The Average Size of 2-Selmer Groups of Elliptic Curves in Characteristic 2

Niven Achenjang*

October 2, 2023

Abstract

Let K be the function field of a smooth curve B over a finite field k of arbitrary characteristic. We prove that the average size of the 2-Selmer groups of elliptic curves E/K is at most $1 + 2\zeta_B(2)\zeta_B(10)$, where ζ_B is the zeta function of the curve B/k. In particular, in the limit as $q = \#k \to \infty$ (with the genus $g(B)$ fixed), we see that the average size of 2-Selmer is bounded above by 3, even in "bad" characteristics. Along the way, we also produce new bounds on 2-Selmer groups of elliptic curves over characteristic 2 global function fields.

Contents

*MIT, nivent@mit.edu

1 Introduction

Much recent work in arithmetic statistics has been centered around the question of understanding the distribution of ranks of elliptic curves over a fixed global field K. In particular, one would like to understand the average value of the rank of elliptic curves E/K, when they are ordered by height. While some early work in this direction (e.g. [Bru92, Gol79]) employed analytic techniques, since the papers [dJ02, BS15] of de Jong and Bhargava-Shankar, it has become much more common to tackle this question by first choosing a value of n and then bounding the average size of n-Selmer groups of the elliptic curves E/K. De Jong [dJ02] does this for $n = 3$ and $K = \mathbb{F}_q(t)$, for any q, while Bhargava and Shankar [BS15] do this for $n = 2$ and $K = \mathbb{Q}$. Recall that, for an elliptic curve E over a global field K, its `n-Selmer group` is

$$\mathrm{Sel}_n(E) := \ker\left(\mathrm{H}^1(K, E[n]) \longrightarrow \prod_v \mathrm{H}^1(K_v, E)\right),$$

where v ranges over all places of K. This group fits into a short exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{Sel}_n(E) \longrightarrow Ш(E)[n] \longrightarrow 0, \tag{1.1}$$

where $Ш(E)[n]$ denotes the n-torsion in the Shafarevich-Tate group of E, and so provides an upper bound on $\mathrm{rank}_{\mathbb{Z}}\, E(K)$. The main conjecture concerning statistics of Selmer groups relevant to our paper is the following.

Conjecture A. *Let K be a global field. When all elliptic curves E/K are ordered by height, the average size of their n-Selmer groups is $\sum_{d|n} d$.*

Conjecture A (or variations of it) has appeared in many places in the literature, see e.g. [dJ02, Section 2], [PR12, Conjecture 1.4], [BS13, Conjecture 4], and [BKL+15, Section 5.7]. One can see [Lan21b, Remark 1.4] for a summary of a few different heuristics leading to Conjecture A. Furthermore, Conjecture A (or variations of it) has been verified in a number of situations. A non-exhaustive list of papers verifying cases of variations of Conjecture A includes [dJ02, BS15, Sha13, BS13, HLHN14, Tho19, Lan21b, FLR23, PW23]. However, to the best of the author's knowledge, there is not a single paper which investigates Conjecture A for an arbitrary global function field K (and fixed n). Usually authors will at least require that $\mathrm{char}\, K \nmid 2n$ and/or that K be of the form $\mathbb{F}_q(t)$. In this paper, we study the average size of 2-Selmer groups of elliptic curves over an *arbitrary* global function field K. Note that Conjecture A predicts that this average size should be $3 = 1 + 2$. Our main result (Theorem B) is to produce an upper bound for this average size which tends to 3 as "$q \to \infty$." In characteristics ≥ 5 (with mild additional assumptions), such an upper bound was obtained already in [HLHN14], so one of the main novelties of our paper is that it works even in bad characteristics.

Before stating our main theorem, we briefly introduce some notation.

Setup 1.1. Let $k = \mathbb{F}_q$ be a finite field, let B/k be a smooth k-curve of genus $g = g(B)$, and let $K = k(B)$ be its function field. Let

$$\zeta_B(s) = \prod_{v \in B} \frac{1}{1 - q^{-s \deg v}},$$

with v ranging over *closed* points of B, be the zeta function of B.

Throughout most sections of this paper, we will work in the context of Setup 1.1. In this context, given a nonnegative integer d, we set

$$\mathrm{AS}_B(d) := \frac{\displaystyle\sum_{\substack{E/K \\ \mathrm{ht}(E) \leq d}} \frac{\#\,\mathrm{Sel}_2(E)}{\#\,\mathrm{Aut}(E)}}{\displaystyle\sum_{\substack{E/K \\ \mathrm{ht}(E) \leq d}} \frac{1}{\#\,\mathrm{Aut}(E)}} \quad \text{and} \quad \mathrm{AR}_B(d) := \frac{\displaystyle\sum_{\substack{E/K \\ \mathrm{ht}(E) \leq d}} \frac{\mathrm{rank}_{\mathbb{Z}}\, E(K)}{\#\,\mathrm{Aut}(E)}}{\displaystyle\sum_{\substack{E/K \\ \mathrm{ht}(E) \leq d}} \frac{1}{\#\,\mathrm{Aut}(E)}}. \tag{1.2}$$

Above, $\mathrm{AS}_B(d)$ is the (weighted) average size of 2-Selmer groups of elliptic curves over K of height at most d, and $\mathrm{AR}_B(d)$ is the (weighted) average size of their ranks. See Section 2 for the definition of height.

Theorem B (= Theorem 7.2.7)**.** *With notation as in Setup 1.1,*

$$\limsup_{d \to \infty} \mathrm{AS}_B(d) \leq 1 + 2\zeta_B(2)\zeta_B(10).$$

Thus, if we let $\#k$ go to infinity as well, then

$$\limsup_{n \to \infty} \limsup_{d \to \infty} \mathrm{AS}_{B_{\mathbb{F}_{q^n}}}(d) \leq 3.$$

As a corollary to Theorem B, using the simple fact that $2x \leq 2^x$ along with (1.1), we obtain the following.

Corollary C. *With notation as in Setup 1.1, we have*

$$\limsup_{d \to \infty} \mathrm{AR}_B(d) \leq \frac{1}{2} + \zeta_B(2)\zeta_B(10)$$

Along the road towards establishing Theorem B, we obtain a few other results which may be of independent interest. Some of these are collected below.

Theorem D. *With notation as in Setup 1.1,*

$$\sum_{\substack{E/K \\ \mathrm{ht}(E) = d}} \frac{1}{\#\,\mathrm{Aut}(E)} \sim \#\,\mathrm{Pic}^0(B) \cdot \frac{q^{10d + 2(1-g)}}{(q-1)\zeta_B(10)}$$

as $d \to \infty$. See Theorem 3.4.4 for a more precise asymptotic.

Remark 1.2. When $B = \mathbb{P}^1_{\mathbb{F}_q}$, de Jong [dJ02] gave an *exact* weighted count of (isomorphism classes) of elliptic curves of height d (his result is recalled in Remark 3.4.3), so the utility of Theorem D is that it applies to more general bases. Prior to de Jong, Brumer [Bru92] computed an asymptotic count of the (unweighted) number of elliptic curves over $K = \mathbb{F}_q(t)$ (using a slightly different height function) when $\operatorname{char} K \geq 5$. ◦

Theorem E (= Theorem 7.1.2 + Theorem 7.1.4)**.** *Use notation as in Setup 1.1. Then,*

$$\sum_{\substack{E/K \\ \mathrm{ht}(E)=d \\ E[2](K)\neq 0}} \frac{1}{\#\operatorname{Aut}(E)} = O\big(q^{Cd}\big) \quad \text{where } C = \begin{cases} 6 & \text{if } \operatorname{char} K \neq 2 \\ 9 & \text{if } \operatorname{char} K = 2 \end{cases}$$

as $d \to \infty$.

Theorem F. *Use notation as in Setup 1.1. Assume* $\operatorname{char} K \neq 3$. *Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) = O\bigg(\frac{\deg N(E)}{\log \deg N(E)}\bigg) \leq O\bigg(\frac{\mathrm{ht}(E)}{\log \mathrm{ht}(E)}\bigg)$$

as $\deg N(E) \to \infty$, where $N(E)$ denotes the conductor of E. See Theorem 6.3.4 for explicit bounds.

Remark 1.3. We expect that Theorem F holds even when $\operatorname{char} K = 3$. However, when $\operatorname{char} K = 3$, we were only able to prove such a bound under the additional assumption that $E[2](K) \neq 0$. ◦

Remark 1.4. Use notation as in Setup 1.1. For an elliptic curve E/K, let $N(E) \in \operatorname{Div}(B)$ denote its conductor. Brumer [Bru92, Proposition 6.9] has already shown that, if $\operatorname{char} K \geq 5$, one has

$$\operatorname{rank}_{\mathbb{Z}} E(K) = O\bigg(\frac{\deg N(E)}{\log \deg N(E)}\bigg).$$

He proved this via analytic means, bounding the analytic rank of E via "Weil's explicit formula". In contrast, Theorem F gives an algebraic proof of a bound of this form with the larger quantity $\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E)$ in place of $\operatorname{rank}_{\mathbb{Z}} E(K)$ and which applies also in characteristic 2. However, Brumer's bound has a smaller coefficient on the main term than the ones appearing in Theorem 6.3.4. ◦

Brief Comparison with [HLHN14] We briefly explicitly state the difference between our Theorem B and the main theorem of [HLHN14], stated below.

Theorem G ([HLHN14, Corollary 2.2.3])**.** *Use notation as in Setup 1.1, and assume that* $\operatorname{char} K \geq 5$. *If $q > 64$, then*

$$3\zeta_B(10)^{-1} \leq \limsup_{d\to\infty} \mathrm{AS}_B(d) \leq 3 + \frac{T}{q-1}$$

for some constant $T = T(g)$ depending only on the genus of B.

Our statement of Theorem G above differs slightly from the statement of [HLHN14, Corollary 2.2.3]; we will explain this difference at the end of this brief comparison, in Warning 1.6.

Our Theorem B shows that one can still bound $\limsup_{d\to\infty} \mathrm{AS}_B(d)$ by a quantity of the form $3 + o(1)$ (with the $o(1)$ going to 0 and $q \to \infty$) even when $\operatorname{char} K$ (or $\#k$) is small. However, it produces a different $o(1)$ term than the one appearing in Theorem G. Furthermore, we do not obtain an analogous lower bound.

Remark 1.5. We further remark that it is possible to slightly strengthen Theorem G by replacing parts of [HLHN14] with results from our paper. The requirement $q > 64$ in Theorem G only exists because this is needed in their argument for showing that that elliptic curves with non-trivial 2-torsion do not contribute to the average size of 2-Selmer. However, our Proposition 7.2.4 proves this even for small q, and so shows that Theorem G remains valid for all K of characteristic ≥ 5. ◦

Warning 1.6. In [HLHN14], the authors claim that their main result only requires $q > 32$ (instead of $q > 64$) and that they obtain an upper bound of the form $3 + T/(q-1)^2$ (instead of $3 + T/(q-1)$). The parts of their paper where this '32' and '$T/(q-1)^2$' originate appear to contain minor errors.

- This restriction on the size of the base field originates in [HLHN14, Section 6.2]. At one point the authors write that the degree of the discriminant divisor of a height d elliptic curve is $10d$, whereas it should really be $12d$. Redoing the computations at the end of that section with this in mind shows that they need $q^4 > 4^{12}$ (i.e. $q > 64$) in order to rule out the contribution coming from elliptic curves with non-trivial 2-torsion.

- The summand $T/(q-1)^2$ originates in [HLHN14, Case 3 in Section 6.1]. Use notation as in Setup 1.1 (so B for us will be C for them). Following [HLHN14], write $\mathrm{Sym}^m_B(\mathbb{F}_q)$ for the set of effective, degree m divisors on B. In the first series of displayed equations/inequalities appearing there, the authors implicitly appeal to
$$\sum_{\mathscr{M} \in \mathrm{Pic}^{2d-n}(B)} \# \mathrm{H}^0(B, \mathscr{M}) = \# \mathrm{Sym}^{2d-n}_B(\mathbb{F}_q),$$
whereas the correct identity is
$$\sum_{\mathscr{M} \in \mathrm{Pic}^{2d-n}(B)} \frac{\# \mathrm{H}^0(B, \mathscr{M}) - 1}{q-1} = \# \mathrm{Sym}^{2d-n}_B(\mathbb{F}_q).$$
Redoing [HLHN14, Case 3 in Section 6] using this identity instead results in an upper bound of the form $T/(q-1)$. •

Proof Strategy and Organization The proof of Theorem B, broadly speaking, follows the usual "parameterize and count" strategy often employed in arithmetic statistics, with extra complications arising from allowing "bad" characteristics. One of the main tasks in implementing this strategy is finding suitable geometric representatives for 2-Selmer elements. When $\mathrm{char}\, K \neq 2$, one most often parameterizes 2-Selmer elements using binary quartic forms $f(x,z)$ (or families of them over B). However, when $\mathrm{char}\, K = 2$, these objects no longer parameterize 2-Selmer elements. In their place, we will parameterize our 2-Selmer elements using suitable curves over B (locally cut out by equations of the form $y^2 + h(x,z)y = f(x,z)$ with h, f homogeneous of degrees $2, 4$, respectively), which are analogous to the curves $y^2 = f(x,z)$ implicit in the usual use of binary quartic forms. With that said, a decent chunk of our paper (Sections 4 and 5) is devoted to setting up these curves and their basic properties ahead of performing the actual "count" in Section 5.3.

In Section 2 we lay out common conventions and notation used throughout the paper. In Section 3, we obtain an asymptotic count of elliptic curves (ordered by height) over an arbitrary global function field (Theorem 3.4.4), i.e. we estimate the denominator of (1.2). In Section 4, we define the objects – in this paper, dubbed 'hyper-Weierstrass curves' (see Definition 4.1.2) – which will serve as our integral models of 2-Selmer elements. In the same section, we make explicit their relation to 2-Selmer groups of elliptic curves via the introduction of a '2-Selmer groupoid' (see Definition 4.2.1). This groupoid is used to define a modified average count $\mathrm{MAS}_B(d)$ which is closely related, but not exactly equal, to $\mathrm{AS}_B(d)$. In Section 5, we implement the "count" part of the "parameterize and count" strategy, obtaining the desired upper bound on the modified average $\limsup_{d\to\infty} \mathrm{MAS}_B(d)$ defined in terms of the 2-Selmer groupoid (see Theorem 5.3.15). After that, all that remains is to compare $\limsup_{d\to\infty} \mathrm{MAS}_B(d)$ and $\limsup_{d\to\infty} \mathrm{AS}_B(d)$. For fixed finite d, $\mathrm{MAS}_B(d)$ and $\mathrm{AS}_B(d)$ differ only in their contributions coming from elliptic curves with extra automorphisms or with non-trivial 2-torsion. Curves with extra automorphisms contribute *more* to $\mathrm{MAS}_B(d)$ than they do to $\mathrm{AS}_B(d)$, while curves with non-trivial 2-torsion contribute *less* to $\mathrm{MAS}_B(d)$ than they do to $\mathrm{AS}_B(d)$. Hence, to prove the upper bound $\limsup_{d\to\infty} \mathrm{AS}_B(d) \leq \limsup_{d\to\infty} \mathrm{MAS}_B(d)$, it suffices to show that curves with non-trivial 2-torsion *do not contribute* to these averages. Towards this end, in Section 6, we produce upper bounds on the size of the 2-Selmer group of an elliptic curve E/K of height d (see Theorem 6.3.4). In Section 7, this is combined with a count of the number of elliptic curves with non-trivial 2-torsion (see Theorems 7.1.2 and 7.1.4) in order to prove that $\limsup_{d\to\infty} \mathrm{AS}_B(d) \le \limsup_{d\to\infty} \mathrm{MAS}_B(d)$, and so deduce our main result (Theorem 7.2.7).

Remark 1.7. We remark that Section 6, in which we prove Theorem F, is logically independent of the sections preceding it, and so can be read independently of the rest of the paper. ∘

Acknowledgements I would like to extend immense gratitude towards Bjorn Poonen for suggesting this project and for providing much helpful guidance throughout its duration. I would also like to thank Aise Johan de Jong for answering questions about his paper [dJ02] and to thank Aaron Landesman for suggesting the use of hypercohomology in Proposition 6.2.5. In addition, I thank Levent Alpöge, Armand Brumer, and Douglas Ulmer for helpful conversations/email exchanges. Finally, over the course of completing this project, I was supported at various points by MIT's Dean of Science Fellowship as well as by National Science Foundation grants DGE-2141064, DMS-1601946 and DMS-2101040.

2 Conventions

In this paper, we work throughout in the fppf topology. All unadorned cohomology groups should be interpreted as fppf cohomology. For G a sheaf of groups, we say `G-torsor` to mean an fppf-locally trivial right G-torsor sheaf.

Vector bundles Let $\mathscr{V}$ be a vector bundle (by which, we mean locally free sheaf of finite rank) on a scheme B. We write $\mathscr{V}^\vee := \mathscr{H}om(\mathscr{V}, \mathscr{O}_B)$ for the dual bundle. If $\mathscr{L}$ is a line bundle, we also denote this by $\mathscr{L}^{-1} := \mathscr{L}^\vee$.

If $\mathscr{V}$ is a vector bundle on a scheme B, we write $\mathrm{GL}(\mathscr{V})$ to denote its group of $\mathscr{O}_B$-linear automorphisms. We write $\underline{\mathrm{GL}}(\mathscr{V})$ to denote its automorphism sheaf, i.e., for U a B-scheme, we set $\Gamma(U/B, \underline{\mathrm{GL}}(\mathscr{V})) = \mathrm{GL}(\mathscr{V}|_U)$.

Finally, for $\mathscr{V}$ a vector bundle on a scheme B, its associated projective bundle is $\mathbb{P}(\mathscr{V}) := \mathbf{Proj}_B(\mathrm{Sym}(\mathscr{V}))$.

Duality Let $f : X \to Y$ be a morphism of schemes. The dualizing sheaf, when it exists, of this morphism will be denoted $\omega_{X/Y}$. If $Y = \operatorname{Spec} F$ is the spectrum of a field, then we often simply denote this by $\omega_X := \omega_{X/F} := \omega_{X/\operatorname{Spec} F}$.

Curves Let B be an arbitrary scheme. We say that a B-scheme $C \to B$ is a `B-curve` (or `curve over B` or simply a `curve`) if it is flat, proper, and finitely presented over B with Gorenstein, connected, 1-dimensional geometric fibers. Note that, for $C \to B$ a curve, the dualizing sheaf $\omega_{C/B}$ exists and is invertible.

If E_1, E_2 are elliptic curves (so, in particular, they are equipped with choices of identity points), then by an isomorphism $E_1 \xrightarrow{\sim} E_2$, we always mean an isomorphism of group schemes.

Heights Let B be a smooth curve over a field F. Let $X \xrightarrow{\pi} B$ be a curve over B such that $\pi_*\mathscr{O}_X = \mathscr{O}_B$ and whose relative dualizing sheaf $\omega_{X/B}$ is isomorphic to $\pi^*\mathscr{L}$ for some $\mathscr{L} \in \mathrm{Pic}(B)$. Then, we define the `height` of X/B to be

$$\mathrm{ht}(X/B) := \deg(\mathscr{L}) = \deg(\pi_*\omega_{X/B}) \in \mathbb{Z},$$

with the latter equality holding by the projection formula. In this situation, we call $\mathscr{L} \simeq \pi_*\omega_{X/B}$ the `Hodge bundle` of the curve.

Let K be a global function field, with corresponding curve B. If C/K is a curve of genus at least 1, then we define its height to be

$$\mathrm{ht}(C/K) := \mathrm{ht}(\mathcal{C}/B),$$

with $\mathcal{C}/B$ the minimal proper regular model of C. In this situation, the Hodge bundle of C is defined to be the Hodge bundle of its minimal proper regular model.

Global Function Fields Let K be the function field of a smooth curve $B/\mathbb{F}_q$. We implicitly identify places v of K with closed points $v \in B$. Given such a place, we let K_v denote the completion of K at v, and we let $\mathscr{O}_v$ denote the valuation ring of K_v, i.e. the completion of the stalk $\mathscr{O}_{B,v}$. We let $\kappa(v)$ denote the residue field at v.

Asymptotics When working within the context of Setup 1.1, we allow our big-O constants to depend on the function field K. That is, when we write $f(x) = O(g(x))$ we mean that there exists some $C = C(K) > 0$ such that $|f(x)| \leq Cg(x)$ for all large values of x.

Groupoids Let $\mathcal{G}$ be a groupoid. We write $|\mathcal{G}|$ to denote the set of isomorphism classes of its objects. Its groupoid cardinality (or simply cardinality) is

$$\#\mathcal{G} := \sum_{x \in |\mathcal{G}|} \frac{1}{\# \operatorname{Aut}_{\mathcal{G}}(x)}.$$

If we say that $\mathcal{G}' \hookrightarrow \mathcal{G}$ is a subgroupoid, we always mean that it is a *full* subgroupoid, i.e. $\operatorname{Aut}_{\mathscr{G}'}(x) = \operatorname{Aut}_{\mathscr{G}}(x)$ for any $x \in \mathcal{G}'$.

3 An Asymptotic Count of Elliptic Curves of Bounded Height

The main result of this section (Theorem 3.4.4) produces an asymptotic count of the number of elliptic curves of bounded height over an arbitrary global function field. For elliptic curves over $\mathbb{F}_q(t)$, for arbitrary q, an exact count was produced already by de Jong [dJ02, Proposition 4.12]. In this section, we adapt his argument to work over a general base curve B instead of just $\mathbb{P}^1$.

For K a global function field, we introduce the following notation.

Notation 3.1. Let $\mathcal{M}_{1,1}(K)$ denote the groupoid of elliptic curves over K. For any $d \geq 0$, we let $\mathcal{M}_{1,1}^{=d}(K), \mathcal{M}_{1,1}^{\leq d}(K) \hookrightarrow \mathcal{M}_{1,1}(K)$ denote, respectively, the (full) subgroupoids consisting of those elliptic curves of height $= d$ and those of height $\leq d$.

In order to count elliptic curves over K, we first briefly recall the main results of the theory of Weierstrass models. We then related the (unweighted) count of minimal Weierstrass equations of to the (weighted) count of elliptic curves, and use this to obtain as asymptotic for the latter.

3.1 Background on Weierstrass Models

Definition 3.1.2. For an arbitrary base scheme B, a Weierstrass curve $(W \xrightarrow{\pi} B, S)$ over B is a curve W/B whose fibers are geometrically integral of arithmetic genus 1, equipped with a section $S \subset W$ of π which is contained in π's smooth locus. ◇

Theorem 3.1.3 (Summary of the theory of Weierstrass curves)**.** *Let B be an arbitrary base scheme, let $(W \xrightarrow{\pi} B, S)$ be a Weierstrass curve, and let $\mathscr{L} := \pi_* \omega_{W/B}$ be its Hodge bundle. Then,* *(1)* $\pi_*\mathscr{O}_W \simeq \mathscr{O}_B$ *and* $R^1\pi_*\mathscr{O}_W \simeq \mathscr{L}^{-1}$ *both hold after arbitrary base change.*

(2) *For any integer* $n \geq 1$*,*

- $\pi_*\mathscr{O}_X(nS)$ *is a locally free sheaf of rank* n *on* B *whose formation commutes with arbitrary base change.*
- $R^1\pi_*\mathscr{O}_X(nS) = 0$*.*

(3) *For* $n \geq 2$*, there are exact sequences*

$$0 \longrightarrow \pi_*\mathscr{O}_W((n-1)S) \longrightarrow \pi_*\mathscr{O}_W(nS) \longrightarrow \mathscr{L}^{-n} \longrightarrow 0. \tag{3.1}$$

Furthermore, $\pi_*\mathscr{O}_W(S) \simeq \mathscr{O}_B$*.*

(4) *The natural map* $\pi^*\pi_*\mathscr{O}_W(3S) \to \mathscr{O}_W(3S)$ *is a surjection, and induces an embedding*

$$W \hookrightarrow \mathbb{P}(\pi_*\mathscr{O}_W(3S)) := \mathbf{Proj}_B(\mathrm{Sym}(\pi_*\mathscr{O}_W(3S)))$$

over B *such that* $\mathscr{O}_W(1) := \mathscr{O}_{\mathbb{P}(\pi_*\mathscr{O}_W(3S))}(1)|_W \simeq \mathscr{O}_W(3S)$*.*

(5) *There is a canonical section* $\Delta \in \mathrm{H}^0(B, \mathscr{L}^{12})$*, called the* ***discriminant*** *of* W*, whose zero scheme is supported exactly on the points with non-smooth fiber.*

Proof. All of this can be found e.g. in [Del75]. Technically, [Del75] only claims that **(4)** holds Zariski locally on the base, but this suffices to conclude the claim as stated above. ■

Remark 3.1.4. In connection with Theorem 3.1.3**(4)** above, we remark that for a vector bundle $\mathscr{V}$ on B (an arbitrary base scheme) with associated projective bundle $\mathbb{P}(\mathscr{V}) \xrightarrow{p} B$, one has

$$p_*\mathscr{O}_{\mathbb{P}(\mathscr{V})}(n) \simeq \mathrm{Sym}^n(\mathscr{V})$$

for any $n \geq 0$ (see [Har77, Proposition II.7.11(a)]. ○

We next attach global equations to Weierstrass curves. It is these equations that we will be able to count most easily. The existence and shape of these equations is well-known, but we include a treatment here because of their importance to the count.

Proposition 3.1.5. *Let* $(W \xrightarrow{\pi} B, S)$ *be a Weierstrass curve with Hodge bundle* $\mathscr{L} := \pi_*\omega_{W/B}$*. Let* $\mathbb{P} := \mathbb{P}(\pi_*\mathscr{O}_W(3S)) \xrightarrow{p} B$*, so there is a natural embedding* $W \hookrightarrow \mathbb{P}$*. Then,* $W \hookrightarrow \mathbb{P}$ *is the zero scheme of some global section of*

$$\mathscr{O}_{\mathbb{P}}(W) \simeq \mathscr{O}_{\mathbb{P}}(3) \otimes p^*(\mathscr{L}^6) = \left(p^*\mathscr{L}^6\right)(3).$$

Hence, we may via $W \hookrightarrow \mathbb{P}$ *as being cut out by some global section of*

$$p_*\mathscr{O}_{\mathbb{P}}(W) \simeq \mathscr{L}^6 \otimes \mathrm{Sym}^3(\pi_*\mathscr{O}_W(3S))\,.$$

Proof. The main content of the above proposition is the computation of the line bundle $\mathscr{O}_{\mathbb{P}}(W)$ on $\mathbb{P}$. Once we know $\mathscr{O}_{\mathbb{P}}(W) \simeq \left(p^*\mathscr{L}^6\right)(3)$, the claimed computation of $p_*\mathscr{O}_{\mathbb{P}}(W)$ follows from the projection formula and Remark 3.1.4.

We will find it more natural to directly compute its dual $\mathscr{O}_{\mathbb{P}}(-W)$ instead. It is classical that, on fibers, $X \hookrightarrow \mathbb{P}$ is cut out by a cubic equation, so the line bundle $\mathscr{O}_{\mathbb{P}}(-W)(3)$ on $\mathbb{P}$ is trivial on each fiber. Thus (e.g. by [Vak23, Proposition 25.1.11]), $\mathscr{O}_{\mathbb{P}}(-W)(3) \simeq p^*p_*\mathscr{O}_{\mathbb{P}}(-W)(3)$. Hence, it will suffice to compute that

$$p_*\mathscr{O}_{\mathbb{P}}(-W)(3) \simeq \mathscr{L}^{-6}.$$

With this in mind, consider the exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}}(-W)(3) \longrightarrow \mathscr{O}_{\mathbb{P}}(3) \longrightarrow \mathscr{O}_W(3) \longrightarrow 0,$$

and push forward along p. Since $\mathscr{O}_W(1) \simeq \mathscr{O}_W(3S)$ by Theorem 3.1.3**(4)**, we obtain the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & p_*\mathscr{O}_{\mathbb{P}}(-W)(3) \arrow[r] & p_*\mathscr{O}_{\mathbb{P}}(3) \arrow[r] \arrow[d, equal, "\text{Remark 3.1.4}"] & p_*\mathscr{O}_W(3) \arrow[r] \arrow[d, equal] & R^1p_*\mathscr{O}_{\mathbb{P}}(-W)(3) \arrow[d, equal] \\ & & \mathrm{Sym}^3(\pi_*\mathscr{O}_W(3S)) & \pi_*\mathscr{O}_W(9S) & 0. \end{tikzcd} \tag{3.2}$$

Above, $R^1p_*\mathscr{O}_{\mathbb{P}}(-W)(3) = 0$ by Theorem A.1 since $\mathscr{O}_{\mathbb{P}}(-W)(3)$ restricts to the trivial bundle on $\mathbb{P}^2$ in each fiber. Observe that the kernel $p_*\mathscr{O}_{\mathbb{P}}(-W)(3)$ above is a line bundle, so it can be computed by taking determinants. By repeated use of Theorem 3.1.3**(3)** to compute $\det(\pi_*\mathscr{O}_W(9S))$ and $\det(\pi_*\mathscr{O}_W(3S))$, it is straightforward to compute that $p_*\mathscr{O}_{\mathbb{P}}(-W)(3) \simeq \mathscr{L}^{-6}$ as desired. ■

Assumption. For the rest of this section, we work within the context of Setup 1.1. In particular, k is a finite field, and B is a smooth k-curve of genus g with function field $K = k(B)$.

Remark 3.1.6. Let E/K be an elliptic curve. Let $\mathcal{C}/B$ denote its minimal proper regular model, and let W/B denote its minimal Weierstrass model. Then, $\mathcal{C}$ and W have isomorphic Hodge bundles. One can deduce this e.g. from [Con05, Theorem 8.1]. In light of Theorem 3.1.3**(5)**, this in particular means that $12\,\mathrm{ht}(E) = \deg \Delta$, where Δ denotes E's minimal discriminant. ∘

Notation 3.1.7. We set $N(g) := \max\{-1, 2g-2\}$. Note that if $\mathscr{L}$ is a line bundle on B of degree $> N(g)$, then $\mathrm{H}^1(B, \mathscr{L}) = 0$ and $\deg \mathscr{L} \geq 0$.

Remark 3.1.8. Say $(W \xrightarrow{\pi} B, S)$ is a Weierstrass curve with Hodge bundle $\mathscr{L} := \pi_*\omega_{W/B}$ of degree $d > N(g)$. Then, the exact sequences (see Theorem 3.1.3**(3)**)

$$0 \longrightarrow \mathscr{O}_B \longrightarrow \pi_*\mathscr{O}_W(2S) \longrightarrow \mathscr{L}^{-2} \longrightarrow 0 \ \text{ and } \ 0 \longrightarrow \pi_*\mathscr{O}_W(2S) \longrightarrow \pi_*\mathscr{O}_W(3S) \longrightarrow \mathscr{L}^{-3} \longrightarrow 0$$

both split since they represent elements of

$$\mathrm{Ext}^1_{\mathscr{O}_B}(\mathscr{L}^{-2}, \mathscr{O}_B) \simeq \mathrm{Ext}^1_{\mathscr{O}_B}(\mathscr{O}_B, \mathscr{L}^2) \simeq \mathrm{H}^1(\mathscr{L}^2) = 0 \ \text{ and } \ \mathrm{Ext}^1(\mathscr{L}^{-3}, \pi_*\mathscr{O}_W(2S)) \simeq \mathrm{H}^1(\mathscr{L}^3) \oplus \mathrm{H}^1(\mathscr{L}) = 0,$$

respectively. In particular, $\pi_*\mathscr{O}_W(3S) \simeq \mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3}$. In this case, Proposition 3.1.5 tells us that $W \hookrightarrow \mathbb{P}$ is given as the zero scheme of some global section of

$$\begin{aligned} p_*\mathscr{O}_{\mathbb{P}}(W) &\simeq p_*\mathscr{O}_{\mathbb{P}}(3) \otimes \mathscr{L}^6 \simeq \mathrm{Sym}^3(\pi_*\mathscr{O}_W(3S)) \otimes \mathscr{L}^6 \\ &\simeq \mathscr{L}^6 \oplus \mathscr{L}^4 \oplus \mathscr{L}^3 \oplus \mathscr{L}^2 \oplus \mathscr{L} \oplus \mathscr{O}_B \oplus \mathscr{O}_B \oplus \mathscr{L}^{-1} \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3}. \end{aligned}$$

Symbolically, this is telling us that $W \hookrightarrow B$ is given by an equation of the form

$$\lambda Y^2Z + a_1XYZ + a_3YZ^2 = \mu X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and $a_i \in \mathrm{H}^0(B, \mathscr{L}^i)$. Finally, it is classic that we can always that $\lambda = 1 = \mu$ above and that $S \subset W$ is the subscheme $\{Z = 0\}$. ∘

Definition 3.1.9. An equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.3}$$

i.e. the data of a tuple $(\mathscr{L}, a_1, a_2, a_3, a_4, a_6)$ with $\mathscr{L} \in \mathrm{Pic}(B)$ and $a_i \in \mathrm{H}^0(B, \mathscr{L}^i)$, is called a `Weierstrass equation`. We call $\mathscr{L}$ the `Hodge bundle` of the equation. $\diamond$

The point of Remark 3.1.8 is that, from it, one obtains the following proposition.

Proposition 3.1.10. *Let $(W \xrightarrow{\pi} B, S)$ be a Weierstrass curve of height $> N(g)$. Then, (W, S) is isomorphic to the curve cut out by some Weierstrass equation (3.3) whose Hodge bundle is $\pi_*\omega_{W/B}$, equipped with the subscheme $\{Z = 0\}$.*

Remark 3.1.11 (See the discussion after Theorem 1 of Section 3 of [MS72])**.** To correctly interpret equation (3.3), one should regard X, Y, Z are sections of various line bundles; specifically,

$$X \in \mathrm{H}^0(\mathbb{P}, p^*(\mathscr{L}^2)(1)), \ \ Y \in \mathrm{H}^0(\mathbb{P}, p^*(\mathscr{L}^3)(1)), \ \text{ and } \ Z \in \mathrm{H}^0(\mathbb{P}, p^*(\mathscr{O}_B^{-1})(1)).$$

Above, $\mathbb{P} := \mathbb{P}\big(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3}\big) \cong \mathbb{P}(\pi_*\mathscr{O}_W(3S))$. This way (3.3) – or rather, the difference of its two sides – defines a section of the line bundle $p^*(\mathscr{L}^6)(3)$ on $\mathbb{P}$ (as should be expected by Proposition 3.1.5), and the zero scheme of this section in $\mathbb{P}$ is W.

Let us indicate where these sections X, Y, Z come from. Note that $\mathscr{H}\!om(\mathscr{L}^{-2}, \pi_*\mathscr{O}_W(3S)) \simeq \pi_*\mathscr{O}_W(3S) \otimes \mathscr{L}^2$, and let $\eta_X \in \mathrm{H}^0(B, \pi_*\mathscr{O}_W(3S) \otimes \mathscr{L}^2)$ be the global section corresponding to the natural inclusion $\mathscr{L}^{-2} \hookrightarrow \mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3} \simeq \pi_*\mathscr{O}_W(3S)$. Note that, by definition of $\mathbb{P}$, it comes with a morphism $p^*\pi_*\mathscr{O}_W(3S) \to \mathscr{O}_{\mathbb{P}}(1)$. Now, $X \in \mathrm{H}^0(\mathbb{P}, p^*(\mathscr{L}^2)(1))$ is the image of η_X under the induced map

$$p^*\big(\pi_*\mathscr{O}_W(3S) \otimes \mathscr{L}^2\big) \simeq p^*(\pi_*\mathscr{O}_W(3S)) \otimes p^*(\mathscr{L}^2) \to p^*(\mathscr{L}^2)(1).$$

We similarly define $Y \in \mathrm{H}^0(p^*(\mathscr{L}^3)(1))$ using the inclusion $\mathscr{L}^{-3} \hookrightarrow \pi_*\mathscr{O}_W(3S)$ and define $Z \in \mathrm{H}^0(\mathscr{O}_{\mathbb{P}}(1))$ using $\mathscr{O}_B \hookrightarrow \pi_*\mathscr{O}_W(3S)$. $\circ$

Recall that we are attempting to compute (an asymptotic) for

$$\#\mathcal{M}_{1,1}^{\le d}(K) = \sum_{E/K : \mathrm{ht}(E) \le d} \frac{1}{\#\mathrm{Aut}(E)} = \sum_{\substack{\mathscr{L} \in \mathrm{Pic}(B) \\ \deg \mathscr{L} \le d}} \sum_{\substack{E/K \\ \mathscr{L}_E \simeq \mathscr{L}}} \frac{1}{\#\mathrm{Aut}(E)},$$

where $\mathscr{L}_E$ denotes the Hodge bundle of the elliptic curve E. In order to capture the relationship between counts of elliptic curves and Weierstrass curves, we introduce the following notation.

Notation 3.1.12. For any $\mathscr{L} \in \mathrm{Pic}(B)$,

- let $\mathrm{UW}_{\mathscr{L}}$ denote the (unweighted) number of isomorphism classes of generically smooth, *minimal* Weierstrass equations with Hodge bundle isomorphic to $\mathscr{L}$.
- Let $\mathrm{WE}_{\mathscr{L}}$ denote the weighted number of isomorphism classes of elliptic curves with Hodge bundle isomorphic to $\mathscr{L}$, i.e.

$$\mathrm{WE}_{\mathscr{L}} := \sum_{\substack{E/K \\ \mathscr{L}_E \simeq \mathscr{L}}} \frac{1}{\#\mathrm{Aut}(E)}.$$

Proposition 3.1.13. *Fix $\mathscr{L} \in \mathrm{Pic}(B)$ with $d := \deg \mathscr{L} > N(g)$. Let E/K be an elliptic curve, and let $(W \to B, S)$ be a Weierstrass curve with generic fiber $\cong E$ and Hodge bundle $\cong \mathscr{L}$. The number of Weierstrass equations (3.3) cutting out Weierstrass curves isomorphic to $(W \to B, S)$ is*

$$\frac{(q-1)q^{6d+3(1-g)}}{\#\mathrm{Aut}(W/B, S)}.$$

Proof. From the previous discussion (in particular, Remark 3.1.11), we see that the Weierstrass equation (3.3) one obtains is determined up to scaling (i.e. up to choosing an isomorphism $\pi_*\omega_{W/B} \simeq \mathscr{L}$) by the choice of splittings in Remark 3.1.8. Such splittings give rise to the coordinates X, Y, Z in Remark 3.1.11, and once these are determined, there will be a single equation they satisfy. The set of splittings for the short exact sequence $0 \to \mathscr{O}_B \to \pi_*\mathscr{O}_W(2S) \to \mathscr{L}^{-2} \to 0$ form a torsor for $\operatorname{Hom}(\mathscr{L}^{-2}, \mathscr{O}_B) \simeq \mathrm{H}^0(B, \mathscr{L}^2)$ while splittings for $0 \to \pi_*\mathscr{O}_W(2S) \to \pi_*\mathscr{O}_W(3S) \to \mathscr{L}^{-3} \to 0$ form a torsor for

$$\operatorname{Hom}(\mathscr{L}^{-3}, \pi_*\mathscr{O}_W(2S)) \simeq \operatorname{Hom}(\mathscr{L}^{-3}, \mathscr{O}_B \oplus \mathscr{L}^{-2}) \simeq \mathrm{H}^0(B, \mathscr{L}^3) \oplus \mathrm{H}^0(B, \mathscr{L}).$$

Thus, including scaling, we have a total of

$$(\# k^\times) \cdot \# \mathrm{H}^0(B, \mathscr{L}^2) \cdot \# \mathrm{H}^0(B, \mathscr{L}^3) \cdot \# \mathrm{H}^0(B, \mathscr{L}) = (q-1)q^{6d+3(1-g)}$$

choices of data leading to Weierstrass equations for $(W \to B, S)$. Changing the choice of splittings and scaling corresponds to modifying (3.3) by an automorphism of $\mathbb{P}(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3})$, and so two choices give the same equation if and only if they differ by an automorphism of the Weierstrass curve, i.e. if and only if they differ by an automorphism of $\mathbb{P} := \mathbb{P}(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3})$ which carries $W \hookrightarrow \mathbb{P}$ onto itself. ■

Lemma 3.1.14. *Let R be a dvr, let $F = \operatorname{Frac}(R)$, and let $(W_1/R, S_1)$, $(W_2/R, S_2)$ be two Weierstrass curves over R with smooth generic fibers. Let $\varphi : W_{1,F} \xrightarrow{\sim} W_{2,F}$ be an isomorphism between their generic fibers such that $\varphi(S_{1,F}) = S_{2,F}$. Suppose that W_1, W_2 have discriminants with equal valuation. Then, φ uniquely extends to an isomorphism $\Phi : W_1 \xrightarrow{\sim} W_2$ of R-schemes satisfying $\Phi(S_1) = S_2$.*

Proof. Uniqueness of Φ holds simply because $W_{1,F}$ is (schematically) dense in W_1. For $i = 1, 2$, we can write W_i as the zero set of some Weierstrass equation

$$Y^2Z + a_1^{(i)}XYZ + a_3^{(i)}YZ^2 = X^3 + a_2^{(i)}X^2Z + a_3^{(i)}XZ^2 + a_6^{(i)}Z^3 \text{ with } a_j^{(i)} \in R$$

inside $\mathbb{P}^2_R$. Having done so, the isomorphism φ will be of the form

$$\varphi([X : Y : Z]) = \left[u^2X + rZ : u^3Y + u^2sX + tZ : Z\right]$$

for some $u \in F^\times$ and $r, s, t \in F$. By using the change of variables formula in [Sil09, Table III.3.1] and arguing as in [Sil09, Proposition VII.1.3(b)], since W_1, W_2 have discriminates with the same valuation, we must in fact have $u \in R^\times$ and $r, s, t \in R$. Thus, φ does in fact extend to a $\Phi : W_1 \xrightarrow{\sim} W_2$ as desired. ■

Corollary 3.1.15. *Let $(W_1/B, S_1)$, $(W_2/B, S_2)$ be two Weierstrass curves with smooth generic fibers, and let $\varphi : W_{1,K} \xrightarrow{\sim} W_{2,K}$ be an isomorphism between their generic fibers such that $\varphi(S_{1,K}) = S_{2,K}$. Suppose that W_1, W_2 have equal discriminant divisors. Then, φ uniquely extends to an isomorphism $\Phi : W_1 \xrightarrow{\sim} W_2$ of B-schemes satisfying $\Phi(S_1) = S_2$.*

Proof. Uniqueness of Φ holds simply because $W_{1,K}$ is (schematically) dense in W_1. Existence holds because φ automatically spreads out out to an isomorphism over some open $U \subset B$, and then further can be extended over the remaining points by Lemma 3.1.14. ■

Corollary 3.1.16. *Let $(W/B, S)$ be a Weierstrass curve with smooth generic fiber $E := W_K$, an elliptic curve. Then, the restriction map $\operatorname{Aut}(W/B, S) \to \operatorname{Aut}(E)$ is an isomorphism.*

Corollary 3.1.17. *Fix E be an elliptic curve. Let $(W/B, S)$ be a Weierstrass curve with generic fiber $\cong E$ and height $d > N(g)$. Then, the number of Weierstrass equations cutting out a Weierstrass curve isomorphic to $(W/B, S)$ is*

$$\frac{(q-1)q^{6d+3(1-g)}}{\# \operatorname{Aut}(E)}.$$

Corollary 3.1.18. *Choose $\mathscr{L} \in \mathrm{Pic}(B)$ of degree $> N(g)$. Then,*

$$\mathrm{WE}_{\mathscr{L}} = \frac{\mathrm{UW}_{\mathscr{L}}}{(q-1)q^{6d+3(1-g)}}.$$

Proof. For any elliptic curve E/K, let α_E denote (the iso. class of) its minimal Weierstrass model, and let $\mathscr{L}_E \in \mathrm{Pic}(B)$ denote its Hodge bundle. By Corollary 3.1.17, we have

$$\mathrm{UW}_{\mathscr{L}} = \sum_{\substack{E/K \\ \mathscr{L}_E \simeq \mathscr{L}}} \frac{(q-1)q^{6d+3(1-g)}}{\#\,\mathrm{Aut}(E)} = (q-1)q^{6d+3(1-g)}\,\mathrm{WE}_{\mathscr{L}}\,.$$

Rearrange to get the claimed equality. ■

At this point, we would like to determine the number $\mathrm{UW}_{\mathscr{L}}$ of generically smooth minimal Weierstrass equations over B with Hodge bundle isomorphic to $\mathscr{L}$. We do so by counting Weierstrass equations which are generically singular or which are non-minimal, and then subtracting these from the total number.

Remark 3.1.19. Fix $\mathscr{L} \in \mathrm{Pic}(B)$ of degree $> N(g)$. By Riemann-Roch, the number of Weierstrass equations with Hodge bundle $\cong \mathscr{L}$ is

$$\prod_{\substack{i=0 \\ i\neq 5}}^{6} \#\,\mathrm{H}^0(B, \mathscr{L}^i) = q^{16d+5(1-g)}. \qquad \circ$$

3.2 Counting Generically Singular Weierstrass Curves

To count Weierstrass curve over B with singular generic fiber, one argues exactly as in [dJ02, Section 4.11].

Proposition 3.2.1. *Let $\mathscr{L} \in \mathrm{Pic}(B)$ satisfy $\deg \mathscr{L} > N(g)$. Then, the number of generically singular Weierstrass curves with Hodge bundle $\cong \mathscr{L}$ is*

$$\#\,\mathrm{H}^0(B, \mathscr{L}) \cdot \#\,\mathrm{H}^0(B, \mathscr{L}^2)^2 \cdot \mathrm{H}^0(B, \mathscr{L}^3) = q^{8d+4(1-g)}.$$

Proof. Suppose $(W \xrightarrow{\pi} B, S)$ is a Weierstrass curve with singular generic fiber and Hodge bundle $\mathscr{L}$. Then, every fiber of $W \to B$ has exactly one singular point, and so these are the image of a unique section $\tau \in W(B)$, the section extending the singular K-point in the generic fiber. The composition $B \overset{\tau}{\hookrightarrow} W \hookrightarrow \mathbb{P} := \mathbb{P}(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3})$ shows that τ corresponds to a line bundle quotient $\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3} \twoheadrightarrow \mathscr{M}$. However, the image of τ is disjoint from the (smooth) zero section $S \subset W$, so the composition $\mathscr{O}_B \hookrightarrow \mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3} \twoheadrightarrow \mathscr{M}$ must be everywhere nonzero, i.e. $\mathscr{O}_B \xrightarrow{\sim} \mathscr{M}$. Thus, we may view τ as a triple $[\tau_X, \tau_Y, 1]$ where $\tau_X \in \Gamma(B, \mathscr{L}^2) = \mathrm{Hom}(\mathscr{L}^{-2}, \mathscr{O}_B)$ and $\tau_Y \in \Gamma(B, \mathscr{L}^3) = \mathrm{Hom}(\mathscr{L}^{-3}, \mathscr{O}_B)$. Since τ lands in the singular locus, applying the Jacobian criterion for smoothness to (3.3), we conclude that counting generically singular Weierstrass equations (3.3) amounts to counting tuples $(a_1, a_2, a_3, a_4, a_6, \sigma_X, \sigma_Y)$ with $a_i \in \mathrm{H}^0(\mathscr{L}^i)$, $\sigma_X \in \mathrm{H}^0(\mathscr{L}^2)$ and $\sigma_Y \in \mathrm{H}^0(\mathscr{L}^3)$ satisfying

$$\begin{aligned}
\sigma_Y^2 + a_2\sigma_X\sigma_Y + a_3\sigma_X &= \sigma_X^3 + a_2\sigma_X^2 + a_4\sigma_X + a_6 \\
-a_1\sigma_Y &= 3\sigma_X^2 + 2a_2\sigma_X + a_4 \\
2\sigma_Y + a_2\sigma_X + a_3 &= 0.
\end{aligned}$$

By the above equations, any such tuple is uniquely determined by the choice of $a_1, a_2, \sigma_X, \sigma_Y$ from whence the claim follows. ■

3.3 Counting Non-Minimal Weierstrass Curves

Our main tool for counting non-minimal Weierstrass curves is the following description of their origin.

Remark 3.3.1. All non-minimal Weierstrass curves of height $d \geq 0$ arise in the following manner.

Start with a *minimal* Weierstrass curve $(W' \xrightarrow{\pi'} B, S')$ of height $d' < d$ along with an effective divisor $D \in \mathrm{Div}(B)$ of degree $d - d'$, write $D = \sum_{i=1}^r n_i[b_i]$. Consider also the embedding $f : W' \hookrightarrow \mathbb{P}(\pi'_*\mathscr{O}_{W'}(3S'))$. Choose open neighborhoods $U_i \subset B$ of b_i, for each $i \in \{1, \ldots, r\} =: [r]$, which satisfy

- f restricts to an embedding $W'_{U_i} \hookrightarrow \mathbb{P}^2_{U_i}$ with image cut out by

$$Y^2Z + a_1^{(i)}XYZ + a_3^{(i)}YZ^2 = X^3 + a_2^{(i)}X^2Z + a_4^{(i)}XZ^2 + a_6^{(i)}Z^3$$

  ($a_j^{(i)} \in \Gamma(U_i, \mathscr{O}_B)$); and
- There exists some $\varpi^{(i)} \in \Gamma(U_i, \mathscr{O}_B)$ restricting to a uniformizer of $\mathscr{O}_{B,b_i}$, but to a unit of $\mathscr{O}_{B,b}$ for all $b \in U_i \setminus \{b_i\}$; and
- $b_j \notin U_i$ if $j \neq i$.

Let $U_0 = B \setminus \{b_1, \ldots, b_r\}$ and $\varpi^{(0)} := 1$. For each $i \in [r]$, let $c_j^{(i)} := \left(\varpi^{(i)}\right)^{j \cdot n_i} a_j^{(i)} \in \Gamma(U_i, \mathscr{O}_B)$, and consider the curve

$$W_i := \left\{Y^2Z + c_1^{(i)}XYZ + c_3^{(i)}YZ^2 = X^3 + c_2^{(i)}X^2Z + c_4^{(i)}XZ^2 + c_6^{(i)}Z^3\right\} \subset \mathbb{P}^2_{U_i}.$$

Also, let $W_0 := W'|_{U_0}$. By construction, for distinct $i, j \in \{0, 1, \ldots, r\}$, there is a natural isomorphism $\alpha_{ij} : W_i|_{U_i \cap U_j} \xrightarrow{\sim} W_j|_{U_i \cap U_j}$ which is given in coordinates as

$$\alpha_{ij} : [X : Y : Z] \longmapsto \left[\frac{\left(\varpi^{(j)}\right)^{2n_j}}{\left(\varpi^{(i)}\right)^{2n_i}}X : \frac{\left(\varpi^{(j)}\right)^{3n_j}}{\left(\varpi^{(i)}\right)^{3n_i}}Y : Z\right]$$

(note above that $\varpi^{(i)}, \varpi^{(j)} \in \Gamma(U_i \cap U_j, \mathscr{O}_B)^\times$). These isomorphisms visibly satisfy the cocycle condition, and so these W_i's glue to form a global curve W/B. Furthermore, the α_{ij}'s all respect the distinguished section ($[0 : 1 : 0]$) of each W_i and so one obtains a corresponding section $S \subset W$. This $(W/B, S)$ is, by construction, a non-minimal Weierstrass curve of height d; in fact, if $\mathscr{L}'$ is the Hodge bundle of W', then W has Hodge bundle $\mathscr{L}'(D)$. Furthermore, the resulting $(W/B, S)$ is, up to isomorphism, independent of the choices made by Corollary 3.1.15. ◦

The upshot of the above remark is that each generically smooth non-minimal Weierstrass *curve* (say, of height d) is determined by a unique choice of minimal Weierstrass *curve* (say, of height $e < d$) along with an effective divisor D of degree $d - e$ keeping track of the non-minimality of the equation. We use this observation to obtain a recursive count as in [dJ02, Proposition 4.12].

Proposition 3.3.2. *Fix some $\mathscr{L} \in \mathrm{Pic}^d(B)$ with $d > N(g)$. The number of non-minimal (generically smooth) Weierstrass equations with Hodge bundle $\cong \mathscr{L}$ is*

$$q^{6d+3(1-g)} \sum_{e=0}^{d-1} \sum_{\mathscr{M} \in \mathrm{Pic}^e(B)} \left(\# \mathrm{H}^0(B, \mathscr{L} \otimes \mathscr{M}^\vee) - 1\right) \mathrm{WE}_{\mathscr{M}}.$$

Proof. As remarked above, each non-minimal (generically smooth) Weierstrass *curve* with Hodge bundle $\cong \mathscr{L}$ is determined by a unique minimal Weierstrass curve $(W'/B, S')$, say with Hodge bundle $\mathscr{L}'$, along with an effective divisor D such that $\mathscr{L} \cong \mathscr{L}'(D)$. Recall each Weierstrass *curve* is cut out by $(q -$

$1)q^{6d+3(1-g)}/\#\operatorname{Aut}(E)$ different Weierstrass *equations*, by Corollary 3.1.17. Thus, the total number of (generically smooth) non-minimal Weierstrass equations with Hodge bundle $\cong \mathscr{L}$ is

$$\sum_{e=0}^{d-1} \sum_{D \in \operatorname{Div}_+^{d-e}(B)} \sum_{\substack{E/K \\ \mathscr{L}_E \simeq \mathscr{L}(-D)}} \frac{(q-1)q^{6d+3(1-g)}}{\#\operatorname{Aut}(E)} = (q-1)q^{6d+3(1-g)} \sum_{e=0}^{d-1} \sum_{D \in \operatorname{Div}_+^{d-e}(B)} \mathrm{WE}_{\mathscr{L}(-D)}, \tag{3.4}$$

where $\operatorname{Div}_+^n(B)$ is the set of effective divisors of degree n on B. Note that if $\mathscr{M} \simeq \mathscr{L}(-D)$, then $\mathscr{O}(D) \simeq \mathscr{L} \otimes \mathscr{M}^\vee$, so there are $(\#\operatorname{H}^0(B, \mathscr{L} \otimes \mathscr{M}^\vee) - 1)/(q-1)$ different effective divisors $D' \sim D$. Thus, (3.4) equals

$$(q-1)q^{6d+3(1-g)} \sum_{e=0}^{d-1} \sum_{\mathscr{M} \in \operatorname{Pic}^e(B)} \frac{\#\operatorname{H}^0(B, \mathscr{L} \otimes \mathscr{M}^\vee) - 1}{q-1} \mathrm{WE}_{\mathscr{M}}. \qquad \blacksquare$$

3.4 Counting Elliptic Curves

Proposition 3.4.1. *Fix any $\mathscr{L} \in \operatorname{Pic}^d(B)$ with $d > N(g)$. Then,*

$$\mathrm{UW}_{\mathscr{L}} = q^{16d+5(1-g)} - q^{8d+4(1-g)} - q^{6d+3(1-g)} \sum_{e=0}^{d-1} \sum_{\mathscr{M} \in \operatorname{Pic}^e(B)} \left(\#\operatorname{H}^0(B, \mathscr{L} \otimes \mathscr{M}^\vee) - 1\right) \mathrm{WE}_{\mathscr{M}},$$

and

$$\mathrm{WE}_{\mathscr{L}} = \frac{\mathrm{UW}_{\mathscr{L}}}{(q-1)q^{6d+3(1-g)}}.$$

Proof. The part after the word "and" is simply a restatement of Corollary 3.1.18. To compute $\mathrm{UW}_{\mathscr{L}}$, we make the simple observation that the (unweighted) number of generically smooth minimal Weierstrass equations is the total number of all Weierstrass equations minus the number of those which are generically singular minus the number of those which are generically smooth but non-minimal. With this in mind, the proposition follows combining Remark 3.1.19, Proposition 3.2.1, and Proposition 3.3.2. $\blacksquare$

Notation 3.4.2. We set

$$Z_B(T) := \prod_{\text{closed } x \in B} \frac{1}{1 - T^{\deg x}} = \sum_{n \geq 0} \#\operatorname{Sym}^n(B) \cdot T^n,$$

so $\zeta_B(s) = Z_B(q^{-s})$.

Remark 3.4.3. In the case that $B = \mathbb{P}^1$, we have $Z_{\mathbb{P}^1}(T) = [(1-T)(1-qT)]^{-1}$, and [dJ02, Proposition 4.12] gives an exact count

$$\#\mathcal{M}_{1,1}^{=d}(k(t)) = q^{10d+1}\left[1 + \frac{1 - q^{-8} - q^{-9} + q^{-18}}{q-1} - q^{-8d-1} + q^{-8d-3}\right] = \frac{q^{10d+2}}{(q-1)\zeta_{\mathbb{P}^1}(10)} - \frac{q^{2d+1}}{(q-1)\zeta_{\mathbb{P}^1}(2)},$$

when $d \geq 2$. $\circ$

Theorem 3.4.4. *For any $\varepsilon > 0$, we have*

$$\#\mathcal{M}_{1,1}^{=d}(K) = \#\operatorname{Pic}^0(B)\left[\frac{q^{10d+2(1-g)}}{(q-1)\zeta_B(10)} - \frac{q^{2d+(1-g)}}{(q-1)\zeta_B(2)}\right] + O_\varepsilon\left((q+\varepsilon)^d\right)$$

as $d \to \infty$, with implicit big-O constant dependent on ε. In particular,

$$\#\mathcal{M}_{1,1}^{=d}(K) \sim \#\operatorname{Pic}^0(B) \cdot \frac{q^{10d+2(1-g)}}{(q-1)\zeta_B(10)}.$$

Proof. We may and do assume throughout that $d \gg 1$. First note that

$$\#\mathcal{M}_{1,1}^{=d}(K) = \sum_{\mathscr{L}\in\mathrm{Pic}^d(B)} \mathrm{WE}_{\mathscr{L}} = \frac{a_d}{(q-1)q^{6d+3(1-g)}} \quad \text{where } a_d := \sum_{\mathscr{L}\in\mathrm{Pic}^d(B)} \mathrm{UW}_{\mathscr{L}}\,. \tag{3.5}$$

(by Corollary 3.1.18). Proposition 3.4.1 tells us that

$$\begin{aligned}
a_d &= \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] - q^{6d+3(1-g)} \sum_{\mathscr{L}\in\mathrm{Pic}^d(B)} \sum_{e=0}^{d-1} \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \big(\#\,\mathrm{H}^0(B,\mathscr{L}\otimes\mathscr{M}^{-1})-1\big)\,\mathrm{WE}_{\mathscr{M}} \\
&= \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] - q^{6d+3(1-g)}(q-1) \sum_{e=0}^{d-1} \sum_{\mathscr{L}\in\mathrm{Pic}^d(B)} \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \frac{\#\,\mathrm{H}^0(B,\mathscr{L}\otimes\mathscr{M}^{-1})-1}{q-1}\,\mathrm{WE}_{\mathscr{M}} \\
&= \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] - q^{6d+3(1-g)}(q-1) \sum_{e=0}^{d-1} \sum_{\mathscr{N}\in\mathrm{Pic}^{d-e}(B)} \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \frac{\#\,\mathrm{H}^0(B,\mathscr{N})-1}{q-1}\,\mathrm{WE}_{\mathscr{M}} \\
&= \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] - q^{6d+3(1-g)}(q-1) \sum_{e=0}^{d-1} \left(\sum_{\mathscr{N}\in\mathrm{Pic}^{d-e}(B)} \frac{\#\,\mathrm{H}^0(B,\mathscr{N})-1}{q-1} \right) \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \\
&= \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] - q^{6d+3(1-g)}(q-1) \sum_{e=0}^{d-1} \#\,\mathrm{Sym}^{d-e}(B) \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}}\,. \qquad (3.6)
\end{aligned}$$

We would like to turn (3.6) into a recursive formula for a_d by relating a_e to $\sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}}$. Since $\mathrm{WE}_{\mathscr{M}}$ is most mysterious when $\deg\mathscr{M} \le N(g)$, we deal with these terms by observing that

$$\begin{aligned}
\sum_{e=0}^{N(g)} \#\,\mathrm{Sym}^{d-e}(B) \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} &= \sum_{e=0}^{N(g)} \#\mathbb{P}^{d-e-g}(k) \cdot \#\,\mathrm{Pic}^{d-e}(B) \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \\
&\le \#\,\mathrm{Pic}^0(B) \cdot \sum_{e=0}^{N(g)} q^{d+1-g} \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \\
&\le \#\,\mathrm{Pic}^0(B) \cdot q^{d+1-g} \sum_{e=0}^{N(g)} \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \\
&= O\big(q^d\big) \qquad (3.7)
\end{aligned}$$

if $d = \deg\mathscr{L} \gg 1$. Thus, (3.6) can be simplified to

$$\begin{aligned}
a_d - \#\,\mathrm{Pic}^0(B)\Big[q^{16d+5(1-g)} - q^{8d+4(1-g)}\Big] &= -q^{6d+3(1-g)}(q-1) \sum_{e=0}^{d-1} \#\,\mathrm{Sym}^{d-e}(B) \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \\
&= -q^{6d+3(1-g)}(q-1) \left[O\big(q^d\big) + \sum_{e=N(g)+1}^{d-1} \#\,\mathrm{Sym}^{d-e}(B) \cdot \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \mathrm{WE}_{\mathscr{M}} \right] \\
&= O\big(q^{7d}\big) - q^{6d+3(1-g)}(q-1) \sum_{e=N(g)+1}^{d-1} \#\,\mathrm{Sym}^{d-e}(B) \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} \frac{\mathrm{UW}_{\mathscr{M}}}{(q-1)q^{6e+3(1-g)}} \\
&= O\big(q^{7d}\big) - \sum_{e=N(g)+1}^{d-1} \#\,\mathrm{Sym}^{d-e}(B) \sum_{\mathscr{M}\in\mathrm{Pic}^e(B)} q^{6(d-e)}\,\mathrm{UW}_{\mathscr{M}}
\end{aligned}$$

$$= O\big(q^{7d}\big) - \sum_{e=0}^{d-1} \#\operatorname{Sym}^{d-e}(B) \cdot q^{6(d-e)} a_e, \tag{3.8}$$

where we implicitly used Corollary 3.1.18 (which required $\deg \mathscr{M} > N(g)$) in the third equality, and that

$$\sum_{e=0}^{2g-2} \#\operatorname{Sym}^{d-e}(B) q^{6(d-e)} \sum_{\mathscr{M} \in \operatorname{Pic}^e(B)} \mathrm{UW}_{\mathscr{M}} = O\big(q^{7d}\big)\,,$$

via reasoning as in (3.7), in the fifth equality. At this point, we introduce the sequence c_d defined by $a_d = \#\operatorname{Pic}^0(B) q^{16d+5(1-g)} c_d$ and remark that (by (3.5)) the theorem statement is equivalent to the claim that

$$c_d = \zeta_B(10)^{-1} - q^{-8d-(1-g)} \zeta_B(2)^{-1} + O_\varepsilon\Big(\big(q^{-9} + \varepsilon\big)^d\Big) \tag{3.9}$$

for any $\varepsilon > 0$. To prove (3.9), consider the generating function $C(T) := \sum_{d \geq 0} c_d T^d$. From (3.8), one obtains:

$$\sum_{e=0}^{d} \#\operatorname{Sym}^{d-e}(B) \cdot q^{-10(d-e)} c_e = 1 - q^{-8d-(1-g)} + O\big(q^{-9d}\big)\,.$$

Multiplying both sides by T^d and summing over $d \geq 0$, this becomes

$$C(T) Z_B\big(q^{-10}T\big) = \sum_{d \geq 0} \left[\sum_{e=0}^{d} \#\operatorname{Sym}^{d-e}(B) q^{-10(d-e)} \cdot c_e\right] T^d = \frac{1}{1-T} - \frac{q^{g-1}}{1 - Tq^{-8}} + \sum_{d \geq 0} O\big(q^{-9d}\big)\, T^d.$$

Hence, $C(T) = Z_B\big(q^{-10}T\big)^{-1} M(T) + E(T)$, where

$$M(T) := \frac{1}{1-T} - \frac{q^{g-1}}{1 - Tq^{-8}} \quad \text{and} \quad E(T) := Z_B\big(q^{-10}T\big)^{-1} \sum_{d \geq 0} O\big(q^{-9d}\big)\, T^d.$$

Note that, by the Weil conjectures, $Z_B(T) = P(T)/[(1-T)(1-qt)]$ for some polynomial $P(T) \in \mathbb{C}[T]$ all of whose roots $\alpha \in \mathbb{C}$ satisfy $|\alpha| = 1/\sqrt{q}$. Thus, $Z_B\big(q^{-10}T\big)^{-1}$ is holomorphic on a disk of radius $q^{9.5}$, so $E(T)$ above is holomorphic on a disk of radius q^9. Now, set

$$\begin{aligned} F(T) &:= Z_B\big(q^{-10}T\big)^{-1} M(T) - \left[\frac{Z_B\big(q^{-10}\big)^{-1}}{1-T} - \frac{q^{g-1} Z_B\big(q^{-2}\big)^{-1}}{1 - q^{-8}T}\right] \\ &= \frac{Z_B\big(q^{-10}T\big)^{-1} - Z_B\big(q^{-10}\big)^{-1}}{1-T} + \frac{q^{g-1}\Big[Z_B\big(q^{-2}\big)^{-1}\Big] - Z_B\big(q^{-10}T\big)^{-1}}{1 - q^{-8}T}. \end{aligned}$$

Above, note that the zeros of the numerators at $T = 1$ and $T = q^8$, respectively, cancel out the simple zeros of the denominators there. Therefore, $F(T)$ has poles only where $Z_B\big(q^{-10}T\big)^{-1}$ has poles, so $F(T)$ is holomorphic on a disk of radius $q^{9.5}$. Consequently,

$$C(T) = Z_B\big(q^{-10}T\big)^{-1} M(T) + E(T) = \frac{Z_B\big(q^{-10}\big)^{-1}}{1-T} - \frac{q^{g-1} Z_B\big(q^{-2}\big)^{-1}}{1 - q^{-8}T} + F(T) + E(T).$$

Since $F(T) + E(T)$ is holomorphic on a disk of radius q^9, comparing Taylor coefficients shows that

$$c_d = Z_B\big(q^{-10}\big)^{-1} - q^{-8d-(1-g)} Z_B\big(q^{-2}\big)^{-1} + O_\varepsilon\Big(\big(q^{-9} + \varepsilon\big)^d\Big)$$

for any $\varepsilon > 0$, proving the claim. ■

4 Hyper-Weierstrass Curves

In Section 3, we computed $\#\mathcal{M}_{1,1}^{\le d}(K)$, the denominator of (1.2). In the current section, we turn our attention towards its numerator. In order to count 2-Selmer elements, we attach to them certain "integral models" whose definition and basic properties are the focus of this section.

4.1 Definitions and Geometric Preliminaries

The definition of the titular objects of this section is inspired by the following description of 2-Selmer elements.

Remark 4.1.1. Let K be as in Setup 1.1. Let E/K be an elliptic curve, and fix any $n \ge 1$. Every $\alpha \in \mathrm{Sel}_n(E) \subset \mathrm{H}^1(K, E[n])$ can be represented by a pair (C, D) where C is locally solvable E-torsor, and $D \subset C$ is an effective divisor of degree n. Explicitly, given such a pair, one associates to it the $E[n]$-torsor $T \subset C$ consisting of points $P \in C$ for which $nP \sim D$. Put another way, T is the preimage of $\mathscr{O}_C(D) \in \mathrm{Pic}^n(C)$ under the multiplication-by-n map

$$C \xrightarrow{\sim} \underline{\mathrm{Pic}}^1_{C/K} \longrightarrow \underline{\mathrm{Pic}}^n_{C/K}.$$

Two such pairs (C_1, D_1) and (C_2, D_2) represent the same n-Selmer element if and only if there is an isomorphism $\varphi : C_1 \xrightarrow{\sim} C_2$ of E-torsors for which $\mathscr{O}_{C_1}(D_1) \simeq \varphi^*\mathscr{O}_{C_2}(D_2)$. Finally, a pair (C, D) represents the identity element of $\mathrm{Sel}_n(E)$ if and only if $D \sim nO$ for some $O \in C(K)$.

This description of n-Selmer elements can be obtained, for example, by combining [CFO+08, Section 1.1] with [O'N02, Remark after Proposition 2.3]. ∘

Definition 4.1.2. For an arbitrary base scheme B, we let $\mathcal{H}(B)$ denote the groupoid whose

- objects are pairs $(H \xrightarrow{\pi} B, D)$ of a curve H/B along with a subscheme $D \subset H$ satisfying
  - **(a)** $\pi_*\mathscr{O}_H \simeq \mathscr{O}_B$ holds after arbitrary base change.
  - **(b)** $\omega_{H/B} \simeq \pi^*\mathscr{L}$ for some $\mathscr{L} \in \mathrm{Pic}(B)$.
  - **(c)** $D \subset H/B$ is an effective relative Cartier divisor of degree 2.
    By 'of degree 2', we mean that $D_b \subset H_b$ is locally principal of degree 2 for all $b \in B$.
  - **(d)** The line bundle $\mathscr{O}_H(D)$ is relatively ample over B.
- (iso)morphisms $(H \xrightarrow{\pi} B, D) \to (H' \xrightarrow{\pi'} B, D')$ are isomorphisms $\varphi : H \xrightarrow{\sim} H'$ over B such that

$$\varphi^*\mathscr{O}_{H'}(D') \in \mathscr{O}_H(D) \otimes \pi^* \mathrm{Pic}(B).$$

We call an element of $\mathcal{H}(B)$ a `hyper-Weierstrass curve` (or simply an `hW curve`) over B. ⋄

Remark 4.1.3. Condition **(a)** above implies that the fibers of H/B are geometrically connected. Condition **(b)** implies that that each fiber has trivial dualizing sheaf. Together, these two can be thought of as saying that H/B is a family of genus 1 curves. ∘

Remark 4.1.4. The definition of $\mathcal{H}(B)$ was greatly inspired by the definition of the class $\mathcal{A}_{n,d}$ of curves appearing in [dJ02, Paragraph 5.2]. ∘

Remark 4.1.5. Classes of curves which satisfy the criteria of Definition 4.1.2 have been studied before, e.g. in [Liu22] (where they are called "Weierstrass models") and [Sad11] (where they are called "Degree 2 models of genus 1 curves"). Neither citation considers them over an arbitrary base, and they both only consider such models whose generic fiber is smooth. Here, we allow of arbitrary bases and singular generic fibers, at least in setting up their basic geometric properties. Finally, since usual Weierstrass models of elliptic curves play a role in this paper, we opted to give these particular curves a different name. ∘

In this section (as well as the Section 5), we aim to develop a theory of hyper-Weierstrass curves akin to the theory of Weierstrass curves used in Section 3 and summarized in Theorem 3.1.3. Our first goal in such a development will be to show, analogous to Theorem 3.1.3**(4)**, that any hW curve can, locally on the base, be embedded in $\mathbb{P}(1,2,1)$ where it can be cut out by an equation of the form

$$Y^2 + (a_0X^2 + a_1XZ + a_2Z^2)Y = c_0X^4 + c_1X^3Z + c_2X^2Z^2 + c_3XZ^3 + c_4Z^4.$$

4.1.1 Fundamental Exact Sequences

Setup 4.1.6. Fix an arbitrary base scheme B.

Lemma 4.1.7. *Let k be a field, and let X/k be a k-curve with trivial dualizing sheaf $\omega = \omega_{X/k} \cong \mathscr{O}_X$ and with $\mathrm{H}^0(X, \mathscr{O}_X) = k$. Let $D \subset X$ be a Cartier divisor, and let $d = h^0(\mathscr{O}_D)$. Assume that $d \geq 1$. Then, $h^1(\mathscr{O}_X(D)) = 0$, $h^0(\mathscr{O}_X(D)) = d$. If furthermore $d \geq 2$, then $\mathscr{O}_X(D)$ is globally generated.*

Proof. Consider the exact sequences

$$0 \to \mathscr{O}_X(-D) \to \mathscr{O}_X \to \mathscr{O}_D \to 0 \text{ and } 0 \to \mathscr{O}_X \to \mathscr{O}_X(D) \to \mathscr{O}_D(D) \to 0. \tag{4.1}$$

By duality, $\chi(\mathscr{O}_X) = h^0(\mathscr{O}_X) - h^0(\omega) = h^0(\mathscr{O}_X) - h^0(\mathscr{O}_X) = 0$ since $\omega \cong \mathscr{O}_X$. Hence, the exact sequence on the right of (4.1) gives

$$\chi(\mathscr{O}_X(D)) = \chi(\mathscr{O}_X) + \chi(\mathscr{O}_D(D)) = \chi(\mathscr{O}_D(D)).$$

Since $\mathscr{O}_D$ is a skyscraper sheaf, we must have $\mathscr{O}_D \simeq \mathscr{O}_D(D)$. The above thus says

$$\chi(\mathscr{O}_X(D)) = \chi(\mathscr{O}_D(D)) = \chi(\mathscr{O}_D) = d. \tag{4.2}$$

We now claim that $\mathrm{H}^1(\mathscr{O}_X(D)) = 0$. By duality, $h^0(\mathscr{O}_X(D)) = h^0(\omega_X \otimes \mathscr{O}_X(-D)) = h^0(\mathscr{O}_X(-D))$. At the same time, the exact sequence on the left of (4.1) gives rise to

$$0 \longrightarrow \mathrm{H}^0(X, \mathscr{O}_X(-D)) \longrightarrow \mathrm{H}^0(X, \mathscr{O}_X) \longrightarrow \mathrm{H}^0(D, \mathscr{O}_D).$$

The restriction map $k = \mathrm{H}^0(X, \mathscr{O}_X) \to \mathrm{H}^0(D, \mathscr{O}_D)$ is nonzero, so we conclude that $\mathrm{H}^0(X, \mathscr{O}_X(-D)) = 0$; hence also $\mathrm{H}^1(X, \mathscr{O}_X(D)) = 0$. Combining this with (4.2), we must have $h^0(\mathscr{O}_X(D)) = \chi(\mathscr{O}_X(D)) = d$. Finally, that $\mathscr{O}_X(D)$ is globally generated when $d \geq 2$ now follows from [dJ02, Lemma 8.4(a)]. ■

In developing a theory of hW curves, we will find it useful to also consider pairs $(X/B, D)$ satisfying properties **(a)** – **(c)** (but not necessarily **(d)**) of Definition 4.1.2. Hence, we now name such curves.

Definition 4.1.8. A `hyper almost-Weierstrass curve` (or simply `hawc`) is a pair $(X \xrightarrow{\pi} B, D)$ consisting of a curve X/B along with a subscheme $D \subset X$ satisfying properties **(a)** – **(c)** of Definition 4.1.2. ⋄

Remark 4.1.9. We will see in Corollary 4.1.18 that hawcs give rise to hW curves. In Section 4.2.2, we will apply this to show that every 2-Selmer element can be represented by an hW curve. In brief, Remark 4.1.1 will let us represent a 2-Selmer element by a pair (C, D) with C a locally solvable genus 1 curve, and $D \subset C$

a degree 2 divisor. In Section 4.2.2, we will show that the minimal proper regular model of C can be given the structure of a hawc, and so will give rise to an hW curve with (C, D) as its generic fiber. ∘

Lemma 4.1.10. *Let $\pi : X \to B$ be a curve satisfying $\pi_*\mathscr{O}_X \simeq \mathscr{O}_B$ and $\omega_{X/B} \simeq \pi^*\mathscr{L}$ for some $\mathscr{L} \in \operatorname{Pic}(B)$. Let $E \subset X$ be an effective relative Cartier divisor of degree $n \geq 1$. Then,*

- *$\pi_*\mathscr{O}_X(E)$ is a locally free sheaf of rank n on B, whose formation commute with arbitrary base change; and*
- *$R^1\pi_*\mathscr{O}_X(E) = 0$.*

Proof. Since E is degree n over the base, 'Riemann-Roch of the fibers' (i.e. Lemma 4.1.7) shows that $h^0(E_b) = n$ and $h^1(E_b) = 0$ for any $b \in B$. We now apply cohomology and base change, Theorem A.1, with $\mathscr{F} = \mathscr{O}_X(E)$ and $i = 1$. Part **(0)** of Theorem A.1 implies that $R^1\pi_*\mathscr{O}_X(E) = 0$, so part **(2)** implies that φ_b^0 (with notation as in the theorem statement) is surjective for all b. Given this, we can apply Theorem A.1 a second time, now with $i = 0$ and $\mathscr{F} = \mathscr{O}_X(E)$. Part **(2)** shows that $\pi_*\mathscr{O}_X(E)$ is a vector bundle on B, part **(1)** shows that its formation commutes with arbitrary base change, and part **(0)** shows that it has rank $h^0(E_b) = n$. ■

Remark 4.1.11. Let $(X \xrightarrow{\pi} B, D)$ be a hawc. We will most commonly apply Lemma 4.1.10 to the divisors $nD \subset X$, for $n \geq 1$. In this context, Lemma 4.1.10 says, among other things, that $\pi_*\mathscr{O}_X(nD)$ is a vector bundle of rank $2n$. ∘

Proposition 4.1.12. *Let $(X \xrightarrow{\pi} B, D)$ be a hawc with Hodge bundle $\mathscr{L} := \pi_*\omega_{X/B}$. For any integer $n \geq 2$, there is an exact sequence*

$$0 \longrightarrow \pi_*\mathscr{O}_X((n-1)D) \otimes \det(\pi_*\mathscr{O}_X(D)) \longrightarrow \pi_*\mathscr{O}_X(nD) \otimes \pi_*\mathscr{O}_X(D) \longrightarrow \pi_*\mathscr{O}_X((n+1)D) \longrightarrow 0 \tag{4.3}$$

of vector bundles on B, where the right map above is the natural multiplication map. When $n = 1$, there is an exact sequence

$$0 \longrightarrow \operatorname{Sym}^2(\pi_*\mathscr{O}_X(D)) \longrightarrow \pi_*\mathscr{O}_X(2D) \longrightarrow \mathscr{L}^{-1} \otimes \det(\pi_*\mathscr{O}_X(D)) \longrightarrow 0 \tag{4.4}$$

of vector bundles on B, where the left map is the natural multiplication map.

Proof. Note that $\mathscr{O}_{X_b}(D_b)$ is globally generated for all $b \in B$ by Lemma 4.1.7. Hence, Lemmas 4.1.10 and A.2 tell us that the natural counit map is a surjection $\pi^*\pi_*\mathscr{O}_X(D) \twoheadrightarrow \mathscr{O}_X(D)$. Consider the exact sequence

$$0 \longrightarrow \mathscr{K} \longrightarrow \pi^*\pi_*\mathscr{O}_X(D) \longrightarrow \mathscr{O}_X(D) \longrightarrow 0, \tag{4.5}$$

and note that $\mathscr{K}$ is a kernel of a surjection between vector bundles, and so a vector bundle itself. Since $\mathscr{O}_X(D)$ is a line bundle while $\pi^*\pi_*\mathscr{O}_X(D)$ is rank 2 (by Lemma 4.1.10), $\mathscr{K}$ is a line bundle, so we can take determinants to compute $\mathscr{K} \simeq \mathscr{O}_X(-D) \otimes \pi^* \det(\pi_*\mathscr{O}_X(D))$.

Now, fix an integer $n \geq 1$. Twisting (4.5) by $\mathscr{O}_X(nD)$, pushing forward the resulting sequence, and applying the projection formula[1] to both $\mathscr{K}(nD) \simeq \mathscr{O}_X((n-1)D) \otimes \pi^* \det(\pi_*\mathscr{O}_X(D))$ and $\mathscr{O}_X(nD) \otimes \pi^*\pi_*\mathscr{O}_X(D)$, we obtain the exact sequence

$$\begin{aligned} 0 \longrightarrow \pi_*\mathscr{O}_X((n-1)D) \otimes \det(\pi_*\mathscr{O}_X(D)) &\longrightarrow \pi_*\mathscr{O}_X(nD) \otimes \pi_*\mathscr{O}_X(D) \longrightarrow \pi_*\mathscr{O}_X((n+1)D) \\ &\longrightarrow R^1\pi_*\mathscr{O}_X((n-1)D) \otimes \det(\pi_*\mathscr{O}_X(D)) \longrightarrow R^1\pi_*\mathscr{O}_X(nD) \otimes \pi_*\mathscr{O}_X(D). \end{aligned}$$

[1] $R^k\pi_*(\mathscr{F} \otimes \pi^*\mathscr{G}) \simeq R^k\pi_*\mathscr{F} \otimes \mathscr{G}$ when $\mathscr{G}$ is a vector bundle, [Har77, Exercise III.8.3]

By Lemma 4.1.10, $R^1\pi_*\mathscr{O}_X(nD) = 0$. If $n \geq 2$, then also $R^1\pi_*\mathscr{O}_X((n-1)D) = 0$, so the sequence becomes

$$0 \longrightarrow \pi_*\mathscr{O}_X((n-1)D) \otimes \det(\pi_*\mathscr{O}_X(D)) \longrightarrow \pi_*\mathscr{O}_X(nD) \otimes \pi_*\mathscr{O}_X(D) \longrightarrow \pi_*\mathscr{O}_X((n+1)D) \longrightarrow 0,$$

as claimed. If $n = 1$, then the map $\pi_*\mathscr{O}_X(D) \otimes \pi_*\mathscr{O}_X(D) \to \pi_*\mathscr{O}_X(2D)$ factors through $\mathrm{Sym}^2(\pi_*\mathscr{O}_X(D))$ and – recalling that $R^1\pi_*\mathscr{O}_X \simeq \mathscr{L}^{-1}$ by duality – we obtain the exact sequence

$$\mathrm{Sym}^2(\pi_*\mathscr{O}_X(D)) \longrightarrow \pi_*\mathscr{O}_X(2D) \longrightarrow \mathscr{L}^{-1} \otimes \det(\pi_*\mathscr{O}_X(D)) \longrightarrow 0$$

Now, we claim that the map $\mathrm{Sym}^2(\pi_*\mathscr{O}_X(D)) \to \pi_*\mathscr{O}_X(2D)$ is injective. This follows from the fact that the kernel of a surjection between vector bundles is a vector bundle. Indeed, exactness of the sequence tells us that the image of this map is the rank 3 vector bundle $\ker\big(\pi_*\mathscr{O}_X(2D) \twoheadrightarrow \mathscr{L}^{-1} \otimes \det(\pi_*\mathscr{O}_X(D))\big)$, and so its kernel is the rank 0 vector bundle

$$\ker\big(\mathrm{Sym}^2(\pi_*\mathscr{O}_X(D)) \twoheadrightarrow \ker\big(\pi_*\mathscr{O}_X(2D) \to \mathscr{L}^{-1} \otimes \det(\pi_*\mathscr{O}_X(D))\big)\big) = 0.$$

Hence, the sequence above is exact on the left, finishing the proof of the claim. ■

Corollary 4.1.13. *Let $(X \xrightarrow{\pi} B, D)$ be a hawc with Hodge bundle $\mathscr{L} := \pi_*\omega_{X/B}$. Let $\mathscr{D} := \det(\pi_*\mathscr{O}_X(D))$. Then,*

$$\det(\pi_*\mathscr{O}_X(nD)) \simeq \mathscr{D}^{n^2} \otimes \mathscr{L}^{1-n} \ \textit{ for all } \ n \geq 1.$$

Proof. This is true for $n = 1$ by definition. For $n = 2$, this then follows from taking determinants in (4.4). For $n > 2$, one inductively takes determinants in (4.3). ■

Proposition 4.1.12 (in particular, surjectivity of the relevant multiplication morphisms when $n \geq 2$) is our main workhorse for obtaining local equations for hyper-Weierstrass curves.

4.1.2 Local Projective Embeddings

We will soon show (Theorem 4.1.16) that hW curves have local models of the shape mentioned near the introduction of this section, and (Corollary 4.1.18) that one can use a hawc to construct an hW curve. This will be achieved by considering a certain Proj construction. Before stating and proving things precisely, we want to give an indication of what this construction is doing fiberwise, i.e. of what it is doing when $B = \mathrm{Spec}\, F$ is a field.

Remark 4.1.14. Let F be a field, and let (C, D) be a hawc over F. Consider the F-scheme

$$H := \mathrm{Proj}\left(\underbrace{\bigoplus_{n \geq 0} \mathrm{H}^0(C, \mathscr{O}_C(nD))}_{\Gamma_*(C,D)}\right).$$

Let $p : C \to H$ be the natural map. We make the following remarks:

- If $D \subset C$ is ample, i.e. if $(C, D) \in \mathcal{H}(\mathrm{Spec}\, F)$, then in fact $p : C \xrightarrow{\sim} H$ (see e.g. [Sta21, Tag 01Q3(2)]).
- Because C is curve, the Cartier divisor $D \subset C$ is ample if and only if it meets every irreducible component of C. Let $\{C_i\}_{i \in I}$ be the irreducible components of C which D does *not* meet, and let $U := C \setminus \bigcup_{i \in I} C_i \overset{\text{open}}{\subset} C$. Then, $D \subset U$ is ample, and $p : C \to H$ restricts to an open immersion $U \hookrightarrow H$ with dense image. We carefully prove this in Lemma 4.1.15.

- As a consequence of the previous bullet point, the scheme-theoretic image D_H of D under p is an effective Cartier divisor of degree 2 on H, which is furthermore ample. Indeed, $p(U)$ is a dense open in H containing D_H and $U \xrightarrow{\sim} p(U)$; hence H is a curve and $D_H \subset H$ is an effective, ample, degree 2 Cartier divisor if and only if $D \subset U$ is. ∘

Lemma 4.1.15. *Use notation as in the second bullet point of Remark 4.1.14. Then, $p : C \to H$ restricts to an open immersion $U \hookrightarrow H$ with dense image. In other words, $p : C \to H$ is a contraction of the components of C not meeting D.*

Proof. Fix any $x \in U$. We will find an open neighborhood of x which maps isomorphically onto an open in H. Let $\overline{U} \subset C$ be the closed subscheme with ideal sheaf $\ker(\mathscr{O}_X \to j_*\mathscr{O}_U)$, with $j : U \hookrightarrow X$ the natural inclusion. Note that $D \subset \overline{U}$ is ample as it meets every irreducible component of $\overline{U}$. Fix N large enough that $\mathscr{O}_{\overline{U}}(ND)$ is very ample, and let $f : C \to \mathbb{P}^M$ be the morphism induced by the complete linear system on $\mathscr{O}_C(ND)$ (recall $\mathscr{O}_C(ND)$ is globally generated by Lemma 4.1.7).

Let $S := \overline{U} \setminus U = \{s_1, \ldots, s_k\}$. By construction $f|_{\overline{U}}$ is an immersion, so the points $f(x), f(s_1), \ldots, f(s_k) \in \mathbb{P}^M$ are distinct. Hence, we can find some hypersurface in $\mathbb{P}^M$ which passes through $f(s_1), \ldots, f(s_k)$, but which avoids $f(x)$. In other words, we can find some $n \geq 1$ along with some section $\sigma \in \mathrm{H}^0(C, \mathscr{O}_C(nD))$ which vanishes at $s_1, \ldots, s_k$, but which is nonvanishing at x. Recall that $\{C_i\}$ denotes the components of C not meeting D, so $\mathscr{O}_C(D)|_{C_i} \simeq \mathscr{O}_{C_i}$ for all i and hence σ restricts to a constant function on each C_i. Hence, because C is connected and σ vanishes on $\{s_1, \ldots, s_k\}$, one sees that, possibly after replacing σ with a power, it in fact vanishes along C_i for all i. Thus, the nonvanishing locus C_σ of σ is contained in U.

Now, $C_\sigma = U_\sigma$ is affine since it's closed in the affine $\{\sigma \neq 0\} \subset \mathbb{P}^M$. Furthermore, [Sta21, Tag 01PW(2)] shows that p induces an isomorphism

$$\Gamma_*(C, D)_{(\sigma)} \xrightarrow{\sim} \Gamma(C_\sigma, \mathscr{O}_{C_\sigma}) = \Gamma(U_\sigma, \mathscr{O}_{U_\sigma}),$$

so p maps U_σ isomorphically onto $D_+(\sigma) \subset H$. Since $x \in U$ was arbitrary, we see that p maps U isomorphically onto an open subset of H.

All that remains is to show that $p(U) \subset H$ is dense. Choose any $n \geq 1$ and section $\sigma \in \mathrm{H}^0(C, \mathscr{O}_C(nD))$ such that $D_+(\sigma) \subset H$ does not meet $p(U)$. We will show that $\sigma = 0$, so the only open subset of $H \setminus p(U)$ is $D_+(0) = \emptyset$. By assumption, $U_\sigma = p^{-1}(D_+(\sigma)) = \emptyset$, so σ vanishes everywhere along U. Hence, σ vanishes everywhere along its closure $\overline{U}$. As before, because C is connected and $\mathscr{O}_C(D)|_{C_i} \simeq \mathscr{O}_{C_i}$ for all $i \in I$, after possibly replacing σ by a power, one can easily concludes from this that σ vanishes along C_i for all $i \in I$. That is, σ vanishes everywhere along C, so $\sigma = 0$. ■

Theorem 4.1.16. *Let $(X \to B, D)$ be a hawc. Let*

$$H := \mathbf{Proj}_B \left(\bigoplus_{n \geq 0} \pi_* \mathscr{O}_X(nD) \right).$$

Let $p : X \to H$ be the natural map, induced by the surjections $\pi^*\pi_*\mathscr{O}_X(nD) \twoheadrightarrow \mathscr{O}_X(nD)$ (see [Sta21, Tag 01O8]), and let $D_H \subset X$ be the (scheme-theoretic) image of D under p.

Then, each point of the base B has an affine neighborhood $U = \operatorname{Spec} R$ such that $H_U \to U$ is isomorphic over U to the subscheme of $\mathbb{P}(1,2,1)_U$ defined by

$$Y^2 + (uX^2 + vXZ + wZ^2)Y = aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4 \tag{4.6}$$

for some $u, v, w, a, b, c, d, e \in R$. Furthermore, we may choose the coordinates X, Y, Z above so that Z extends to a global section of $\mathscr{O}_H(1)$, and so that D_H is the divisor $\{Z = 0\}$; hence, $\mathscr{O}_H(1) \simeq \mathscr{O}_H(D_H)$.

Finally, if $D \subset X$ is relatively ample over B, i.e. if $(X \to B, D) \in \mathcal{H}(B)$, then $X \simeq H$ as B-schemes, so $(X \to B, D)$ itself satisfies the above properties.

Proof. Each point of B has an affine neighborhood $U = \operatorname{Spec} R$ above which both $\pi_*\mathscr{O}_X(D)$ and $\mathscr{L}$ trivialize, so we may and do assume wlog that $B = U = \operatorname{Spec} R$. Even after passing to this case, we continue to write U for the base instead of B in order to emphasize the fact that we're working over an affine.

We want to carefully construct $x, z \in \Gamma(U, \pi_*\mathscr{O}_X(D))$ and $y \in \Gamma(U, \pi_*\mathscr{O}_X(2D))$ which will give the coordinates on our weighted projective space. For this, we first consider the exact sequence $0 \to \mathscr{O}_X \to \mathscr{O}_X(D) \to \mathscr{O}_D(D) \to 0$ which pushes forward to

$$0 \longrightarrow \mathscr{O}_U \longrightarrow \pi_*\mathscr{O}_X(D) \longrightarrow \pi_*\mathscr{O}_D(D) \longrightarrow \mathscr{L}^{-1} \longrightarrow 0.$$

Let $\mathfrak{Q} := \operatorname{coker}(\mathscr{O}_U \to \pi_*\mathscr{O}_X(D)) = \ker(\pi_*\mathscr{O}_D(D) \twoheadrightarrow \mathscr{L}^{-1})$, and note that this is a vector bundle. Consider the exact sequence (recall that $U = \operatorname{Spec} R$ is affine)

$$\begin{tikzcd} 0 \arrow[r] & \Gamma(U, \mathscr{O}_U) \arrow[r] \arrow[d, equal] & \Gamma(U, \pi_*\mathscr{O}_X(D)) \arrow[r] \arrow[d, equal] & \Gamma(U, \mathscr{Q}) \arrow[r] & 0. \\ & R & R^2 & & \end{tikzcd}$$

We let $z \in \Gamma(U, \pi_*\mathscr{O}_X(D)) \simeq R^2$ be the image of $1 \in R$ under the first map above. Since $\Gamma(U, \mathscr{Q})$ is a projective R-module, taking determinants shows that $\Gamma(U, \mathscr{Q}) \simeq R$ is free, so we can and do fix some $x \in \Gamma(U, \mathscr{O}_X(D))$ with image generating $\Gamma(U, \mathscr{Q})$. Hence, $x, z \in \Gamma(U, \pi_*\mathscr{O}_X(D))$ give a basis. We went through the trouble of carefully choosing a particular z to be part of our basis in order to know that the subscheme $\{z = 0\} \subset X$ is equal to D.

Now, by Proposition 4.1.12, the cokernel of the map $\operatorname{Sym}^2 \Gamma(U, \pi_*\mathscr{O}_X(D)) \hookrightarrow \Gamma(U, \pi_*\mathscr{O}_X(2D))$ is free, so we can find some $y \in \Gamma(U, \pi_*\mathscr{O}_X(2D))$ such that x^2, xz, z^2, y form a basis for $\Gamma(U, \pi_*\mathscr{O}_X(2D))$. We want to use these to produce a basis for $\Gamma(U, \pi_*\mathscr{O}_X(3D))$. First note that the multiplication map

$$\Gamma(U, \pi_*\mathscr{O}_X(2D)) \otimes \Gamma(U, \pi_*\mathscr{O}_X(D)) \twoheadrightarrow \Gamma(U, \pi_*\mathscr{O}_X(3D))$$

is surjective due to Proposition 4.1.12. Since the domain is $R\left\langle x^2, xz, z^2, y\right\rangle \otimes R\left\langle x, z\right\rangle$, we see by inspection that this map factors through a map

$$R\left\langle x^3, x^2z, xz^2, xy, z^3, zy\right\rangle \longrightarrow \Gamma(U, \pi_*\mathscr{O}_X(3D))$$

which is moreover necessarily a surjection. At the same time, Lemma 4.1.10 tells us that $\pi_*\mathscr{O}_X(3D)$ is a rank 6 vector bundle on U, so the above is a surjection of equal rank projective R-modules, and hence an isomorphism. A similar argument shows that

$$R\left\langle x^4, x^3z, x^2z^2, xz^3, z^4, x^2y, xzy, z^2y\right\rangle \xrightarrow{\sim} \Gamma(U, \pi_*\mathscr{O}_X(4D)).$$

Since we have $y^2 \in \Gamma(U, \pi_*\mathscr{O}_X(4D))$ as well, there must be some relation of the form

$$y^2 + (ux^2 + vxz + wz^2)y = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4 \tag{4.7}$$

with $u, v, w, a, b, c, d, e \in R$.

Now, a straightforward induction argument using logic as above shows that the natural map

$$B_n := \bigoplus_{a+2b=n} \left(\operatorname{Sym}^a \Gamma(U, \pi_*\mathscr{O}_X(D)) \otimes Ry^b\right) \longrightarrow \Gamma(U, \pi_*\mathscr{O}_X(nD)) =: A_n$$

is surjective for all $n \geq 0$. Thus, letting $\mathscr{B} := \bigoplus_{n\geq 0} B_n$ and $\mathscr{A} = \bigoplus_{n\geq 0} A_n$, the natural surjection $\mathscr{B} \twoheadrightarrow \mathscr{A}$ of graded R-algebras gives rise to a closed embedding

$$H = \operatorname{Proj} \mathscr{A} \hookrightarrow \operatorname{Proj} \mathscr{B} \simeq \mathbb{P}(1,2,1)_U$$

upon taking Proj. Above, $\operatorname{Proj} \mathscr{B} \simeq \mathbb{P}(1,2,1)_U$ since it is easy to check that the natural graded map

$$R[X,Y,Z] \longrightarrow \mathscr{B} \text{ sending } X \mapsto x, Y \mapsto y, Z \mapsto z$$

(in particular, X, Z are degree 1, while Y is degree 2) is an isomorphism, e.g. since it is visibly surjective and its graded pieces have the same rank. Combining this observation with the relation (4.7), we see that we have a natural surjection

$$\frac{R[X,Y,Z]}{(Y^2 + (uX^2 + vXZ + wZ^2)Y - (aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4))} \overset{\sim}{\twoheadrightarrow} \mathscr{A}$$

which is once more an isomorphism as both sides have nth graded piece of rank $2n$. This exactly says that $H = \operatorname{Proj} \mathscr{A}$ is the subscheme of $\mathbb{P}(1,2,1)_U$ cut out by an equation of the form (4.6), as desired.

Finally, in the case that X is hyper-Weierstrass, we have $X \simeq H = \operatorname{Proj} \mathscr{A}$ by [Sta21, Tag 01Q1] (+ X being proper) since $D \subset X$ is relatively ample. ∎

Among other things, Theorem 4.1.16 describes a local model (4.6) for hyper-Weierstrass curves. We now establish a converse by showing that hyper-Weierstrass curves are exactly those with such a local model.

Theorem 4.1.17. *Let $H \xrightarrow{\pi} B$ be a B-scheme equipped with a closed subscheme $D \subset H$ satisfying the following property: Every point of B has an affine neighborhood $U = \operatorname{Spec} R$ above which $H_U \to U$ becomes isomorphic to a subscheme of $\mathbb{P}(1,2,1)$ defined by an equation of the form (4.6) such that $D_U \subset H_U$ is the subscheme $\{Z = 0\}$. Then, $(H \xrightarrow{\pi} B, D) \in \mathcal{H}(B)$.*

Proof. Every part of Definition 4.1.2 is local on the base, so we may and do assume that $B = \operatorname{Spec} R$ is affine, that

$$H = \left\{Y^2 + (uX^2 + vXZ + wZ^2)Y = aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4\right\} \subset \mathbb{P}(1,2,1)_R$$

(for some $u, v, w, a, b, c, d, e \in R$), and that $D = \{Z = 0\} \subset H$. Note H is visibly proper and finitely presented over R. We first show that H is flat over R. Note that it is covered by the open sets $\{X \neq 0\}$ and $\{Z \neq 0\}$. By symmetry, to show that it is flat over R, it suffices to show that

$$A := \frac{R[x,y]}{(f(x,y))} \text{ where } f(x,y) = y^2 + (ux^2 + vx + w)y - (ax^4 + bx^3 + cx^2 + dx + e)$$

is a flat R-module. This is the case simply because $A \cong R[x] \oplus R[x]y \cong R[x]^{\oplus 2}$ as an R-module, and $R[x]$ is R-flat.

We next show that the fibers of π are Gorenstein curves with trivial dualizing sheaves. For any $b \in B$, we simply note that the open subset $\{X \neq 0\} \cup \{Z \neq 0\} \subset \mathbb{P}(1,2,1)_{\kappa(b)}$ is a regular scheme containing H_b, so H_b is a local complete intersection, and hence a Gorenstein, 1-dimensional scheme. In particular, each H_b is a 'weighted hypersurface of degree 4' in the sense of [Dol82], so [Dol82, Theorem 3.3.4] (see Corollary B.3) tells us that $\omega_H \cong \mathscr{O}_H$. Furthermore, from our explicit description of $H_b \hookrightarrow \mathbb{P}(1,2,1)_{\kappa(b)}$, one can show that $\mathrm{H}^0(H_b, \mathscr{O}_{H_b}) = \kappa(b)$, e.g. by computing Čech cohomology with respect to the affine open covering $\{X \neq 0\} \cup \{Z \neq 0\} = H_b$. Thus, Lemma A.3 tells us that $\pi_*\mathscr{O}_H = \mathscr{O}_B$ holds after arbitrary base change, and that $\omega_{H/B} \in \pi^* \operatorname{Pic}(B)$.

What remains is to show that $D \subset X/B$ is a relatively ample effective Cartier divisor of degree 2 over B. Since $D = \{Z = 0\} \subset H$, it is certainly an effective Cartier divisor on H. Furthermore, D is flat over B by essentially the same argument used to show that H is flat over B, so D is in fact an effective relative Cartier divisor over B. As $D \subset \{X \neq 0\} \subset H$, we see that for any $b \in B$

$$D_b \simeq \operatorname{Spec} \frac{\kappa(b)[y]}{(y^2 + uy - a)}$$

is a degree 2 scheme, so D is of degree 2. Finally, $\mathscr{O}_H(D) \simeq \mathscr{O}_H(1) := \mathscr{O}_{\mathbb{P}(1,2,1)}(1)|_H$ is indeed a relatively ample line bundle over B. ■

Corollary 4.1.18. *Let $(X \to B, D)$ be a hawc. Then,*

$$H := \mathbf{Proj}_B \left(\bigoplus_{n \geq 0} \pi_* \mathscr{O}_X(nD) \right)$$

equipped with the scheme-theoretic image of D under the natural map $X \to H$ is a hyper-Weierstrass curve over B such that $\mathscr{O}_H(1) \simeq \mathscr{O}_H(D)$.

Proof. Combine Theorems 4.1.16 and 4.1.17. ■

Finally, for later use in the proof of Proposition 4.2.21, we prove

Proposition 4.1.19. *Let F be a field, and let (C, D) be a hawc over F. Let $S := \bigoplus_{n \geq 0} \mathrm{H}^0(C, \mathscr{O}_C(nD))$ and $X := \operatorname{Proj} S$. Consider the natural morphism $p : C \to X$ induced by the identity map $S = \bigoplus_{n \geq 0} \mathrm{H}^0(C, \mathscr{O}_C(nD))$ via [Sta21, Tag 01N8] with $d = 1$; in applying this citation, we use Lemma 4.1.7 to know that $\mathscr{O}_C(D)$ is generated by global sections. Then,*

- ***(a)*** *The locus $U_1 := \bigoplus_{f \in S_1} D_+(f)$ referenced in the citation is all of X. Consequently, the citation gives an isomorphism $\alpha : p^* \mathscr{O}_X(1) \xrightarrow{\sim} \mathscr{O}_C(D)$.*
- ***(b)*** *The induced maps $\mathrm{H}^0(X, \mathscr{O}_X(n)) \to \mathrm{H}^0(C, \mathscr{O}_C(nD))$ are isomorphisms for all $n \geq 1$.*
- ***(c)*** *The accompanying map $\mathscr{O}_X \to p_* \mathscr{O}_C$ is an isomorphism of sheaves.*
- ***(d)*** *The induced map $\mathrm{H}^0(C, \omega_C) \to \mathrm{H}^0(X, \omega_X)$, dual to $\mathrm{H}^1(X, \mathscr{O}_X) \to \mathrm{H}^1(C, \mathscr{O}_C)$, is an isomorphism.*

Proof. First, let $D_X \subset X$ be the scheme-theoretic image of $D \subset C$ under $p : C \to X$. Note that Corollary 4.1.18 tells us that $(XFk, D_X) \in \mathcal{H}(\operatorname{Spec} F)$ is an hW curve with $\mathscr{O}_X(D_X) \simeq \mathscr{O}_X(1)$. In particular, by applying Lemma 4.1.7 twice,

$$h^0(X, \mathscr{O}_X(n)) = h^0(X, \mathscr{O}_X(nD_X)) = 2n = h^0(C, \mathscr{O}_C(nD)) \text{ for all } n \geq 1.$$

Similarly, we have $h^0(X, \mathscr{O}_X) = 1 = h^0(C, \mathscr{O}_C)$ by assumption on C and since X is hyper-Weierstrass over k. Hence, $h^0(X, \mathscr{O}_X(n)) = h^0(C, \mathscr{O}_C(nD))$ for all $n \geq 0$.

(a) We first show that X is covered by distinguished affines coming from elements in degree 1, i.e. that $X = U_1$. Theorem 4.1.16 gives an embedding $X \hookrightarrow \mathbb{P}(1, 2, 1)_k \simeq \operatorname{Proj} k[X, Y, Z]$, with X, Z in degree 1 and Y in degree 2, so that X is cut out by an equation of the form (4.6). Consequently, $X = D_+(X) \cup D_+(Z) \subset U_1 \subset X$, so $X = U_1$ as claimed. [Sta21, Tag 01N8] then tells us that $p^* \mathscr{O}_X(1) \simeq \mathscr{O}_C(D)$.

(b) By taking powers, $p^* \mathscr{O}_X(n) \simeq \mathscr{O}_C(nD)$ for all $n \in \mathbb{Z}$. We tensor the map $\mathscr{O}_X \to p_* \mathscr{O}_C$ with $\mathscr{O}_X(n)$, apply the projection formula, and then apply this isomorphism $p^* \mathscr{O}_X(n) \simeq \mathscr{O}_C(nD)$ in order to obtain

$$\mathscr{O}_X(n) \longrightarrow p_* \mathscr{O}_C \otimes \mathscr{O}_X(n) \simeq p_*(\mathscr{O}_C \otimes p^* \mathscr{O}_X(n)) \simeq p_* \mathscr{O}_C(nD). \tag{4.8}$$

Taking global section, we obtain a map

$$\Gamma(X, \mathscr{O}_X(n)) \longrightarrow \Gamma(C, \mathscr{O}_C(nD))$$

for all $n \geq 0$, which is furthermore surjective as [Sta21, Tag 01N8] shows it fits in a commutative diagram

$$\begin{tikzcd} S_n \arrow[r] \arrow[rr, bend left, "\mathrm{id}"] & \Gamma(X, \mathscr{O}_X(n)) \arrow[r] & \Gamma(C, \mathscr{O}_C(nD)). \end{tikzcd}$$

We proved earlier that $\dim_F \Gamma(X, \mathscr{O}_X(n)) = \dim_F \Gamma(C, \mathscr{O}_C(nD))$, so we in fact have isomorphisms $\Gamma(X, \mathscr{O}_X(n)) \xrightarrow{\sim} \Gamma(C, \mathscr{O}_C(nD))$ for all $n \geq 0$.

(c) To show that the induced map $\mathscr{O}_X \to p_*\mathscr{O}_C$ is an isomorphism. we simply observe that **(b)** tells us that (4.8) induces the following isomorphism of coherent sheaves on $X = \operatorname{Proj} S$ (see [Sta21, Tag 0AG5] for the outer isomorphisms)

$$\mathscr{O}_X \simeq \left(\bigoplus_{n\geq 0} \Gamma(X, \mathscr{O}_X(n))\right)^{\sim} \xrightarrow{\sim} \left(\bigoplus_{n\geq 0} \Gamma(X, p_*\mathscr{O}_C \otimes \mathscr{O}_X(n))\right)^{\sim} \simeq p_*\mathscr{O}_C.$$

(d) Finally, we will show that p induces an isomorphism $\mathrm{H}^0(C, \omega_C) \xrightarrow{\sim} \mathrm{H}^0(X, \omega_X)$. The Leray spectral sequence $\mathrm{H}^p(X, R^q p_*\mathscr{O}_C) \implies \mathrm{H}^{p+q}(C, \mathscr{O}_C)$ gives an embedding $\mathrm{H}^1(X, p_*\mathscr{O}_C) \hookrightarrow \mathrm{H}^1(C, \mathscr{O}_C)$. By **(c)**, this is $\mathrm{H}^1(X, \mathscr{O}_X) \hookrightarrow \mathrm{H}^1(C, \mathscr{O}_C)$. The dual of this is a surjection $\mathrm{H}^0(C, \omega_C) \twoheadrightarrow \mathrm{H}^0(X, \omega_X)$. $\mathrm{H}^0(C, \omega_C) = \mathrm{H}^0(C, \mathscr{O}_C) = k$ by assumption on C and similarly $\mathrm{H}^0(X, \omega_X) = \mathrm{H}^0(X, \mathscr{O}_X) = k$ since X is hyper-Weierstrass over k, so we conclude that $\mathrm{H}^0(C, \omega_C) \overset{\sim}{\twoheadrightarrow} \mathrm{H}^0(X, \omega_X)$ is in fact an isomorphism. ■

4.2 Connection to 2-Selmer

Throughout this section, We work in the context of Setup 1.1. In particular, k is a finite field, and (unless otherwise stated) B is a smooth k-curve of genus g with function field $K = k(B)$.

4.2.1 Selmer Groupoid

We want to reduce counting Selmer elements to counting hyper-Weierstrass curves. In either case, when counting these objects, we do so in a weighted fashion, e.g. for E an elliptic curve, we will count some $\alpha \in \mathrm{Sel}_2(E)$ with weight $1/\#\operatorname{Aut}(E)$. Thus, these Selmer elements are best thought of as belong not to some set, but instead to some groupoid. With that in mind, we take a moment to set up this language before formally relating 2-Selmer elements to hyper-Weierstrass curves.

The following definition is inspired by Remark 4.1.1.

Definition 4.2.1. Fix an integer $n \geq 1$. The `n-Selmer groupoid` (over K) is the groupoid whose

- objects are tuples (C, E, ρ, D) where
  - E/K is an elliptic curve.
  - C/K is a locally solvable genus 1 curve.
  - $\rho : C \times E \to C$ is a group action making C into an E-torsor.
    We will write $c \cdot x := \rho(c, x)$ when $c \in C(S)$ and $x \in E(S)$ for any K-scheme S.
  - $D \subset C$ is a degree n effective divisor, defined over K.
- (iso)morphisms $(C, E, \rho, D) \to (C', E', \rho', D')$ are pairs $\left(\varphi : C \xrightarrow{\sim} C', \psi : E \xrightarrow{\sim} E'\right)$ where

– ψ is an isomorphism of K-group schemes.
– $\varphi(c \cdot x) = \varphi(c) \cdot \psi(x)$ for all $c \in C, x \in E$.[2]
– $\varphi^* \mathscr{O}_{C'}(D') \simeq \mathscr{O}_C(D)$.

We denote this groupoid by $\mathcal{S}el_n = \mathcal{S}el_{n,K}$. Given, any $(C, E, \rho, D) \in \mathcal{S}el_n$, we define its `height` to be the height of E, i.e. $\mathrm{ht}(C, E, \rho, D) := \mathrm{ht}(E)$. Furthermore, we say $(C, E, \rho, D) \in \mathcal{S}el_n$ is `trivial` if $D \sim nP$ for some $P \in C(K)$, i.e. if (C, D) represents the identity element of $\mathrm{Sel}_n(E)$. ⋄

Example 4.2.2. Say $(C, E, \rho, D) \in \mathcal{S}el_n$ is trivial, and choose $P \in C(K)$ such that $D \sim nP$. Let $O \in E(K)$ denote the identity element. Then, $(C, E, \rho, D) \simeq (E, E, \rho_E, nO)$, where $\rho_E : E \times E \to E$ is E's multiplication map. Indeed, one can $\varphi : C \xrightarrow{\sim} E$ to be the "subtract P" map defined by

$$P \cdot \varphi(c) = c \text{ for any } c \in C,$$

and can take $\psi = \mathrm{id}_E$. △

Remark 4.2.3. Let E/K be an elliptic curve, and let C/K be a locally solvable E-torsor. Then, $\mathrm{ht}(E) = \mathrm{ht}(C)$. One can see this, for example, in [dJ02, Section 5.12], which proves this when $B = \mathbb{P}^1$, but whose argument works for any B. ∘

Lemma 4.2.4. *Fix some $n \geq 1$ as well as some $(C, E, \rho, D) \in \mathcal{S}el_n$. Let $\alpha = [(C, D)] \in \mathrm{Sel}_n(E)$ be the corresponding Selmer element. Then, there is an exact sequence*

$$0 \longrightarrow E[n](K) \longrightarrow \mathrm{Aut}_{\mathcal{S}el_n}(C, E, \rho, D) \longrightarrow \mathrm{Stab}_{\mathrm{Aut}(E)}(\alpha) \longrightarrow 0,$$

where $\mathrm{Aut}(E) \curvearrowright \mathrm{Sel}_n(E)$ in the natural way.

Proof. Consider the map $f : \mathrm{Aut}_{\mathcal{S}el_n}(C, E, \rho, D) \to \mathrm{Aut}(E)$, $(\varphi, \psi) \mapsto \psi$. We will show that is has kernel $E[n](K)$ and image $\mathrm{Stab}_{\mathrm{Aut}(E)}(\alpha)$.

First say $(\varphi, \psi) \in \mathrm{Aut}(C, E, \rho, D)$ is an automorphism with $\psi = \mathrm{id}_E$. Then, $\varphi(c \cdot x) = \varphi(c) \cdot x$ for any $c \in C, x \in E$, so φ is an isomorphism of E-torsors. Thus, there is some $x_0 \in E(K)$ so that $\varphi(c) = c \cdot x_0$ for all $c \in C$. We claim that x_0 must be n-torsion. The action $\rho : C \times E \to C$ induces an isomorphism $f : E \xrightarrow{\sim} \underline{\mathrm{Pic}}^0_{C/K}$ so that E's action on C correspond to $\underline{\mathrm{Pic}}^0_{C/K}$'s natural action on $\underline{\mathrm{Pic}}^1_{C/K} \simeq C$ (coming from adding a degree 0 line bundle). Thus, φ acts on $\mathrm{Pic}^n_{C/K} \ni \mathscr{O}_C(D)$ via translation by nx_0. This action is trivial if and only if $x_0 \in E[n](K)$.

Fix some $\psi \in \mathrm{Aut}(E)$. When is ψ in the image of f? Well, consider some E-torsor structure $C_1 = (C, \rho_1)$ on C, by which we mean an action $\rho_1 : C \times E \to C$ making C into an E-torsor. Let $C_2 = (C, \rho_2)$ be another E-torsor structure on C. By definition, given an automorphism $\varphi : C \xrightarrow{\sim} C$, the pair $(\varphi, \psi) \in \mathrm{Aut}(C, E, \rho, D)$ if and only if $\varphi : C_1 \to C_2$ is an E-torsor map preserving $\mathscr{O}_C(D)$. Thus, $\psi \in \mathrm{im}(f)$ if and only if there exists such a φ if and only if (C_1, D) and (C_2, D) represent the same element of $\mathrm{H}^1(K, E[n])$. By construction, (C_2, D) represents the element $\psi^*[(C_1, D)]$, so we get the claimed description of $\mathrm{im}(f)$. ■

Remark 4.2.5. When $n = 2$, $\mathrm{H}^1(K, E[2])$ is 2-torsion, so $\{\pm 1\} \subset \mathrm{Stab}_{\mathrm{Aut}(E)}(C, E, \rho, D)$ always. Thus, Lemma 4.2.4 implies that we always have

$$\{\pm 1\} \subset \mathrm{im}(\mathrm{Aut}_{\mathcal{S}el_2}(C, E, \rho, D) \to \mathrm{Aut}(E)) \qquad \circ.$$

With $\mathcal{S}el_n$ introduced, recall the groupoid $\mathcal{H}(B)$ of hyper-Weierstrass curves over B (Definition 4.1.2). We are going to show that for every 2-Selmer element $(C, E, \rho, D) \in \mathcal{S}el_2$, there is some "nice" hW curve $(H/B, D_H) \in \mathcal{H}(B)$ whose generic fiber is (C, D). This will allow us to relate counting 2-Selmer elements to the problem of counting "nice" hW curves. We begin by making explicit what we mean by "nice".

[2] by which we really mean $c \in C(S)$ and $x \in E(S)$ for S any K-scheme

Definition 4.2.6. Let $(H \xrightarrow{f} B, D) \in \mathcal{H}(B)$ be an hW curve. We say that it is minimal if it's normal, its generic fiber is smooth, and it has at worst *rational singularities*, i.e. for some (equivalently, any) proper birational map $p : \mathcal{C} \to H$ with $\mathcal{C}$ regular, the sheaf $R^1 p_* \mathscr{O}_{\mathcal{C}}$ vanishes, see [Art86]. ◇

Remark 4.2.7. A Weierstrass model of an elliptic curve is minimal (in the usual sense) if and only if it has at worst rational singularities [Con05, Corollary 8.4]. ○

Warning 4.2.8. Even in good characteristics, the question of how many minimal hW models a given elliptic curve has is a subtle one, see e.g. [Sad11, Theorem 4.2]. •

Notation 4.2.9.

- Let $\mathcal{H}_M(B) \hookrightarrow \mathcal{H}(B)$ denote the full subgroupoid consisting of minimal hW curves.
- Let $\mathcal{H}_{M,NT}(B) \hookrightarrow \mathcal{H}_M(B)$ denote the full subgroupoid consisting of minimal hW curves $(H \xrightarrow{\pi} B, D)$ such that D_K is not twice a point (on the generic fiber).

  These curves will correspond to non-trivial Selmer elements.
- Let $\mathcal{H}_{LS}(B) \hookrightarrow \mathcal{H}_M(B)$ denote the full subgroupoid consisting of minimal hW curves $(H \to B, D)$ whose generic fiber H_K is locally solvable.
- Let $\mathcal{H}_{LS,NT}(B) \hookrightarrow \mathcal{H}_{LS}(B)$ denote the full subgroupoid $\mathcal{H}_{LS,NT}(B) = \mathcal{H}_{LS}(B) \cap \mathcal{H}_{M,NT}(B)$.

Notation 4.2.10. Given $d \in \mathbb{Z}$, we write $\mathcal{S}el_n^{\le d}, \mathcal{H}^{\le d}(B), \mathcal{H}_M^{\le d}(B)$, etc. to denote the corresponding full subgroupoid consisting of objects of height $\le d$. We similarly use a ${}^{=d}$ superscript to denote the full subgroupoid of objects of height $= d$.

Proposition 4.2.11 (To be proven in Section 4.2.2)**.** *There is an essentially surjective, faithful functor $F : \mathcal{H}_{LS}(B) \to \mathcal{S}el_2$ such that for every $\alpha \in \mathcal{S}el_2$, there exists some (minimal) $\beta \in \mathcal{H}_{LS}(B)$ satisfying $F(\beta) \simeq \alpha$ and $\operatorname{ht}(\beta) = \operatorname{ht}(\alpha)$. Furthermore, if α is non-trivial, then we may choose β lying in $\mathcal{H}_{LS,NT}(B)$.*

Accepting this proposition for now, let us explain its utility by giving an overview of the ultimate proof of Theorem B. Recall the quantity $\mathrm{AS}_B(d)$ defined in (1.2), and that our goal is to produce an upper bound for $\limsup_{d\to\infty} \mathrm{AS}_B(d)$. In place of $\mathrm{AS}_B(d)$, we will find it more convenient to study the following modified average size of 2-Selmer:

$$\mathrm{MAS}_B(d) := \frac{\#\,\mathcal{S}el_2^{\le d}}{\#\mathcal{M}_{1,1}^{\le d}(K)}. \tag{4.9}$$

In Section 7 (Propositions 7.2.4 and 7.2.5), we will show that

$$\limsup_{d\to\infty} \mathrm{AS}_B(d) \le \limsup_{d\to\infty} \mathrm{MAS}_B(d) \tag{4.10}$$

(though we in fact expect an equality above, see Remark 7.2.6). By Lemma 4.2.4 and Remark 4.2.5, the difference of the two sides of (4.10) is accounted for by elliptic curves with nontrivial 2-torsion or with extra automorphisms. Therefore, we will prove (4.10) by analyzing the contributions of such curves. Accepting (4.10) for now, we will be interested in bounding $\mathrm{MAS}_B(d)$. As Proposition 4.2.11 suggests, we will find it helpful to separately bound the contributions coming from trivial and non-trivial 2-Selmer elements.

Notation 4.2.12. Let $\mathcal{S}el_{2,T}$ (resp. $\mathcal{S}el_{2,NT}$) denote the full subgroupoid of $\mathcal{S}el_2$ consisting of trivial (resp. non-trivial) objects.

Note that $\#\,\mathcal{S}el_2^{\le d} = \#\,\mathcal{S}el_{2,T}^{\le d} + \#\,\mathcal{S}el_{2,NT}^{\le d}$. Let us separately analyze each summand.

- We begin with $\#\,\mathcal{S}el_{2,NT}^{\le d}$. This is the summand which makes use of Proposition 4.2.11.

Corollary 4.2.13 (of Proposition 4.2.11)**.** $\#\,\mathcal{S}el_{2,NT}^{\leq d} \leq \#\mathcal{H}_{LS,NT}^{\leq d}(B) \leq \#\mathcal{H}_{M,NT}^{\leq d}(B)$

Proof. The first inequality follows directly from Proposition 4.2.11. The second inequality holds simply because $\mathcal{H}_{LS,NT}^{\leq d}(B) \hookrightarrow \mathcal{H}_{M,NT}^{\leq d}(B)$ is a full subgroupoid. ■

As this corollary suggests, we will bound $\#\,\mathcal{S}el_{2,NT}^{\leq d}$ by bounding $\#\mathcal{H}_{M,NT}^{\leq d}$, that is, by counting hW curves. This count will be carried out in Section 5, culminating in Corollary 5.3.14, which says that

$$\limsup_{d\to\infty} \frac{\#\mathcal{H}_{M,NT}^{\leq d}(B)}{\#\mathcal{M}_{1,1}^{\leq d}(K)} \leq 2\zeta_B(2)\zeta_B(10). \tag{4.11}$$

- For the trivial Selmer elements, we use a separate argument. Note that (e.g. by Example 4.2.2)

$$\#\,\mathcal{S}el_{2,T}^{\leq d} = \sum_{\substack{E/K \\ \mathrm{ht}(E)\leq d}} \frac{1}{\#\,\mathrm{Aut}_{\mathcal{S}el_2}(E,E,\rho_E,2O)},$$

where, for an elliptic curve E/K, $\rho_E : E \times E \to E$ is the multiplication map, and $O \in E(K)$ is the identity element. By Lemma 4.2.4, there is a short exact sequence

$$0 \longrightarrow E[2](K) \longrightarrow \mathrm{Aut}_{\mathcal{S}el_2}(E,E,\rho_E,2O) \longrightarrow \mathrm{Aut}(E) \longrightarrow 0,$$

so $\#\,\mathrm{Aut}_{\mathcal{S}el_2}(E,E,\rho_E,2O) = \#E[2](K)\cdot\#\,\mathrm{Aut}(E)$. Consequently,

$$\#\,\mathcal{S}el_{2,T}^{\leq d} = \sum_{\substack{E/K \\ \mathrm{ht}(E)\leq d}} \frac{1}{\#E[2](K)\cdot\#\,\mathrm{Aut}(E)}. \tag{4.12}$$

In Section 7 (see Proposition 7.2.2), we will show that

$$\#\,\mathcal{S}el_{2,T}^{\leq d} = \sum_{\substack{E/K \\ \mathrm{ht}(E)\leq d}} \frac{1}{\#E[2](K)\cdot\#\,\mathrm{Aut}(E)} \sim \sum_{\substack{E/K \\ \mathrm{ht}(E)\leq d}} \frac{1}{\#\,\mathrm{Aut}(E)} = \#\mathcal{M}_{1,1}^{\leq d}(K). \tag{4.13}$$

Once we have established (4.10) in Section 7, (4.11) in Corollary 5.3.14, and (4.13) in Section 7, Theorem B (= Theorem 7.2.7) will immediately follow.

4.2.2 Proof of Proposition 4.2.11

We want to construct an essentially surjective, faithful functor

$$F : \mathcal{H}_{LS}(B) \to \mathcal{S}el_2$$

along with a choice of nice preimage for any object in $\mathcal{S}el_2$.

Construction 4.2.14. The desired functor F is defined on objects by

$$F(H \to B, D) := (H_K, \underline{\mathrm{Pic}}^0_{H_K}, \rho_{H_K}, D_K),$$

with the $_K$ subscript denoting the generic fiber, and $\rho_{H_K} : H_K \times \mathrm{Pic}^0_{H_K} \to H_K$ being the natural action (coming from identifying $H_K \xrightarrow{\sim} \mathrm{Pic}^1_{H_K}$). That this is functorial, i.e. defined on morphisms, comes from the fact that $\underline{\mathrm{Pic}}^0_{H_K}$ is the Albanese variety of H_K. Hence, any morphism $\varphi : (H/B, D) \to (H'/B, D')$ in $\mathcal{H}_{LS}(B)$ will induce a $\psi : \underline{\mathrm{Pic}}^0_{H_K} \to \underline{\mathrm{Pic}}^0_{H'_K}$ so that $(\varphi,\psi) : F(H/B,D) \to F(H'/B,D)$. ○

With F defined, to prove Proposition 4.2.11, we still need to construct nice preimages and show faithfulness. We begin with faithfulness.

Proposition 4.2.15. *For $(H \to B, D) \in \mathcal{H}_{LS}(B)$ with $(C, E, \rho, D) := F(X/B, D)$, the induced map*

$$F_* : \mathrm{Aut}_{\mathcal{H}(B)}(H \to B, D) \longrightarrow \mathrm{Aut}_{\mathcal{S}el_2}(C, E, \rho, D)$$

is injective. That is, $F : \mathcal{H}_{LS}(B) \to \mathcal{S}el_2$ is faithful.

Proof. Fix any hW automorphism $\varphi : H \xrightarrow{\sim} H$ such that $F_*(\varphi) = (\varphi_K, \psi)$ is the identity. Because $H \to B$ is flat with reduced generic fiber $H_K = C$, [Liu02, Proposition 4.3.8] tells us that H is reduced. Thus, H_K is schematically dense in H; hence, $\varphi_K = \mathrm{id}_{H_K} \implies \varphi = \mathrm{id}_H$. ■

essential surjectivity of F The proof that F is essentially surjective will occupy us for the next several pages. The rough idea is to first start with a Selmer element (C, D), consider the minimal proper regular model $\mathcal{C}/B$ of C, and then to extend D to a divisor $\mathcal{D}$ on $\mathcal{C}$. We will do this in such a way that the pair $(\mathcal{C}, \mathcal{D})$ becomes a hawc. Then, using Corollary 4.1.18, we can construct from this a particular hW model H/B of C. This H will be our choice of nice preimage. The bulk of the remainder of this section will be spent verifying H has all the properties claimed in the statement of Proposition 4.2.11.

Setup 4.2.16. Fix any $(C, E, \rho, D) \in \mathcal{S}el_2$. Let $\pi : \mathcal{C} \to B$ denote the minimal proper regular model of C, and let $\mathcal{D} \subset \mathcal{C}$ denote the scheme-theoretic closure of $D \subset C = \mathcal{C}_K \subset \mathcal{C}$. Note that $\mathcal{D}$ is a Cartier divisor because $\mathcal{C}$ is regular.

Lemma 4.2.17. *The pair $(\mathcal{C}, \mathcal{D})$ is a hawc over B. That is, $\mathcal{C}/B$ is a curve satisfying **(a)** $\pi_*\mathscr{O}_{\mathcal{C}} \simeq \mathscr{O}_B$, **(b)** $\omega_{\mathcal{C}/B} \in \pi^* \mathrm{Pic}(B)$, and **(c)** $\mathcal{D} \subset \mathcal{C}$ is an effective relative Cartier divisor of degree 2. In fact, $\omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{L}$, where $\mathscr{L} = \pi_*\omega_{\mathcal{C}/B} \in \mathrm{Pic}(B)$.*

Proof. It is clear that $\mathcal{C}$ is a curve over B.

(a,b) Because C has a K_v-point for every place v of K, [dJ02, Lemma 9.1] shows that **(a)**,**(b)** hold fiberwise, i.e. that

$$\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = \kappa(b) \text{ and } \omega_{\mathcal{C}_b} \simeq \mathscr{O}_{\mathcal{C}_b},$$

for every closed $b \in B$. By Lemma A.3, we conclude that $\mathscr{L} := \pi_*\omega_{\mathcal{C}/B}$ is a line bundle, and that

$$\pi_*\mathscr{O}_{\mathcal{C}} = \mathscr{O}_B \text{ and } \omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{L}$$

(both holding after arbitrary base change).

(c) Given the definition of $\mathcal{D}$, to prove that it is an effective *relative* Cartier divisor of degree 2, it suffices to show that it is flat over B. Thus, for any scheme point $d \in \mathcal{D}$, we need to show that the ring map $\mathscr{O}_{B,\pi(d)} \to \mathscr{O}_{\mathcal{D},d}$ is flat. Because B is a Dedekind scheme, this holds if and only if $\mathscr{O}_{\mathcal{D},d}$ is $\mathscr{O}_{B,\pi(d)}$-torsion-free. Note that, by definition, $\mathscr{O}_{\mathcal{D}} = \mathscr{O}_{\mathcal{C}}/\ker(\mathscr{O}_{\mathcal{C}} \to i_*\mathscr{O}_D)$, where $i : D \hookrightarrow \mathcal{C}$ is the natural inclusion. Hence, $\mathscr{O}_{\mathcal{D},d}$ is contained in the K-vector space $\mathscr{O}_D$, and so is certainly $\mathscr{O}_{B,\pi(d)}$-torsion-free (note $K = \mathrm{Frac}\,\mathscr{O}_{B,\pi(d)}$). ■

Now, let

$$H := \mathbf{Proj}_B\left(\bigoplus_{n\geq 0} \pi_*\mathscr{O}_{\mathcal{C}}(n\mathcal{D})\right) \xrightarrow{f} B,$$

and let $D_H \subset H$ be the scheme-theoretic image of $\mathcal{D}$ under the natural map $p : \mathcal{C} \to H$. Then, Lemma 4.2.17 and Corollary 4.1.18 together tells us that (H, D_H) is an hW curve over B.

Remark 4.2.18. Note that $H_K = \mathrm{Proj}\Big(\bigoplus_{n\geq 0} \mathrm{H}^0(C, \mathscr{O}_C(nD))\Big) = C$ because $D \subset C$ is ample. ◦

Remark 4.2.19. Let $\{F_i\}_{i\in I}$ be the (finite) set of fibral components $F_i \subset \mathcal{C}/B$ *not* meeting $\mathcal{D}$, and let $U := \mathcal{C} \setminus \bigcup_{i\in I} F_i \overset{\text{open}}{\subset} \mathcal{C}$. Then, $\mathcal{D} \subset U$ by definition, and

$$U \xrightarrow{p} p(U) \subset H$$

is an open immersion with dense image. Indeed, Lemma 4.1.15 proves this holds on each fiber over B. Thus, the fibral open immersion criterion [Gro67, Corollaire 17.9.5] says the same is true of p globally. In particular, $D_H \subset p(U) \subset X$ can alternatively be described as the pullback of $\mathcal{D} \subset U$ along the isomorphism $(p|_U)^{-1} : p(U) \xrightarrow{\sim} U$. ◦

Remark 4.2.20. We remark that H is normal. Indeed, H is Gorenstein because Theorem 4.1.16 shows that it is locally a hypersurface in $\mathbb{P}(1, 2, 1)$. Further, Remark 4.2.19 above shows that H is isomorphic to $\mathcal{C}$ away from a codimension 2 subset (the images of the fibral components F_i *not* meeting $\mathcal{D}$), so H is regular in codimension 1. Thus, H must be normal by Serre's criterion. ◦

At this point, it is clear that the (H, D_H) just constructed is an hW curve whose generic fiber is (C, D). To finish the proof of Proposition 4.2.11, we still need to prove the following:

- $\mathrm{ht}(H) = \mathrm{ht}(C, E, \rho, D) := \mathrm{ht}(E)$. By Remark 4.2.3, it is equivalent to prove that $\mathrm{ht}(H) = \mathrm{ht}(C) := \mathrm{ht}(\mathcal{C})$. We show this in Proposition 4.2.21.
- (H, D_H) is minimal in the sense of Definition 4.2.6. We show this in Corollary 4.2.22. Given this, it follows from definitions that if (C, E, ρ, D) is non-trivial, then $(H, D_H) \in \mathcal{H}_{LS,NT}(B)$.

Proposition 4.2.21. *The above constructed* $(H \xrightarrow{f} B, D_H)$ *satisfies both*

(1) $\pi_*\omega_{\mathcal{C}/B} \simeq f_*\omega_{H/B}$*; and*

(2) $\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \simeq f_*\mathscr{O}_H(D_H)$.

In particular, by ***(1)*** *above, the height of* X *equals the height of* $\mathcal{C}$.

Proof. **(1)** The Grothendieck spectral sequence $R^p f_*(R^q p_*\mathscr{O}_{\mathcal{C}}) \implies R^{p+q}\pi_*\mathscr{O}_{\mathcal{C}}$ gives us a morphism $R^1 f_*(p_*\mathscr{O}_{\mathcal{C}}) \to R^1\pi_*\mathscr{O}_{\mathcal{C}}$. Dualizing, and recalling also the map $\mathscr{O}_H \to p_*\mathscr{O}_{\mathcal{C}}$, below we define $\varphi : \pi_*\omega_{\mathcal{C}/B} \to f_*\omega_{H/B}$ as the composition

$$\pi_*\omega_{\mathcal{C}/B} \simeq \big(R^1\pi_*\mathscr{O}_{\mathcal{C}}\big)^\vee \to \big(R^1 f_*(p_*\mathscr{O}_{\mathcal{C}})\big)^\vee \to \big(R^1 f_*\mathscr{O}_H\big)^\vee \simeq f_*\omega_{H/B}.$$

For each $b \in B$, one has $\omega_{\mathcal{C}/B}|_{\mathcal{C}_b} = \omega_{\mathcal{C}_b}$ (and similarly for $\omega_{H/B}$) by [Sta21, Tag 0E6R], so one obtains a commutative diagram

$$\begin{tikzcd} \pi_*\omega_{\mathcal{C}/B} \otimes \kappa(b) \arrow[r, "\varphi_b"] \arrow[d] & f_*\omega_{X/B} \otimes \kappa(b) \arrow[d] \\ \mathrm{H}^0(\mathcal{C}_b, \omega_{\mathcal{C}_b}) \arrow[r, "\sim"] & \mathrm{H}^0(X_b, \omega_{X_b}) \end{tikzcd}$$

whose bottom horizontal map is an isomorphism by Proposition 4.1.19**(d)**. Furthermore, both vertical maps above are isomorphisms as well, e.g. by Lemma A.3. We also remark that $\pi_*\omega_{\mathcal{C}/B}, f_*\omega_{H/B}$ are both line bundles, e.g. by Lemma A.3. Hence, φ is a map of line bundles inducing isomorphisms on the fibers, and so itself an isomorphism.

(2) The argument that $\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \simeq f_*\mathscr{O}_H(D_H)$ is even simpler. It follows from Remark 4.2.19 that $\mathcal{D} = p^*D_H$. Hence, p induces a natural map $f_*\mathscr{O}_H(D_H) \to \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D})$. Since both sides of this map are vector bundles whose formations commute with arbitrary base change (e.g. by Lemma 4.1.10), this map is an isomorphism if and only if it is an isomorphism on fibers, and on fibers, this map is the isomorphism of Proposition 4.1.19**(b)**. ■

Corollary 4.2.22. *The above constructed* $(H \xrightarrow{f} B, D_H)$ *is minimal.*

Proof. Note that H is normal by Remark 4.2.20 and has smooth generic fiber by construction. Hence, it suffices to show that $R^1 p_* \mathscr{O}_{\mathcal{C}}$ vanishes. Because H is normal, [Art86, (3.3)] provides a short exact sequence

$$0 \longrightarrow p_*\omega_{\mathcal{C}/B} \longrightarrow \omega_{H/B} \longrightarrow \mathscr{E}xt^2_{\mathscr{O}_H}\left(R^1 p_* \mathscr{O}_{\mathcal{C}}, \omega_{H/B}\right) \longrightarrow 0.$$

As a consequence of Proposition 4.2.21**(1)**, $\omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{L}$ and $\omega_{H/B} \simeq f^*\mathscr{L}$ for the same $\mathscr{L} \in \mathrm{Pic}(B)$. Hence, $p_*\omega_{\mathcal{C}/B} \xrightarrow{\sim} \omega_{H/B}$, so $\mathscr{E}xt^2(R^1p_*\mathscr{O}_{\mathcal{C}}, \omega_{H/B}) = 0$. By [Art86, (1.5)], this means that $R^1 p_* \mathscr{O}_{\mathcal{C}} = 0$. ■

This completes the proof of Proposition 4.2.11.

4.3 A Geometric Lemma for Minimal hW Curves

For later use in Section 5.3, we now prove a technical lemma (Corollary 4.3.7) involving minimal hW curves. The reader is encouraged to skip this section for now, only returning to it when its results are needed.

Setup 4.3.1. We continue to work within the context of Setup 1.1. Let $(H \xrightarrow{f} B, D)$ be a minimal hW curve, and let $p : \mathcal{C} \to H$ be a minimal resolution of singularities (so $\mathcal{C}$ regular, and $\mathcal{C}_K \xrightarrow{\sim} H_K$). Let $\mathcal{D} := p^*D$, and let $\pi = f \circ p$. Thus, we have a commutative triangle

$$\begin{tikzcd} \mathcal{C} \arrow[rr, "p"] \arrow[dr, "\pi"'] & & H \arrow[dl, "f"] \\ & B. & \end{tikzcd}$$

Remark 4.3.2. We remark that $\mathcal{C}$ is the minimal proper regular model of its generic fiber $\mathcal{C}_K = H_K$. Indeed, [Art86, Proposition (5.1)] shows that $\omega_{\mathcal{C}/B} \simeq p^*\omega_{H/B}$, so $\omega_{\mathcal{C}/B} \simeq \pi^*(p_*\omega_{H/B})$ is fibral and hence minimality of $\mathcal{C}$ follows from [Liu02, Corollary 3.26]. ∘

Lemma 4.3.3. $p_*\omega_{\mathcal{C}/B} \simeq \omega_{H/B}$ *and* $p_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \simeq \mathscr{O}_H(D)$*. Consequently,* $\pi_*\omega_{\mathcal{C}/B} \simeq f_*\omega_{H/B}$ *and* $\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \simeq f_*\mathscr{O}_H(D)$*.*

Proof. Because H has rational singularities, the first of these follows from the short exact sequence $0 \to p_*\omega_{\mathcal{C}/B} \to \omega_{H/B} \to \mathscr{E}xt^2(R^1p_*\mathscr{O}_{\mathcal{C}}, \omega_{H/B}) \to 0$, [Art86, (3.3)]. For the second, we use the projection formula to compute

$$p_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \simeq p_*(\mathscr{O}_{\mathcal{C}} \otimes p^*\mathscr{O}_H(D)) \simeq p_*\mathscr{O}_{\mathcal{C}} \otimes \mathscr{O}_H(D) \simeq \mathscr{O}_H(D).$$ ■

In the below lemmas, we define the `degree` of a vector bundle $\mathscr{V}$ on a possibly singular curve Y/k to be $\deg \mathscr{V} := \deg(\nu^*\mathscr{V})$, where $\nu : \widetilde{Y} \to Y$ is its normalization. Note that Riemann-Roch tells us that $\deg \mathscr{V} = \chi(\mathscr{V}) - \mathrm{rank}(\mathscr{V})\chi(\mathscr{O}_Y)$.

Lemma 4.3.4. *Let* Y/k *be an irreducible curve equipped with a finite map* $f \colon Y \to B$*. Choose any* $\mathscr{M} \in \mathrm{Pic}(Y)$*. Then,*

$$\deg(f_*\mathscr{M}) = \deg(f_*\mathscr{O}_Y) + \deg \mathscr{M}.$$

Proof. Riemann-Roch on B, [Har77, Exercise III.4.1], and then Riemann-Roch on Y yields

$$\deg(f_*\mathscr{M}) - \deg(f_*\mathscr{O}_Y) = \chi(f_*\mathscr{M}) - \chi(f_*\mathscr{O}_Y) = \chi(\mathscr{M}) - \chi(\mathscr{O}_Y) = \deg \mathscr{M}.$$ ■

Lemma 4.3.5. *Let Y/k be an irreducible curve equipped with a finite map $f\colon Y \to B$. Let $\nu : \widetilde{Y} \to Y$ be its normalization. Then,*

$$\deg \omega_{Y/B} \geq \deg \omega_{\widetilde{Y}/B}.$$

Proof. [Kle80, Remark (26)(vii)] applied to the composition $\widetilde{Y} \to Y \to B$, and then to the composition $\widetilde{Y} \to Y \to \operatorname{Spec} K$ tells us that

$$\omega_{\widetilde{Y}/B} \otimes \left(\nu^*\omega_{Y/B}\right)^{-1} \simeq \omega_{\widetilde{Y}/Y} \simeq \omega_{\widetilde{Y}/k} \otimes \left(\nu^*\omega_{Y/k}\right)^{-1}.$$

Taking degrees, we see that

$$\deg \omega_{\widetilde{Y}/B} - \deg \omega_{Y/B} = \deg \omega_{\widetilde{Y}/Y} = \deg \omega_{\widetilde{Y}/k} - \deg \omega_{Y/k} = (2p_a(\widetilde{Y}) - 2) - (2p_a(Y) - 2) = 2(p_a(\widetilde{Y}) - p_a(Y)),$$

with the penultimate equality holding by Riemann-Roch for possibly singular curves (e.g [Har77, Exercise IV.1.9]). The claim now holds as $p_a(\widetilde{Y}) \geq p_a(Y)$. ∎

Proposition 4.3.6. *Use notation as in Setup 4.3.1. Suppose that $\mathcal{D} \subset \mathcal{C}$ is the closure of its generic fiber D_K. Let $\mathscr{E} := \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D})$, $\mathscr{L} := \pi_*\omega_{\mathcal{C}/B}$, and let $d := \deg \mathscr{L}$. Then, one of the following holds:*

(1) *$D_K = 2P$ for some $P \in \mathcal{C}(K)$. In this case ,$\det(\mathscr{E}) \simeq \mathscr{L}^{-2}$, so $\deg \mathscr{E} = -2d$.*

(2) *$\deg \mathscr{E} \geq -d$.*

(3) *$\operatorname{char} K = 2$, D_K is a closed point with residue field inseparable over K, and $\deg \mathscr{E} \geq 1 - (d + g)$.*

Proof. Keep in mind that $\mathscr{L} \simeq \left(R^1\pi_*\mathscr{O}_{\mathcal{C}}\right)^\vee$ by duality. To prove that one of **(1)**,**(2)**,**(3)** above holds, we break into cases depending on the form of the divisor $D_K \subset \mathcal{C}_K =: C$.

- Case 1: $D_K = P + Q$ for some (possibly equal) $P, Q \in C(K)$.

  Extend P, Q to sections $\mathcal{P}, \mathcal{Q} \in \mathcal{C}(B)$, respectively (so $\mathcal{D} = \mathcal{P} + \mathcal{Q}$). The exact sequence $0 \to \mathscr{O}_{\mathcal{C}} \to \mathscr{O}_{\mathcal{C}}(\mathcal{P}) \to \mathcal{O}_{\mathcal{P}}(\mathcal{P}) \to 0$ pushes forward to

  $$0 \longrightarrow \mathscr{O}_B \longrightarrow \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{P}) \longrightarrow \pi_*\mathcal{O}_{\mathcal{P}}(\mathcal{P}) \longrightarrow R^1\pi_*\mathscr{O}_{\mathcal{C}} \longrightarrow R^1\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{P}) = 0,$$

  with last equality holding by Lemmas 4.1.10 and 4.2.17. An easy cohomology and base change argument shows that every object above is a line bundle, so we quickly conclude that

  $$\pi_*\mathscr{O}_{\mathcal{P}}(\mathcal{P}) \xrightarrow{\sim} R^1\pi_*\mathscr{O}_{\mathcal{C}} \cong \mathscr{L}^{-1}, \text{ and so } \mathscr{O}_B \xrightarrow{\sim} \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{P}). \tag{4.14}$$

  By symmetry, the same is true with $\mathcal{Q}$ in place of $\mathcal{P}$. Note that π restricts to an isomorphism $\mathcal{P} \to B$, so π_* preserves tensor products of sheaves supported on $\mathcal{P}$. With this in mind, the exact sequence $0 \to \mathscr{O}_{\mathcal{C}}(\mathcal{Q}) \to \mathcal{O}_{\mathcal{C}}(\mathcal{D}) \to \mathcal{O}_{\mathcal{P}}(\mathcal{P} + \mathcal{Q}) \to 0$ pushes forward to

  $$0 \longrightarrow \mathscr{O}_B \longrightarrow \mathscr{E} \longrightarrow \pi_*\mathscr{O}_{\mathcal{P}}(\mathcal{P}) \otimes \pi_*\mathscr{O}_{\mathcal{P}}(\mathcal{Q}) \longrightarrow 0.$$

  If $\mathcal{Q} = \mathcal{P}$ (i.e. if $Q = P$, i.e. if $D_K = 2P$), then $\det \mathscr{E} \simeq \mathscr{L}^{-2}$ (recall (4.14)), which is **(a)** of the proposition. If $\mathcal{Q} \neq \mathcal{P}$, then $n := \deg \pi_*\mathcal{O}_{\mathcal{P}}(\mathcal{Q}) = \deg \mathcal{O}_{\mathcal{P}}(\mathcal{Q}) = \mathcal{P} \cdot \mathcal{Q} \geq 0$ (since it is the intersection number of distinct irreducible curves), so $\deg \mathscr{E} = n - d \geq -d$, which is **(b)** of the proposition.

- Case 2: D_K is a closed point with residue field L quadratic over K.

  The sequence $0 \to \mathscr{O}_{\mathcal{C}} \to \mathscr{O}_{\mathcal{C}}(\mathcal{D}) \to \mathscr{O}_{\mathcal{D}}(\mathcal{D}) \to 0$ pushes forward to

  $$0 \longrightarrow \mathscr{O}_B \longrightarrow \mathscr{E} \longrightarrow \pi_*\mathscr{O}_{\mathcal{D}}(\mathcal{D}) \longrightarrow \mathscr{L}^{-1} \longrightarrow 0.$$

Note $\pi_*\mathscr{O}_{\mathcal{D}}(\mathcal{D})$ is a vector bundle, as its the pushforward of a line bundle along a finite map of curves, so we can compute $\det \mathscr{E}$ by taking determinants above: $\det \mathscr{E} \simeq \det(\pi_*\mathscr{O}_{\mathcal{D}}(\mathcal{D})) \otimes \mathscr{L}$. Lemma 4.3.4 then gives

$$\deg \mathscr{E} = \deg \pi_*\mathscr{O}_{\mathcal{D}} + \deg \mathscr{O}_{\mathcal{D}}(\mathcal{D}) + \deg \mathscr{L} = \deg \pi_*\mathscr{O}_{\mathcal{D}} + \mathcal{D}\cdot\mathcal{D} + d. \tag{4.15}$$

We are now interested in computing $\det \pi_*\mathscr{O}_{\mathcal{D}}$. For this, we turn to the exact sequence $0 \to \mathscr{O}_{\mathcal{C}}(-\mathcal{D}) \to \mathcal{O}_{\mathcal{C}} \to \mathscr{O}_{\mathcal{D}} \to 0$, which pushes forward to

$$0 \longrightarrow \pi_*\mathscr{O}_{\mathcal{C}}(-\mathcal{D}) \longrightarrow \mathscr{O}_B \longrightarrow \pi_*\mathscr{O}_{\mathcal{D}} \longrightarrow R^1\pi_*\mathscr{O}_{\mathcal{C}}(-\mathcal{D}) \longrightarrow \mathscr{L}^{-1} \longrightarrow 0. \tag{4.16}$$

Note that, on each fiber, $\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}(-\mathcal{D}_b))$ is the subset of $\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b})$ vanishing along $\mathcal{D}_b$, but $\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = \kappa(b)$ by Lemma 4.2.17, so $\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}(-\mathcal{D}_b)) = 0$. Hence, Theorem A.1 implies that $\pi_*\mathscr{O}_{\mathcal{C}}(-\mathcal{D}) = 0$. By Lemma 4.2.17, $\omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{L}$, duality and the projection formula tell us that

$$R^1\pi_*\mathscr{O}_{\mathcal{C}}(-\mathcal{D}) \simeq \left[\pi_*\left(\mathscr{O}_{\mathcal{C}}(\mathcal{D}) \otimes \omega_{\mathcal{C}/B}\right)\right]^\vee \simeq \mathscr{E}^\vee \otimes \mathscr{L}^{-1}.$$

Hence, (4.16) becomes $0 \to \mathscr{O}_B \to \pi_*\mathscr{O}_{\mathcal{D}} \to \mathscr{E}^\vee \otimes \mathscr{L}^{-1} \to \mathscr{L}^{-1} \to 0$. Taking determinants (and using that $\operatorname{rank} \mathscr{E} = 2$), we have

$$\det \pi_*\mathscr{O}_{\mathcal{D}} \simeq \det(\mathscr{E})^{-1} \otimes \mathscr{L}^{-1}. \tag{4.17}$$

Combining (4.15) and (4.17),

$$\deg \mathscr{E} = \frac{1}{2}\mathcal{D}\cdot\mathcal{D} = \frac{1}{2}\deg \mathscr{O}_{\mathcal{D}}(\mathcal{D}).$$

Thus, it suffices to show that $\deg \mathscr{O}_{\mathcal{D}}(\mathcal{D})$ is either $\geq -2d$ or $\geq 2-2(g+d)$. Recalling that $\omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{L}$, we apply adjunction [Kle80, Corollary (19)] to $\mathcal{D} \hookrightarrow \mathcal{C}$, which tells us that

$$\omega_{\mathcal{D}/B} \simeq \omega_{\mathcal{C}/B}(\mathcal{D})|_{\mathcal{D}} \simeq (\pi^*\mathscr{L})\,|_{\mathcal{D}} \otimes \mathscr{O}_{\mathcal{D}}(\mathcal{D}).$$

Taking degrees, we see that

$$\deg \omega_{\mathcal{D}/B} = 2\deg \mathscr{L} + \mathcal{D}\cdot\mathcal{D} = 2d + \mathcal{D}\cdot\mathcal{D}. \tag{4.18}$$

Now, let $\widetilde{\mathcal{D}}$ be the normalization of $\mathcal{D}$. If $\mathcal{D} \to B$ is generically separable, then $\deg \omega_{\widetilde{\mathcal{D}}/B} \geq 0$ because it is the degree of the ramification divisor of $\widetilde{\mathcal{D}} \to B$ (e.g. by [Har77, Proposition IV.2.3]), so Lemma 4.3.5 and (4.18) tell us that

$$2d + \mathcal{D}\cdot\mathcal{D} = \deg \omega_{\mathcal{D}/B} \geq \deg \omega_{\widetilde{\mathcal{D}}/B} \geq 0, \text{ so } \mathcal{D}\cdot\mathcal{D} \geq -2d,$$

which is **(b)** of the proposition. Finally, if $\mathcal{D} \to B$ is generically inseparable, then $\widetilde{\mathcal{D}} \xrightarrow{f} B$ is Frobenius, so $g(\widetilde{\mathcal{D}}) = g(B)$, which means (by [Kle80, Remark (26)(vii)]) that

$$\deg \omega_{\widetilde{\mathcal{D}}/B} = \deg \omega_{\widetilde{\mathcal{D}}/k} - \deg f^*\omega_{B/k} = \deg \omega_{\widetilde{\mathcal{D}}/k} - 2\deg \omega_{B/k} = 2 - 2g.$$

Hence, Lemma 4.3.5 and (4.18) tell us that

$$2d + \mathcal{D}\cdot\mathcal{D} = \deg \omega_{\mathcal{D}/B} \geq \deg \omega_{\widetilde{\mathcal{D}}/B} = 2 - 2g \implies \mathcal{D}\cdot\mathcal{D} \geq 2 - 2(g+d),$$

which is **(c)** of the proposition. ∎

Corollary 4.3.7. *Use notation as in Setup 4.3.1. Let $\mathscr{E} := f_*\mathscr{O}_H(D)$, let $\mathscr{L} := \pi_*\omega_{\mathcal{C}/B}$, and let $d := \deg \mathscr{L}$. Assume that D_K is not twice a point. Then, $\deg \mathscr{E} \geq -(d+g)$. Furthermore, if $\operatorname{char} K \neq 2$, then $\deg \mathscr{E} \geq -d$.*

Proof. By Lemma 4.3.3, $\mathscr{L} \simeq \pi_*\omega_{\mathcal{C}/B}$ and $\mathscr{E} \simeq \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D})$. Write $\mathcal{D} = \mathcal{D}' + \mathcal{V}$, where $\mathcal{D}'$ is the closure of D_K in $\mathcal{C}$ and $\mathcal{V}$ is an effective vertical divisor. The exact sequence $0 \to \mathscr{O}_{\mathcal{C}}(\mathcal{D}') \to \mathscr{O}_{\mathcal{C}}(\mathcal{D}) \to \mathscr{O}_{\mathcal{V}}(\mathcal{D}) \to 0$ pushes forward to

$$0 \longrightarrow \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}') \longrightarrow \mathscr{E} \longrightarrow \pi_*\mathscr{O}_{\mathcal{V}}(\mathcal{D}) \longrightarrow 0 = R^1\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}'), \tag{4.19}$$

where the last equality holds by Lemma 4.1.10 (whose hypotheses are satisfied by combining Remark 4.3.2 and Lemma 4.2.17). Furthermore, $\pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}')$ is a rank 2 vector bundle by Lemma 4.1.10 while $\pi_*\mathscr{O}_{\mathcal{V}}(\mathcal{D})$ is a skyscraper sheaf supported on the (finite) image of $\mathcal{V}$ in B. Thus, taking Euler characteristics in (4.19) and applying Riemann-Roch shows that

$$\deg \mathscr{E} = \deg \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}') + h^0(\pi_*\mathscr{O}_{\mathcal{V}}(\mathcal{D})) \geq \deg \pi_*\mathscr{O}_{\mathcal{C}}(\mathcal{D}').$$

The claim follows from applying Proposition 4.3.6 to $\mathcal{D}'$, recalling that $(\mathcal{D}')_K = D_K$ is not twice a point. ■

5 An Upper Bound on the Cardinality of the 2-Selmer Groupoid

Recall, in the context of Setup 1.1, the function

$$\mathrm{MAS}_B(d) := \frac{\#\,\mathcal{S}el_2^{\leq d}}{\#\mathcal{M}_{1,1}^{\leq d}(K)}$$

introduced in (4.9). The main result of this section (Theorem 5.3.15) is that

$$\limsup_{d\to\infty} \mathrm{MAS}_B(d) \leq 1 + 2\zeta_B(2)\zeta_B(10).$$

In the sections after this one, we will show that $\limsup_{d\to\infty} \mathrm{AS}_B(d) \leq \limsup_{d\to\infty} \mathrm{MAS}_B(d)$, and so deduce Theorem B.

As in Section 3, we begin by studying "the form of the equation needed to cut out an hW curve over B."

5.1 Global Equations for hW Curves

Setup 5.1.1. Fix an arbitrary base scheme B.

Recall (Theorem 4.1.16) that an hW curve $(H \xrightarrow{\pi} B, D) \in \mathcal{H}(B)$ can locally (on B) be embedded into $\mathbb{P}(1,2,1)$. In this section, we globalize this result by embedding H into a $\mathbb{P}(1,2,1)$-bundle $\mathbb{P}$ over B and then studying the line bundle $\mathscr{O}_{\mathbb{P}}(H)$ (see Propositions 5.1.11 and 5.1.14). The proof of Theorem 4.1.16 suggests that H should embed into a $\mathbb{P}(1,2,1)$-bundle whose homogeneous coordinate ring is generated, as a graded $\mathscr{O}_B$-algebra, by $\pi_*\mathscr{O}_H(D)$ (in degree 1) and $\pi_*\mathscr{O}_H(2D)$ (in degree 2). Inspired by this, we make the following definition.

Definition 5.1.2. Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a tuple consisting of

- a rank 2 vector bundle $\mathscr{E}_1$ on B,
- a rank 4 vector bundle $\mathscr{E}_2$ on B, and
- a monomorphism $\mu : \mathrm{Sym}^2(\mathscr{E}_1) \hookrightarrow \mathscr{E}_2$ whose cokernel is a line bundle.

We call such a tuple a `(1,2,1)-datum` (over B) as it will allow us to define a $\mathbb{P}(1,2,1)$-bundle over B (see Lemma 5.1.6). We say $\mathbf{D}$ is `isomorphic to another (1,2,1)-datum` $(\mathscr{V}_1, \mathscr{V}_2, \nu)$ is there exists a line bundle

$\mathscr{M} \in \mathrm{Pic}(B)$ and isomorphisms $\varphi : \mathscr{E}_1 \otimes \mathscr{M} \xrightarrow{\sim} \mathscr{V}_1$ and $\psi : \mathscr{E}_2 \otimes \mathscr{M}^2 \to \mathscr{V}_2$ such that

$$\begin{tikzcd} \mathrm{Sym}^2(\mathscr{E}_1 \otimes \mathscr{M}) \arrow[r, "\mu_{\mathscr{M}}"] \arrow[d, "\mathrm{Sym}^2(\varphi)"'] & \mathscr{E}_2 \otimes \mathscr{M}^2 \arrow[d, "\psi"] \\ \mathrm{Sym}^2(\mathscr{V}_1) \arrow[r, "\nu"] & \mathscr{V}_2 \end{tikzcd}$$

commutes, where $\mu_{\mathscr{M}}$ is the natural composition $\mathrm{Sym}^2(\mathscr{E}_1 \otimes \mathscr{M}) \simeq \mathrm{Sym}^2(\mathscr{E}_1) \otimes \mathscr{M}^2 \xrightarrow{\mu \otimes \mathrm{id}} \mathscr{E}_2 \otimes \mathscr{M}^2$. ⋄

Construction 5.1.3. Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum over B. Form the sheaf of graded $\mathscr{O}_B$-algebras $\mathscr{T}(\mathscr{E}_1, \mathscr{E}_2) := \mathrm{Sym}(\mathscr{E}_1 \oplus \mathscr{E}_2)$ graded by declaring $\mathscr{E}_1$,$\mathscr{E}_2$ to be in degrees 1,2, respectively, i.e.

$$\mathscr{T}(\mathscr{E}_1, \mathscr{E}_2)_n = \bigoplus_{a+2b=n} \mathrm{Sym}^a(\mathscr{E}_1) \otimes \mathrm{Sym}^b(\mathscr{E}_2)$$

for any $n \geq 0$. Let $\mathscr{I}(\mathscr{E}_1, \mathscr{E}_2, \mu) \subset \mathscr{T}(\mathscr{E}_1, \mathscr{E}_2)$ be the (graded) ideal sheaf generated by sections of the form $\alpha\beta - \mu(\alpha\beta)$ with α, β both local sections of $\mathscr{E}_1$. Finally, set

$$\mathscr{B}(\mathbf{D}) := \mathscr{B}(\mathscr{E}_1, \mathscr{E}_2, \mu) := \frac{\mathscr{T}(\mathscr{E}_1, \mathscr{E}_2)}{\mathscr{I}(\mathscr{E}_1, \mathscr{E}_2, \mu)} \text{ and } \mathbb{P}(\mathbf{D}) := \mathbf{Proj}_B\, \mathscr{B}(\mathbf{D}).$$ ○

Example 5.1.4. Say $(H \xrightarrow{\pi} B, D)$ is an hW curve. Then, by Lemma 4.1.10 and Proposition 4.1.12, the triple

$$\mathbf{D}(H/B, D) := (\pi_*\mathscr{O}_H(D), \pi_*\mathscr{O}_H(2D), \mu),$$

where $\mu : \mathrm{Sym}^2(\pi_*\mathscr{O}_H(D)) \to \pi_*\mathscr{O}_H(2D)$ is the natural multiplication map, is a (1,2,1)-datum, called the curve's `associated (1,2,1)-datum`. In this case, we write $\mathbb{P}(H/B, D) := \mathbb{P}(\mathbf{D}(H/B, D))$, and we similarly define $\mathscr{T}(H/B, D), \mathscr{I}(H/B, D)$, and $\mathscr{B}(H/B, D)$. △

Definition 5.1.5. Inspired by the above example, along with Proposition 4.1.12, given any (1,2,1)-datum $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$, we define its `Hodge bundle` to be $\mathscr{L} := \det(\mathscr{E}_1) \otimes \mathrm{coker}(\mu)^{-1}$. ⋄

Lemma 5.1.6. *Let $\mathbf{D} := (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum. Then,*

$$\mathbb{P}(\mathbf{D}) \xrightarrow{p} B$$

is a Zariski-locally trivial $\mathbb{P}(1, 2, 1)$-bundle over B.

Proof. We may assume without loss of generality that $\mathscr{E}_1 \simeq \mathscr{O}_B^{\oplus 2}$, $\mathscr{E}_2 \simeq \mathscr{O}_B^{\oplus 4}$, and $\mathrm{coker}(\mu) \simeq \mathscr{O}_B$ since these all hold Zariski locally on B. Let X, Z be a global basis for $\mathscr{E}_1$, and let $Y \in \Gamma(B, \mathscr{E}_2)$ restrict to a global basis for $\mathrm{coker}(\mu)$. Then,

$$\mathscr{T}(\mathscr{E}_1, \mathscr{E}_2) \simeq \mathscr{O}_B\left[X, Y, Z, \mu(X^2), \mu(XZ), \mu(Z^2)\right]$$

is a polynomial algebra with X, Z in degree 1, and $Y, \mu(X^2), \mu(XZ), \mu(Z^2)$ all in degree 2. Furthermore, the ideal $\mathscr{I}(\mathbf{D})$ is generated by

$$X^2 - \mu(X^2), XZ - \mu(XZ), Z^2 - \mu(Z^2),$$

so $\mathscr{B}(\mathbf{D}) \simeq \mathscr{O}_B[X, Y, Z]$ and $\mathbb{P}(\mathbf{D}) \simeq \mathbb{P}(1, 2, 1)_B$. ■

Remark 5.1.7. Let $\mathbf{D}$ be a (1,2,1)-datum. As a consequence of (the proof of) Lemma 5.1.6, we see that the rank of $\mathscr{B}(\mathbf{D})_n$ is equal to the number of (monic) degree n monomials in $\mathbb{Z}[X, Y, Z]$ where X, Z have degree 1 and Y has degree 2. We will see below (Lemma 5.1.8) that $\mathscr{B}(\mathbf{D})_n \simeq p_*\mathscr{O}_{\mathbb{P}(\mathbf{D})}(n)$, so this also computes the rank of $p_*\mathscr{O}_{\mathbb{P}(\mathbf{D})}(n)$. ◦

Lemma 5.1.8. *Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum over B, and consider $\mathbb{P} := \mathbb{P}(\mathbf{D}) \xrightarrow{p} B$. For any $n \geq 0$, the natural map*

$$\mathscr{B}(\mathbf{D})_n \longrightarrow p_*\mathscr{O}_{\mathbb{P}}(n)$$

is an isomorphism.

Proof. We will apply cohomology and base change, Theorem A.1. By Lemma B.4, $\mathrm{H}^1(\mathbb{P}_b, \mathscr{O}_{\mathbb{P}_b}(n)) = 0$ for all $b \in B$, so Theorem A.1**(0,2)** applied to $\mathscr{F} = \mathscr{O}_{\mathbb{P}}(n)$ with $i = 1$ shows that $R^1p_*\mathscr{O}_{\mathbb{P}}(n) = 0$ and that the comparison map

$$\varphi_b^0 : p_*\mathscr{O}_{\mathbb{P}}(n) \otimes \kappa(b) \longrightarrow \mathrm{H}^0(\mathbb{P}_b, \mathscr{O}_{\mathbb{P}^b}(n))$$

is surjective for all $b \in B$. Thus, a second application of Theorem A.1**(0,2)**, now to $\mathscr{F} = \mathscr{O}_{\mathbb{P}}(n)$ with $i = 0$, shows that $p_*\mathscr{O}_{\mathbb{P}}(n)$ is a locally free sheaf on B. Hence, one can check that the natural map $\mathscr{B}(\mathbf{D})_n \to p_*\mathscr{O}_{\mathbb{P}}(n)$ is an isomorphism by checking this on fibers, where it becomes the classical fact that $k[X, Y, Z]_n \xrightarrow{\sim} \mathrm{H}^0(\mathbb{P}(1, 2, 1), \mathscr{O}(n))$, see e.g. [Dol82, Theorem 1.4.1(i) and Notations 1.1]. ∎

Lemma 5.1.9. *Let $(H \xrightarrow{\pi} B, D) \in \mathcal{H}(B)$ be a hyper-Weierstrass curve. Then, there is a natural embedding*

$$H \hookrightarrow \mathbb{P}(H/B, D) =: \mathbb{P},$$

for which $\mathscr{O}_H(n) := \mathscr{O}_{\mathbb{P}}(n)|_H \simeq \mathscr{O}_H(nD)$ for all $n \geq 0$.

Proof. Since $D \subset H$ is relatively ample, $H \simeq \mathbf{Proj}_B \bigoplus_{n\geq 0} \pi_*\mathscr{O}_H(nD)$, and the claimed embedding comes from the natural morphism

$$\mathscr{B}(H/B, D) = \frac{\mathrm{Sym}^*(\pi_*\mathscr{O}_H(D) \oplus \pi_*\mathscr{O}_H(2D))}{\mathscr{I}(H/B, D)} \longrightarrow \bigoplus_{n\geq 0} \pi_*\mathscr{O}_H(nD)$$

(induced by the multiplication maps $\pi_*\mathscr{O}_H(D)^{\oplus a} \otimes \pi_*\mathscr{O}_H(2D)^{\oplus b} \longrightarrow \pi_*\mathscr{O}_H((a + 2b)D))$. This morphism is surjective (and so induces a closed embedding upon taking $\mathbf{Proj}_B$) because this was verified locally in the proof of Theorem 4.1.16. ∎

Lemma 5.1.9 provides us with an embedding of an hW curve H into some $\mathbb{P}(1, 2, 1)$-bundle $\mathbb{P}$. We now want to understand "the shape of the equation cutting out H," i.e. to understand the line bundle $\mathscr{O}_{\mathbb{P}}(H)$ supporting a section cutting out H, as well as its pushforward to B.

Lemma 5.1.10. *Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum, and let $\mathscr{Y} := \mathrm{coker}\big(\mu : \mathrm{Sym}^2(\mathscr{E}_1) \hookrightarrow \mathscr{E}_2\big)$. Then, there is a short exact sequence*

$$0 \longrightarrow \mathrm{Sym}^4(\mathscr{E}_1) \xrightarrow{\nu} \mathscr{B}(\mathbf{D})_4 \longrightarrow \mathscr{E}_2 \otimes \mathscr{Y} \longrightarrow 0. \tag{5.1}$$

Above, ν is the composition $\mathrm{Sym}^4(\mathscr{E}_1) \hookrightarrow \mathscr{T}(\mathscr{E}_1, \mathscr{E}_2)_4 \twoheadrightarrow \mathscr{B}(\mathbf{D})_4$.

Proof. We construct (5.1) locally, and then glue by observing that the locally constructed maps are independent of any choices. That being said, let $U \overset{\text{open}}{\subset} B$ be small enough that $\mathscr{E}_1|_U \cong \mathscr{O}_U^{\oplus 2}$ and $\mathscr{E}_2|_U \cong \mathscr{O}_U^{\oplus 4}$ (so then also $\mathscr{Y}|_U \cong \mathscr{O}_U$). Let $X, Z \in \Gamma(U, \mathscr{E}_1)$ be a basis for $\mathscr{E}_1|_U$, and choose $Y \in \Gamma(U, \mathscr{E}_2)$ so that $\mu(X^2), \mu(XZ), \mu(Z^2), Y$ form a basis for $\mathscr{E}_2|_U$. Let $\overline{Y} \in \Gamma(U, \mathscr{Y})$ be the image of Y. Then, it is not difficult to see that the images of

$$X^4 \quad X^3Z \quad X^2Z^2 \quad XZ^3 \quad Z^4 \quad X^2 \otimes Y \quad XZ \otimes Y \quad Z^2 \otimes Y \quad Y \otimes Y$$

under the quotient map $\mathscr{T}(\mathscr{E}_1, \mathscr{E}_2)_4 \twoheadrightarrow \mathscr{B}(\mathbf{D})_4$ form a basis over U. Define a map $\mathscr{B}(\mathbf{D})_4|_U \to \mathscr{E}_2|_U \otimes \mathscr{Y}|_U$ by sending

$$\begin{array}{rclcrcl} X^2 \otimes Y & \longmapsto & \mu(X^2) \otimes \overline{Y}, & \qquad & XZ \otimes Y & \longmapsto & \mu(XZ) \otimes \overline{Y}, \\ Z^2 \otimes Y & \longmapsto & \mu(Z^2) \otimes \overline{Y}, & & Y \otimes Y & \longmapsto & \overline{Y} \otimes \overline{Y}, \end{array}$$

and sending all other basis elements to 0. By construction, the kernel of this map is (isomorphic to) $\mathrm{Sym}^4(\mathscr{E}_1)|_U$, i.e. we have an exact sequence

$$0 \longrightarrow \mathrm{Sym}^4(\mathscr{E}_1)|_U \longrightarrow \mathscr{B}(\mathbf{D})_4|_U \longrightarrow \mathscr{E}_2|_U \otimes \mathscr{Y}|_U \longrightarrow 0$$

over U. Finally, one can check that the above maps are independent of the choice of $Y \in \Gamma(U, \mathscr{E}_2)$ making $\mu(X^2), \mu(XZ), \mu(Z^2), Y$ a basis for $\mathscr{E}_2|_U$ and are independent of the choice of basis $X, Z \in \Gamma(U, \mathscr{E}_1)$ for $\mathscr{E}_1|_U$. Therefore, the above short exact sequence globalizes to give the claimed sequence (5.1). ∎

Proposition 5.1.11. *Let $(H \xrightarrow{\pi} B, D) \in \mathcal{H}(B)$ be an hW curve, and consider the natural embedding $H \hookrightarrow \mathbb{P}(H/B, D) =: \mathbb{P}$, constructed in Lemma 5.1.9. Then, $H \hookrightarrow \mathbb{P}$ is a Cartier divisor, and so is the zero scheme of some global section of the line bundle $\mathscr{O}_{\mathbb{P}}(H)$. Furthermore, we compute this line bundle to be*

$$\mathscr{O}_{\mathbb{P}}(H) \simeq \mathscr{O}_{\mathbb{P}}(4) \otimes p^*(\mathscr{D}^{-2} \otimes \mathscr{L}^2) = p^*\left(\mathscr{D}^{-2} \otimes \mathscr{L}^2\right)(4),$$

where $\mathscr{D} := \det(\pi_* \mathscr{O}_H(D))$, $\mathscr{L} := \pi_* \omega_{H/B}$, and $p : \mathbb{P} \to B$ is the structure morphism. That is, we can view $H \hookrightarrow \mathbb{P}$ as being cut out by some global section of

$$p_* \mathscr{O}_{\mathbb{P}}(H) \simeq \mathscr{B}(H/B, D)_4 \otimes \mathscr{D}^{-2} \otimes \mathscr{L}^2.$$

Proof. Once we know $\mathscr{O}_{\mathbb{P}}(H) \simeq p^*\left(\mathscr{D}^{-2} \otimes \mathscr{L}^2\right)(4)$, the claimed computation of $p_* \mathscr{O}_{\mathbb{P}}(H)$ follows from the projection formula and Lemma 5.1.8.

We will find it more natural to instead directly compute the dual $\mathscr{O}_{\mathbb{P}}(-H)$. First note that $H \hookrightarrow \mathbb{P}$ is Cartier by Theorem 4.1.16, which shows that it is locally cut out by a single equation. That same theorem also shows that the fibers of $H \hookrightarrow \mathbb{P}$ (over B) are cut out by weighted degree 4 equations, so the line bundle $\mathscr{O}_{\mathbb{P}}(-H)(4)$ on $\mathbb{P}$ is trivial on each fiber. Thus, e.g. by [Vak23, Proposition 25.1.11], $\mathscr{O}_{\mathbb{P}}(-H)(4) \simeq p^* p_* \mathscr{O}_{\mathbb{P}}(-H)(4)$. Hence, it will suffice to compute that

$$p_* \mathscr{O}_{\mathbb{P}}(-H)(4) \simeq \mathscr{D}^2 \otimes \mathscr{L}^{-2}.$$

With this in mind, consider the exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}}(-H)(4) \longrightarrow \mathscr{O}_{\mathbb{P}}(4) \longrightarrow \mathscr{O}_H(4) \longrightarrow 0,$$

and push forward along p. We know that $\mathscr{O}_H(4) \simeq \mathscr{O}_H(4D)$ by Lemma 5.1.9, that $p_* \mathscr{O}_{\mathbb{P}}(4) \simeq \mathscr{B}(H/B, D)_4$ by Lemma 5.1.8, and that $R^1 p_* \mathscr{O}_{\mathbb{P}}(-H)(4) = 0$ by Theorem A.1 combined with Lemma B.4. Hence, we obtain

$$0 \longrightarrow p_* \mathscr{O}_{\mathbb{P}}(-H)(4) \longrightarrow \mathscr{B}(H/B, D)_4 \longrightarrow \pi_* \mathscr{O}_H(4D) \longrightarrow 0. \tag{5.2}$$

Because $\operatorname{rank} \mathscr{B}(H/B, D)_4 = 9$ (by Remark 5.1.7) and $\operatorname{rank} \pi_* \mathscr{O}_H(4D) = 8$ (by Lemma 4.1.10), the kernel $p_* \mathscr{O}_{\mathbb{P}}(-H)(4)$ above must be a line bundle, and so it can be computed by taking determinants. Corollary 4.1.13 tells us that

$$\det(\pi_* \mathscr{O}_H(4D)) \simeq \mathscr{D}^{16} \otimes \mathscr{L}^{-3} \quad \text{and} \quad \det(\pi_* \mathscr{O}_H(2D)) \simeq \mathscr{D}^4 \otimes \mathscr{L}^{-1}.$$

Taking determinants in the exact sequence (5.1) with $\mathscr{E}_1 = \pi_* \mathscr{O}_H(D)$ and $\mathscr{E}_2 = \pi_* \mathscr{O}_H(2D)$ (and note that

$\mathscr{Y} \simeq \mathscr{L}^{-1} \otimes \mathscr{D}$ by Proposition 4.1.12), one computes that $\det \mathscr{B}(H/B, D)_4 \simeq \mathscr{D}^{18} \otimes \mathscr{L}^{-5}$. Finally, taking determinants in (5.2) shows that $p_* \mathscr{O}_{\mathbb{P}}(-H)(4) \simeq \mathscr{D}^2 \otimes \mathscr{L}^{-2}$, proving the claim. ■

The last thing we want to take care of here is improving our understanding of the rank 9 vector bundle

$$p_* \mathscr{O}_{\mathbb{P}}(H) \simeq \mathscr{B}(H/B, D)_4 \otimes \mathscr{D}^{-2} \otimes \mathscr{L}^2$$

appearing in Proposition 5.1.11. We will do this by endowing it with a filtration, all of whose graded pieces are line bundles.

Definition 5.1.12. Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum. We say that $\mathbf{D}$ is `normalized` if either

(1) $\mathscr{E}_1$ has Harder-Narasimhan filtration of the form

$$0 \longrightarrow \mathscr{O}_B \longrightarrow \mathscr{E}_1 \longrightarrow \mathscr{D} \longrightarrow 0,$$

necessarily with $u := \deg \mathscr{D} < 0$. In this case, we call u the `unstable degree` of $\mathbf{D}$.

(2) $\mathscr{E}_1$ is semistable. In this case, we say $\mathbf{D}$ has `unstable degree` $u = 0$. ◇

The above definition was inspired by [HLHN14, Section 6.1], though our "unstable degree" is the negation of the one appearing there. This is to allow for easier application of Corollary 4.3.7 when we do the actual counting.

Lemma 5.1.13. *Every hW curve is isomorphic to one whose associated (1,2,1)-datum is normalized.*

Proof. Let $(H \xrightarrow{\pi} B, D)$ be an hW curve, and let $\mathscr{E}_1 := \pi_* \mathscr{O}_H(D)$. If $\mathscr{E}_1$ is semistable, then $\mathbf{D}(H/B, D)$ is already normalized. Hence, assume that $\mathscr{E}_1$ is unstable. Let $\mathscr{M} \hookrightarrow \mathscr{E}$ be a destabilizing line subbundle, so $\mathscr{O}_B$ is destabilizing line subbundle of $\mathscr{F} := \mathscr{E} \otimes \mathscr{M}^{-1}$. Let

$$S := \mathbf{Proj}_B \left(\bigoplus_{n \geq 0} \left(\pi_* \mathscr{O}_H(nD) \otimes \mathscr{M}^{-n} \right) \right) \xrightarrow{\rho} B,$$

and let $f : S \xrightarrow{\sim} H$ be the natural isomorphism [Sta21, Tag 02NB]. Let $\mathbb{P} := \mathbb{P}(H/B, D) \xrightarrow{p} B$ and consider its line bundle $p^*(\mathscr{M}^{-1})(1)$. By the projection formula and Lemma 5.1.8, $p_* p^*(\mathscr{M}^{-1})(1) \cong \mathscr{E} \otimes \mathscr{M}^{-1} = \mathscr{F}$; thus, $H^0(\mathbb{P}, p^*(\mathscr{M}^{-1})(1)) = H^0(B, \mathscr{F})$ is nonzero (recall $\mathscr{O}_B \hookrightarrow \mathscr{F}$). Embed $S \xrightarrow{f} H \hookrightarrow \mathbb{P}$, and let $E \subset S$ be the zero scheme of some nonzero section of $p^*(\mathscr{M}^{-1})(1)$. One can use Theorem 4.1.17 to show that $(S/B, E)$ is an hW curve over B. By construction, this hW is isomorphic to H and its associated (1,2,1)-datum is normalized. ■

Proposition 5.1.14. *Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum. Let $\mathscr{D} := \det(\mathscr{E}_1)$, and let $\mathscr{Y} := \operatorname{coker}(\mu)$. Then, there is a filtration $0 = \mathscr{F}_0 \subset \mathscr{F}_5 \subset \mathscr{F}_8 \subset \mathscr{F}_9 = \mathscr{B}(\mathbf{D})_4$ such that $\mathscr{F}_i$ is a rank i vector bundle on B, where*

$$\mathscr{F}_5 = \operatorname{Sym}^4(\mathscr{E}_1), \quad \frac{\mathscr{F}_8}{\mathscr{F}_5} \cong \operatorname{Sym}^2(\mathscr{E}_1) \otimes \mathscr{Y}, \quad \textit{and} \quad \frac{\mathscr{F}_9}{\mathscr{F}_8} \cong \mathscr{Y}^2.$$

Furthermore, if $\mathbf{D}$ is normalized with $\mathscr{E}_1$ unstable, then this filtration extends to a filtration

$$0 = \mathscr{F}_0 \subset \mathscr{F}_1 \subset \cdots \subset \mathscr{F}_8 \subset \mathscr{F}_9 = \mathscr{B}(\mathbf{D})_4$$

by vector bundles on B with graded pieces

$$\frac{\mathscr{F}_{i+1}}{\mathscr{F}_i} \cong \begin{cases} \mathscr{D}^i & \text{if } 0 \le i \le 4 \\ \mathscr{D}^{i-5} \otimes \mathscr{Y} & \text{if } 5 \le i \le 7 \\ \mathscr{Y}^2 & \text{if } i = 8. \end{cases}$$

Proof Sketch. This follows from the existence of the exact sequences

$$\begin{array}{ccccccccll} 0 & \longrightarrow & \mathrm{Sym}^4(\mathscr{E}_1) & \longrightarrow & \mathscr{B}(\mathbf{D})_4 & \longrightarrow & \mathscr{E}_2 \otimes \mathscr{Y} & \longrightarrow & 0 & \text{by Lemma 5.1.10;} \\ 0 & \longrightarrow & \mathrm{Sym}^2(\mathscr{E}_1) & \longrightarrow & \mathscr{E}_2 & \longrightarrow & \mathscr{Y} & \longrightarrow & 0 & \text{by definition of (1,2,1)-datum; and} \\ 0 & \longrightarrow & \mathscr{O}_B & \longrightarrow & \mathscr{E}_1 & \longrightarrow & \mathscr{D} & \longrightarrow & 0 & \text{if } \mathscr{E}_1 \text{ is unstable and } \mathbf{D} \text{ is normalized.} \end{array}$$ ■

Remark 5.1.15. Let $(H/B, D)$ be an hW curve with Hodge bundle $\mathscr{L}$. Suppose that $\pi_*\mathscr{O}_H(D)$ is unstable and that the (1,2,1)-datum $\mathbf{D}(H/B, D)$ is normalized. Let $\mathscr{D} := \det(\pi_*\mathscr{O}_H(D))$. If the filtration of Proposition 5.1.14 applied to $\mathbf{D}(H/B, D)$ splits, then $\mathbb{P} := \mathbb{P}(H/B, D)$ has global coordinates X, Y, Z with Y defined using the splitting of $0 \to \mathrm{Sym}^2(\mathscr{E}_1) \to \mathscr{E}_2 \to \mathscr{L}^{-1} \otimes \mathscr{D} \to 0$, and X, Z defined using the splitting of $0 \to \mathscr{O}_B \to \mathscr{E}_1 \to \mathscr{D} \to 0$ (analogously to Remark 3.1.11). Defined appropriately, these "global coordinates" X, Y, Z are sections

$$X \in \mathrm{H}^0\left(\mathbb{P}, p^*\left(\mathscr{O}_B^{-1}\right)(1)\right), \quad Y \in \mathrm{H}^0\left(\mathbb{P}, p^*\left(\mathscr{L} \otimes \mathscr{D}^{-1}\right)(2)\right), \quad \text{and} \quad Z \in \mathrm{H}^0\left(\mathbb{P}, p^*\left(\mathscr{D}^{-1}\right)(1)\right).$$

With this in mind, in this case, the vector bundle $p_*\mathscr{O}_{\mathbb{P}}(H)$ naturally splits as a sum of line bundles (compare Propositions 5.1.11 and 5.1.14), and $H \hookrightarrow \mathbb{P}$ can be described as the zero set of an equation

$$\lambda Y^2 + (a_0X^2 + a_1XZ + a_2Z^2)Y = c_0X^4 + c_1X^3Z + c_2X^2Z^2 + c_3XZ^3 + c_4Z^4$$

with $\lambda \in \mathrm{H}^0(B, \mathscr{O}_B)$, $a_i \in \mathrm{H}^0(B, \mathscr{D}^{i-1} \otimes \mathscr{L})$ and $c_j \in \mathrm{H}^0(B, \mathscr{D}^{j-2} \otimes \mathscr{L}^2)$. Furthermore, by comparing with the local equations of Theorem 4.1.16, we see that λ above must be nonzero, so after scaling, $H \hookrightarrow \mathbb{P}$ is cut out by an equation of the form

$$Y^2 + (a_0X^2 + a_1XZ + a_2Z^2)Y = c_0X^4 + c_1X^3Z + c_2X^2Z^2 + c_3XZ^3 + c_4Z^4, \tag{5.3}$$

akin to the Weierstrass equations of Definition 3.1.9. ○

5.2 Properly Embedded hW Curves

In order to count hW curves, we will partition them according to their (1,2,1)-data. To that end, we begin by fixing such a choice of datum and studying the hW curves which embed into the corresponding $\mathbb{P}(1,2,1)$-bundle.

Setup 5.2.1. We continue to let B denote an arbitrary base scheme. We also fix any choice of (1,2,1)-datum $\mathbf{D} := (\mathscr{E}_1, \mathscr{E}_2, \mu)$ over B. Finally, we write $\mathbb{P} := \mathbb{P}(\mathbf{D})$ and let $p : \mathbb{P} \to B$ denote its structure map.

Definition 5.2.2. We say that an hW curve $(H/B, D)$ equipped with an embedding $H \hookrightarrow \mathbb{P}$ is `properly embedded` if $\mathscr{O}_H(1) := \mathscr{O}_{\mathbb{P}}(1)|_H \simeq \mathscr{O}_H(D)$. ◇

Lemma 5.2.3. *Every hW curve is isomorphic to one which properly embeds into a $\mathbb{P}(\mathbf{D})$ with $\mathbf{D}$ normalized.*

Proof. This follows immediately from Lemmas 5.1.9 and 5.1.13. ■

Lemma 5.2.4. *Let $(H \xrightarrow{\pi} B, D)$ be an hW curve properly embedded in $\mathbb{P}$. Then, the natural map*

$$p_*\mathscr{O}_{\mathbb{P}}(n) \longrightarrow \pi_*\mathscr{O}_H(n) \simeq \pi_*\mathscr{O}_H(nD)$$

is surjective for all $n \in \mathbb{Z}$. Furthermore, it is an isomorphism for $n = 0, 1, 2, 3$.

Proof. Consider the exact sequence $0 \to \mathscr{O}_{\mathbb{P}}(-H)(n) \to \mathscr{O}_{\mathbb{P}}(n) \longrightarrow \mathscr{O}_H(n) \to 0$. By Lemma B.4 and the isomorphisms $\mathscr{O}_{\mathbb{P}}(-H)(n)_b \simeq \mathscr{O}_{\mathbb{P}(1,2,1)_{\kappa(b)}}(n-4)$, we have $\mathrm{H}^1(\mathbb{P}(1,2,1)_b, \mathscr{O}_{\mathbb{P}}(-H)(n)_b) = 0$ for all $b \in B$. Thus, Theorem A.1 tells us that $R^1p_*\mathscr{O}_{\mathbb{P}}(-H)(n) = 0$. Given this, our short exact sequence induces a surjection

$$p_*\mathscr{O}_{\mathbb{P}}(n) \twoheadrightarrow \pi_*\mathscr{O}_H(n) \simeq \pi_*\mathscr{O}_H(nD).$$

When $n \in \{0, 1, 2, 3\}$, $p_*\mathscr{O}_{\mathbb{P}}(n)$ and $\pi_*\mathscr{O}_H(n)$ are vector bundles of rank the same rank (by Remark 5.1.7 and Lemma 4.1.10), so this must be an isomorphism. ∎

Corollary 5.2.5. *An hW curve $(H/B, D)$ properly embeds into some $\mathbb{P}(\mathbf{D})$ for a unique, up to isomorphism, (1,2,1)-datum $\mathbf{D}$, necessarily $\mathbf{D} \cong \mathbf{D}(H/B, D)$.*

Lemma 5.2.6. *Let $(H \xrightarrow{\pi} B, D)$ and $(S \xrightarrow{\rho} B, E)$ be two hW curves properly embedded in $\mathbb{P}$. Let $f : H \xrightarrow{\sim} S$ be a hyper-Weierstrass isomorphism. Then, $f^*\mathscr{O}_S(nE) \simeq \mathscr{O}_H(nD)$ for all n.*

Proof. Since pullbacks commute with tensor products, it suffices to prove the claim when $n = 1$. By definition, there exists some $\mathscr{M} \in \mathrm{Pic}(B)$ such that $f^*\mathscr{O}_S(E) \simeq \mathscr{O}_H(D) \otimes \pi^*\mathscr{M}$. Pushing forwards along π, we see that $\rho_*\mathscr{O}_S(E) \simeq \pi_*\mathscr{O}_H(D) \otimes \mathscr{M}$. At the same time, Lemma 5.2.4 shows that $\pi_*\mathscr{O}_H(D) \simeq p_*\mathscr{O}_{\mathbb{P}}(1) \simeq \rho_*\mathscr{O}_S(E)$. Taken together, these two statements imply that $\mathscr{M} \simeq \mathscr{O}_B$, from which the claim follows. ∎

Notation 5.2.7. Let $G(\mathbf{D})$ denote the (abstract) group of pairs (φ, ψ) of automorphisms of $\mathscr{E}_1, \mathscr{E}_2$ which are compatible with multiplication, i.e.

$$G(\mathbf{D}) := \left\{ (\varphi,\psi) \in \mathrm{GL}(\mathscr{E}_1) \times \mathrm{GL}(\mathscr{E}_2) \;\middle|\; \begin{array}{ccc} \mathrm{Sym}^2(\mathscr{E}_1) & \xrightarrow{\mu} & \mathscr{E}_2 \\ {\scriptstyle \mathrm{Sym}^2(\varphi)}\downarrow & & \downarrow{\scriptstyle \psi} \\ \mathrm{Sym}^2(\mathscr{E}_1) & \xrightarrow{\mu} & \mathscr{E}_2 \end{array} \text{ commutes.} \right\}$$

We let $\mathbb{P}G := \mathbb{P}G(\mathbf{D})$ denote the quotient of $G(\mathbf{D})$ by the scalar subgroup $k^\times \hookrightarrow G(\mathbf{D}), \lambda \mapsto (\lambda, \lambda^2)$, where $k := \Gamma(B, \mathscr{O}_B)$.

Remark 5.2.8. If you imagine you have an hW curve $H \hookrightarrow \mathbb{P}(1,2,1)$ with degree 1 coordinates X, Z and degree 2 coordinate Y, then $\varphi : \mathscr{E}_1 \xrightarrow{\sim} \mathscr{E}_1$ as above corresponds to some linear change of variables $(X, Z) \rightsquigarrow (\alpha X + \beta Z, \gamma X + \delta Z)$ and the extension to $\psi : \mathscr{E}_2 \xrightarrow{\sim} \mathscr{E}_2$ corresponds to also choosing $Y \rightsquigarrow \lambda Y + rX^2 + sXZ + tZ^2$. ◦

Remark 5.2.9. We remark that $G(\mathbf{D})$ acts on $\mathbb{P}$. Indeed, elements of $G(\mathbf{D})$ induce (graded) automorphisms of the sheaf $\mathscr{B}(\mathbf{D})$ of graded $\mathscr{O}_B$-algebras (recall Construction 5.1.3), and so induce automorphisms of $\mathbb{P} \simeq \mathbf{Proj}_B\,\mathscr{B}(\mathbf{D})$. Furthermore, this action descends to one of $\mathbb{P}G$ on $\mathbb{P}$. ◦

Proposition 5.2.10. *Let $(H \xrightarrow{\pi} B, D)$ and $(S \xrightarrow{\rho} B, E)$ be two hyper-Weierstrass curves properly embedded in $\mathbb{P}$. Then, there is a natural isomorphism*

$$\mathrm{Hom}_{\mathcal{H}(B)}((H/B, D), (S/B, E)) \xrightarrow{\sim} \{g \in \mathbb{P}G : g(H) = S\}$$

(Above, '$g(H) = S$' means equality as subschemes of $\mathbb{P}$).

Proof. We simply construct maps in both directions.

($\to$) Let $f : H \xrightarrow{\sim} S$ be an hW isomorphism. Since H, X are both properly embedded in $\mathbb{P}$, Lemma 5.2.6 tells us that $f^*\mathscr{O}_S(nE) \simeq \mathscr{O}_H(nD)$ for any $n \in \mathbb{Z}$, so f induces isomorphisms

$$\alpha_n(f) : \rho_*\mathscr{O}_S(nE) \xrightarrow{\sim} \pi_*\mathscr{O}_H(nD).$$

At the same time, Lemma 5.2.4 tells us that the proper embeddings $H, S \hookrightarrow \mathbb{P}$ induce isomorphisms $\mathscr{E}_n = p_*\mathscr{O}_{\mathbb{P}}(n) \simeq \pi_*\mathscr{O}_H(nD)$ and $\mathscr{E}_n = p_*\mathscr{O}_{\mathbb{P}}(n) \simeq \rho_*\mathscr{O}_S(nE)$ when $n = 1, 2$. Composing these with $\alpha_n(f)$ then shows that f induces automorphisms

$$\varphi(f) : \mathscr{E}_1 \xrightarrow{\sim} \mathscr{E}_1 \text{ and } \psi(f) : \mathscr{E}_2 \xrightarrow{\sim} \mathscr{E}_2.$$

The map in one direction is $f \mapsto (\varphi(f), \psi(f))$.

($\leftarrow$) Fix some $g \in \mathbb{P}G$ carrying $H \hookrightarrow \mathbb{P}$ onto $G \hookrightarrow \mathbb{P}$. Then, by assumption, g give an isomorphism $f_g : H \xrightarrow{\sim} G$ over B. To see that is an hW isomorphism, we note that the action of $\mathbb{P}G$ on $\mathbb{P}$ preserves $\mathscr{O}_{\mathbb{P}}(1)$, so

$$f^*\mathscr{O}_S(E) \simeq f^*\mathscr{O}_S(1) \simeq \mathscr{O}_H(1) \simeq \mathscr{O}_H(D).$$

The assignment $g \mapsto f_g$ gives the inverse map. ∎

Let us now introduce/recall some notation. Let $0 = \mathscr{F}_0 \subset \cdots \subset \mathscr{F}_9 = \mathscr{B}(\mathbf{D})_4$ denote the filtration of Proposition 5.1.14. Let $\mathscr{Y} := \operatorname{coker}(\mu)$ and $\mathscr{D} := \det(\mathscr{E}_1)$ as usual, and let $\mathscr{L} := \mathscr{D} \otimes \mathscr{Y}^{-1}$ be the Hodge bundle of $\mathbf{D}$. Let $\mathscr{G}_i := \mathscr{F}_i \otimes \mathscr{L}^2 \otimes \mathscr{D}^{-2} \simeq \mathscr{F}_i \otimes \mathscr{Y}^{-2}$ for all i. Note in particular that

$$\mathscr{G}_9 = \mathscr{B}(\mathbf{D})_4 \otimes \mathscr{D}^{-2} \otimes \mathscr{L}^2 \text{ and } \mathscr{G}_9/\mathscr{G}_8 \simeq \mathscr{O}_B.$$

We next count the (weighted) number of hW curves properly embedded in $\mathbb{P} = \mathbb{P}(\mathbf{D})$, see Proposition 5.2.13.

Assumption. Assume from now on that $k := \Gamma(B, \mathscr{O}_B)$ is a field, and let $q := \#k$. This is not strictly necessary for what comes below, but it does simplify some statements.

Construction 5.2.11. Let $\mathcal{G}$ denote the groupoid whose objects are global sections $s \in \mathrm{H}^0(B, \mathscr{G}_9)$ *with nonzero image* in $\mathrm{H}^0(B, \mathscr{G}_9/\mathscr{G}_8)$, and whose Hom-sets are the transporters

$$\mathrm{Hom}_{\mathcal{G}}(s_1, s_2) := \{g \in G(\mathbf{D}) : g \cdot s_1 = s_2\}$$

where $G(\mathbf{D}) \curvearrowright \mathscr{G}_9$ via its action on $\mathbb{P}$.

Assume that $h^0(\mathscr{E}_1) > 0$, and implicitly fix a choice of nonzero section $\sigma_0 \in H^0(B, \mathscr{E}_1)$. Recall (Lemma 5.1.8) that $\mathscr{E}_1 \simeq p_*\mathscr{O}_{\mathbb{P}}(1)$. Let $L \subset \mathbb{P}$ denote the hyperplane cut out by $\sigma_0 \in \mathrm{H}^0(\mathbb{P}, \mathscr{O}_{\mathbb{P}}(1))$. There is a functor $F : \mathcal{G} \to \mathcal{H}(B)$ given on objects by $F(s) := (Z(s), D_s)$, with $Z(s) \hookrightarrow \mathbb{P}$ the zero scheme of s and $D_s := Z(s) \cap L$. That $F(s)$ is an hW curve over B can be deduced from Theorem 4.1.17. ○

Notation 5.2.12. Whenever we write

$$\sum_{H \hookrightarrow \mathbb{P}} (*),$$

we mean that the sum ranges over isomorphism classes of hW curves properly embedded in $\mathbb{P}$.

Proposition 5.2.13. *The weighted number of hW curves properly embedded in* $\mathbb{P} = \mathbb{P}(\mathbf{D})$ *is*

$$\sum_{H \hookrightarrow \mathbb{P}} \frac{1}{\#\,\mathrm{Aut}_{\mathcal{H}(B)}(H)} = \#\mathcal{G} \leq \frac{\#\,\mathrm{H}^0(B, \mathscr{G}_8)}{\#\mathbb{P}G},$$

with equality if the left hand side is nonzero. As indicated in Notation 5.2.12, the sum above ranges over isomorphism classes of hW curves properly embedded in $\mathbb{P}$.

Proof. Suppose the left hand side is nonzero, i.e. that there exists some hW curve properly embedded in $\mathbb{P}$. Note that this forces $h^0(\mathscr{E}_1) > 0$. We first claim that the image of the functor F of Construction 5.2.11 consists exactly of the hW curves which can be properly embedded in $\mathbb{P}$. By definition, any curve in the image is properly embedded in $\mathbb{P}$. Conversely, if $H \hookrightarrow \mathbb{P}$ is properly embedded, then Proposition 5.1.11 shows that H is the zero set of some global section s of $\mathscr{G}_9$. Furthermore, the local models in Theorem 4.1.16 show that the "Y^2 coefficieint" of the equation cutting out H is always nonzero, i.e. that s has nonzero image in $\mathrm{H}^0(B, \mathscr{G}_9/\mathscr{G}_8)$. As a consequence of Proposition 5.2.10, given $s, s' \in \mathcal{G}$, the induced map $\mathrm{Hom}_{\mathcal{G}}(s, s') \to \mathrm{Hom}_{\mathcal{H}(B)}(F(s), F(s'))$ is bijective. Thus, $\mathcal{G}$ is equivalent to the groupoid of hW curves properly embedded in $\mathbb{P}$, proving the first equality in the claim. Since $\mathcal{G}$ is the groupoid associated to action of $G := G(\mathbf{D})$ on the set $X := \mathrm{ob}\,\mathcal{G}$, one easily computes $\#\mathcal{G} = \#X/\#G$. Finally $\mathscr{G}_9/\mathscr{G}_8 \cong \mathscr{O}_B$ and $\#G = (q-1)\cdot\#\mathbb{P}G$, from which the rest of the claim follows. ■

Assumption. From here on out, assume we are working within the context of Setup 1.1. In particular, $k = \mathbb{F}_q$ is a finite field and B/k is a smooth k-curve of genus $g = g(B)$.

Proposition 5.2.14. *Let $d := \deg \mathscr{L}$, and let $\mathscr{V} := \mathscr{H}\!om(\mathscr{Y}, \mathrm{Sym}^2(\mathscr{E}_1))$. Then,*

$$\#\,\mathrm{GL}(\mathscr{E}_1) q^{3d+3(1-g)} \le \#\mathbb{P}G(\mathbf{D}) \le \#\,\mathrm{GL}(\mathscr{E}_1)\cdot\#\,\mathrm{H}^0(B, \mathscr{V})$$

Proof. We first compute $\#G(\mathbf{D})$, and then we divide by $(q-1) = \#k^\times$. To do this, we upgrade $G(\mathbf{D})$ by considering the (Zariski) sheaf $\underline{G}$ on B defined by

$$\underline{G}(U) := \left\{ (\varphi,\psi) \in \mathrm{GL}(\mathscr{E}_1|_U)\times\mathrm{GL}(\mathscr{E}_2|_U) \;\middle|\; \begin{array}{ccc} \mathrm{Sym}^2(\mathscr{E}_1|_U) & \xrightarrow{\mu} & \mathscr{E}_2|_U \\ {\scriptstyle \mathrm{Sym}^2(\varphi)}\downarrow & & \downarrow{\scriptstyle\psi} \\ \mathrm{Sym}^2(\mathscr{E}_1|_U) & \xrightarrow{\mu} & \mathscr{E}_2|_U \end{array} \text{ commutes} \right\}$$

with the obvious restriction maps. In particular, $\underline{G}(B) = G(\mathbf{D})$. We next note that there is a map $\underline{G} \to \underline{\mathrm{GL}}(\mathscr{E}_1)\times\mathbb{G}_m$ given, on sections over some $U \overset{\text{open}}{\subset} B$, by $(\varphi,\psi)\mapsto(\varphi,\lambda)$ where $\lambda \in \mathbb{G}_m(U)$ is uniquely chosen so that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sym}^2(\mathscr{E}_1|_U) & \longrightarrow & \mathscr{E}_2|_U & \longrightarrow & \mathscr{Y}|_U & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Sym}^2(\varphi)} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\lambda} & & \\ 0 & \longrightarrow & \mathrm{Sym}^2(\mathscr{E}_1|_U) & \longrightarrow & \mathscr{E}_2|_U & \longrightarrow & \mathscr{Y}|_U & \longrightarrow & 0 \end{array}$$

commutes. Finally this map fits into a sequence

$$0 \longrightarrow \underbrace{\mathscr{H}\!om(\mathscr{Y}, \mathrm{Sym}^2(\mathscr{E}_1))}_{\mathscr{V}} \longrightarrow \underline{G} \longrightarrow \underline{\mathrm{GL}}(\mathscr{E}_1)\times\mathbb{G}_m \longrightarrow 0$$

which is furthermore exact, as can be checked over an open cover trivializing $\mathscr{E}_1, \mathscr{E}_2$. Recall we are interested in computing the order of $G(\mathbf{D}) = \mathrm{H}^0(B, \underline{G})$. The utility of phrasing things as above is that [Gir71, Proposition 3.3.2.2 + Corollaire 3.3.2.3] now gives us an exact sequence

$$0 \longrightarrow \mathrm{H}^0(B,\mathscr{V}) \longrightarrow \mathrm{H}^0(B,\underline{G}) \xrightarrow{F} \mathrm{GL}(\mathscr{E}_1)\times k^\times \xrightarrow{d} \mathrm{H}^1(B,\mathscr{V}) \tag{5.4}$$

of pointed sets whose differential d induces an injection (of sets) $\mathrm{im}(F)\backslash(\mathrm{GL}(\mathscr{E}_1)\times k^\times) \hookrightarrow \mathrm{H}^1(B,\mathscr{V})$. Because $\mathrm{im}(F) = \ker(d)$ acts freely on $\mathrm{GL}(\mathscr{E}_1)\times k^\times$, we can take an alternating product of cardinalities in

(5.4) to conclude that

$$\frac{\#\,\mathrm{H}^0(B,\mathscr{V})}{\#\,\mathrm{H}^0(B,\underline{G})}\cdot\#(\mathrm{GL}(\mathscr{E}_1)\times k^\times)=\#\,\mathrm{im}(d).$$

The trivial inequalities $1\le\#\,\mathrm{im}(d)\le\#\,\mathrm{H}^1(B,\mathscr{V})$ thus give

$$(q-1)\#\,\mathrm{GL}(\mathscr{E}_1)q^{\chi(\mathscr{V})}=(q-1)\#\,\mathrm{GL}(\mathscr{E}_1)\cdot\frac{\#\,\mathrm{H}^0(B,\mathscr{V})}{\#\,\mathrm{H}^1(B,\mathscr{V})}\le\#\,\mathrm{H}^0(B,\underline{G})\le(q-1)\#\,\mathrm{GL}(\mathscr{E}_1)\cdot\#\,\mathrm{H}^0(B,\mathscr{V}).$$

One easily computes $\deg\mathscr{V}=3\deg\mathscr{L}=3d$, so the claimed lower bound follows from Riemann-Roch. ∎

5.3 Counting Minimal hW Curves

We continue to work in the context of Setup 1.1.

Recall 5.3.1 (see Notation 4.2.9)**.** Recall that $\mathcal{H}_M(B)\hookrightarrow\mathcal{H}(B)$ denotes the full subgroupoid consisting of minimal hW curves, and that $\mathcal{H}_{M,NT}(B)\hookrightarrow\mathcal{H}_M(B)$ denotes the full subgroupoid consisting of those minimal hW curves $(H\xrightarrow{\pi}B,D)$ for which D_K is not twice a point. ⊙

Recall that every hW curve is isomorphic to one which can be properly embedded in the projective bundle associated to some unique (up to isomorphism), normalized (1,2,1)-datum (Lemma 5.2.3 and Corollary 5.2.5). In order to bound the number of minimal hW curves, we will partition them according to their normalized (1,2,1)-datum, and then count the number of curves w/ given (1,2,1)-datum using a combination of Propositions 5.2.13 and 5.2.14. In order to compute the quantities appearing in these propositions, we will make use of the filtration constructed in Proposition 5.1.14. That being said, let us first name the objects which will appear in our analysis.

Notation 5.3.2. Given a normalized (1,2,1)-datum $\mathbf{D}=(\mathscr{E}_1,\mathscr{E}_2,\mu)$, define the following myriad of objects.

- Let $\mathscr{D}=\mathscr{D}(\mathbf{D}):=\det(\mathscr{E}_1)$. If $\mathscr{E}_1$ is unstable, it has Harder-Narasimhan filtration

$$0\longrightarrow\mathscr{O}_B\longrightarrow\mathscr{E}_1\longrightarrow\mathscr{D}\longrightarrow0.\tag{5.5}$$

- Let $u=u(\mathbf{D})$ be the unstable degree of $\mathscr{E}_1$. This is 0 if $\mathscr{E}_1$ is semistable, but is otherwise $\deg\mathscr{D}<0$, see Definition 5.1.12.
- Let $\mathscr{L}=\mathscr{L}(\mathbf{D}):=\det(\mathscr{E}_1)\otimes\mathrm{coker}(\mu)^{-1}$ be the Hodge bundle of the datum.
- Let $d=d(\mathbf{D}):=\deg\mathscr{L}$.
- Let $0=\mathscr{F}_0\subset\cdots\subset\mathscr{F}_9=\mathscr{B}(\mathbf{D})_4$ denote the filtration of Proposition 5.1.14. Only $\mathscr{F}_0,\mathscr{F}_5,\mathscr{F}_8,\mathscr{F}_9$ are defined if $\mathscr{E}_1$ is semistable.
- Let $\mathscr{G}_i:=\mathscr{F}_i\otimes\mathscr{L}^2\otimes\mathscr{D}^{-2}$ for all i. By Proposition 5.1.14, we always have an exact sequence

$$0\longrightarrow\underbrace{\mathrm{Sym}^4(\mathscr{E}_1)\otimes\mathscr{D}^{-2}\otimes\mathscr{L}^2}_{\mathscr{G}_5}\longrightarrow\mathscr{G}_8\longrightarrow\mathrm{Sym}^2(\mathscr{E}_1)\otimes\mathscr{D}^{-1}\otimes\mathscr{L}\longrightarrow0,\tag{5.6}$$

  and if $\mathscr{E}_1$ is unstable (i.e. if $u<0$), we further have

$$\frac{\mathscr{G}_{i+1}}{\mathscr{G}_i}\simeq\begin{cases}\mathscr{D}^{i-2}\otimes\mathscr{L}^2 & \text{if } 0\le i\le4\\ \mathscr{D}^{i-6}\otimes\mathscr{L} & \text{if } 5\le i\le7\\ \mathscr{O}_B & \text{if } i=8.\end{cases}\tag{5.7}$$

Motivated by Proposition 5.2.13, our first task will be to find an upper bound for $\#\,\mathrm{H}^0(B,\mathscr{G}_8)$. Equivalently, in light of Riemann-Roch, we first bound $\#\,\mathrm{H}^1(B,\mathscr{G}_8)$ for the $(1,2,1)$-data relevant to our count. For later use, we also bound $\#\,\mathrm{H}^1(B,\mathscr{G}_8/\mathscr{G}_5)$.

Remark 5.3.3. By Corollary 4.3.7, all normalized (1,2,1)-data associated to an hW curve in $\mathcal{H}_{M,NT}(B)$ satisfy $-(d+g)\le u$. Recall also that $u\le 0$ always, by definition, and that every hW curve is isomorphic to one whose associated (1,2,1)-datum is normalized, by Lemma 5.1.13. ◦

Lemma 5.3.4. *Let* $\mathbf{D}$ *be a normalized (1,2,1)-datum with* $-(d+g)\le u<0$*. Furthermore, assume* $d>3g$*. Then,* $h^1(\mathscr{G}_8)\le 7g-2$ *and* $h^1(\mathscr{G}_8/\mathscr{G}_5)\le 3g-1$*.*

Proof. The existence of the filtration $\mathscr{G}_i$ of Notation 5.3.2 shows that $h^1(\mathscr{G}_8)\le\sum_{i=0}^{7}h^1(\mathscr{G}_{i+1}/\mathscr{G}_i)$ and $h^1(\mathscr{G}_8/\mathscr{G}_5)\le\sum_{i=5}^{7}h^1(\mathscr{G}_{i+1}/\mathscr{G}_i)$. With our bounds on u, for $i\ne 4,7$, $\deg(\mathscr{G}_{i+1}/\mathscr{G}_i)>2g-2$ (see (5.7)), so $h^1(\mathscr{G}_{i+1}/\mathscr{G}_i)=0$ unless $i=4,7$ (i.e. excluding the graded pieces $\mathscr{D}^2\otimes\mathscr{L}^2$ and $\mathscr{D}\otimes\mathscr{L}$). Recalling that $u+d\ge -g$ by assumption, for these pieces, one has

$$h^1(\mathscr{D}^2\otimes\mathscr{L}^2)=h^0(\omega_B\otimes\mathscr{D}^{-2}\otimes\mathscr{L}^{-2})\le\deg(\omega_B\otimes\mathscr{D}^{-2}\otimes\mathscr{L}^{-2})+1=2g-2-2(u+d)+1\le 4g-1,$$

and similarly $h^1(\mathscr{D}\otimes\mathscr{L})\le 3g-1$. ■

We still need to bound $h^1(\mathscr{G}_8)$ when $u=0$, i.e. when $\mathscr{E}_1$ is semistable.

Lemma 5.3.5. *Let* $\mathscr{E}$ *be a rank* $r\ge 1$ *semistable vector bundle on* B*, and fix an integer* $k\ge 1$*. Let* $\mathscr{M}$ *be a line bundle on* B *with* $\deg\mathscr{M}\ge 2grk-1$*. Then,*

$$H^1\Big(B,\operatorname{Sym}^{rk}(\mathscr{E})\otimes(\det\mathscr{E})^{-k}\otimes\mathscr{M}\Big)=0.$$

Proof. First note that the vector bundle $\operatorname{Sym}^{rk}(\mathscr{E})\otimes(\det\mathscr{E})^{-k}$ is unchanged under the substitution $\mathscr{E}\rightsquigarrow\mathscr{E}\otimes\mathscr{N}$ for any line bundle $\mathscr{N}$ on B. Thus, we may twist $\mathscr{E}$ in order to assume that

$$(2g-1)r<\deg(\mathscr{E})\le 2gr,$$

in particular, that it has slope $\mu(\mathscr{E})>2g-1$. Since $\mathscr{E}$ is semistable of high slope, [Muk03, Proposition 10.27] tells us that it is globally generated. Fix a surjection $\mathscr{O}_B^{\oplus N}\twoheadrightarrow\mathscr{E}$. From this, one obtains a surjection $\mathscr{E}^{\oplus N(rk-1)}=\mathscr{E}\otimes\big(\mathscr{O}_B^{\oplus N}\big)^{\otimes(rk-1)}\twoheadrightarrow\mathscr{E}\otimes\mathscr{E}^{\otimes(rk-1)}\twoheadrightarrow\operatorname{Sym}^{rk}(\mathscr{E})$. Tensoring with $(\det\mathscr{E})^{-k}\otimes\mathscr{M}$ then gives the surjection

$$F:\Big[\mathscr{E}\otimes(\det\mathscr{E})^{-k}\otimes\mathscr{M}\Big]^{\oplus N(rk-1)}\twoheadrightarrow\operatorname{Sym}^{rk}(\mathscr{E})\otimes(\det\mathscr{E})^{-k}\otimes\mathscr{M}. \tag{5.8}$$

Because $\mathrm{H}^2(B,\ker F)=0$, (5.8) induces a surjection on H^1's, so it suffices to show that $\mathrm{H}^1(B,\mathscr{E}\otimes(\det\mathscr{E})^{-k}\otimes\mathscr{M})=0$. Because $\mathscr{E}\otimes(\det\mathscr{E})^{-k}\otimes\mathscr{M}$ is semistable with slope

$$\mu(\mathscr{E})-k\deg(\mathscr{E})+\deg(\mathscr{M})>(2g-1)-2grk+(2grk-1)=2g-2,$$

we win by [Muk03, Proposition 10.26]. ■

Corollary 5.3.6. *Let* $\mathbf{D}$ *be a normalized (1,2,1)-datum with* $u=0$*. Furthermore, assume* $d\ge 4g$*. Then,* $h^1(\mathscr{G}_8)=0$ *and* $h^1(\mathscr{G}_8/\mathscr{G}_5)=0$*.*

Proof. That $u=0$ means that $\mathscr{E}_1$ is semistable. Thus, this follows from (5.6) along with Lemma 5.3.5. ■

Given some $(1,2,1)$-datum $\mathbf{D}$, Propositions 5.2.13 and 5.2.14 tell us that

$$\sum_{H\hookrightarrow\mathbb{P}(\mathbf{D})}\frac{1}{\#\operatorname{Aut}_{\mathcal{H}(B)}(H)}\le\frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{\#\mathbb{P}G}\le\frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{\#\operatorname{GL}(\mathscr{E}_1)q^{3d+3(1-g)}}.$$

Recall (Definition 5.1.2) that $\mathscr{E}_1$ above is not an isomorphism invariant of $\mathbf{D}$, but its associated PGL_2-torsor is. Thus, we would like a bound given only in terms of this PGL_2-torsor.

Lemma 5.3.7. *Let $\mathscr{E}$ be a rank 2 vector bundle on B, with associated PGL_2-torsor $P=\underline{\operatorname{Isom}}(\mathscr{O}^{\oplus 2},\mathscr{E})\overset{\mathrm{GL}_2}{\times}\mathrm{PGL}_2$. Then,*

$$\#\operatorname{Aut}(P)=\frac{\#\operatorname{GL}(\mathscr{E})}{q-1}.$$

Proof. Taking inner twists in $1\to\mathbb{G}_m\to\mathrm{GL}_2\to\mathrm{PGL}_2\to 1$ by a cocycle defining $\mathscr{E}$ gives the exact sequence

$$0\longrightarrow\mathbb{G}_m\longrightarrow\underline{\mathrm{GL}}(\mathscr{E})\longrightarrow\underline{\operatorname{Aut}}(P)\longrightarrow 0.$$

To prove the claim, it suffices to show that this sequence remains exact after taking global sections. Consider the following commutative diagram with top row exact:

$$\begin{tikzcd}
\mathrm{GL}(\mathscr{E}) \arrow[r, "(1)"] & \operatorname{Aut}(P) \arrow[r] & \operatorname{H}^1(B,\mathbb{G}_m) \arrow[r, "(2)"] \arrow[d, equal] & \operatorname{H}^1(B,\underline{\mathrm{GL}}(\mathscr{E})) \arrow[d] & \ni & T \arrow[d, mapsto] \\
 & & \operatorname{H}^1(B,\mathbb{G}_m) \arrow[r, "(3)"] & \operatorname{H}^1(B,\mathrm{GL}_2) & \ni & T\overset{\mathrm{GL}(\mathscr{E})}{\times}\underline{\operatorname{Isom}}(\mathscr{O}^{\oplus 2},\mathscr{E})
\end{tikzcd}$$

Surjectivity of (1) is equivalent, by exactness of the top row, to injectivity of (2). Commutativity tells us that (2) is injective if (3) is. Finally, (3) is injective because it can be identified with the map sending a line bundle $\mathscr{L}$ to the rank 2 vector bundle $\mathscr{L}\oplus\mathscr{L}$. ■

Corollary 5.3.8. *Let $\mathbf{D}$ be a normalized (1,2,1)-datum. Then,*

$$\sum_{H\hookrightarrow\mathbb{P}(\mathbf{D})}\frac{1}{\#\operatorname{Aut}_{\mathcal{H}(B)}(H)}\le\frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{(q-1)\cdot\#\operatorname{Aut}(P)q^{3d+3(1-g)}}.$$

Proof. This follows from Propositions 5.2.13 and 5.2.14 and Lemma 5.3.7. ■

In the end, we will need to understand the sum of the above expressions as $\mathbf{D}$ varies over isomorphism classes of (1,2,1)-data.

Notation 5.3.9.

- Let P be a PGL_2-torsor on B. We let $\mathscr{V}(P)$ denote the rank 3 vector bundle (associated the to the GL_3-torsor) obtained by pushing P along the PGL_2-representation $\operatorname{Sym}^2(\texttt{taut})\otimes\texttt{det}^{-1}:\mathrm{PGL}_2\to\mathrm{GL}_3$.
- Furthermore, extending Notation 5.3.2, given a (1,2,1)-datum $\mathbf{D}=(\mathscr{E}_1,\mathscr{E}_2,\mu)$, we let $P=P(\mathbf{D})$ denote the PGL_2-torsor associated to $\mathscr{E}_1$.

  Note that, in this context, $\mathscr{V}(P)\cong\operatorname{Sym}^2(\mathscr{E}_1)\otimes(\det\mathscr{E}_1)^{-1}=\operatorname{Sym}^2(\mathscr{E}_1)\otimes\mathscr{D}^{-1}$.

Lemma 5.3.10. *There is a bijection between isomorphism classes of $(1,2,1)$-data and triples $(P,\mathscr{L},\varepsilon)$, where $P\in\operatorname{H}^1(B,\mathrm{PGL}_2)$, $\mathscr{L}\in\operatorname{Pic}(B)$, and $\varepsilon\in\operatorname{Ext}^1(\mathscr{L}^{-1},\mathscr{V}(P))\cong\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})$.*

Proof. Let $\mathbf{D} = (\mathscr{E}_1, \mathscr{E}_2, \mu)$ be a (1,2,1)-datum. Then, $\mathscr{V}(P(\mathbf{D})) \cong \mathrm{Sym}^2(\mathscr{E}_1) \otimes \mathscr{D}^{-1}$, so the extension $0 \to \mathrm{Sym}^2(\mathscr{E}_1) \xrightarrow{\mu} \mathscr{E}_2 \to \mathscr{L}(\mathbf{D})^{-1} \otimes \mathscr{D} \to 0$, after tensoring with $\mathscr{D}^{-1}$, gives rise to a class $\varepsilon(\mathbf{D}) \in \mathrm{Ext}^1(\mathscr{L}^{-1}, \mathscr{V}(P))$. In one direction, the bijection is given by $\mathbf{D} \mapsto (P(\mathbf{D}), \mathscr{L}(\mathbf{D}), \varepsilon(\mathbf{D}))$. This triple is easily checked to be an isomorphism invariant.

Conversely, suppose we're given $(P, \mathscr{L}, \varepsilon)$. Because $H^2(B, \mathbb{G}_m) = 0$ by [Mil80, Example III.2.22 Case (g)], we can choose some rank 2 vector bundle $\mathscr{E}$ lifting P. Having made such a choice, ε defines an extension $0 \to \mathrm{Sym}^2(\mathscr{E}) \otimes (\det \mathscr{E})^{-1} \xrightarrow{\mu'} \mathscr{E}' \to \mathscr{L}^{-1} \to 0$. Observe that $(\mathscr{E}, \mathscr{E}' \otimes \det \mathscr{E}, \mu' \otimes 1)$ is a (1,2,1)-datum and that its isomorphism class is independent of the choices made. This gives the other direction of the bijection. ∎

Notation 5.3.11. Given $P, \mathscr{L}, \varepsilon$ as in Lemma 5.3.10, let $\mathscr{G}_8 = \mathscr{G}_8(P, \mathscr{L}, \varepsilon)$ denote the (isomorphism class of the) rank 8 vector bundle $\mathscr{G}_8(\mathbf{D})$ associated to any (1,2,1)-datum $\mathbf{D}$ associated to the triple $(P, \mathscr{L}, \varepsilon)$ via Lemma 5.3.10.

Let $\mathrm{Bun}_{\mathrm{PGL}_2}(k)$ denote the groupoid of PGL_2-torsors over B, and set

$$M := |\mathrm{Bun}_{\mathrm{PGL}_2}(k)| = \mathrm{H}^1(B, \mathrm{PGL}_2),$$

the set of isomorphism classes of PGL_2-torsors over B. Endow M with the discrete measure m where each $[P] \in \mathrm{H}^1(B, \mathrm{PGL}_2)$ is weighted by $1/\# \mathrm{Aut}(P)$.

Lemma 5.3.12. $\# \mathrm{Bun}_{\mathrm{PGL}_2}(k) = \int_M \mathrm{d}m = 2q^{3(g-1)}\zeta_B(2)$

Proof. Note that the first equality is by definition. Siegel's formula [BD09, Theorem 4.8 + Proposition 4.13] tells us that the Tamagawa number $\tau(\mathrm{PGL}_2)$ of PGL_2 is related to the groupoid cardinality of $\mathrm{Bun}_{\mathrm{PGL}_2}(k)$ via

$$\frac{\tau(\mathrm{PGL}_2)}{\# \mathrm{Bun}_{\mathrm{PGL}_2}(k)} = q^{(1-g)\dim \mathrm{PGL}_2} \prod_{\text{closed } x \in B} \frac{\# \mathrm{PGL}_2(\kappa(x))}{(\#\kappa(x))^{\dim \mathrm{PGL}_2}} = q^{3(1-g)} \prod_{\text{closed } x \in B} \left(1 - q^{-2\deg x}\right) = q^{3(1-g)}\zeta_B(2)^{-1}.$$

It is well-know that $\tau(\mathrm{PGL}_2) = 2$; this can be deduced e.g. from the main result of [GL19] (see also [BD09, Theorem 6.1]). Thus, we conclude that $\# \mathrm{Bun}_{\mathrm{PGL}_2}(k) = 2q^{3(g-1)}\zeta_B(2)$. ∎

Theorem 5.3.13. *Use notation as in Setup 1.1. Then,*

$$\limsup_{d \to \infty} \frac{\#\mathcal{H}^{=d}_{M,NT}(B)}{\#\mathcal{M}^{=d}_{1,1}(K)} \le 2\zeta_B(2)\zeta_B(10).$$

Proof. We begin with a bit of notation. For any $u \in \mathbb{Z}_{<0}$, let $M^{\ge u} \subset M$ denote the subset consisting of isomorphism classes of PGL_2-torsors over B which lift to a rank 2 vector bundle $\mathscr{V}$ on B which is either semistable or has Harder-Narasimhan filtration of the form $0 \to \mathscr{O}_B \to \mathscr{V} \to \det \mathscr{V} \to 0$, with $\deg \mathscr{V} \ge u$.

Below, when we write $\sum_{\mathbf{D}}$, we mean that the sum is over isomorphism classes of *normalized* (1,2,1)-data.

$$\begin{aligned}
\#\mathcal{H}^{=d}_{M,NT}(B) &= \sum_{\substack{\alpha \in |\mathcal{H}_{M,NT}(B)| \\ \mathrm{ht}(\alpha) = d}} \frac{1}{\# \mathrm{Aut}_{\mathcal{H}(B)}(\alpha)} \\
&= \sum_{\substack{\mathbf{D} \\ d(\mathbf{D}) = d}} \sum_{\substack{H \in |\mathcal{H}_{M,NT}(B)| \\ \mathbf{D}(H) \cong \mathbf{D}}} \frac{1}{\# \mathrm{Aut}_{\mathcal{H}(B)}(H)} && \text{by Lemma 5.1.13} \\
&= \sum_{\substack{\mathbf{D} \\ d(\mathbf{D}) = d}} \sum_{\substack{H \hookrightarrow \mathbb{P}(\mathbf{D}) \\ H \in |\mathcal{H}_{M,NT}(B)|}} \frac{1}{\# \mathrm{Aut}_{\mathcal{H}(B)}(H)} && \text{by Corollary 5.2.5}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{\mathbf{D}\\ d(\mathbf{D})=d \\ -(d+g)\le u(\mathbf{D})\le 0}} \sum_{\substack{H\hookrightarrow \mathbb{P}(\mathbf{D})\\ H\in|\mathcal{H}_{M,NT}(B)|}} \frac{1}{\#\operatorname{Aut}_{\mathcal{H}(B)}(H)} && \text{by Remark 5.3.3}\\
&\le \sum_{\substack{\mathbf{D}\\ d(\mathbf{D})=d \\ -(d+g)\le u(\mathbf{D})\le 0}} \frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{(q-1)\cdot\#\operatorname{Aut}(P)q^{3d+3(1-g)}} && \text{by Corollary 5.3.8}\\
&= \sum_{P\in M^{\ge -(d+g)}} \sum_{\mathscr{L}\in\operatorname{Pic}^d(B)} \sum_{\varepsilon\in\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})} \frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{(q-1)\cdot\#\operatorname{Aut}(P)q^{3d+3(1-g)}} && \text{by Lemma 5.3.10}\\
&= \int_{M^{\ge -(d+g)}} \sum_{\mathscr{L}\in\operatorname{Pic}^d(B)} \sum_{\varepsilon\in\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})} \frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{(q-1)q^{3d+3(1-g)}}\mathrm{d}m\\
&= \frac{1}{q-1}\int_M \chi_d(P) \sum_{\mathscr{L}\in\operatorname{Pic}^d(B)} \sum_{\varepsilon\in\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})} \frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{q^{3d+3(1-g)}}\mathrm{d}m,
\end{aligned}
$$

where $\chi_d : M \to \{0,1\}$ is the characteristic function of $M^{\ge -(d+g)}$. By Theorem 3.4.4, $\#\mathcal{M}_{1,1}^{=d}(K) \sim \#\operatorname{Pic}^0(B)\cdot q^{10d+2(1-g)}/[(q-1)\zeta_B(10)]$. Thus,

$$
\begin{aligned}
\limsup_{d\to\infty} \frac{\#\mathcal{H}_{M,NT}^{=d}(B)}{\#\mathcal{M}_{1,1}^{=d}(K)} &= \limsup_{d\to\infty}(q-1)\zeta_B(10)\frac{\#\mathcal{H}_{M,NT}^{=d}(B)}{\#\operatorname{Pic}^0(B)\cdot q^{10d+2(1-g)}}\\
&\le \frac{\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \lim_{d\to\infty}\int_M \chi_d(P) \sum_{\mathscr{L}\in\operatorname{Pic}^d(B)} \sum_{\varepsilon\in\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})} \frac{\#\operatorname{H}^0(B,\mathscr{G}_8)}{q^{13d+5(1-g)}}\mathrm{d}m\\
&= \frac{q^{3(1-g)}\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \lim_{d\to\infty}\int_M \chi_d(P) \underbrace{\sum_{\mathscr{L}\in\operatorname{Pic}^d(B)} \sum_{\varepsilon\in\operatorname{H}^1(B,\mathscr{V}(P)\otimes\mathscr{L})} q^{h^1(\mathscr{G}_8)}}_{I_d(P)}\mathrm{d}m, \qquad (5.9)
\end{aligned}
$$

with last equality holding by Riemann-Roch (note that $\deg\mathscr{G}_8 = 13d$). We would like to commute the limit and integral in (5.9), so we will bound $I_d(P)$ and then apply dominated convergence. Observe (5.6) $\mathscr{V}(P)\otimes\mathscr{L}\cong\mathscr{G}_8/\mathscr{G}_5$, so Lemma 5.3.4 and Corollary 5.3.6 tell us that $h^1(\mathscr{G}_8)\le 7g-2$ and $h^1(\mathscr{V}(P)\otimes\mathscr{L})\le 3g-1$ whenever $d\gg_g 1$. Putting these together, whenever $d\gg_g 1$ and $P\in M^{\ge -(d+g)}$, we have (with $I_d(P)$ defined as indicated in (5.9))

$$
I_d(P) \le \#\operatorname{Pic}^0(B)\cdot q^{3g-1}\cdot q^{7g-2} = \#\operatorname{Pic}^0(B)q^{10g-3}. \qquad (5.10)
$$

Observe that $\int_M \#\operatorname{Pic}^0(B)q^{10g-3}\mathrm{d}m < \infty$ and $\int_M \lim_{d\to\infty} I_d(P)\mathrm{d}m = \int_M \#\operatorname{Pic}^0(B)\mathrm{d}m < \infty$ (with equality by Serre vanishing) by Lemma 5.3.12. Thus, (5.10) allows us to apply the Dominated Convergence Theorem (DCT) below:

$$
\begin{aligned}
\limsup_{d\to\infty} \frac{\#\mathcal{H}_{M,NT}^{=d}(B)}{\#\mathcal{M}_{1,1}^{=d}(K)} &\le \frac{q^{3(1-g)}\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \lim_{d\to\infty}\int_M \chi_d(P)I_d(P)\mathrm{d}m && \text{by (5.9)}\\
&= \frac{q^{3(1-g)}\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \int_M \lim_{d\to\infty}\chi_d(P)I_d(P)\mathrm{d}m && \text{by DCT}\\
&= \frac{q^{3(1-g)}\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \int_M \#\operatorname{Pic}^0(B)\mathrm{d}m && \text{by Serre vanishing}\\
&= \frac{q^{3(1-g)}\zeta_B(10)}{\#\operatorname{Pic}^0(B)} \cdot\#\operatorname{Pic}^0(B)\cdot 2q^{3(g-1)}\zeta_B(2) && \text{by Lemma 5.3.12}
\end{aligned}
$$

$$= 2\zeta_B(2)\zeta_B(10).$$ ■

Corollary 5.3.14. *Use notation as in Setup 1.1. Then,*

$$\limsup_{d\to\infty} \frac{\#\mathcal{H}^{\le d}_{M,NT}(B)}{\#\mathcal{M}^{\le d}_{1,1}(K)} \le 2\zeta_B(2)\zeta_B(10).$$

Proof. This is a consequence of Theorems 3.4.4 and 5.3.13. ■

Theorem 5.3.15 (= Corollary 7.2.3)**.** *Use notation as in Setup 1.1. Then,*

$$\limsup_{d\to\infty} \mathrm{MAS}_B(d) \le 1 + 2\zeta_B(2)\zeta_B(10).$$

We postpone a proof of Theorem 5.3.15 until Section 7. In light of (4.12), the key to deducing Theorem 5.3.15 from Corollary 5.3.14 is showing that 0% of elliptic curves have a nonzero 2-torsion point. We will verify this in Section 7.1, and then afterwards prove Theorem 5.3.15 (See Corollary 7.2.3).

6 Asymptotic Bounds on 2-Selmer

With notation as in Setup 1.1, we have just seen that

$$\limsup_{d\to\infty} \mathrm{MAS}_B(d) \le 1 + 2\zeta_B(2)\zeta_B(10).$$

As a consequence of Lemma 4.2.4, in order to get from this to Theorem B, it will suffice to show that elliptic curves with non-trivial 2-torsion contribute 0 to the asympotic average size of 2-Selmer. We will do this in two steps. First, in the current section, we will produce uniform upper bounds on the size of the 2-Selmer groups of elliptic curves of bounded height. Then, in Section 7, we will count the number of elliptic curves with non-trivial 2-torsion, and this count combined with the bounds here will let us show that $\limsup_{d\to\infty} \mathrm{AS}_B(d) \le \limsup_{d\to\infty} \mathrm{MAS}_B(d)$, and so let us deduce Theorem B from Theorem 5.3.15.

Namely, in this section, we will prove a bound of the form

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \le O\left(\frac{\mathrm{ht}(E)}{\log \mathrm{ht}(E)}\right)$$

for elliptic curves E/K in various situations. We will obtain this bound by using different arguments in characteristics 2 and $\ne 2$. First, when $\operatorname{char} K \ne 2$, we bound $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E)$ (under the additional assumption that $E[2](K) \ne 0$) using an argument in the spirit of [Sil09, Exercise VIII.1]. While not strictly necessary for the proof of Theorem B, we then show how to obtain a similar bound without assuming $E[2](K) \ne 0$, if furthermore $\operatorname{char} K \ne 3$. In characteristic 2, our main technical tool is an extension of [Lan21b, Proposition 3.26] to all characteristics (see Proposition 6.2.5). We use this to produce two slightly different bounds for $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E)$, one "horizontal" (Corollary 6.2.16) and one "vertical" (Theorem 6.2.20). Neither of these alone suffices for our purposes, but we will show that the minimum of these two bounds is always at most $O(\mathrm{ht}(E)/\log \mathrm{ht}(E))$.

Carrying out the arguments referenced above produces bounds expressible in terms of the conductor of E. In Section 6.3, we show how to convert these into bounds in terms of the height of E. Afterwards, in Theorem 6.3.4, we summarize all the bounds obtained in this section.

Before separating into cases, we include a lemma which will be used in both of the following sections.

Lemma 6.1. *Let S be an arbitrary scheme, and let $\mathscr{E}/S$ be an elliptic scheme. Let $\alpha \hookrightarrow \mathscr{E}$ be a finite, flat S-group scheme of order n, and let $\alpha^\vee := \underline{\mathrm{Hom}}(\alpha, \mathbb{G}_m)$ be its Cartier dual. Then, there is a short exact* *sequence*

$$0 \longrightarrow \alpha \longrightarrow \mathscr{E}[n] \longrightarrow \alpha^\vee \longrightarrow 0$$

of abelian sheaves on S_{fppf}.

Proof. Consider the quotient map $q : \mathscr{E} \twoheadrightarrow \mathscr{E}/\alpha =: \mathscr{E}'$ as well as its dual $q^\vee : \mathscr{E}' \to \mathscr{E}$. Since $q^\vee q = [n] : \mathscr{E} \to \mathscr{E}$, we get a short exact sequence of kernels

$$0 \longrightarrow \ker q \longrightarrow \mathscr{E}[n] \longrightarrow \ker q^\vee \longrightarrow 0.$$

Now, $\ker q = \alpha$ by construction, and so $\ker q^\vee \simeq \alpha^\vee$ by [Oda69, Corollary 1.3(ii)]. ■

Throughout the remainder of this section, we work within the context of Setup 1.1.

6.1 Bound in Characteristic $\neq 2$

Setup 6.1.1. In addition to Setup 1.1, we fix an elliptic curve E/K. Furthermore, we assume that $p := \operatorname{char} K \neq 2$.

Lemma 6.1.2. *Let*

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, "\alpha"] & B_1 \arrow[r] \arrow[d, "\beta"] & C_1 \arrow[r] \arrow[d, "\gamma"] & D_1 \arrow[r, "g_1"] \arrow[d, "\delta"] & E_1 \arrow[d, "\varepsilon"] \\
A_2 \arrow[r, "f_2"] & B_2 \arrow[r] & C_2 \arrow[r] & D_2 \arrow[r, "g_2"] & E_2
\end{tikzcd}$$

be a homomorphism of exact sequences of abelian groups. Then,

$$\#\ker\gamma \leq \#\ker\beta \cdot \#(\ker\delta \cap \ker g_1) \cdot \#\operatorname{coker}\Big(\operatorname{im}(f_1) \xrightarrow{\beta} \operatorname{im}(f_2)\Big) \leq \#\ker\beta \cdot \#\ker\delta \cdot \#\operatorname{im} f_2.$$

Proof. Consider the homomorphisms

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{coker} f_1 \arrow[r] \arrow[d, "\overline{\beta}"] & C_1 \arrow[r] \arrow[d, "\gamma"] & \ker g_1 \arrow[r] \arrow[d, "\delta"] & 0 \\
0 \arrow[r] & \operatorname{coker} f_2 \arrow[r] & C_2 \arrow[r] & \ker g_2 \arrow[r] & 0
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
0 \arrow[r] & \operatorname{im} f_1 \arrow[r] \arrow[d] & B_1 \arrow[r] \arrow[d, "\beta"] & \operatorname{coker} f_1 \arrow[r] \arrow[d, "\overline{\beta}"] & 0 \\
0 \arrow[r] & \operatorname{im} f_2 \arrow[r] & B_2 \arrow[r] & \operatorname{coker} f_2 \arrow[r] & 0
\end{tikzcd}$$

of short exact sequences. Applying the snake lemma to both of them immediately shows that

$$\#\ker\gamma \leq \#\ker\overline{\beta} \cdot \#(\ker\delta \cap \ker g_1) \;\; \text{and} \;\; \#\ker\overline{\beta} \leq \#\ker\beta \cdot \#\operatorname{coker}(\operatorname{im}(f_1) \to \operatorname{im}(f_2))\,.$$ ■

Proposition 6.1.3. *Let $S \subset B$ be the set of places of bad reduction for E. Assume that $E[2](K) \neq 0$. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq 3\#S + 2\dim_{\mathbb{F}_2} \operatorname{Pic}^0(B)[2] + 2 \leq 3\#S + 4g + 2.$$

Proof. Let $U = B \setminus S$ be the locus of good reduction for E, and let $\mathscr{E}/U$ be E's Néron model. Note that $[2] : \mathscr{E} \to \mathscr{E}$ is a flat (even étale) cover, so we can form the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{\mathscr{E}(U)}{2\mathscr{E}(U)} \arrow[r] \arrow[d] & \mathrm{H}^1(U, \mathscr{E}[2]) \arrow[r] \arrow[d] & \mathrm{H}^1(U, \mathscr{E})[2] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \displaystyle\prod_{v\in S} \frac{E(K_v)}{2E(K_v)} \arrow[r, "\prod_v \delta_v"] & \displaystyle\prod_{v\in S} \mathrm{H}^1(K_v, E[2]) \arrow[r] & \displaystyle\prod_{v\in S} \mathrm{H}^1(K_v, E)[2] \arrow[r] & 0.
\end{tikzcd}$$

Now, it is not hard to show that $\mathrm{H}^1(U,\mathscr{E}[2]) \subset \mathrm{H}^1(K,E[2])$ consists exactly of cohomology classes which are everywhere unramified over U, and so produce a injection

$$\mathrm{Sel}_2(E) \hookrightarrow \left\{c \in \mathrm{H}^1(U,\mathscr{E}[2]) : c_v \in \operatorname{im}\delta_v \text{ for all } v \in S\right\} =: G.$$

Hence, it suffices to bound $\dim_{\mathbb{F}_2} G$. For this, we observe that it sits in a short exact sequence

$$0 \longrightarrow \underbrace{\ker\left(\mathrm{H}^1(U,\mathscr{E}[2]) \longrightarrow \prod_{v\in S}\mathrm{H}^1(K_v,E[2])\right)}_{A} \longrightarrow G \longrightarrow \prod_{v\in S}\frac{E(K_v)}{2E(K_v)} \longrightarrow 0.$$

We separately bound the sizes of A (defined in the above displayed sequence) and $\prod_{v\in S} E(K_v)/2E(K_v)$.

- For A, we first remark that, by Lemma 6.1, we have a short exact sequence $0 \to \underline{\mathbb{Z}/2\mathbb{Z}}_U \to \mathscr{E}[2] \to \mu_{2,U} \to 0$. Comparing this with the analogous sequences over K_v for $v \in S$, taking cohomology, and observing that $\underline{\mathbb{Z}/2\mathbb{Z}}_U \simeq \mu_{2,U}$, we obtain

$$\begin{tikzcd} \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d] & \mathrm{H}^1(U,\mathbb{Z}/2\mathbb{Z}) \arrow[r] \arrow[d, "\beta"] & \mathrm{H}^1(U,\mathscr{E}[2]) \arrow[r] \arrow[d, "\gamma"] & \mathrm{H}^1(U,\mathbb{Z}/2\mathbb{Z}) \arrow[r] \arrow[d, "\delta"] & \mathrm{H}^2(U,\mathbb{Z}/2\mathbb{Z}) \arrow[d] \\ (\mathbb{Z}/2\mathbb{Z})^{\#S} \arrow[r] & \prod_{v\in S}\mathrm{H}^1(K_v,\mathbb{Z}/2\mathbb{Z}) \arrow[r] & \prod_{v\in S}\mathrm{H}^1(K_v,E[2]) \arrow[r] & \prod_{v\in S}\mathrm{H}^1(K_v,\mathbb{Z}/2\mathbb{Z}) \arrow[r] & \prod_{v\in S}\mathrm{H}^2(K_v,\mathbb{Z}/2\mathbb{Z}). \end{tikzcd}$$

  We now apply Lemma 6.1.2 to conclude that

$$\dim_{\mathbb{F}_2} A = \dim_{\mathbb{F}_2}\ker\gamma \le \dim_{\mathbb{F}_2}\ker\beta + \dim_{\mathbb{F}_2}\ker\delta + \#S = 2\dim_{\mathbb{F}_2}\ker\beta + \#S, \tag{6.1}$$

  so we are reduced to bounding the size of

$$B := \ker\left(\mathrm{H}^1(U,\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\beta} \prod_{v\in S}\mathrm{H}^1(K_v,\mathbb{Z}/2\mathbb{Z})\right).$$

  Note that

$$\mathrm{H}^1(U,\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{Hom}_{\mathrm{cts}}(G_{K,U},\mathbb{Z}/2\mathbb{Z}) \text{ and } \mathrm{H}^1(K_v,E[2]) \simeq \mathrm{Hom}_{\mathrm{cts}}(G_{K_v},\mathbb{Z}/2\mathbb{Z}),$$

  where K^s (resp. K_v^s) is the maximal separable extension of K (resp. K_v), G_K (resp. G_{K_v}) is the absolute Galois group of K (resp. K_v), and $G_{K,U} = \mathrm{Gal}(K_U/K)$, where K_U is the maximal extension of K unramified above U. Thus any element of B is represented by an everywhere unramified continuous homomorphism $G_K \to \mathbb{Z}/2\mathbb{Z}$, so $B \subset \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Pic}(B),\mathbb{Z}/2\mathbb{Z})$ by class field theory. As $\mathrm{Pic}(B) \cong \mathrm{Pic}^0(B)\times\mathbb{Z}$, this says that $B \subset \mathrm{Hom}(\mathbb{Z},\mathbb{Z}/2\mathbb{Z}) \times \mathrm{Hom}(\mathrm{Pic}^0(B),\mathbb{Z}/2\mathbb{Z})$. The first factor here is $\cong \mathbb{Z}/2\mathbb{Z}$, while the second factor has dimension $\dim_{\mathbb{F}_2}\mathrm{Pic}^0(B)[2]$. Recalling (6.1), we conclude

$$\dim_{\mathbb{F}_2} A \le 2 + 2\dim_{\mathbb{F}_2}\mathrm{Pic}^0(B)[2] + \#S.$$

- For $\prod_{v\in S} E(K_v)/2E(K_v)$, we simply use the fact that, for each v, $E(K_v)$ is a profinite group with a finite index pro-p subgroup (recall $p = \operatorname{char} K \ne 2$), and so $\#E(K_v)/2E(K_v) = \#E(K_v)[2] \le 4$. Thus, $\dim_{\mathbb{F}_2}\prod_{v\in S} E(K_v)/2E(K_v) \le 2\#S$.

The claim follows from combining these two bullet points. ■

Proposition 6.1.3 suffices for later applications in Section 7.2 when we prove Theorem B. However, when $\operatorname{char} K \geq 5$, we can use Proposition 6.1.3 in order to obtain a bound on the sizes of 2-Selmer groups of arbitrary elliptic curves E/K. The basic idea is to compare $\operatorname{Sel}_2(E/K)$ with $\operatorname{Sel}_2(E/L)$, where $L = K(E[2])$.

Lemma 6.1.4. *Let $L = K(E[2])$, let k' be the algebraic closure of k in L, and let C/k' be the smooth k'-curve with function field L. Assume that $\operatorname{char} K \geq 5$. Then,*

$$g(C) \leq 15\#S + 6g(B) + 1,$$

where $S \subset B$ denotes the set of places of bad reduction for E/K.

Proof. Let $K' = Kk'$. The cover $f : C \to B_{k'}$ is unramified above all places of good reduction for E/K'. Hence, letting $S' \subset B_{k'}$ denote the set of places of bad reduction for E/K', Riemann-Hurwitz shows that

$$2g(C) - 2 = \deg(f)(2g(B) - 2) + \sum_{v \in S'} (e_v - 1) \leq \deg(f)(2g(B) - 2) + 5\#S' \leq \deg(f)(2g(B) - 2) + 30\#S.$$

Above, we used the naive bound $\#S' \leq [K' : K]\#S \leq 6\#S$. Rearranging gives

$$g(C) \leq \deg(f)(g(B) - 1) + 15\#S + 1 \leq \deg(f)g(B) + 15\#S + 1 \leq 6g(B) + 15\#S + 1. \qquad \blacksquare$$

Proposition 6.1.5. *Let $S \subset B$ denote the set of places of bad reduction for E/K. Assume $\operatorname{char} K \geq 5$. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq 78\#S + 24g(B) + 6.$$

Proof. Let $L = K(E[2])$ and $G = \operatorname{Gal}(L/K)$. Consider the Hochschild-Serre spectral sequence [Mil80, Theorem III.2.20] $E_2^{pq} = \mathrm{H}^p(G, \mathrm{H}^q(K, E[2])) \implies \mathrm{H}^{p+q}(K, E[2])$. Its low-degree terms form an inflation-restriction sequence $0 \to \mathrm{H}^1(G, E[2](L)) \to \mathrm{H}^1(K, E[2]) \to \mathrm{H}^1(L, E[2])$. Since $G \leq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, one can easily show that $\mathrm{H}^1(G, E[2](L)) \cong \mathrm{H}^1(G, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ has size at most 4. Thus, the inflation-restriction sequences shows that

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E/K) \leq \dim_{\mathbb{F}_2} \operatorname{Sel}_2(E/L) + 2.$$

The claim now follows from Proposition 6.1.3 combined with Lemma 6.1.4. $\blacksquare$

6.2 Bound in Characteristic 2

Setup 6.2.1. In addition to Setup 1.1, we fix an elliptic curve E/K. We let $\mathscr{E}/B$ denote its Néron model, and we let $\mathscr{E}^0 \hookrightarrow \mathscr{E}$ denote the identity component of its Néron model. We also let $N, \Delta \in \operatorname{Div}(B)$ respectively denote the conductor and minimal discriminant of E. At this point, we make no restrictions on $\operatorname{char} K$.

We begin by extending [Lan21b, Proposition 3.26] to the "bad characteristic" case. Following ideas of [Lan21a, Lan21c], our main technical tool for doing so will be to replace the cohomology of the sheaf $\mathscr{E}[2]$ with the (hyper)cohomology of the two term complex $\mathscr{E} \xrightarrow{[2]} \mathscr{E}$.

Proposition 6.2.2. *Let $\mathscr{C} := [\mathscr{F} \xrightarrow{\varphi} \mathscr{G}]$ be a two term complex of abelian sheaves over an arbitrary scheme S, with $\mathscr{F}$ in degree 0 and $\mathscr{G}$ in degree 1. Write $\mathrm{H}^1(S, \mathscr{F} \xrightarrow{\varphi} \mathscr{G}) := \mathbb{H}^1(S, \mathscr{C})$ and $\mathrm{H}^1(S, \mathscr{F})[\varphi] := \ker\big(\mathrm{H}^1(\varphi) : \mathrm{H}^1(S, \mathscr{F}) \to \mathrm{H}^1(S, \mathscr{G})\big)$. Then,*

(a) *There are distinguished triangles*

$$\mathscr{G}[-1] \to \mathscr{C} \to \mathscr{F} \quad \text{and} \quad \ker \varphi \to \mathscr{C} \to (\operatorname{coker} \varphi)[-1].$$

In particular, these give rise to exact sequences

$$0 \longrightarrow \frac{\mathrm{H}^0(S,\mathscr{G})}{\varphi\,\mathrm{H}^0(S,\mathscr{F})} \longrightarrow \mathrm{H}^1(S,\mathscr{F} \xrightarrow{\varphi} \mathscr{G}) \longrightarrow \mathrm{H}^1(S,\mathscr{F})[\varphi] \longrightarrow 0 \tag{6.2}$$

$$0 \longrightarrow \mathrm{H}^1(S,\ker\varphi) \longrightarrow \mathrm{H}^1(S,\mathscr{F} \xrightarrow{\varphi} \mathscr{G}) \longrightarrow \mathrm{H}^0(S,\operatorname{coker}\varphi). \tag{6.3}$$

(b) $\mathrm{H}^1(S,\mathscr{F} \xrightarrow{\varphi} \mathscr{G})$ *is in natural bijection with pairs* $(T,\psi:\varphi_*T \to \mathscr{G})$ *– where* T *is an* $\mathscr{F}$*-torsor and* ψ *is an isomorphism of* $\mathscr{G}$*-torsors – up to isomorphism of torsors.*

Proof. Part **(a)** is an exercise in unpacking definitions. Part **(b)** is [Lan21c, Lemma 2.3.8]. In that lemma, **(b)** is stated only in the case that $\mathscr{F},\mathscr{G}$ are both (represented by) smooth, commutative group schemes, but the proof given works in general.[3] ∎

The proposition we wish to generalize is the following.

Proposition 6.2.3 ([Lan21b, Proposition 3.26])**.** *Fix* $n \geq 1$ *such that* $\operatorname{char} K \nmid n$*. Then,*

$$\#\operatorname{Sel}_n(E) \leq \#\,\mathrm{H}^0(B,\mathscr{E}[n]) \cdot \#\,\mathrm{H}^1(B,\mathscr{E}^0[n]).$$

We want a version of this result which works in arbitrary characteristics. As previously alluded, the key will be to replace $\mathrm{H}^1(B,\mathscr{E}^0[n])$ with $\mathrm{H}^1(B,\mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0)$, resulting in Proposition 6.2.5. We prove this generalization by simply making the necessary adjustments to Landesman's proof of Proposition 6.2.3. We first remark that [Lan21b, Lemma 3.29] holds as stated in arbitrary characteristic with exactly the same proof (the main point is that [Č16, Proposition 4.5] does not require any characteristic assumption).

Lemma 6.2.4 ([Lan21b, Lemma 3.29])**.** *Fix any* $n \geq 1$*. Then,* $\#\text{Ш}(E)[n] \leq \#\,\mathrm{H}^1(B,\mathscr{E}^0)[n]$

Proposition 6.2.5. *Fix any* $n \geq 1$*. Then,*

$$\#\operatorname{Sel}_n(E) \leq \#\,\mathrm{H}^0(B,\mathscr{E}[n]) \cdot \#\,\mathrm{H}^1(B,\mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0)$$

Proof. For a sheaf $\mathscr{F}$ on B, let $Q_n(\mathscr{F}) := \mathrm{H}^0(B,\mathscr{F})/n\,\mathrm{H}^0(B,\mathscr{F})$. Consider the following exact sequences, the former coming from [Sil09, Theorem X.4.2] (as $\mathrm{H}^0(B,\mathscr{E}) = E(K)$) and the latter coming from (6.2).

$$0 \longrightarrow Q_n(\mathscr{E}) \longrightarrow \operatorname{Sel}_n(E) \longrightarrow \text{Ш}(E)[n] \longrightarrow 0$$

$$0 \longrightarrow Q_n(\mathscr{E}^0) \longrightarrow \mathrm{H}^1(B,\mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0) \longrightarrow \mathrm{H}^1(B,\mathscr{E}^0)[n] \longrightarrow 0,$$

From these, it follows that

$$\frac{\#\operatorname{Sel}_n(E)}{\#\,\mathrm{H}^1(B,\mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0)} = \frac{\#Q_n(\mathscr{E})}{\#Q_n(\mathscr{E}^0)} \cdot \frac{\#\text{Ш}(E)[n]}{\#\,\mathrm{H}^1(B,\mathscr{E}^0)[n]}.$$

Now, [Lan21b, (3-17) in the proof of Lemma 3.28] shows that

$$\frac{\#Q_n(\mathscr{E})}{\#Q_n(\mathscr{E}^0)} = \frac{\#\,\mathrm{H}^0(B,\mathscr{E}[n])}{\#\,\mathrm{H}^0(B,\mathscr{E}^0[n])} \text{ and so } \frac{\#\operatorname{Sel}_n(E)}{\#\,\mathrm{H}^1(B,\mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0)} = \frac{\#\,\mathrm{H}^0(B,\mathscr{E}[n])}{\#\,\mathrm{H}^0(B,\mathscr{E}^0[n])} \cdot \frac{\#\text{Ш}(E)[n]}{\#\,\mathrm{H}^1(B,\mathscr{E}^0)[n]}.$$

The claim now follows by appealing to the bounds $\#\text{Ш}(E)[n]/\#\,\mathrm{H}^1(B,\mathscr{E}^0)[n] \leq 1$ (by Lemma 6.2.4) and $1/\#\,\mathrm{H}^0(B,\mathscr{E}^0[n]) \leq 1$. ∎

[3] Recall that, for us, 'torsor' means fppf-locally trivial right torsor sheaf

Corollary 6.2.6. *Fix any $n \geq 1$. Then*

$$\#\operatorname{Sel}_n(E) \leq \#E(K)[n] \cdot \#\operatorname{H}^1(B, \mathscr{E}^0[n]) \cdot \#\operatorname{H}^0(B, \mathscr{E}^0/n\mathscr{E}^0).$$

Proof. This follows from Proposition 6.2.5, noting that $\operatorname{H}^0(B, \mathscr{E}[n]) = E(K)[n]$ by the Néron mapping property and that $\#\operatorname{H}^1(B, \mathscr{E}^0 \xrightarrow{[n]} \mathscr{E}^0) \leq \#\operatorname{H}^1(B, \mathscr{E}[n]) \cdot \operatorname{H}^0(B, \mathscr{E}/n\mathscr{E})$ by (6.3). ■

Remark 6.2.7. When $\operatorname{char} K \nmid n$, or when E has everywhere semistable reduction, $[n] : \mathscr{E}^0 \to \mathscr{E}^0$ is surjective, so in these cases, Corollary 6.2.6 states

$$\#\operatorname{Sel}_n(E) \leq \#E(K)[n] \cdot \#\operatorname{H}^1(B, \mathscr{E}^0[n]) = \#\operatorname{H}^0(B, \mathscr{E}[n]) \cdot \#\operatorname{H}^1(B, \mathscr{E}^0[n]).$$

In particular, it recovers [Lan21b, Proposition 3.26]. ◦

Assumption. For the remainder of the section, assume that $\operatorname{char} K = 2$.

As suggested by Corollary 6.2.6, in order to bound $\#\operatorname{Sel}_2(E)$, we work out upper bounds for $\#\operatorname{H}^1(B, \mathscr{E}^0[2])$ and $\#\operatorname{H}^0(B, \mathscr{E}^0/2\mathscr{E}^0)$. Our strategy for obtaining these upper bounds will be to stratify B according to the reduction type of E, and so reduce ourselves to bounding the cohomology of various well-understood finite group schemes.

Notation 6.2.8. Let $D = \sum_{i=1}^k n_i[p_i]$ be a divisor on B, so $\deg D = \sum_{i=1}^k n_i \deg p_i$. Define the functions

$$\operatorname{Tr}(D) := \sum_{i=1}^k n_i \quad \text{and} \quad \operatorname{rdeg}(D) := \sum_{i=1}^k \deg p_i.$$

Remark 6.2.9. Below, we will produce two different bounds on $\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E)$. The first (Corollary 6.2.16) will roughly be of the form $O(\operatorname{rdeg}(N))$ and so will be "horizontal" in the sense that it is big whenever E has bad reduction at lots of places. In contract, the second bound (Theorem 6.2.20) will roughly be of the form $O(\operatorname{Tr}(N))$ and so will be "vertical" in the sense that it is big whenever E has bad reduction at a few places whose coefficients in N are large. Neither of these bounds alone will suffice for our purposes, but Proposition 6.3.2 will show that $\min\{\operatorname{rdeg}(N), \operatorname{Tr}(N)\} = O(\deg N/\log\deg N)$, so the minimum of these bounds will be of the desired form (we will justify later that $\deg N = O(\operatorname{ht}(E))$). ◦

Lemma 6.2.10. *Let $i_0 : S_0 \hookrightarrow B$ be the (reduced) closed subscheme consisting of points of additive reduction for E, and let $U' = B \setminus S_0$. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{H}^0(B, \mathscr{E}^0/2\mathscr{E}^0) = \dim_{\mathbb{F}_2} \operatorname{H}^0(S_0, \mathbb{G}_a) \leq \operatorname{rdeg}(N).$$

Proof. Note that $[2] : \mathscr{E}^0_{U'} \to \mathscr{E}^0_{U'}$ is surjective and that $\mathscr{E}^0_{S_0} \simeq \mathbb{G}_{a,S_0}$ since S_0 is a disjoint union of spectra of perfect fields. Hence, $\mathscr{E}^0/2\mathscr{E}^0 \simeq i_{0,*}\mathscr{E}^0_{S_0}/2\mathscr{E}^0_{S_0} \simeq i_{0,*}\mathbb{G}_{a,S_0}$. The claim follows. ■

Lemma 6.2.11. *Let $p = 2$. Then,*

$$\begin{aligned}
\dim_{\mathbb{F}_p} \operatorname{H}^1(B, \quad \mu_p) &\leq g \\
\dim_{\mathbb{F}_p} \operatorname{H}^1(B, \mathbb{Z}/p\mathbb{Z}) &\leq g+1 \\
\dim_{\mathbb{F}_p} \operatorname{H}^1(B, \quad \alpha_p) &\leq [k : \mathbb{F}_p]g = rg
\end{aligned}$$

Proof. These can all be deduced from [Mil80, Section III.4]; we briefly indicate the relevant computations here. The short exact sequences $0 \to \mu_p \to \mathbb{G}_m \xrightarrow{(-)^p} \mathbb{G}_m \to 0$, $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \xrightarrow{x \mapsto x^p - x} \mathbb{G}_a \to 0$, and

$0 \to \alpha_p \to \mathbb{G}_a \xrightarrow{(-)^p} \mathbb{G}_a \to 0$ induce the following exact sequences on cohomology:

$$\begin{array}{lcll} 0 \longrightarrow & \dfrac{k^\times}{(k^\times)^p} & \longrightarrow \mathrm{H}^1(B,\mu_p) & \longrightarrow \mathrm{Pic}^0(B)[p] \longrightarrow 0 \\ 0 \longrightarrow & \mathrm{coker}\Big(k \xrightarrow{x\mapsto x^p - x} k\Big) & \longrightarrow \mathrm{H}^1(B,\mathbb{Z}/p\mathbb{Z}) & \longrightarrow \mathrm{H}^1(B,\mathscr{O}_B)^F \longrightarrow 0 \\ 0 \longrightarrow & \dfrac{k}{k^p} & \longrightarrow \mathrm{H}^1(B,\alpha_p) & \longrightarrow \mathrm{H}^1(B,\mathscr{O}_B). \end{array}$$

The claimed bounds now follow from the facts that k is perfect, $\dim_{\mathbb{F}_p} \mathrm{Pic}^0(B)[p] \le g$, $\dim_k \mathrm{H}^1(B,\mathscr{O}_B) = g$, $\dim_{\mathbb{F}_p} \mathrm{coker}\Big(k \xrightarrow{x\mapsto x^p-x} k\Big) = \dim_{\mathbb{F}_p} \ker\Big(k \xrightarrow{x\mapsto x^p-x} k\Big) = \dim_{\mathbb{F}_p} \mathbb{F}_p = 1$, $\dim_{\mathbb{F}_p} \mathrm{H}^1(B,\mathscr{O}_B)^F \le g$ (by [Mum08, Corollary on Page 133]), and $\dim_{\mathbb{F}_p} \mathrm{H}^1(B,\mathscr{O}_B) = [k:\mathbb{F}_p]\dim_k \mathrm{H}^1(B,\mathscr{O}_B) = rg$. ■

Lemma 6.2.12. *Let S be a finite, reduced k-scheme. Then, $\mathrm{H}^1(S,\mu_2) = 0 = \mathrm{H}^1(S,\alpha_2)$.*

Proof. It suffices to prove this when $S = \mathrm{Spec}\, F$ for a finite (so perfect) field F of characteristic 2. Then,

$$0 \longrightarrow \mu_2 \longrightarrow \mathbb{G}_m \xrightarrow{(-)^2} \mathbb{G}_m \longrightarrow 0 \text{ and } 0 \longrightarrow \alpha_2 \longrightarrow \mathbb{G}_a \xrightarrow{(-)^2} \mathbb{G}_a \longrightarrow 0,$$

show that $\mathrm{H}^1(F,\mu_2) \cong F^\times/(F^\times)^2$ and $\mathrm{H}^1(F,\alpha_2) \cong F/F^2$. Both of these vanish because F is perfect. ■

Lemma 6.2.13. *Let $i_0 : S_0 \hookrightarrow B$ be the (reduced) closed subscheme consisting of points of additive reduction for E, and let $U' = B \setminus S_0$ with open embedding $j' : U' \hookrightarrow B$. Then,*

$$\#\,\mathrm{H}^1(B,\mathscr{E}^0[2]) \le \#\,\mathrm{H}^1(B, j'_!\mathscr{E}^0_{U'}[2]),$$

where $j'_!$ is the usual extension-by-zero functor.[4]

Proof. Consider the exact sequence

$$0 \longrightarrow j'_!\mathscr{E}^0_{U'}[2] \longrightarrow \mathscr{E}^0[2] \longrightarrow i_{0,*}\mathscr{E}^0_{S_0}[2] \longrightarrow 0 \tag{6.4}$$

of abelian sheaves on B_{fppf}. Note that $\mathscr{E}^0_{S_0} \simeq \mathbb{G}_{a,S_0}$, so also $\mathscr{E}^0_{S_0}[2] \simeq \mathbb{G}_{a,S_0}[2] = \mathbb{G}_{a,S_0}$. The Leray spectral sequence for $\mathscr{E}^0_{S_0}[2]$ relative to $i_0 : S_0 \hookrightarrow B$ gives an inclusion $\mathrm{H}^1(B, i_{0,*}\mathscr{E}^0_{S_0}[2]) \longleftrightarrow \mathrm{H}^1(S_0,\mathscr{E}^0[2]) \cong \mathrm{H}^1(S_0,\mathbb{G}_a) = 0$. Hence, from (6.4), we obtain an exact sequence $\mathrm{H}^1(B, j'_!\mathscr{E}^0_{U'}[2]) \longrightarrow \mathrm{H}^1(B,\mathscr{E}^0[2]) \longrightarrow 0$, from whence the claim follows. ■

Proposition 6.2.14. *Suppose that E/K is ordinary. Let δ be the number of places of supersingular or bad reduction for E. Then,*

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(B,\mathscr{E}^0[2]) \le 2g + \max\{1,\delta\} \le 2g+1+\delta.$$

Proof. Let $i_0 : S_0 \hookrightarrow B$ and $j' : U' \hookrightarrow B$ be as in Lemma 6.2.13. By that lemma, it suffices to bound $\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_!\mathscr{E}^0_{U'}[2])$. Let $i_1 : S_1 \hookrightarrow B$ (resp. $i_2 : S_2 \hookrightarrow B$) be the reduced closed subscheme consisting of points of multiplicative (resp. supersingular) reduction. Let $U = U' \setminus (S_1 \cup S_2)$ with open embedding $j : U \hookrightarrow B$. Consider the exact sequence

$$0 \longrightarrow j_!\mathscr{E}^0_U[2] \longrightarrow j'_!\mathscr{E}^0_{U'}[2] \longrightarrow i_{1,*}\mathscr{E}^0_{S_1}[2] \oplus i_{2,*}\mathscr{E}^0_{S_2}[2] \longrightarrow 0,$$

[4] For any sheaf $\mathscr{F}$ on U'_{fppf}, $j'_!\mathscr{F}$ is the sheafification of the presheaf on B_{fppf} given by

$$(X \to B) \longmapsto \begin{cases} \mathscr{F}(X \to U') & \text{if } \mathrm{im}(X \to B) \subset U' \\ 0 & \text{otherwise.} \end{cases}$$

from which we deduce that

$$h^1\left(j'_!\mathscr{E}^0_{U'}[2]\right) \le h^1\left(j_!\mathscr{E}^0_U[2]\right) + h^1\left(i_{1,*}\mathscr{E}^0_{S_1}[2]\right) + h^1\left(i_{2,*}\mathscr{E}^0_{S_2}[2]\right), \tag{6.5}$$

where $h^1(\mathscr{F}) := \dim_{\mathbb{F}_2} \mathrm{H}^1(B, \mathscr{F})$ for any 2-torsion abelian sheaf on B_{fppf}. For $n = 1, 2,$, the Leray spectral sequence for $\mathscr{E}^0_{S_n}[2]$ relative to the inclusion $i_n : S_n \hookrightarrow B$ gives an embedding $\mathrm{H}^1(B, i_{n,*}\mathscr{E}^0_{S_n}[2]) \hookrightarrow \mathrm{H}^1(S_n, \mathscr{E}^0_{S_n}[2])$, so

$$h^1\left(i_{n,*}\mathscr{E}^0_{S_n}[2]\right) \le \dim_{\mathbb{F}_2} \mathrm{H}^1(S_n, \mathscr{E}^0[2]). \tag{6.6}$$

We now estimate each summand in (6.5) separately.

- Since $\mathscr{E}^0$ has multiplicative reduction over S_1, $\mathscr{E}^0_{S_1}[2]$ is a twist of μ_2 over S_1, and so must be isomorphic to μ_2 as $\underline{\mathrm{Aut}}(\mu_2)$ is trivial. Thus, $\mathrm{H}^1(S_1, \mathscr{E}^0[2]) = \mathrm{H}^1(S_1, \mu_2) = 0$ by Lemma 6.2.12.
- Since $\mathscr{E}^0$ has supersingular reduction over S_2, the kernel of the Frobenius isogeny is isomorphic to α_2 (e.g. by [Ulm91, Proposition 2.1]), and so Lemma 6.1 produces an exact sequence $0 \to \alpha_2 \to \mathscr{E}^0_{S_2}[2] \to \alpha_2 \to 0$. Hence, $\dim_{\mathbb{F}_2} \mathrm{H}^1(S_2, \mathscr{E}^0[2]) \le 2 \dim_{\mathbb{F}_2} \mathrm{H}^1(S_2, \alpha_2) = 0$ with the equality by Lemma 6.2.12.
- This leaves the good, ordinary locus U. In this case, the kernel of the Frobenius isogeny is a twist μ_2, so itself isomorphic to μ_2. Lemma 6.1 gives $0 \to \mu_2 \to \mathscr{E}^0_U[2] \to \underline{\mathbb{Z}/2\mathbb{Z}} \to 0$, so

  $$h^1\left(j_!\mathscr{E}^0_U[2]\right) \le h^1(j_!\mu_2) + h^1(j_!\underline{\mathbb{Z}/2\mathbb{Z}}) \tag{6.7}$$

  To bound these summands, we appeal to the exact sequences

  $$0 \longrightarrow j_!\mu_2 \longrightarrow \mu_2 \longrightarrow \bigoplus_{n=0}^{2} i_{n,*}\mu_2 \longrightarrow 0 \text{ and } 0 \longrightarrow j_!\underline{\mathbb{Z}/2\mathbb{Z}} \longrightarrow \underline{\mathbb{Z}/2\mathbb{Z}} \longrightarrow \bigoplus_{n=0}^{2} i_{n,*}\underline{\mathbb{Z}/2\mathbb{Z}} \longrightarrow 0.$$

  From the first of these, we deduce that (see Lemma 6.2.11)

  $$h^1(j_!\mu_2) \le h^1(\mu_2) \le g. \tag{6.8}$$

  The second of these gives rise to the sequence $\mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^{\#S_0+\#S_1+\#S_2} \to \mathrm{H}^1(B, j_!\underline{\mathbb{Z}/2\mathbb{Z}}) \to \mathrm{H}^1(B, \underline{\mathbb{Z}/2\mathbb{Z}})$ from which we deduce

  $$h^1(j_!\underline{\mathbb{Z}/2\mathbb{Z}}) \le h^1(\underline{\mathbb{Z}/2\mathbb{Z}}) + \max\{0, \#S_0 + \#S_1 + \#S_2 - 1\} \le g + \max\{1, \#S_0 + \#S_1, \#S_2\} \tag{6.9}$$

  (with later inequality by Lemma 6.2.11). Finally, combining (6.7), (6.8), and (6.9) shows

  $$h^1(j_!\mathscr{E}^0_U[2]) \le h^1(j_!\mu_2) + h^1(j_!\underline{\mathbb{Z}/2\mathbb{Z}}) \le 2g + \max\{1, \#S_0 + \#S_1 + \#S_2\}.$$

To finish, combine the above three bullet points with (6.5) and (6.6). ■

Proposition 6.2.15. *Suppose that E/K is supersingular and recall $r = [k : \mathbb{F}_2]$. Then,*

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(B, \mathscr{E}^0[2]) \le 2rg.$$

Proof. Let $i_0 : S_0 \hookrightarrow B$ and $j' : U' \hookrightarrow B$ be as in Lemma 6.2.13. By that lemma, it suffices to bound $\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_!\mathscr{E}^0_{U'}[2])$. Note that, because E/K is supersingular, it has constant j-invariant and so has everywhere potentially good reduction. Hence, all of its bad reduction is additive, so $\mathscr{E}^0_{U'}$ is an elliptic scheme over U'. Let α be the kernel of the Frobenius isogeny on $\mathscr{E}^0_{U'}$, and let $\alpha^\vee$ be its Cartier dual. By applying $j'_!$ to Lemma 6.1, there is an exact sequence

$$0 \longrightarrow j'_! \alpha \longrightarrow j'_! \mathscr{E}^0_{U'}[2] \longrightarrow j'_! \alpha^\vee \longrightarrow 0,$$

so $\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_! \mathscr{E}^0_{U'}[2]) \leq \dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_! \alpha) + \dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_! \alpha^\vee)$. Now, let $U \subset U'$ be an open such that $\operatorname{Pic} U = 0$, and let $Z := U' \setminus U$ with its reduced scheme structure. Note that $\operatorname{Pic} Z = 0$ as well, since Z is finite. Hence, [Ulm91, Proposition 2.1] tells us that $\alpha_U \simeq \alpha_{2,U}$ and $\alpha_Z \simeq \alpha_{2,Z}$. Letting $j : U \hookrightarrow B$ and $i : Z \hookrightarrow B$ be the natural immersions, we get an exact sequence

$$0 \longrightarrow j_! \alpha_{2,U} \longrightarrow j'_! \alpha \longrightarrow i_* \alpha_{2,Z} \longrightarrow 0,$$

as well as a similar one with $j'_! \alpha^\vee$ in place of $j'_! \alpha$. Thus,

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j'_! \mathscr{E}^0_{U'}[2]) \leq 2\big(\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j_! \alpha_{2,U}) + \dim_{\mathbb{F}_2} \mathrm{H}^1(B, i_* \alpha_{2,Z})\big)\,. \tag{6.10}$$

We separately bound the two summands in (6.10).

- The exact sequence $0 \to j_! \alpha_{2,U} \to \alpha_{2,B} \to i_* \alpha_{2,Z} \oplus i_{0,*} \alpha_{2,S_0} \to 0$ shows that

  $$\dim_{\mathbb{F}_2} \mathrm{H}^1(B, j_! \alpha_{2,U}) \leq \dim_{\mathbb{F}_2} \mathrm{H}^1(B, \alpha_2) + \dim_{\mathbb{F}_2} \mathrm{H}^0(Z \sqcup S_0, \alpha_2) \leq rg,$$

  with the latter inequality by Lemma 6.2.11.

- From the Leray spectral sequence, we get an embedding $\mathrm{H}^1(B, i_* \alpha_2) \hookrightarrow \mathrm{H}^1(Z, \alpha_2)$, and $\mathrm{H}^1(Z, \alpha_2) = 0$ by Lemma 6.2.12.

The two above bullet points combined with (6.10) give the desired result. ∎

Corollary 6.2.16.

$$\operatorname{Sel}_2(E) \leq \begin{cases} 2g + 2 + \delta + \operatorname{rdeg}(N) & \text{if } E \text{ ordinary} \\ 2rg + \operatorname{rdeg}(N) & \text{if } E \text{ supersingular,} \end{cases}$$

Proof. Combine Corollary 6.2.6, Lemma 6.2.10, and Propositions 6.2.14 and 6.2.15. ∎

Remark 6.2.17. Because $\operatorname{rdeg}(N) = \operatorname{rdeg}(\Delta)$ can grow like $\deg \Delta = 12 \operatorname{ht}(E)$ (with equality by Remark 3.1.6), Corollary 6.2.16 is not a strong enough bound for our purposes. In order to remedy the situation, we now produce a second bound for $\operatorname{Sel}_2(E)$ whose main term is instead of the form $\operatorname{Tr}(N)$. We will later show that the minimum of these two bounds is $O(\operatorname{ht}(E)/\log \operatorname{ht}(E))$. ∘

Our second bound will come from passing to a field extension where E attains everywhere semistable reduction.

Proposition 6.2.18. *Suppose that E has everywhere semistable reduction. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq \begin{cases} 2g + 2 + \delta & \text{if } E \text{ ordinary} \\ 2rg & \text{if } E \text{ supersingular,} \end{cases}$$

where δ is the number of places of bad or supersingular reduction for E.

Proof. Combine Remark 6.2.7 and Propositions 6.2.14 and 6.2.15. ∎

Lemma 6.2.19. *Let $L = K(E[3])$. Then, E_L has everywhere semistable reduction, and L has genus*

$$g(L) \leq 24 \operatorname{Tr}(N) + 48 g(K).$$

Proof. Let $\ell = 3$, let $G_K = \operatorname{Gal}(K^s/K)$, and let $\rho_K : G_K \to \operatorname{Aut}(T_\ell(E))$ be the Galois action on E's ℓ-adic Tate module, so $\operatorname{Gal}(L/K) \cong \operatorname{im}(\rho_K \bmod \ell)$ has size dividing $\#\operatorname{GL}_2(\mathbb{F}_\ell) = 48$. Furthermore, Raynaud's semistability criterion [GRR72, Exposé IX, Proposition 4.7] shows that E_L has everywhere semistable reduction over L.

To bound the genus of L, we analyze ramification in L/K. Let $k' = L \cap \overline{k}$, and let C denote the smooth k'-curve with function field L. Let $K' := Kk'$, the function field of $B_{k'}$. Since K'/K is simply an extension of the constant field, all ramification in L/K arises from ramification in L/K'. For a place $w \in C$ of L, set

$$G_i(w) := \left\{\sigma \in \operatorname{Gal}(L/K') : \sigma(x) \equiv x \bmod \mathfrak{p}_w^{i+1} \text{ for all } x \in \mathscr{O}_w\right\} \text{ and } g_i(w) := \#G_i(w).$$

Riemann-Hurwitz combined with [Ser79, Proposition IV.1.4] tells us that

$$2g(L) - 2 = [L : K'](2g(K) - 2) + \sum_w \sum_{i \geq 0} (g_i(w) - 1). \tag{6.11}$$

For any $w \in C$ above some $v \in B_{k'}$, we have an injection $T_\ell(E)^{G_0(w)} \hookrightarrow E[\ell]^{G_0(w)}$ so $\dim_{\mathbb{Q}_\ell} V_\ell(E)^{G_0(w)} \leq \dim_{\mathbb{F}_\ell} E[\ell]^{G_0(w)}$. Letting $N' \in \operatorname{Div}(B_{k'})$ denote the pullback of N, this gives the below inequality:

$$\operatorname{ord}_v(N') = \dim_{\mathbb{Q}_\ell}\left(\frac{V_\ell(E)}{V_\ell(E)^{G_0(w)}}\right) + \sum_{i \geq 1} \frac{g_i(w)}{g_0(w)} \dim_{\mathbb{F}_\ell}\left(\frac{E[\ell]}{E[\ell]^{G_i(w)}}\right) \geq \sum_{i \geq 0} \frac{g_i(w)}{g_0(w)} \dim_{\mathbb{F}_\ell}\left(\frac{E[\ell]}{E[\ell]^{G_i(w)}}\right).$$

Furthermore, for any $w \in C$ above some $v \in B_F$ and any $i \geq 0$, one has $E[\ell] = E[\ell]^{G_i(w)} \iff g_i(w) = 1$ (since $G_i(w) \subset \operatorname{Gal}(L/K) \hookrightarrow \operatorname{GL}(E[\ell])$), and so $g_i(w) \dim_{\mathbb{F}_\ell}(E[\ell]/E[\ell]^{G_i(w)}) \geq (g_i(w) - 1)$ always. Hence,

$$g_0(w) \operatorname{ord}_v(N) \geq \sum_{i \geq 0} g_i(w) \dim_{\mathbb{F}_\ell}\left(\frac{E[\ell]}{E[\ell]^{G_i(w)}}\right) \geq \sum_{i \geq 0} (g_i(w) - 1) \tag{6.12}$$

Thus,

$$\begin{aligned}
2g(L) - 2 &= [L : K'](2g(K) - 2) + \sum_{w \in C} \sum_{i \geq 0} (g_i(w) - 1) && \text{by (6.11)} \\
&\leq [L : K'](2g(K) - 2) + \sum_{v \in B_{k'}} \left(\sum_{w \mid v} g_0(w)\right) \operatorname{ord}_v(N') && \text{by (6.12)} \\
&\leq [L : K'](2g(K) - 2) + \sum_{v \in B_{k'}} [L : K'] \operatorname{ord}_v(N') \\
&= [L : K'](2g(K) - 2) + [L : K'] \operatorname{Tr}(N') \\
&= [L : K'](2g(K) - 2) + [L : K] \operatorname{Tr}(N) && \text{because } \operatorname{Tr}(N') = [K' : K] \operatorname{Tr}(N).
\end{aligned}$$

Rearranging gives $g(L) \leq [L : K']g(K) + \frac{1}{2}[L : K] \operatorname{Tr}(N) + (1 - [L : K']) \leq [L : K]g(K) + \frac{1}{2}[L : K] \operatorname{Tr}(N)$. The claim follows as $[L : K] \leq 48$. ∎

Theorem 6.2.20.

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq \begin{cases} 48 \operatorname{Tr}(N) + 48\delta + 96g + 6 & \text{if } E \text{ ordinary} \\ 2304r(\operatorname{Tr}(N) + 2g) & \text{if } E \text{ supersingular,} \end{cases}$$

where δ is the number of places of bad or supersingular reduction for E and $r = [k : \mathbb{F}_2]$.

Proof. Let $L = K(E[3])$, so E_L has everywhere semistable reduction (Lemma 6.2.19). The Hochschild-

Serre spectral sequence [Mil80, Remark III.2.21(a)] gives rise to an inflation-restriction sequence $0 \to \mathrm{H}^1(\mathrm{Gal}(L/K), E[2](L)) \to \mathrm{H}^1(K, E[2]) \to \mathrm{H}^1(L, E[2])$ which shows that

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \le \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/L) + \dim_{\mathbb{F}_2} \mathrm{H}^1(\mathrm{Gal}(L/K), E[2](L)). \tag{6.13}$$

Note that $\mathrm{Gal}(L/K) \le \mathrm{GL}_2(\mathbb{F}_3)$ and that the composition factors of $\mathrm{GL}_2(\mathbb{F}_3)$ are four copies of $\mathbb{Z}/2\mathbb{Z}$ and one copy of $\mathbb{Z}/3\mathbb{Z}$. This bounds the composition factors of $\mathrm{Gal}(L/K)$; since the cohomology of a cyclic group acting on a module M is always a subquotient of M, one can inductively apply inflation-restriction in order to conclude that

$$\dim_{\mathbb{F}_2} \mathrm{H}^1(\mathrm{Gal}(L/K), E[2](L)) \le 4 \dim_{\mathbb{F}_2} E[2](L) \le \begin{cases} 4 & \text{if } E \text{ ordinary} \\ 0 & \text{if } E \text{ supersingular.} \end{cases} \tag{6.14}$$

Let δ_L (resp. δ) denote the number of places of bad or supersingular reduction for E_L (resp. E). Then,

$$\begin{aligned} \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/L) &\le \begin{cases} 2g(L) + 2 + \delta_L & \text{if } E \text{ ordinary} \\ 2[(L \cap \overline{\mathbb{F}}_2) : \mathbb{F}_2] g(L) & \text{if } E \text{ supersingular} \end{cases} && \text{by Proposition 6.2.18} \\ &\le \begin{cases} 2(24\,\mathrm{Tr}(N) + 48g(K)) + 2 + 48\delta & \text{if } E \text{ ordinary} \\ 96r(24\,\mathrm{Tr}(N) + 48g(K)) & \text{if } E \text{ supersingular} \end{cases} && \text{by Lemma 6.2.19 and } [L:K] \le 48 \\ &= \begin{cases} 48\,\mathrm{Tr}(N) + 96g(K) + 48\delta + 2 & \text{if } E \text{ ordinary} \\ 2304r(\mathrm{Tr}(N) + 2g(K)) & \text{if } E \text{ supersingular.} \end{cases} \end{aligned}$$

The claim now follows from the above combined with (6.13) and (6.14). ■

Corollary 6.2.21.

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \le \begin{cases} 48 \min\{\mathrm{Tr}(N), \mathrm{rdeg}(N)\} + 48\delta + 96g + 6 & \text{if } E \text{ ordinary} \\ 2304r \cdot \min\{\mathrm{Tr}(N), \mathrm{rdeg}(N)\} + 4608rg & \text{if } E \text{ supersingular,} \end{cases}$$

where δ is the number of places of bad or supersingular reduction for E.

Proof. Combine Theorem 6.2.20 and Corollary 6.2.16. ■

6.3 Summary of all Obtained Bounds

We obtained above, in various situations, bounds for the size of 2-Selmer groups of elliptic curves over global function fields. However, in each case, the bound was given in terms of the certain functions (e.g. $\mathrm{Tr}, \mathrm{rdeg}$; see Notation 6.2.8) on $\mathrm{Div}(B)$ which we now bound in terms of the usual degree function.

Lemma 6.3.1. *Let $D \subset B$ be an effective divisor. Fix $x \in \mathbb{R}$ such that every point in the support of D has degree $< x$. Then,*

$$\#\operatorname{supp} D \le \frac{2g+2}{q-1} q^{x+1}.$$

Proof. One can deduce from the Hasse-Weil bound that $\#B(\mathbb{F}_{q^r}) \le (2g+2)q^r$ for any $r \ge 1$. Hence,

$$\#\operatorname{supp} D \le \sum_{1 \le r < x} \#B(\mathbb{F}_{q^r}) \le (2g+2) \sum_{r=1}^{\lfloor x \rfloor} q^r \le \frac{2g+2}{q-1} q^{x+1}.$$ ■

Proposition 6.3.2. *Let $D \subset B$ be an effective divisor of degree $d \geq 2$. Then,*

$$\min\{\mathrm{Tr}(D), \mathrm{rdeg}(D)\} \leq \frac{2d \log q}{\log d} + \frac{(2g+2)q}{q-1}\sqrt{d}\log_q\left(\sqrt{d}\right) = O\left(\frac{d}{\log d}\right) \tag{6.15}$$

$$\#\operatorname{supp} D \leq \frac{2d \log q}{\log d} + \frac{(2g+2)q}{q-1}\sqrt{d} = O\left(\frac{d}{\log d}\right). \tag{6.16}$$

Proof. To ease notation, define the function $M(D) := \min\{\mathrm{Tr}(D), \mathrm{rdeg}(D)\}$. Write $D = \sum_p n_p[p]$, so $d = \deg D = \sum_p n_p \deg p$. Consider the function $f(x) := \frac{1}{2}\frac{\log x}{\log q} = \log_q(\sqrt{x})$, and split D as $D = D_1 + D_2$, where

$$D_1 = \sum_{\substack{p \\ \deg p < f(d)}} n_p[p] \quad \text{and} \quad D_2 = \sum_{\substack{p \\ \deg p \geq f(d)}} n_p[p].$$

By Lemma 6.3.1, we have

$$\#\operatorname{supp} D_1 \leq \frac{2g+2}{q-1}q^{f(d)+1} = \frac{(2g+2)q}{q-1}\sqrt{d} \text{ and so } M(D_1) \leq \mathrm{rdeg}(D_1) \leq \#\operatorname{supp} D_1 \cdot f(d) \leq \frac{(2g+2)q}{q-1}\sqrt{d}\log_q(\sqrt{d}).$$

Furthermore,

$$d = \deg D \geq \deg D_2 \geq f(d) \sum_{\deg p \geq f(d)} n_p = f(d)\,\mathrm{Tr}(D_2) \text{ and so } M(D_2) \leq \mathrm{Tr}(D_2) \leq \frac{d}{f(d)} = \frac{2d\log q}{\log d}.$$

The claim follows, as $M(D) \leq M(D_2) + M(D_1)$ and $\#\operatorname{supp} D \leq \mathrm{Tr}(D_2) + \#\operatorname{supp} D_1$. ■

Lemma 6.3.3. *Let E/K be a non-isotrivial elliptic curve with j-invariant $j : B \to \mathbb{P}^1$. Let $N, \Delta \in \mathrm{Div}(B)$ denote, respectively, the conductor and minimal discriminant of E. Then,*

$$\deg_s(j) \leq \frac{\deg \Delta}{\deg_i(j)} \leq 6(\deg N + 2g - 2),$$

where $\deg_s(j)$ (resp. $\deg_i(j)$) denotes the separable (resp. inseparable) degree of the j-map.

Proof. We first remark that the usual formula for the j-invariant (see [Sil09, Section III.1]), applied to minimal models of E at every place of K, directly shows that $j^*[\infty] \leq \Delta$, so $\deg(j) \leq \deg \Delta$. Furthermore, "Szpiro's conjecture for function fields" [PS00, Théorème 0.1] asserts that $\deg \Delta \leq 6\deg_i(j)(\deg N + 2g - 2)$. Taken together, these say

$$\deg(j) \leq \deg \Delta \leq 6\deg_i(j)(\deg N + 2g - 2).$$

Divide by $\deg_i(j)$ to conclude. ■

Theorem 6.3.4. *Use notation as in Setup 1.1. Let E/K be an elliptic curve with conductor $N \in \mathrm{Div}(B)$. Let $n := \deg N$.*

(a) *Assume $\mathrm{char}\, K = 2$ and that E is ordinary. Then,*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \leq 48\left[\frac{4n\log q}{\log n} + \frac{12(n+2g-2)\log q}{\log(n+2g-2)+\log 6} + \frac{(2g+2)q}{q-1}\left(\sqrt{6(n+2g-2)} + \sqrt{n} + \sqrt{n}\log_q\left(\sqrt{n}\right)\right)\right] + 96g + 6$$

if $n \geq 2$.

(b) *Assume $\mathrm{char}\, K = 2$, and that E is ordinary and isotrivial. Then,*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E) \leq 48\left[\frac{4n\log q}{\log n} + \frac{(2g+2)q}{q-1}\left(\sqrt{n} + \sqrt{n}\log_q\left(\sqrt{n}\right)\right)\right] + 96g + 6$$

if $n \geq 2$.

(c) *Assume* $\operatorname{char} K = 2$ *and that* E *is supersingular. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq 2304r\left[\frac{2n \log q}{\log n} + \frac{(2g+2)q}{q-1}\sqrt{n}\log_q(\sqrt{n})\right] + 4608rg,$$

if $n \geq 2$*, where* $r = [k : \mathbb{F}_2]$.

(d) *Assume* $\operatorname{char} K \geq 5$*. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq 78\left[\frac{2n \log q}{\log n} + \frac{(2g+2)q}{q-1}\sqrt{n}\right] + 24g + 6,$$

if $n \geq 2$.

(e) *Assume* $\operatorname{char} K \neq 2$ *and that* $E[2](K) \neq 0$*. Then,*

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq 3\left[\frac{2n \log q}{\log n} + \frac{(2g+2)q}{q-1}\sqrt{n}\right] + 4g + 2$$

if $n \geq 2$.

In any of the above cases,

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) = O\left(\frac{n}{\log n}\right) \leq O\left(\frac{\operatorname{ht}(E)}{\log \operatorname{ht}(E)}\right)$$

as $n \to \infty$.

Proof. We start with **(e)**. This follows simply from combining Proposition 6.1.3 with (6.16) along with the observation that the set of bad places for E is precisely $\operatorname{supp} N$. Similarly, **(d)** follows from a combination of Proposition 6.1.5 and (6.16). Parts **(c)**, **(b)**, and **(a)** follow from combining Corollary 6.2.21 with Proposition 6.3.2. The only subtlety is in bounding the quantity δ appearing in Corollary 6.2.21 when proving **(a)**. One does this by appealing to (6.16) twice. To bound the number of places of bad reduction, one applies (6.16) to the conductor of E. To bound the number of places of supersingular reduction, one first recalls that, when $\operatorname{char} K = 2$, these are precisely the zeros of the j-invariant $j \colon B \to \mathbb{P}^1$. Assume j is nonconstant (as is the case for all curves to which part **(a)** applies). Let $Z := j^*[0] \in \operatorname{Div}(B)$ with reduction Z_{red}. We bound the number of zeros of j by applying (6.16) to Z_{red}, making use of the observation

$$\deg Z_{\mathrm{red}} \leq \frac{\deg Z}{\deg_i(j)} = \frac{\deg(j)}{\deg_i(j)} = \deg_s(j) \leq 6(n + 2g - 2),$$

with final inequality holding by Lemma 6.3.3. This proves **(a)**. Let $\Delta \in \operatorname{Div}(B)$ denote the minimal discriminant of E. The final claim of the theorem statement is clear once one notes that $n \leq \deg \Delta = 12 \operatorname{ht}(E)$, with the inequality following e.g. from Ogg's formula [Ogg67, Theorem 2], and the equality holding by Remark 3.1.6. ∎

7 Proof of the Main Result

In this section, we prove Theorem B (see Theorem 7.2.7). We first extend the work of Section 3 by obtaining an upper bound on the the number of elliptic curves (of bounded height) which possess a rational non-trivial 2-torsion point, i.e. we prove Theorem E. This bound allows us to complete the proof of Theorem 5.3.15 which states that

$$\limsup_{d \to \infty} \operatorname{MAS}_B(d) \leq 1 + 2\zeta_B(2)\zeta_B(10),$$

with B, ζ_B as in Setup 1.1 and $\mathrm{MAS}_B(d)$ defined in (4.9). Afterwards, combining this count with the Selmer bounds of Section 6 along with Lemma 4.2.4 (see also the discussion after Proposition 4.2.11) will then allow us to deduce that

$$\limsup_{d\to\infty} \mathrm{AS}_B(d) \le \limsup_{d\to\infty} \mathrm{MAS}_B(d),$$

with $\mathrm{AS}_B(d)$ defined in (1.2), and so obtain Theorem B.

7.1 Counting Elliptic Curves with non-trivial 2-torsion

Work throughout in the context of Setup 1.1. We will bound the number of elliptic curves E/K with $E[2](K) \neq 0$. We will be able to obtain a better bound in characteristic $\neq 2$ than in characteristic 2, so we split into two cases. In both cases, our bound will be based on the existence of Weierstrass equations, so we first recall the following.

Recall 7.1.1 (Proposition 3.1.10)**.** Any Weierstrass curve W/B of height $> N(g) := \max\{-1, 2g-2\}$ is cut out by some Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

in $\mathbb{P} := \mathbb{P}\big(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3}\big)$, where $\mathscr{L}$ is W's Hodge bundle and $a_i \in \mathrm{H}^0(B, \mathscr{L}^i)$. $\odot$

7.1.1 Characteristic $\neq 2$

Assumption. Assume $\operatorname{char} K \neq 2$.

Let E/K be an elliptic curve with Hodge bundle $\mathscr{L}$ of height $d := \deg \mathscr{L} > N(g)$. Let $(W \xrightarrow{\pi} B, S)$ be its minimal Weierstrass model, so W is given by some Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \text{ with } a_i \in \Gamma(B, \mathscr{L}^i)$$

(inside of $\mathbb{P} := \mathbb{P}(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3})$). Note that negation on E extends to the morphism

$$-1 : [X, Y, Z] \longmapsto [X, -Y - a_1X - a_3Z, Z]$$

on $W \subset \mathbb{P}$. Suppose that E has a non-trivial 2-torsion point $P \in E[2](K)$. By the valuative criterion of properness, P extends to a section $\sigma : B \to W$. Using the universal property of $\mathbb{P}$, the map $B \xrightarrow{\sigma} W \hookrightarrow \mathbb{P}$ corresponds to some line bundle $\mathscr{M} \in \mathrm{Pic}(B)$ along with a surjection

$$\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3} \twoheadrightarrow \mathscr{M}.$$

We first observe that, in fact, $\mathscr{M}$ must be trivial. Indeed, it follows from [Sil09, Proposition VII.3.1(a)] that, because $\operatorname{char} K \neq 2$, the image $\sigma(B) \subset W$ is disjoint from the zero section $S \subset W$, i.e. P does not reduce to the identity at any place. Thus, σ misses the subscheme $\{Z = 0\} \subset W$, so the surjection $\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3} \twoheadrightarrow \mathscr{M}$ defining σ restricts to a map $\mathscr{O}_B \to \mathscr{M}$ which is non-vanishing in every fiber. Since $\mathscr{O}_B, \mathscr{M}$ are line bundles, this must in fact be an isomorphism.

The upshot is that we may view the section σ as the triple $[\sigma_X, \sigma_Y, 1]$ where $\sigma_X \in \Gamma(B, \mathscr{L}^2) = \mathrm{Hom}(\mathscr{L}^{-2}, \mathscr{O}_B)$ and $\sigma_Y \in \Gamma(B, \mathscr{L}^3) = \mathrm{Hom}(\mathscr{L}^{-3}, \mathscr{O}_B)$. Since σ lands in $W \subset \mathbb{P}$, these are required to satisfy

$$\sigma_Y^2 + a_1\sigma_X\sigma_Y + a_3\sigma_Y = \sigma_X^3 + a_2\sigma_X^2 + a_4\sigma_X + a_6.$$

Furthermore, since P is 2-torsion, i.e. since $P = -P$, they must also satisfy

$$\sigma_Y = -\sigma_Y - a_1\sigma_X - a_3 \text{ and so } a_3 = -2\sigma_Y - a_1\sigma_X. \tag{7.1}$$

Combining the previous two equations, we get that

$$-\sigma_Y^2 = \sigma_X^3 + a_2\sigma_X^2 + a_4\sigma_X + a_6 \text{ and so } a_6 = -\sigma_Y^2 - \sigma_X^3 - a_2\sigma_X^2 - a_4\sigma_X. \tag{7.2}$$

Theorem 7.1.2. *Assume* $\operatorname{char} K \neq 2$. *The weighted number of elliptic curves* E/K *of height* d *with* $E[2](K) \neq 0$ *is* $O\big(q^{6d}\big)$ *as* $d \to \infty$.

Proof. Consider a pair (E, P) of an elliptic curve E/K of height $d > N(g)$ along with a choice of non-identity point $P \in E[2](K)$. The above discussion shows that (E, P) arises from some tuple

$$(\mathscr{L}, a_1, a_2, a_3, a_4, a_6, \sigma_X, \sigma_Y)$$

with $\mathscr{L} \in \operatorname{Pic}^d(B)$, $a_i \in \mathrm{H}^0(B, \mathscr{L}^i)$, $\sigma_X \in \mathrm{H}^0(B, \mathscr{L}^2)$, and $\sigma_Y \in \mathrm{H}^0(B, \mathscr{L}^3)$. Furthermore, (7.1) shows that a_3 is completely determined once a_1, σ_X, σ_Y are chosen. Similarly, (7.2) shows that a_6 is determined once $a_2, a_4, \sigma_X, \sigma_Y$ are chosen. Thus, the entire tuple is determined once one chooses $\mathscr{L}$ followed by choosing $a_1, a_2, a_4, \sigma_X, \sigma_Y$. Therefore, the total number of possible tuples is bounded above by

$$\#\operatorname{Pic}^d(B) \cdot \#\mathrm{H}^0(\mathscr{L}) \cdot \#\mathrm{H}^0(\mathscr{L}^2) \cdot \#\mathrm{H}^0(\mathscr{L}^4) \cdot \#\mathrm{H}^0(\mathscr{L}^2) \cdot \#\mathrm{H}^0(\mathscr{L}^3) = \#\operatorname{Pic}^0(B) \cdot q^{12d+5(1-g)},$$

with equality by Riemann-Roch since $d > N(g)$. Finally, arguing as in Corollary 3.1.18, we conclude that the count of pairs (E, P), weighted by $1/\#\operatorname{Aut}(E)$, of height d is at most

$$\frac{\#\operatorname{Pic}^0(B) \cdot q^{12d+5(1-g)}}{(q-1)q^{6d+3(1-g)}} = O\big(q^{6d}\big). \qquad \blacksquare$$

7.1.2 Characteristic 2

Assumption. Assume $\operatorname{char} K = 2$.

In characteristic 2, we no longer have [Sil09, Proposition VII.3.1(a)] telling us that the line bundle $\mathscr{M}$ of the previous section is trivial. Without a bound on its degree, the strategy of the previous section no longer works. Instead, we proceed by directly writing down a condition, on just the Weierstrass coefficients a_i, which is necessary for the corresponding curve to support a section preserved by negation.

Lemma 7.1.3. *Fix a line bundle* $\mathscr{L}$, *and suppose that* $a_i \in \mathrm{H}^0(B, \mathscr{L}^i)$ *are such that*

$$W : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

supports a non-identity section $\sigma : B \to W \subset \mathbb{P}(\mathscr{O}_B \oplus \mathscr{L}^{-2} \oplus \mathscr{L}^{-3})$ *preserved by negation*

$$-1 : [X, Y, Z] \longmapsto [X, Y + a_1X + a_3Z, Z].$$

Then, there exists some $z \in \mathrm{H}^0(B, \mathscr{L}^5)$ *such that*

$$z^2 = a_1a_3^3 + a_1^2a_2a_3^2 + a_1^3a_3a_4 + a_1^4a_6.$$

Proof. Fix an embedding $\mathscr{L} \subset \underline{K}$ into the sheaf of meromorphic functions on B. This induces embeddings $\mathscr{L}^n \subset \underline{K}$ for all n, so we may treat the a_i's as elements of K. Let $\eta \in B$ denote the generic point. Since σ

is not the identity section, we may write $\sigma(\eta) = (x, y) \in \mathbb{A}^2(K)$. Thus, we have

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ and } y = y + a_1x + a_3$$

for some $x, y, a_1, a_2, a_3, a_4, a_6 \in K$. The second equation tells us that $0 = a_1x + a_3$, so $y^2 + a_1xy + a_3y = y^2$. Hence, multiplying the above displayed equation by a_1^4, we see that

$$(a_1^2y)^2 = a_1(a_1x)^3 + a_1^2a_2(a_1x)^2 + a_1^3a_4(a_1x) + a_1^4a_6 = a_1a_3^3 + a_1^2a_2a_3^2 + a_1^3a_3a_4 + a_1^4a_6.$$

Set $z = a_1^2y$. Note that $z \in \mathrm{H}^0(B, \mathscr{L}^5)$ since the above equation shows that $z^2 \in \mathrm{H}^0(B, \mathscr{L}^{10})$. ■

Theorem 7.1.4. *Assume* $\operatorname{char} K = 2$. *The weighted number of elliptic curves E/K of height d with $E[2](K) \neq 0$ is $O(q^{9d})$ as $d \to \infty$.*

Proof. Consider an elliptic curve E/K of height $d > N(g)$ for which $E[2](K) \neq 0$. Letting $\mathscr{L} \in \operatorname{Pic}^d(B)$ denote E's Hodge bundle, Lemma 7.1.3 thus tells us that any minimal Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

for E must satisfy

$$z^2 = a_1a_3^3 + a_1^2a_2a_3^2 + a_1^3a_3a_4 + a_1^4a_6$$

for some $z \in \mathrm{H}^0(B, \mathscr{L}^5)$. Note that we must have $a_1 \neq 0$ above since $E[2](K) \neq 0$. Indeed, if $a_1 = 0$, then the existence of a point fixed by negation would force $a_3 = 0$; however, in this case, E, the generic fiber of this equation, would be singular, a contradiction. Because $a_1 \neq 0$, we see that a_6 is determined by the choices of z, a_1, a_2, a_3, a_4. Hence, the total number of Weierstrass equations cutting out curves with Hodge bundle $\cong \mathscr{L}$ and which support a non-trivial 2-torsion point is at most

$$\# \mathrm{H}^0(\mathscr{L}^5) \cdot \prod_{i=1}^{4} \# \mathrm{H}^0(\mathscr{L}^4) = q^{15d+5(1-g)}.$$

Finally, arguing as in Corollary 3.1.18, we conclude that the count of elliptic curves E/K, weighted by $1/\# \operatorname{Aut}(E)$, of height d with $E[2](K) \neq 0$ is at most

$$\frac{\# \operatorname{Pic}^0(B) \cdot q^{15d+5(1-g)}}{(q-1)q^{6d+3(1-g)}} = O\big(q^{9d}\big)\,. \qquad ■$$

Combined with Theorem 7.1.2, this proves Theorem E.

7.2 Bounding the Average Size of 2-Selmer

We are now in a position to prove Theorem B. We begin by completing the proof of Theorem 5.3.15, which we restate below for the reader's convenience.

Recall 7.2.1. Let K be the function field of a smooth curve $B/\mathbb{F}_q$. Recall that $\mathcal{M}_{1,1}(K)$ denotes the groupoid of elliptic curves over K, and that $\mathcal{M}_{1,1}^{\leq d}(K)$ denotes its full subgroupoid consisting elliptic curves of height $\leq d$. Furthermore, recall the functions

$$\operatorname{AS}_B(d) := \frac{\sum_{\substack{E/K \\ \operatorname{ht}(E) \leq d}} \frac{\# \operatorname{Sel}_2(E)}{\# \operatorname{Aut}(E)}}{\# \mathcal{M}_{1,1}^{\leq d}(K)} \quad \text{and} \quad \operatorname{MAS}_B(d) := \frac{\# \mathcal{S}el_2^{\leq d}}{\# \mathcal{M}_{1,1}^{\leq d}(K)}$$

defined in (1.2) and (4.9). ⊙

Proposition 7.2.2. *The groupoid $\mathcal{S}el_{2,T}$ of trivial 2-Selmer elements (Notation 4.2.12) satisfies*

$$\lim_{d\to\infty} \frac{\#\,\mathcal{S}el_{2,T}^{\leq d}}{\#\mathcal{M}_{1,1}^{\leq d}(K)} = 1.$$

Proof. Observe

$$\begin{aligned}
\#\,\mathcal{S}el_{2,T}^{\leq d} &= \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d}} \frac{1}{\#E[2](K)\cdot \#\,\mathrm{Aut}(E)} && \text{by (4.12)}\\
&= \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)\neq 0}} \frac{1}{\#E[2](K)}\cdot\frac{1}{\#\,\mathrm{Aut}(E)} + \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)=0}} \frac{1}{\#\,\mathrm{Aut}(E)}\\
&= \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d}} \frac{1}{\#\,\mathrm{Aut}(E)} - \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)\neq 0}} \left(1-\frac{1}{\#E[2](K)}\right)\frac{1}{\#\,\mathrm{Aut}(E)}\\
&\geq \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d}} \frac{1}{\#\,\mathrm{Aut}(E)} - \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)\neq 0}} \frac{1}{\#\,\mathrm{Aut}(E)} && \text{since } 1-\frac{1}{\#E[2](K)}\leq 1.
\end{aligned}$$

It is clear from (4.12) that $\#\,\mathrm{Sel}_{2,T}^{\leq d} \leq \#\mathcal{M}_{1,1}^{\leq d}(K)$. Combined with the above, we have

$$\#\mathcal{M}_{1,1}^{\leq d}(K) - \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)\neq 0}} \frac{1}{\#\,\mathrm{Aut}(E)} \leq \#\,\mathcal{S}el_{2,T}^{\leq d} \leq \#\mathcal{M}_{1,1}^{\leq d}(K). \tag{7.3}$$

The claim now follows from dividing (7.3) by $\#\mathcal{M}_{1,1}^{\leq d}(K)$ and comparing the asymptotics obtained in Theorem 3.4.4 and Theorem E. ■

Corollary 7.2.3 (= Theorem 5.3.15)**.** *Fix notation as in Setup 1.1. Then,*

$$\limsup_{d\to\infty} \mathrm{MAS}_B(d) \leq 1 + 2\zeta_B(2)\zeta_B(10).$$

Proof. $\#\,\mathcal{S}el_2^{\leq d} = \#\,\mathcal{S}el_{2,T}^{\leq d} + \#\,\mathcal{S}el_{2,NT}^{\leq d}$, so combine Proposition 7.2.2 with Corollaries 4.2.13 and 5.3.14. ■

Continue to work within the context of Setup 1.1. To prove Theorem B, it suffices to prove the inequality

$$\limsup_{d\to\infty} \mathrm{AS}_B(d) \leq \limsup_{d\to\infty} \mathrm{MAS}_B(d).$$

We begin by defining the `intermediate average size of 2-Selmer`:

$$\mathrm{IAS}_B(d) := \frac{N(d)}{\#\mathcal{M}_{1,1}^{\leq d}(K)} \quad\text{where}\quad N(d) := \sum_{\substack{E/K\\ \mathrm{ht}(E)\leq d\\ E[2](K)=0}} \frac{\#\,\mathrm{Sel}_2(E)}{\#\,\mathrm{Aut}(E)}.$$

Proposition 7.2.4.
$$\lim_{d\to\infty} \mathrm{IAS}_B(d) = \lim_{d\to\infty} \mathrm{AS}_B(d).$$

Proof. We first remark that

$$\mathrm{AS}_B(d) - \mathrm{IAS}_B(d) = \frac{E(d)}{\#\mathcal{M}_{1,1}^{\le d}(K)} \quad\text{where}\quad E(d) := \sum_{\substack{E/K \\ \mathrm{ht}(E)\le d \\ E[2](K)\neq 0}} \frac{\#\,\mathrm{Sel}_2(E)}{\#\,\mathrm{Aut}(E)}.$$

By combining Theorem E with Theorem 6.3.4, we see that

$$E(d) = O\big(q^{9d}\big)\cdot O\Big(2^{d/\log d}\Big) = O\Big(q^{9d+d/\log d}\Big)$$

as $d\to\infty$. Since, by Theorem 3.4.4, $\#\mathcal{M}_{1,1}^{\le d}(K) \sim Cq^{10d}$ for some positive constant C, we conclude that $\lim\limits_{d\to\infty} E(d)/\#\mathcal{M}_{1,1}^{\le d}(K) = 0$, from which the claim follows. ■

Proposition 7.2.5.
$$\limsup_{d\to\infty} \mathrm{IAS}_B(d) \le \limsup_{d\to\infty} \mathrm{MAS}_B(d).$$

Proof. Recall the definition of the 2-Selmer groupoid (Definition 4.2.1). By construction, there is a bijection between isomorphism classes of objects of this category and pairs (E,α) where E is an isomorphism class of elliptic curves over K and $\alpha\in\mathrm{Sel}_2(E)$ (See Remark 4.1.1). Recalling the numerator $N(d)$ of $\mathrm{IAS}_B(d)$, this observation lets us express it as a sum over isomorphism classes of objects of $\mathcal{S}el_2$. Combining this with Lemma 4.2.4, which shows that $\#\,\mathrm{Aut}_{\mathcal{S}el_2}(C,E,\rho,D)\le\#\,\mathrm{Aut}(E)$ if $E[2](K)=0$, we obtain:

$$N(d) = \sum_{\substack{[(C,E,\rho,D)]\in|\mathcal{S}el_2| \\ \mathrm{ht}(E)\le d \\ E[2](K)=0}} \frac{1}{\#\,\mathrm{Aut}(E)} \le \sum_{\substack{[(C,E,\rho,D)]\in|\mathcal{S}el_2| \\ \mathrm{ht}(E)\le d \\ E[2](K)=0}} \frac{1}{\#\,\mathrm{Aut}_{\mathcal{S}el_2}(C,E,\rho,D)} \le \#\,\mathcal{S}el_2^{\le d}.$$

The claim follows. ■

Remark 7.2.6. When $\operatorname{char} K\neq 3$, one could bound the number of (isotrivial) elliptic curves with extra automorphism, and combine this with the Selmer bound in Theorem F in order to deduce that

$$\lim_{d\to\infty}\mathrm{AS}_B(d) = \lim_{d\to\infty}\mathrm{IAS}_B(d) = \lim_{d\to\infty}\mathrm{MAS}_B(d).$$

We expect these equalities to hold in arbitrary characteristic (even when $\operatorname{char} K = 3$), but since we did not obtain Selmer bounds for curves with trivial 2-torsion when $\operatorname{char} K = 3$, we settled, in this paper, for only proving the inequality $\limsup_{d\to\infty}\mathrm{AS}_B(d)\le\limsup_{d\to\infty}\mathrm{MAS}_B(d)$. ○

Theorem 7.2.7 (= Theorem B)**.** *Fix notation as in Setup 1.1. Then,* $\limsup_{d\to\infty}\mathrm{AS}_B(d)\le 1+2\zeta_B(2)\zeta_B(10)$.

Proof. Combine Corollary 7.2.3 with Propositions 7.2.4 and 7.2.5. ■

Appendices

A Applications of Cohomology and Base Change

We will need to apply the theorem of cohomology and base change in several places throughout this paper. In order to limit how much we repeat ourselves, we collect some standard consequences in this appendix.

Theorem A.1 (Cohomology and Base Change)**.** *Let $f : X \to B$ be a proper, finitely presented morphism of schemes, and let $\mathscr{F}$ be a finitely presented sheaf on X which is flat over B. Suppose that for a point $b \in B$ and an integer i, the comparison map*

$$\varphi_b^i : R^i f_* \mathscr{F} \otimes \kappa(b) \longrightarrow \mathrm{H}^i(X_b, \mathscr{F}_b)$$

is surjective. Then, all of the following hold.

(0) *φ_b^i is an isomorphism.*

(1) *there is an open neighborhood $V \subset B$ of b s.t. for any morphism $B' \xrightarrow{g} V$ of schemes, the comparison map*

$$\varphi_{B'}^i : g^* R^i f_* \mathscr{F} \xrightarrow{\sim} R^i f'_*(g'^* \mathscr{F})$$

is an isomorphism. Above, f', g' are the morphisms in the Cartesian square

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ B' \arrow[r, "g"] & B. \end{tikzcd}$$

In particular, if φ_b^i is surjective for all $b \in B$, then formation of $R^i f_* \mathscr{F}$ commutes with arbitrary base change.

(2) *φ_b^{i-1} is surjective if and only if $R^i f_* \mathscr{F}$ is a vector bundle in an open neighborhood of b.*

In particular, φ_b^{i-1} is surjective for all $b \in B$ if and only if $R^i f_* \mathscr{F}$ is a vector bundle on B.

Proof. See [Vak23, Theorem 25.1.6] and [Alp22, Theorem A.7.5]. ∎

Lemma A.2. *Let $f : X \to B$ be a morphism of schemes. Let $\mathscr{L}$ be a line bundle on X such that $f_* \mathscr{L}$ is a vector bundle on B whose formation commutes with arbitrary base change. Suppose that, for each $b \in B$, the fibral line bundle $\mathscr{L}_b := \mathscr{L}|_{X_b}$ on X_b is globally generated. Then, the natural map*

$$f^* f_* \mathscr{L} \longrightarrow \mathscr{L}$$

is surjective.

Proof. This argument comes from the proof of [Alp22, Proposition A.7.10]. Surjectivity can be checked on stalks. Applying Nakyama to the cokernels of the maps on stalks, we see that surjectivity can even be checked on the fibers of the line bundles. Thus, it also suffices to check that $(f^* f_* \mathscr{L})\,|_{X_b} \longrightarrow \mathscr{L}|_{X_b} = \mathscr{L}_b$ is surjective for each $b \in B$. Note that the left hand side is the pullback of $f_* \mathscr{L}$ along the composition $X_b \hookrightarrow X \xrightarrow{f} B$, which is equivalently the composition $X_b \xrightarrow{f_b} \operatorname{Spec} \kappa(b) \overset{b}{\hookrightarrow} B$, so we are asking for surjectivity of the induced map

$$\mathrm{H}^0(X_b, \mathscr{L}_b) \otimes \mathscr{O}_{X_b} = f_b^* \left(\widetilde{\mathrm{H}^0(X_b, \mathscr{L}_b)} \right) \simeq f_b^* (f_* \mathscr{L} \otimes \kappa(b)) \longrightarrow \mathscr{L}_b,$$

where the second isomorphism holds since the formation of $f_*\mathscr{L}$ commutes with base change along $\operatorname{Spec}\kappa(b) \overset{b}{\hookrightarrow} B$. The above map is surjective since $\mathscr{L}_b$ is globally generated by assumption, so we win. ■

Lemma A.3. *Let $\pi : \mathcal{C} \to B$ be a B-curve (see Section 2 for our definition of 'curve'). Furthermore, assume that, for all $b \in B$, one has $\mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = \kappa(b)$ and $\omega_{\mathcal{C}_b} \simeq \mathscr{O}_{\mathcal{C}_b}$. Then, $\pi_*\mathscr{O}_{\mathcal{C}} = \mathscr{O}_B$ holds after arbitrary base change, and $\omega_{X/B} = \pi^*\mathscr{L}$ for a unique $\mathscr{L} \in \operatorname{Pic}(B)$. In fact, $\mathscr{L} \simeq \pi_*\omega_{\mathcal{C}/B}$, whose formation will also commute with arbitrary base change.*

Proof. We wish to apply cohomology and base change, Theorem A.1. We will first apply it to $\mathscr{F} = \mathscr{O}_{\mathcal{C}}$ (with $i = 0$). The comparison map

$$\varphi_b^0 : \pi_*\mathscr{O}_{\mathcal{C}} \otimes \kappa(b) \longrightarrow \mathrm{H}^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = \kappa(b)$$

is nonzero (e.g. since it's a ring map, so $1 \mapsto 1$) and so surjective (for all $b \in B$). Therefore, by Theorem A.1, it is an isomorphism and $\pi_*\mathscr{O}_{\mathcal{C}}$ is a line bundle whose formation commutes with arbitrary base change. Now, the natural map $\mathscr{O}_B \to \pi_*\mathscr{O}_{\mathcal{C}}$ is an isomorphism on fibers since it fits into the below commutative diagram (recall φ_b^0 is itself an isomorphism)

$$\begin{tikzcd} \kappa(b) \arrow[r] \arrow[rr, bend left, "\mathrm{id}"] & \pi_*\mathscr{O}_{\mathcal{C}} \otimes \kappa(b) \arrow[r, "\varphi_b^0"'] & \kappa(b). \end{tikzcd}$$

Thus, $\mathscr{O}_B \xrightarrow{\sim} \pi_*\mathscr{O}_{\mathcal{C}}$ as desired.

Now, since $h^2(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = 0$ for all $b \in B$, Theorem A.1 with $i = 2$ applied to $\mathscr{F} = \mathscr{O}_{\mathcal{C}}$ shows that $R^2 f_*\mathscr{O}_{\mathcal{C}} = 0$ and so (by part **(3)** of that theorem) φ_b^1 is surjective for all $b \in B$. Since we saw above that also φ_b^0 is surjective for all $b \in B$, another application of Theorem A.1, this time with $i = 1$, to $\mathscr{F} = \mathscr{O}_{\mathcal{C}}$ shows that $R^1\pi_*\mathscr{O}_{\mathcal{C}}$ is a vector bundle on B of rank

$$h^1(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = h^0(\mathcal{C}_b, \omega_{\mathcal{C}_b}) = h^0(\mathcal{C}_b, \mathscr{O}_{\mathcal{C}_b}) = 1$$

whose formation commutes with arbitrary base change. By duality, we then conclude that $\mathscr{L} := \pi_*\omega_{\mathcal{C}/B} \simeq \left(R^1\pi_*\mathscr{O}_{\mathcal{C}}\right)^\vee$ is a line bundle whose formation commutes with arbitrary base change as well. We claim that $\pi^*\mathscr{L} \simeq \omega_{\mathcal{C}/B}$. This is because Lemma A.2 gives a surjection $\pi^*\mathscr{L} \twoheadrightarrow \omega_{\mathcal{C}/B}$ and a surjective map between equal rank vector bundles is necessarily an isomorphism. Finally, uniqueness of this choice of $\mathscr{L}$ follows from the projection formula, which guarantees that, if $\omega_{\mathcal{C}/B} \simeq \pi^*\mathscr{M}$, then $\pi_*\omega_{\mathcal{C}/B} \simeq \pi_*\mathscr{O}_{\mathcal{C}} \otimes \mathscr{M} \simeq \mathscr{M}$. ■

B Basic Geometry of Weighted Projective Space

At a few points, we would like to use Theorem 1.4.1 and Theorem 3.3.4 from Dolgachev's paper [Dol82] on weighted projective varieties. However, he has a running assumption that for results about $\mathbb{P}(a_0, \dots, a_r)$ over a field k, he always assumes $\operatorname{char} k \nmid a_i$ for all i. In this paper, we need to deal with $\mathbb{P}(1,2,1)$ in characteristic 2. For completeness, here we prove special cases of Dolgachev's results which suffice for our purposes.

Lemma B.1. *Let $f : X \to Y$ be a flat, proper morphism of noetherian schemes with integral geometric fibers. For a line bundle $\mathscr{L}$ on X, the locus*

$$\left\{y \in Y : \mathscr{L}_y \simeq \mathscr{O}_{X_y}\right\} \subset Y$$

is closed.

Proof. Since the fibers of f are geometrically integral and proper, $\mathscr{L}_y \simeq \mathscr{O}_{X_y}$ if and only if both $h^0(X_y, \mathscr{L}_y)$ and $h^0(X_y, \mathscr{L}_y^{-1})$ are nonzero. Given this, the claim follows from semicontinuity [Har77, Theorem 12.8]. ■

To be clear, everything below appears already in [Dol82], except they technically include a mild characteristic restriction there.

Lemma B.2. *Let $\mathbb{P}(a_1, \ldots, a_r)$ with $\gcd(a_i) = 1$, viewed as a scheme over any field k. Then, its dualizing sheaf is $\mathscr{O}(-a_0 - \cdots - a_r)$.*

Proof. Let $\mathbb{P} := \mathbb{P}(a_1, \ldots, a_r)_{\mathbb{Z}}$ be the corresponding weighted projective space over $\operatorname{Spec}\mathbb{Z}$, and let $\mathscr{L} := \omega_{\mathbb{P}} \otimes \mathscr{O}_{\mathbb{P}}(a_0 + \cdots + a_r)$. It suffices to show that $\mathscr{L}$ has trivial fibers over all of $\operatorname{Spec}\mathbb{Z}$. [Dol82, Theorem 3.3.4] tells us that $\mathscr{L}_p := \mathscr{L}|_{\mathbb{P}_{\mathbb{F}_p}} \simeq \mathscr{O}_{\mathbb{P}_{\mathbb{F}_p}}$ for any $p \nmid (a_0 \ldots a_r)$, so Lemma B.1 tells us that $\{p \in \operatorname{Spec}\mathbb{Z} : \mathscr{L}_p \text{ trivial}\}$ is a closed set containing the dense set of p not dividing any a_i and so is all of $\operatorname{Spec}\mathbb{Z}$. ∎

Corollary B.3. *Let $V \subset \mathbb{P}(a_0, \ldots, a_r)$ (with $\gcd(a_i) = 1$) be a degree d hypersurface over any field k. Then, $\omega_V \simeq \mathscr{O}_V(d - a_0 - \cdots - a_r) := \mathscr{O}_{\mathbb{P}(a_0,\ldots,a_r)}(d - a_0 - \cdots - a_r)|_V$.*

Proof. This now follows directly from adjunction [Kle80, Corollary (19)]. ∎

Lemma B.4. *Consider $\mathbb{P}(1, 2, 1)$ over an arbitrary field k. For any $n \in \mathbb{Z}$, we have*

$$\mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n)) = 0.$$

Proof. Write $\mathbb{P}(1, 2, 1) = \operatorname{Proj} k[X, Y, Z]$ with X, Z in degree 1 and Y in degree 2. Note that $\mathbb{P}^1 \hookrightarrow \mathbb{P}(1, 2, 1)$ as the subscheme $Y = 0$, so we have an exact sequence

$$0 \longrightarrow \mathscr{O}_{\mathbb{P}(1,2,1)}(-2) \longrightarrow \mathscr{O}_{\mathbb{P}(1,2,1)} \longrightarrow \mathscr{O}_{\mathbb{P}^1} \longrightarrow 0.$$

The line bundle $\mathscr{O}(2)$ on $\mathbb{P}(1, 2, 1)$ is ample, so Serre vanishing tells us that $\mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n + 2k)) = 0$ for some $k \gg 1$. We induct backwards to get the same conclusion when $k = 0$. Twisting our short exact sequence by $n + 2k$ and taking cohomology gives the exact sequence

$$\mathrm{H}^0(\mathbb{P}(1, 2, 1), \mathscr{O}(n+2k)) \to \mathrm{H}^0(\mathbb{P}^1, \mathscr{O}(n+2k)) \to \mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n+2(k-1))) \to \mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n+2k)) = 0.$$

The leftmost map above is easily seen to be surjective, so exactness gives $\mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n + 2(k - 1)) = 0$. Downwards induction then let's us conclude that $\mathrm{H}^1(\mathbb{P}(1, 2, 1), \mathscr{O}(n)) = 0$ as desired. ∎

References

[Alp22] Jarod Alper. Notes on stacks and moduli. `https://sites.math.washington.edu/~jarod/moduli.pdf`, 2022. 66

[Art86] M. Artin. Lipman's proof of resolution of singularities for surfaces. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 267–287. Springer, New York, 1986. 27, 31

[BD09] Kai Behrend and Ajneet Dhillon. Connected components of moduli stacks of torsors via Tamagawa numbers. *Canad. J. Math.*, 61(1):3–28, 2009. 46

[BKL+15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Jr., Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Camb. J. Math.*, 3(3):275–321, 2015. 2

[Bru92] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992. 2, 4

[BS13] Manjul Bhargava and Arul Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7, 2013. 2

[BS15] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015. 2

[CFO+08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155, 2008. 17

[Con05] Brian Conrad. Minimal models for elliptic curves. `http://math.stanford.edu/~conrad/papers/minimalmodel.pdf`, 2005. 9, 27

[Del75] P. Deligne. Courbes elliptiques: formulaire d'après J. Tate. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 53–73. Lecture Notes in Math., Vol. 476, 1975. 8

[dJ02] A. J. de Jong. Counting elliptic surfaces over finite fields. volume 2, pages 281–311. 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. 2, 3, 6, 7, 12, 13, 14, 17, 18, 26, 29

[Dol82] Igor Dolgachev. Weighted projective varieties. In *Group actions and vector fields (Vancouver, B.C., 1981)*, volume 956 of *Lecture Notes in Math.*, pages 34–71. Springer, Berlin, 1982. 23, 36, 67, 68

[FLR23] Tony Feng, Aaron Landesman, and Eric M. Rains. The geometric distribution of Selmer groups of elliptic curves over function fields. *Math. Ann.*, 387(1-2):615–687, 2023. 2

[Gir71] Jean Giraud. *Cohomologie non abélienne*. Die Grundlehren der mathematischen Wissenschaften, Band 179. Springer-Verlag, Berlin-New York, 1971. 42

[GL19] Dennis Gaitsgory and Jacob Lurie. *Weil's conjecture for function fields. Vol. 1*, volume 199 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2019. 46

[Gol79] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math*, pages pp 108–118. Springer, Berlin, 1979. 2

[Gro67] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967. 30

[GRR72] Alexander Grothendieck, Michel Raynaud, and Dock Sang Rim. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). 57

[Har77] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. 8, 19, 31, 32, 33, 67

[HLHN14] Q. P. Hồ, V. B. Lê Hùng, and B. C. Ngô. Average size of 2-Selmer groups of elliptic curves over function fields. *Math. Res. Lett.*, 21(6):1305–1339, 2014. 2, 3, 4, 5, 38

[Kle80] Steven L. Kleiman. Relative duality for quasicoherent sheaves. *Compositio Math.*, 41(1):39–60, 1980. 32, 33, 68

[Lan21a] Aaron Landesman. A geometric approach to the cohen-lenstra heuristics. `https://arxiv.org/abs/2106.10357`, 2021. 51

[Lan21b] Aaron Landesman. The geometric average size of Selmer groups over function fields. *Algebra Number Theory*, 15(3):673–709, 2021. 2, 48, 51, 52, 53

[Lan21c] Aaron Landesman. A thesis of minimal degree: two. https://stacks.stanford.edu/file/druid:fv070dn6727/landesman-thesis-5-30-21-augmented.pdf, 2021. 51, 52

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. 29, 31

[Liu22] Qing Liu. Global Weierstrass equations of hyperelliptic curves. *Trans. Amer. Math. Soc.*, 375(8):5889–5906, 2022. 18

[Mil80] James S. Milne. *Étale cohomology*. Princeton Mathematical Series, No. 33. Princeton University Press, Princeton, N.J., 1980. 46, 51, 53, 58

[MS72] David Mumford and Kalevi Suominen. Introduction to the theory of moduli. In *Algebraic geometry, Oslo 1970 (Proc. Fifth Nordic Summer School in Math.)*, pages 171–222. Wolters-Noordhoff, Groningen, 1972. 10

[Muk03] Shigeru Mukai. *An introduction to invariants and moduli*, volume 81 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, japanese edition, 2003. 44

[Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. 54

[Oda69] Tadao Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)*, 2:63–135, 1969. 49

[Ogg67] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967. 60

[O'N02] Catherine O'Neil. The period-index obstruction for elliptic curves. *J. Number Theory*, 95(2):329–339, 2002. 17

[PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012. 2

[PS00] J. Pesenti and L. Szpiro. Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.*, 120(1):83–117, 2000. 59

[PW23] Sun Woo Park and Niudun Wang. On the Average of p-Selmer Ranks in Quadratic Twist Families of Elliptic Curves Over Global Function Fields. *International Mathematics Research Notices*, page rnad095, 05 2023. 2

[Sad11] Mohammad Sadek. Counting models of genus one curves. *Math. Proc. Cambridge Philos. Soc.*, 150(3):399–417, 2011. 18, 27

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 57

[Sha13] Arul Shankar. *The average rank of elliptic curves over number fields*. ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–Princeton University. 2

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 11, 48, 52, 59, 61, 62

[Sta21] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2021. 20, 21, 23, 24, 25, 30, 38

[Tho19] Jack A. Thorne. On the average number of 2-Selmer elements of elliptic curves over $\mathbb{F}_q(X)$ with two marked points. *Doc. Math.*, 24:1179–1223, 2019. 2

[Ulm91] Douglas L. Ulmer. p-descent in characteristic p. *Duke Math. J.*, 62(2):237–265, 1991. 55, 56

[Vak23] Ravi Vakil. The rising sea: Foundations of algebraic geometry. `http://math.stanford.edu/~vakil/216blog/FOAGjun2923public.pdf`, June 2023. 8, 37, 66

[Č16] Kęstutis Česnavičius. Selmer groups as flat cohomology groups. *J. Ramanujan Math. Soc.*, 31(1):31–61, 2016. 52