C', a map $E[2] \times_{C'} T \to T$ is determined uniquely by $(E[2] \times_{C'} T)_{k(C)} \to T_{k(C)}$, compatible with the structure maps to $\operatorname{Spec} k(C)$. Since everything here is étale over $k(C)$, both sides they are in fact products of field extensions of $k(C)$. But now, we see at once that the number of such maps is bounded by the product of the dimension of both sides (as $k(C)$-vector spaces), which is $m' = 16 \times 4$.

The contribution of this case to the average is therefore bounded above by

$$\frac{mm'q^{6d+2(1-g)}4^{10d}}{q^{10d+2(1-g)}} = \frac{m''4^{10d}}{q^{4d}}.$$

This goes to zero as d goes to infinity if $q^4 > 4^{10}$ or equivalently, when $q > 32$. This is the only source of restriction on the size of our base field.

6.3 The average in the transversal case

We will show that the average in this case is precisely 3, which is the content of theorem 2.2.5. The main observation is that we can completely ignore the range $d < n < 2d$.

Lemma 6.3.1. *When $d < n < 2d$, for all $s \in \Gamma(C, V(\mathscr{E}, \mathscr{L}))$, $\Delta(s) \in \Gamma(C, \mathscr{L}^{\otimes 12})$ is not square-free (i.e. not transversal).*

Proof. As before, when d is sufficiently large, F splits, which induces a splitting of $V(\mathscr{E}, \mathscr{L})$,

$$V(\mathscr{E}, \mathscr{L}) \cong (\mathscr{L}^{\otimes 2} \otimes \mathscr{L}'^{\otimes 2}) \oplus (\mathscr{L}^{\otimes 2} \otimes \mathscr{L}') \oplus \mathscr{L}^{\otimes 2} \oplus (\mathscr{L}^{\otimes 2} \otimes \mathscr{L}'^{\otimes -1}) \oplus (\mathscr{L}^{\otimes 2} \otimes \mathscr{L}'^{\otimes -2}).$$

And hence, we can write $s = (c_0, c_1, c_2, c_3, c_4)$ where each "coordinate" is a section of the line bundles in the summand above, in the same order. Clearly, $c_4 = 0$ since $\deg \mathscr{L}^{\otimes 2} \otimes \mathscr{L}'^{\otimes -2} < 0$. Moreover, since $\deg \mathscr{L}^{\otimes 2} \otimes \mathscr{L}'^{-1} > 0$, there exists a point $v \in |C|$ such that c_3 vanishes.

But now, at v, the discriminant is

$$\Delta = -27c_0^2c_3^4 + 18c_0c_1c_2c_3^3 - 4c_0c_2^3c_3^2 - 4c_1^3c_3^3 + c_1^2c_2^2c_3^2,$$

which vanishes to order at least 2. □

The result then follows from the computation in subsection 6.1. Indeed, we can ignore case 3 due to lemma 6.3.1, and use the density computation in propositions 5.2.2 and 5.2.3 (instead of proposition 5.2.1) in case 5. Note also that the Weierstrass curves we are counting over are automatically minimal, by the transversality condition.

6.4 The average size of 2-Selmer groups

We will now present the proof of theorem 2.2.2. We have,

$$\begin{aligned}
&\limsup_{\deg \mathscr{L}\to\infty} \frac{\sum_{\mathscr{L}(E)\cong\mathscr{L}} |\mathrm{Sel}_2(E_K)|}{|H^0(C,\mathscr{L}^{\otimes 4}\oplus\mathscr{L}^{\otimes 6})|} \\
&= \limsup_{\deg \mathscr{L}\to\infty} \frac{\sum_{\substack{\mathscr{L}(E)\cong\mathscr{L}\\ E[2](C)=\{0\}}} |\mathrm{Sel}_2(E_K)| + \sum_{\substack{\mathscr{L}(E)\cong\mathscr{L}\\ E[2](C)\neq\{0\}}} |\mathrm{Sel}_2(E_K)|}{|\mathscr{A}_{\mathscr{L}}(k)|} \\
&\leq \limsup_{\deg \mathscr{L}\to\infty} \frac{|\mathscr{M}_{\mathscr{L}}(k)| + \frac{3}{4}\sum_{\substack{\mathscr{L}(E)\cong\mathscr{L}\\ E[2](C)\neq\{0\}}} |\mathrm{Sel}_2(E_K)|}{|\mathscr{A}_{\mathscr{L}}(k)|} && \text{(by proposition 4.3.5)} \\
&= \limsup_{\mathscr{L}\to\infty} \frac{|\mathscr{M}_{\mathscr{L}}(k)|}{|\mathscr{A}_{\mathscr{L}}(k)|} && \text{(by subsection 6.2)} \\
&\leq 3 + \frac{T}{(q-1)^2}. && \text{(by subsection 6.1)}
\end{aligned}$$

Theorem 2.2.2 then follows from this computation and the following remarks:

(i) We can exclude the Weierstrass curves E such that $\Delta E = 0$, because [Poo03, lemma 4.1] shows that their contribution is 0.

(ii) To impose minimality condition of E on the count, we use propositions 5.2.5 and 5.2.6 in case 5, which still gives us the number 2. For case 3, the estimate picks up at most an extra factor of $\zeta_C(10)$. Other cases are not affected.

(iii) In the count, pairs of the form (a,b) and (c^4a, c^6b) with $c \in k^\times$ give the same isomorphism class. By rewriting, we get the expression in (2.2.1).

For the lower bound, we have,

$$\begin{aligned}
&\liminf_{\deg \mathscr{L}\to\infty} \frac{\sum_{\mathscr{L}(E)\cong\mathscr{L}} |\mathrm{Sel}_2(E_K)|}{|H^0(C,\mathscr{L}^{\otimes 4}\oplus\mathscr{L}^{\otimes 6})|} \\
&\geq \liminf_{\deg \mathscr{L}\to\infty} \frac{\sum_{\substack{E \text{ transversal}\\ \mathscr{L}(E)\cong\mathscr{L}}} |\mathrm{Sel}_2(E_K)|}{|H^0(C,\mathscr{L}^{\otimes 4}\oplus\mathscr{L}^{\otimes 6})|} \\
&= 3\zeta_C(10)^{-1} && \text{(from theorem 2.2.5 and proposition 5.2.2.)}
\end{aligned}$$

The same remarks as above apply, and we conclude the proof of theorem 2.2.2.

References

[BS10a] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, arXiv:1006.1002 (June 2010).

[BS10b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, arXiv:1007.0052 (June 2010).

[dJ02] A. J. de Jong, *Counting elliptic surfaces over finite fields*, jour Mosc. Math.~J. **2** (2002), no. 2, 281–311.

[Jac13] Jack Thorne, *Vinberg's representations and arithmetic invariant theory*, Ph.D. Thesis, 2013.

[Liu06] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford; New York, 2006.

[Mil80] J. S Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[Mir81] Rick Miranda, *The moduli of Weierstrass fibration over* $\mathbb{P}^1$, Mathematische Annalen **255** (1981), 379–394.

[Poo03] Bjorn Poonen, *Squarefree values of multivariable polynomials*, Duke Mathematical Journal **118** (June 2003), no. 2, 353–373.

[SM70] Kalevi Suominen and David Mumford, *Introduction to the theory of moduli*, Algebraic geometry: Proceedings of the fifth nordic summer school in mathematics, 1970, pp. 171–222.

[Ulm02] Douglas Ulmer, *Elliptic curves with large rank over function fields*, Annals of Mathematics **155** (January 2002), no. 1, 295.

[Wei54] André Weil, *Remarques sur un mémoire d'Hermite*, Archiv der Mathematik (1954).

[Zha13] Yongqiang Zhao, *On sieve methods for varieties over finite fields*, Ph.D. Thesis, University of Wisconsin, 2013.