Universiteit
Leiden
The Netherlands

Counting curves and their rational points

Spelier, P.

Citation
Spelier, P. (2024, June 12). *Counting curves and their rational points*.
Retrieved from https://hdl.handle.net/1887/3762227

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3762227

Note: To cite this publication please use the final published version (if applicable).

Chapter 6

Geometric quadratic Chabauty and p-adic heights

This chapter has already been published in Expositiones Mathematicae, in a special edition in memory of Bas Edixhoven [DRHS23]. This is joint work with Juanita Duque–Rosero and Sachi Hashimoto. We do not reproduce the appendix of equations [DRHS23, Appendix A].

Abstract. Let X be a curve of genus $g > 1$ over $\mathbb{Q}$ whose Jacobian J has Mordell–Weil rank r and Néron–Severi rank ρ. When $r < g+\rho-1$, the geometric quadratic Chabauty method determines a finite set of p-adic points containing the rational points of X. We describe algorithms for geometric quadratic Chabauty that translate the geometric quadratic Chabauty method into the language of p-adic heights and p-adic (Coleman) integrals. This translation also allows us to give a comparison to the (original) cohomological method for quadratic Chabauty. We show that the finite set of p-adic points produced by the geometric method is contained in the finite set produced by the cohomological method, and give a description of their difference.

6.1 Introduction

Let $X_{\mathbb{Q}}$ be a smooth, projective, geometrically irreducible curve of genus $g > 1$ over $\mathbb{Q}$. The problem of describing $X_{\mathbb{Q}}(\mathbb{Q})$, the set of rational points of $X_{\mathbb{Q}}$, has fascinated mathematicians for centuries. A famous conjecture of Mordell

[Mor22a] is that, for $g > 1$, the set $X_{\mathbb{Q}}(\mathbb{Q})$ is finite. Faltings's theorem states that Mordell's conjecture is true [Fal83b]. However, Faltings's theorem is not effective, meaning that it does not give a method to determine the set of rational points. There is still an ongoing effort to find explicit methods to compute the set $X_{\mathbb{Q}}(\mathbb{Q})$. Chabauty's theorem [Cha41] gives a finiteness result for $X_{\mathbb{Q}}(\mathbb{Q})$ on certain curves by using p-adic analysis. This was made effective by Coleman [Col85a] through the development of Coleman integration; he gave a method to find p-adic power series that vanish on a superset of $X_{\mathbb{Q}}(\mathbb{Q})$ for the curves Chabauty considered. This breakthrough is the starting point for the Chabauty–Kim program [Kim09] of p-adic methods for proving the finiteness of $X_{\mathbb{Q}}(\mathbb{Q})$ generalizing Chabauty and Coleman's method. The quadratic Chabauty method [BBM16, BD18, BD21, EL21, BMS21] is an effective instance of the Chabauty–Kim method, developed by Balakrishnan and Dogra first for finding integral points on affine curves, and later for studying the rational points of $X_{\mathbb{Q}}$.

Let $J_{\mathbb{Q}}$ be the Jacobian of $X_{\mathbb{Q}}$, with Mordell–Weil rank r and Néron–Severi rank $\rho \coloneqq \operatorname{rk}\mathrm{NS}(J_{\mathbb{Q}}) > 1$. Let $p > 2$ be a prime, not necessarily of good reduction for $X_{\mathbb{Q}}$. Quadratic Chabauty is an effective p-adic method for producing a finite set of p-adic points containing the rational points of $X_{\mathbb{Q}}$, when $r < g+\rho-1$. There are several approaches to the quadratic Chabauty method. The (original) cohomological quadratic Chabauty method [BD18, BD21] studies $X_{\mathbb{Q}}(\mathbb{Q})$ using p-adic height functions and works in certain Selmer varieties (for p of good reduction). This method has been applied to determine the rational points on many modular curves [BBB$^+$21, BDM$^+$21], including the cursed curve [BDM$^+$19], a famously difficult problem. The geometric quadratic Chabauty method [EL21] is an algebro-geometric method for quadratic Chabauty, and the computations take place in $\mathbb{G}_m$-torsors over $J_{\mathbb{Q}}$.

In this paper, we give a comparison of the geometric and cohomological methods for quadratic Chabauty in the cases where both methods can be applied. We prove the following theorem.

Theorem H (Comparison Theorem (Theorem 6.8.5))**.** *Assume that p is a prime of good reduction for $X_{\mathbb{Q}}$. Assume that $r = g$, $\rho > 1$, and the p-adic closure $\overline{J_{\mathbb{Q}}(\mathbb{Q})}$ is of finite index in $J_{\mathbb{Q}}(\mathbb{Q}_p)$. Assume $X_{\mathbb{Q}}(\mathbb{Q}) \neq \emptyset$, and let $b \in X_{\mathbb{Q}}(\mathbb{Q})$ be a choice of a rational base point. Let $X(\mathbb{Q}_p)_{\mathrm{Coh}}$ be the finite set of p-adic points obtained under these assumptions with the cohomological quadratic Chabauty method (see Definition 6.8.1 and Remark 6.8.2). Let $X/\mathbb{Z}$ be a proper regular model of $X_{\mathbb{Q}}$. Let $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ be the finite set of p-adic points obtained with the geometric quadratic Chabauty method (see Definition 6.2.3).*

Then we have the inclusions

$$X_{\mathbb{Q}}(\mathbb{Q}) \subseteq X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}} \subseteq X_{\mathbb{Q}}(\mathbb{Q}_p),$$

and we can explicitly characterize $X(\mathbb{Q}_p)_{\mathrm{Coh}} \setminus X(\mathbb{Z}_p)_{\mathrm{Geo}}$.

In [HS22a], it is shown that the classical Chabauty–Coleman method [Col85b] and the geometric linear Chabauty method [Spe20] are related by a similar comparison theorem.

The geometric quadratic Chabauty method studies the Poincaré torsor, the universal $\mathbb{G}_m$-biextension over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}$. By pulling back the Poincaré torsor by a nontrivial trace zero morphism $f\colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$, we can construct a nontrivial torsor T over the Néron model of $J_{\mathbb{Q}}$ whose restriction to $X_{\mathbb{Q}}$ is trivial. This allows us to embed $X_{\mathbb{Q}}$ into T through a section. The idea of the geometric quadratic Chabauty method is to intersect the image of the integer points on a regular model of $X_{\mathbb{Q}}$ with the p-adic closure of the integer points $\overline{T(\mathbb{Z})}$. This intersection contains $X_{\mathbb{Q}}(\mathbb{Q})$.

Suppose further that p is a prime of good reduction for $X_{\mathbb{Q}}$. We give new algorithms for geometric quadratic Chabauty that work mainly in the trivial biextension $\mathbb{Q}_p^g \times \mathbb{Q}_p^g \times \mathbb{Q}_p$. Working on the trivial biextension translates the geometric quadratic Chabauty method into the language of Coleman–Gross heights [CG89] and Coleman integrals [Col85a]. The main contribution of this paper is to explicitly give this translation into the language of heights and Coleman integrals. This translation allows us to prove the comparison theorem between the cohomological quadratic Chabauty method and the geometric quadratic Chabauty method. We also give an algorithm to compute the local heights away from p associated to the curve $X_{\mathbb{Q}}$. These heights are also studied in [BD20].

We further leverage the language of p-adic heights to compute the embedding of $X_{\mathbb{Q}}$ into T and the integer points $\overline{T(\mathbb{Z})}$ as solutions to convergent power series. Then determining up to finite p-adic precision a finite set containing $X_{\mathbb{Q}}(\mathbb{Q})$ reduces to solving simple polynomial equations. Theoretically, by working modulo p^k for large enough $k \in \mathbb{N}$, the geometric quadratic Chabauty method will always produce a finite set of p-adic points with precision k containing $X_{\mathbb{Q}}(\mathbb{Q})$. We describe algorithms for finding this finite set of p-adic points that are practical when $X_{\mathbb{Q}}$ is a hyperelliptic curve. Our `Magma` code implementing these algorithms can be found in [DRHS].

Finally, we present an example of our new method applied to the modular curve $X_0(67)^+$ and a trace zero endomorphism f arising from the Hecke operator T_2.

Even though the rational points on this curve have already been determined [BBB+21], this provides a new way of analyzing the set of rational points.

6.2 Overview and Set-up

We first set up some notation and give a broad overview of the geometric quadratic Chabauty method, then outline the contents of our paper.

Let $X_{\mathbb{Q}}$ be any smooth, projective, geometrically irreducible curve over $\mathbb{Q}$ with a proper regular model X of $X_{\mathbb{Q}}$ over the integers and a fixed base point $b \in X_{\mathbb{Q}}(\mathbb{Q}) = X(\mathbb{Z})$. Let X^{sm} denote the open subscheme of X consisting of points at which X is smooth over $\mathbb{Z}$; then $X^{\mathrm{sm}}(\mathbb{Z}) = X(\mathbb{Z})$. Let $J_{\mathbb{Q}}$ denote the Jacobian of $X_{\mathbb{Q}}$ and J denote the Néron model of $J_{\mathbb{Q}}$ over the integers. Suppose $J_{\mathbb{Q}}$ has Mordell–Weil rank r and Néron–Severi rank $\rho = \rho(J_{\mathbb{Q}})$. Let p be a prime greater than 2 not necessarily of good reduction for $X_{\mathbb{Q}}$.

The goal in geometric quadratic Chabauty is to lift X into a non-trivial $\mathbb{G}_m^{\rho-1}$-torsor T over J through a section $\widetilde{j_b}$ lying over the Abel–Jacobi embedding $j_b \colon X^{\mathrm{sm}} \to J$. Over $\mathbb{Q}$ we find this section $\widetilde{j_b}$ by giving a trivializing section of the $\mathbb{G}_m^{\rho-1}$-torsor $j_b^* T_{\mathbb{Q}}$ over $X_{\mathbb{Q}}$. If we want to spread this out over $\mathbb{Z}$, there is an obstruction coming from the multidegree.

Definition 6.2.1. The *multidegree* of a line bundle $\mathcal{L}$ on a curve C with geometrically irreducible components $(C_i)_{i\in I}$ over $\overline{\mathbb{Q}}$ is $(\deg \mathcal{L}|_{C_i})_{i\in I}$.

The map $\mathrm{Pic}(X) \to \mathrm{Pic}(X_{\mathbb{Q}})$ is not in general an isomorphism, and $j_b^* T$ is not in general trivial over X since its multidegree over the fibers $X_{\mathbb{F}_\ell}$ of X might be non-zero. This is the only obstruction: the torsor can be trivialized over an open $U \subset X^{\mathrm{sm}}$ constructed by picking one geometrically irreducible component in each fiber $X_{\mathbb{F}_\ell}$ and removing the other irreducible components. We call these fiberwise geometrically irreducible open $U \subset X^{\mathrm{sm}}$ *simple open sets*. By [Sta18a, Tag 04KV] every irreducible component of $X_{\mathbb{F}_\ell}$ admitting a smooth $\mathbb{F}_\ell$-point is geometrically irreducible. Hence every point $P \in X^{\mathrm{sm}}(\mathbb{Z})$ is contained in $U(\mathbb{Z})$ for a unique simple open U. There is a finite number $(U_i)_{i\in I}$ of simple open sets that cover $X^{\mathrm{sm}}(\mathbb{Z})$. For every such open, the map $\mathrm{Pic}(U) \to \mathrm{Pic}(X_{\mathbb{Q}})$ is an isomorphism. We fix a simple open U, and obtain a trivialization $\widetilde{j_b} \colon U \to T$ lying over j_b.

Because $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$ is finite, we can expect the closure of $T(\mathbb{Z})$ inside the $(g + \rho - 1)$-dimensional p-adic manifold $T(\mathbb{Z}_p)$ to be of dimension at most r. The image of the p-adic points of U, namely $\widetilde{j_b}(U(\mathbb{Z}_p))$, is of dimension 1. Given this T, we see the analogue of the classical Chabauty's theorem, that

applies for curves satisfying the inequality $r < g$ [Cha41].

Theorem 6.2.2 ([EL21, Section 9.2]). *When $r < g + \rho - 1$, the intersection*

$$\widetilde{j_b}(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p)$$

is finite.

Definition 6.2.3. The *geometric quadratic Chabauty set* $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ is defined to be the union over the simple open sets $i \in I$ of $\widetilde{j_b}^*(\widetilde{j_b}(U_i(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}) \subset U_i(\mathbb{Z}_p) \subset X(\mathbb{Z}_p)$.

The geometric quadratic Chabauty method computes this finite set $X(\mathbb{Z}_p)_{\mathrm{Geo}}$, working in one simple open $U \subset X$ and one residue disk of $U(\mathbb{Z}_p)$ at a time. In Algorithm 6.7.1 we give an algorithm to determine $\widetilde{j_b}(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}$ to finite precision.

To construct the $\mathbb{G}_m^{\rho-1}$-torsor T over J we start with the universal $\mathbb{G}_m$-torsor. In our calculations this takes the form of the Poincaré torsor $\mathcal{M}^\times$ over $J \times J^0$ (this is actually a pullback of the Poincaré torsor over $J \times J^{\vee 0}$; for more details see Section 6.3). Here $J^{\vee 0}$ is the fiberwise connected component of $J^\vee$ containing 0.

Remark 6.2.4. When p is a prime of good reduction for X, we have $J^0_{\mathbb{Z}_{(p)}} = J_{\mathbb{Z}_{(p)}}$ and $J^{\vee 0}_{\mathbb{Z}_{(p)}} = J^\vee_{\mathbb{Z}_{(p)}}$.

By the universality of $\mathcal{M}^\times$, we want to construct T by pulling back $\mathcal{M}^\times$ along morphisms $(\mathrm{id}, \alpha_i) \colon J \to J \times J^0$ for $i = 1, \dots, \rho - 1$. Define

$$m \coloneqq \mathrm{lcm}\{\exp\left((J/J^0)(\overline{\mathbb{F}}_q)\right) \mid q \text{ prime}\}, \tag{6.2.0.1}$$

where $\exp(G) \in \mathbb{N}_{\geq 1}$ is the exponent of a finite group G. Note that $m\cdot \colon J \to J^0$ is then a well-defined morphism. Any morphism of schemes $J \to J$ can be written as a translation composed with an endomorphism, and hence we choose our morphisms $\alpha_i \colon J \to J^0$ to be of the form $m \cdot \circ \mathrm{tr}_{c_i} \circ f_i$ with $c_i \in J(\mathbb{Z})$ and $f_i \colon J \to J$ a morphism of group schemes.

The torsor T is the product $T = \prod_{i=1}^{\rho-1} (\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$ as a fiber product over J. We also let $\mathcal{M}^{\times,\rho-1}$ be the product taken as a fiber product over J via the first projection map $\mathcal{M}^\times \to J \times J^0 \to J$. In order to embed U through a section $\widetilde{j_b} \colon U \to T$, the torsor T pulled back to U must be trivial: that is $j_b^*(\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$ must be trivial over U. The torsor $(\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$ over J can be thought of as the total space of a line bundle without its zero section, and the condition that its pullback $L_{\alpha_i} \coloneqq j_b^*(\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$ to U is trivial forces the

corresponding line bundle to be degree 0. Equivalently, the trace of f_i must be 0. The condition that L_{α_i} is trivial uniquely determines c_i.

$$\begin{array}{ccccc} & & T & \longrightarrow & \mathcal{M}^{\times,\rho-1} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ U & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id},m\cdot\circ\,\mathrm{tr}_{c_i}\circ f_i)_i} & J\times(J^0)^{\rho-1} \end{array} \tag{6.2.0.2}$$

Because the Néron–Severi rank of $J_{\mathbb{Q}}$ is ρ, the Jacobian J has $\rho-1$ independent non-trivial endomorphisms of trace zero.

Definition 6.2.5. For Y a scheme, S a ring with residue field $\operatorname{Spec}\mathbb{F}_p \to \operatorname{Spec} S$ and $Q \in Y(\mathbb{F}_p)$, we define the *residue disk over* Q, denoted by $Y(S)_Q \coloneqq \{y \in Y(S) \mid \overline{y} = Q\}$, to be the set of all S-points specializing to Q.

Let $\overline{P} \in U(\mathbb{F}_p)$. The residue disk $U(\mathbb{Z}_p)_{\overline{P}}$ embeds in the residue disk $T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ of T through the section $\widetilde{j_b}$. Since $p > 2$, we have that 1 and -1 reduce to different points modulo p and hence the map $T(\mathbb{Z})_{\widetilde{j_b}(\overline{P})} \to J(\mathbb{Z})_{j_b(\overline{P})}$ is a bijection. By [Par00, Proposition 2.3] and the fact that $p > 2$ the residue disk $J(\mathbb{Z})_{j_b(\overline{P})}$ is up to a translation isomorphic to $\mathbb{Z}_p^r$. In [EL21, Theorem 4.10] this bijection $T(\mathbb{Z})_{\widetilde{j_b}(\overline{P})} \to J(\mathbb{Z})_{j_b(\overline{P})}$ is upgraded to a morphism $\kappa\colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$.

In this paper we make the geometric quadratic Chabauty method explicit in the case where p is of good reduction by giving algorithms to compute $\widetilde{j_b}$ and κ in a residue disk as polynomials in parameters up to finite precision. This translates the geometric Chabauty method into solving simple polynomial equations. We also give algorithms to work in residue disks of T explicitly using p-adic heights and Coleman integrals. Moreover, by writing the geometric quadratic Chabauty method in terms of p-adic heights and Coleman integrals, we are able to prove Theorem H.

6.2.1 Structure of the paper

In Section 6.3 we provide background on the Poincaré torsor and its realizations. We solve the problem of how to efficiently represent elements of a residue disk of T. We show how to represent elements of the Poincaré torsor $\mathcal{M}^{\times}$ using the following statement that appears in [EL21, Section 9.3].

Proposition 6.2.6. *Let $p > 2$ be a prime of good reduction for X. There is a morphism of biextensions over $J(\mathbb{Z}_p) \times J(\mathbb{Z}_p)$*

$$\Psi\colon \mathcal{M}^{\times}(\mathbb{Z}_p) \to J(\mathbb{Z}_p) \times J(\mathbb{Z}_p) \times \mathbb{Q}_p, \tag{6.2.1.1}$$

with the trivial $\mathbb{Q}_p$-biextension structure on the latter product.

By Remark 6.2.4, we have that $J^0(\mathbb{Z}_p) = J(\mathbb{Z}_p)$. This proposition allows us to record elements of $\mathcal{M}^\times(\mathbb{Z}_p)$ up to finite p-adic precision. In Proposition 6.3.11 we describe the image of integer points of T in this trivial biextension $\mathcal{N} \coloneqq J(\mathbb{Z}_p) \times J(\mathbb{Z}_p) \times \mathbb{Q}_p$.

Since we can construct a bijection from residue disks of $J(\mathbb{Z}_p)$ to $\mathbb{Z}_p^g$ using Coleman integrals, we can explicitly write down a homeomorphism from the residue disk $T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to $\mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ factoring through Ψ; this is done in Corollary 6.3.22. Crucially, we prove that this homeomorphism is given by convergent power series on $\mathbb{Z}_p^{g+\rho-1}$, i.e. power series that modulo every power of p are given by polynomials.

Then in Section 6.4 we give an algorithm to construct the unique line bundle associated to the endomorphism f from a divisor in $U \times X$ satisfying certain properties described in Lemma 6.4.4. Using this line bundle we write down a theoretical formula for the trivializing section $\widetilde{j_b}\colon U \to T$. We give an algorithm for computing the convergent power series describing the embedding of a residue disk of the curve into the biextension $\mathcal{N}$ in Section 6.5. In Section 6.6 we give formulas for computing points in the biextension $\mathcal{N}$ that are the image of generating sections of certain residue disks of $\mathcal{M}$.

In Section 6.7 we tie everything together with the algorithm for geometric quadratic Chabauty in a residue disk $U(\mathbb{Z})_{\overline{P}}$. In this section, we also describe how to compute a finite set of p-adic points to finite precision containing the integer points in a single residue disk $U(\mathbb{Z})_{\overline{P}}$. We do this by reducing our computations to $T(\mathbb{Z}/p^k\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$ and using a Hensel-like lemma [EL21, Theorem 4.12]. By iterating over residue disks we find $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ up to finite precision.

The comparison theorem appears in Section 6.8. Theorem 6.8.5 states that the finite set of points found by the cohomological quadratic Chabauty method is a superset of the points found by the geometric method, and gives an explicit description of the points in their difference.

Section 6.9 shows a worked example of the algorithms applied to the case of $X_0(67)^+$. The rational points on this curve have been determined previously [BBB$^+$21], but the computations here demonstrate the practicality of the geometric quadratic Chabauty algorithms presented here for hyperelliptic modular curves.

6.3 Understanding the biextension and T

A crucial object of study in our paper is the Poincaré torsor. This has four incarnations, which we introduce in the following four subsections. Section 6.3.1 and Section 6.3.2 are expository sections and introduce important background from [EL21]. Section 6.3.3 introduces the trivial biextension, and contains new propositions relating the biextension to p-adic heights. Section 6.3.4 introduces the pseudoparametrization of the torsor that we work with for the rest of the paper, and proves that the pseudoparametrization is given by convergent power series modulo powers of p, with explicit bounds on the degree modulo powers of p.

6.3.1 The Poincaré torsor $\mathcal{P}$

First we introduce the Poincaré torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, its biextension structure, and the torsor $\mathcal{P}^{\times}$ over the integers. For more details on the Poincaré torsor and biextensions, see [MB85, §I.2.5] or Grothendieck's Exposés VII and VIII [GRR72]. The abelian variety $J_{\mathbb{Q}}^{\vee}$ is a moduli space for line bundles algebraically equivalent to zero on $J_{\mathbb{Q}}$; every $[c] \in J_{\mathbb{Q}}^{\vee}$ corresponds to a line bundle $\mathcal{L}_c$ on $J_{\mathbb{Q}}$. The universal line bundle over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$ is the *Poincaré bundle* $\mathcal{P}_{\mathbb{Q}}$. It satisfies the property that $\mathcal{P}_{\mathbb{Q}}|_{J_{\mathbb{Q}} \times [c]} \simeq \mathcal{L}_c$ and it is rigidified at 0, i.e. $\mathcal{P}_{\mathbb{Q}}|_{0 \times J^{\vee}}$ is trivial. Furthermore, under the natural identification $(J_{\mathbb{Q}}^{\vee})^{\vee} = J_{\mathbb{Q}}$, this line bundle is also the universal line bundle over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$ parametrizing line bundles on $J_{\mathbb{Q}}^{\vee}$.

Given a line bundle $\mathcal{L}$ over a scheme S, there is an associated $\mathbb{G}_m$-torsor $\mathcal{L}^{\times}$ defined by taking the sheaf of non-vanishing sections, and similarly given a $\mathbb{G}_m$-torsor Y there is an associated line bundle $Y \otimes_{\mathcal{O}_S^{\times}} \mathcal{O}_S$. Applying these associations to the Poincaré bundle, we obtain the universal $\mathbb{G}_m$-torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, called the *Poincaré torsor*. Alternatively,

$$\mathcal{P}_{\mathbb{Q}}^{\times} = \mathrm{Isom}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}(\mathcal{O}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}, \mathcal{P}_{\mathbb{Q}}),$$

i.e. for a scheme $S/(J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee})$ we have that $\mathcal{P}_{\mathbb{Q}}^{\times}(S)$ consists of isomorphisms of line bundles $\mathcal{O}_S \to (\mathcal{P}_{\mathbb{Q}})_S$. This set $\mathcal{P}_{\mathbb{Q}}^{\times}(S)$ is an $\mathcal{O}_S(S)^{\times}$-pseudotorsor: either empty or an $\mathcal{O}_S(S)^{\times}$-torsor.

The Poincaré torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ has the structure of a *biextension* over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, as we will now explain. Addition in $J_{\mathbb{Q}}^{\vee}$ corresponds to tensoring line bundles on $J_{\mathbb{Q}}$. This, along with the theorem of the square, induces a partial group law

on $\mathcal{P}_{\mathbb{Q}}^{\times}$. Let S be a scheme over $\mathbb{Q}$. For $x \in J_{\mathbb{Q}}(S)$ and $y_1, y_2 \in J_{\mathbb{Q}}^{\vee}(S)$ we have a tensor product which is an isomorphism of $\mathbb{G}_m$-torsors

$$(x, y_1)^* \mathcal{P}_{\mathbb{Q}}^{\times} \otimes (x, y_2)^* \mathcal{P}_{\mathbb{Q}}^{\times} \to (x, y_1 + y_2)^* \mathcal{P}_{\mathbb{Q}}^{\times}$$

that we denote by $\otimes_2$, because we are adding on the second coordinate (while the first coordinate stays fixed). Similarly since $(J_{\mathbb{Q}}^{\vee})^{\vee}$ is canonically identified with $J_{\mathbb{Q}}$, we also have the tensor product

$$(x_1, y)^* \mathcal{P}_{\mathbb{Q}}^{\times} \otimes (x_2, y)^* \mathcal{P}_{\mathbb{Q}}^{\times} \to (x_1 + x_2, y)^* \mathcal{P}_{\mathbb{Q}}^{\times}$$

called $\otimes_1$. These two partial group laws are compatible. Let $x_1, x_2 \in J_{\mathbb{Q}}(S)$, $y_1, y_2 \in J_{\mathbb{Q}}^{\vee}(S)$, and $z_{ij} \in (x_i, y_j)^* \mathcal{P}_{\mathbb{Q}}^{\times}(S)$, for $i, j \in \{1, 2\}$. Then

$$(z_{11} \otimes_2 z_{12}) \otimes_1 (z_{21} \otimes_2 z_{22}) = (z_{11} \otimes_1 z_{21}) \otimes_2 (z_{12} \otimes_1 z_{22}).$$

In other words, tensoring points in the biextension is not order-dependent. The structure of these two partial group laws over the product $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, together with this compatibility, makes $\mathcal{P}_{\mathbb{Q}}^{\times}$ a $\mathbb{G}_m$-biextension over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$.

For our applications, we need to work over the integers. Let J^0 be the fiberwise connected component of J containing 0. This represents line bundles on C that are fiberwise of multidegree 0. Let $J^{\vee}$ be the Néron model of $J_{\mathbb{Q}}^{\vee}$ and similarly let $J^{\vee 0}$ be the fiberwise connected component of $J^{\vee}$ containing 0. The Poincaré torsor extends to a biextension $\mathcal{P}^{\times}$ over $J \times J^{\vee 0}$. In particular, the integer points of $\mathcal{P}^{\times}$ lying over $(x, y) \in (J \times J^{\vee 0})(\mathbb{Z})$ form a $\mathbb{G}_m(\mathbb{Z})$-torsor, i.e. a $\{\pm 1\}$-torsor. So there is exactly one integer point lying over (x, y), up to sign.

6.3.2 The biextension $\mathcal{M}$

To work with explicit computations of points in the Poincaré torsor in practice, we need a few modifications of $\mathcal{P}^{\times}$. We introduce two torsors over $J \times J^0$, $\mathcal{M}^{\times}$ and $\mathcal{N}$ the trivial biextension.

We first discuss the construction of $\mathcal{M}^{\times}$ and the generating sections of its residue disks. The Abel–Jacobi embedding induces an isomorphism $j_b^* \colon J^{\vee} \to J$ and hence an isomorphism $j_b^* \colon J^{\vee 0} \to J^0$. We define

$$\mathcal{M}^{\times} \coloneqq (\mathrm{id}, j_b^{*,-1})^* \mathcal{P}^{\times}. \tag{6.3.2.1}$$

For the torsor $\mathcal{M}^{\times}$, we have an explicit description of the fibers. Let S be a scheme, $x \in J(S)$ be a point corresponding to a line bundle $\mathcal{L}$, and $y \in J^0(S)$

be a point with representing divisor $E = E^+ - E^-$ such that E^+ and E^- are effective and of the same multidegree. We denote the fiber $(x,y)^*\mathcal{M}^\times$ of $\mathcal{M}^\times$ over $(x,y) \in (J \times J^0)(S)$ by $\mathcal{M}^\times(x,y)$. This fiber $\mathcal{M}^\times(x,y)$ is the $\mathbb{G}_m$-torsor

$$E^*\mathcal{L}^\times \coloneqq \mathrm{Norm}_{E^+/S}\left(\mathcal{L}^\times\mid_{E^+}\right) \otimes \mathrm{Norm}_{E^-/S}\left(\mathcal{L}^\times\mid_{E^-}\right)^{-1}, \tag{6.3.2.2}$$

which we also denote by $\mathrm{Norm}_{E/S}\,\mathcal{L}^\times$. When $S = \operatorname{Spec}\mathbb{Z}$ we also write simply $\mathrm{Norm}_E\,\mathcal{L}^\times$. This fiber can be thought of as the aggregate of how $\mathcal{L}$ looks around E.

This description of the fiber is proven in [EL21, Proposition 6.8.7] and more general facts about these norms can be found in [EL21, Section 6]. Because equation (6.3.2.2) may seem a bit opaque, we provide some examples of how to apply the formula in practice.

Definition 6.3.1. Let S be a scheme. Let D and E be two relative Cartier divisors on X_S/S. We say D and E are *disjoint over* S if their support is disjoint as closed subschemes of X_S. In particular, it is not enough to have disjoint S-points if D or E does not split completely over S.

Example 6.3.2. Let S be a scheme, $[D] \in J(S)$, and $[E] \in J^0(S)$ be points of J and J^0 with representing divisors D and E where E has multidegree 0. Assume D and E are disjoint over S, and write $E = E^+ - E^-$ with E^+, E^- effective. Then the $\mathbb{G}_m$-torsor $E^*\mathcal{O}_X(D)^\times$ is generated by $\mathrm{Norm}_{E^+/S}(1) \otimes \mathrm{Norm}_{E^-/S}(1)^{-1}$ where 1 is here seen as a section of $\mathcal{O}_X(D)^\times|_{E^{\pm 1}}$. We also denote this generator by E^*1.

Example 6.3.3. Suppose the fiber of $X^{\mathrm{sm}}/\mathbb{Z}$ over 2 is geometrically irreducible. Let $[D] \in J(\mathbb{Z})$ and $[E] \in J^0(\mathbb{Z})$ be points of J and J^0 with representing divisors D and E. Assume D and E are disjoint over $\mathbb{Z}[\frac{1}{2}]$ and meet with multiplicity 1 over 2. Then $E^*\mathcal{O}_X(D)^\times$ is generated by $2^{-1}E^*1$.

Remark 6.3.4. Let S be a scheme. If $D = \operatorname{Div} g \in \mathsf{Div}^0(X_S/S)$ is the principal divisor of a rational function g and is disjoint from $E \in \mathsf{Div}^0(X_S/S)$, then the isomorphism $\mathcal{O}_X(D) \to \mathcal{O}_X$ given by multiplication by g induces an isomorphism $E^*\mathcal{O}_X(D)^\times \to E^*\mathcal{O}_X^\times$ sending E^*1 to $E^*g(E)$ where $g(E) \in \mathbb{G}_m(S)$.

Remark 6.3.5. In general, if $[D] \in J(\mathbb{Z})$, $[E] \in J^0(\mathbb{Z})$, and we have a choice of representing divisors D and E that are disjoint over $\mathbb{Q}$, using intersection theory we can determine $n \in \mathbb{Q}^\times$ unique up to sign, such that $\mathrm{Norm}_E\,\mathcal{O}_X(D)^\times$ is generated by $n \cdot E^*1$. If E is not of multidegree 0, there is a unique vertical divisor $V \subset C$ with $V + E$ of multidegree 0. In this case, one can compute the unique rational number a up to sign such that $(E+V)^*\mathcal{O}_X(D)^\times = a\,\mathrm{Norm}_E\,\mathcal{O}_X(D)^\times$. This is treated in detail in [EL21, Section 6.9].

The partial group laws on $\mathcal{M}^\times$ are also very explicit: let $[E], [E_1], [E_2] \in J^0(S)$ and $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2 \in J(S)$. They are given by the morphisms

$$E_1^*\mathcal{L}^\times \otimes E_2^*\mathcal{L}^\times \to (E_1 + E_2)^*\mathcal{L}^\times \tag{6.3.2.3}$$

corresponding to $\otimes_2$ and

$$E^*\mathcal{L}_1^\times \otimes E^*\mathcal{L}_2^\times \to E^*(\mathcal{L}_1 \otimes \mathcal{L}_2)^\times \tag{6.3.2.4}$$

corresponding to $\otimes_1$.

Example 6.3.6. Let $x_1, x_2 \in J(\mathbb{Z})$ and $y_1, y_2 \in J^0(\mathbb{Z})$. Let $z_{ij} \in \mathcal{M}^\times(\mathbb{Z})$ be points above (x_i, y_j) for $i \in \{1, 2\}$. Then for $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ we can construct points above $(n_1x_1 + n_2x_2, m_1y_1 + m_2y_2)$ by the formula

$$\left(z_{11}^{\otimes_2 m_1} \otimes_2 z_{12}^{\otimes_2 m_2}\right)^{\otimes_1 n_1} \otimes_1 \left(z_{21}^{\otimes_2 m_1} \otimes_2 z_{22}^{\otimes_2 m_2}\right)^{\otimes_1 n_2}.$$

This allows us to construct many integer points of $\mathcal{M}^\times$ by starting with a few points that lie over generators of the Jacobian and then applying the partial group laws. In Section 6.6 we will use this idea to determine the integer points of the torsor T landing in a specific residue disk of T.

6.3.3 The trivial biextension $\mathcal{N}$

In practice, we will often translate between $\mathcal{M}$ and the trivial biextension $\mathcal{N}$ where we do our computations. We explain how to make this translation following [EL21, Section 9.3]. From now on, we assume $p > 2$ is a prime of good reduction for $X_{\mathbb{Q}}$.

Let $[D] \in J(\mathbb{Q}_p)$ and $[E] \in J^0(\mathbb{Q}_p)$ be divisor classes with a choice of representing divisors D and E that are disjoint over $\mathbb{Q}_p$. Then $E^*\mathcal{O}_X(D)^\times$ is a $\mathbb{Q}_p^\times$-torsor, trivial with generator E^*1 by Example 6.3.2. Let h_p be the cyclotomic Coleman–Gross local height at p with respect to an isotropic splitting $H^1_{\mathrm{dR}}(X) = H^0(X, \Omega^1_X) \oplus W$ of the Hodge filtration [CG89, Section 5]. Choose a branch of the logarithm with $\mathsf{log}p = 0$ so that it is compatible with h_p. The local height h_p is a biadditive, symmetric pairing on disjoint divisors of degree 0, taking values in $\mathbb{Q}_p$. For f a rational function and $\mathsf{Div}f$ its associated divisor, it also satisfies the equality $h_p(D, \mathsf{Div}f) = \mathsf{log}f(D)$.

Remark 6.3.7. The assumption that p is a prime of good reduction for X is used to define the logarithm of $J_{\mathbb{Z}_p}$, and to compute the Coleman–Gross height and iterated Coleman integrals. There is a more general construction using Vologodsky integrals to construct the Coleman–Gross height [Bes22],

but currently there is no known way to compute this more general height for a prime of bad reduction.

We define a map

$$\begin{aligned} \psi\colon \mathcal{M}^\times(\mathbb{Z}_p) &\to \mathbb{Q}_p \\ E^*\lambda \in E^*\mathcal{O}_X(D)^\times &\mapsto \mathsf{log}\lambda + h_p(D,E). \end{aligned} \tag{6.3.3.1}$$

We define $\mathcal{N}$ to be the trivial $\mathbb{Q}_p$-biextension $J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)\times\mathbb{Q}_p$ over $J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)$. By definition, the partial group laws in $\mathcal{N}$ are just addition keeping one coordinate fixed. Let $[D],[D_1],[D_2]\in J(\mathbb{Q}_p)$ and $[E],[E_1],[E_2]\in J^0(\mathbb{Q}_p)$ and $v_1,v_2\in\mathbb{Q}_p$. The first group law is

$$([D_1],[E],v_1)+_1([D_2],[E],v_2)=([D_1]+[D_2],[E],v_1+v_2).$$

The second group law is

$$([D],[E_1],v_1)+_2([D],[E_2],v_2)=([D],[E_1]+[E_2],v_1+v_2).$$

Definition 6.3.8. We define the morphism of biextensions

$$\Psi\colon \mathcal{M}^\times(\mathbb{Z}_p)\to\mathcal{N}$$

to be the projection $\mathcal{M}^\times(\mathbb{Z}_p)\to J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)$ on the first two factors and ψ on the last factor.

Remark 6.3.9. Since $\mathsf{log}(-1)=0$, the morphism Ψ sends the two integer points of $\mathcal{M}^\times(\mathbb{Z})$ above a fixed integer point of $J\times J^0$ to the same point.

The following proposition appears in [EL21, Section 9.3] but is not proven.

Proposition 6.3.10. *The map $\Psi\colon\mathcal{M}^\times(\mathbb{Z}_p)\to\mathcal{N}$ is a morphism of biextensions.*

Proof. First we show that Ψ is well defined. For divisor classes $[D]\in J(\mathbb{Q}_p)$ and $[E]\in J^0(\mathbb{Q}_p)$ we can always choose representing divisors D and E with disjoint support over $\mathbb{Q}_p$; we show that the choice of representing divisors D and E does not matter. Suppose $D=D'+\mathsf{Div}g$ for some rational function g with $\mathrm{Div}\,g$ disjoint from E. Multiplication by g induces an isomorphism $\mathcal{O}_X(D)\to\mathcal{O}_X(D')$ sending $E^*1\mapsto E^*g(E)$ by Remark 6.3.4. Under ψ, the section $E^*\lambda$ in $E^*\mathcal{O}_X(D)$ maps to $\mathsf{log}\lambda+h_p(D,E)$ while $E^*g(E)\lambda$ in $E^*\mathcal{O}_X(D')$ maps to $\mathsf{log}\lambda+\mathsf{log}g(E)+h_p(D',E)$. But since $h_p(\mathsf{Div}g,E)=\mathsf{log}g(E)$ we have the equality $h_p(D',E)+\mathsf{log}g(E)=h_p(D,E)$, so the choice of representing

divisor for $[D]$ does not change the value of Ψ. By symmetry of the norm [EL21, Section 6.5], we can also conclude that Ψ does not depend on the choice of representing divisor for $[E]$.

Finally we show that Ψ preserves the two group laws (6.3.2.3) and (6.3.2.4). Let $[D_1], [D_2] \in J(\mathbb{Q}_p)$, and $[E] \in J^0(\mathbb{Q}_p)$ with E disjoint from D_1 and D_2. Let $E^*\lambda_1 \in E^*\mathcal{O}_X(D_1)$ and $E^*\lambda_2 \in E^*\mathcal{O}_X(D_2)$. Under ψ, the section $E^*\lambda_i$ maps to $\mathsf{log}\lambda_i + h_p(D_i, E)$ for $i = 1, 2$. The group law $\otimes_1$ in $\mathcal{M}^\times$ sends the sections to $E^*(\lambda_1\lambda_2)$ in $E^*\mathcal{O}_X(D_1 + D_2)$. Under the map ψ, the section $E^*(\lambda_1\lambda_2)$ is sent to

$$\mathsf{log}(\lambda_1\lambda_2) + h_p(D_1 + D_2, E) = \mathsf{log}\lambda_1 + \mathsf{log}\lambda_2 + h_p(D_1, E) + h_p(D_2, E).$$

Therefore Ψ preserves $\otimes_1$. By symmetry of the norm it also preserves $\otimes_2$. □

The following proposition relates this to the global p-adic height.

Proposition 6.3.11. *Let $[D] \in J(\mathbb{Z})$ and $[E] \in J^0(\mathbb{Z})$ with representing divisors D and E that have disjoint support over $\mathbb{Z}_{(p)}$. Let F be the unique vertical divisor such that $F + E$ has multidegree 0 on all fibers $X_{\mathbb{F}_q}$. Let $z \in \mathcal{M}^\times([D], [E + F])(\mathbb{Z})$. Then $\psi(z) = h([D], [E])$ where $h(\cdot, \cdot)$ denotes the global p-adic height.*

Proof. Let $\mathcal{L} = \mathcal{O}_X(D)$. Write $F = \sum_q F_{\mathbb{F}_q}$ where q ranges over the primes of bad reduction for X and $F_{\mathbb{F}_q}$ has support in $X_{\mathbb{F}_q}$. Then by [EL21, Proposition 6.9.3] we have the equation

$$\mathcal{M}^\times([D], [E]) = \prod_q q^{-F_{\mathbb{F}_q} \cdot D} \operatorname{Norm}_E(\mathcal{L}^\times)$$

where q ranges over the bad primes.

Recall that $\operatorname{Norm}_E(\mathcal{L}^\times)$ is by definition $\operatorname{Norm}_{E/\operatorname{Spec}\mathbb{Z}}(\mathcal{L}^\times|_E)$; this torsor is canonically identified with

$$\mathcal{O}_{\operatorname{Spec}\mathbb{Z}}(\prod_q q^{-(E \cdot D)_q})^\times$$

and hence has generator $\prod_q q^{-(E \cdot D)_q}$, where $(E \cdot D)_q$ denotes the intersection number of E and D over $\mathbb{Z}_{(q)}$ taking values in $\mathbb{Z}$.

In total, we see that under these identifications $\mathcal{M}^\times([D], [E + F])$ is generated by the element $E^* \prod_q q^{-((E+F) \cdot D)_q}$. By definition, for $q \neq p$, we have that

$h_q(D,E)$ is $-((E+F)\cdot D)_q \mathsf{log} q$, and hence we get

$$\begin{aligned}\psi(z) &= \mathsf{log}\prod_q q^{-((E+F)\cdot D)_q} + h_p(D,E)\\ &= \sum_{q\neq p} h_q(D,E) + h_p(D,E)\\ &= h([D],[E])\end{aligned}$$

as we wanted. □

6.3.4 The torsor T_f

We set up some notation. Recall from Section 6.2 that we have fixed a simple open set $U \subset X^{\mathrm{sm}}$ that contains the smooth points of one geometrically irreducible component of each fiber. Let f be a trace zero endomorphism of J. Recall the integer m from (6.2.0.1). The map $m\cdot\circ f$ is a morphism $J \to J^0$. Let $c \in J(\mathbb{Z})$ denote the unique element such that $j_b^*(\mathrm{id}, m\cdot\circ\mathrm{tr}_c\circ f)^*\mathcal{M}^\times$ is trivial over U. Let $\alpha_f \coloneqq m\cdot\circ\mathrm{tr}_c\circ f$. Let $\xi_f\colon T_f \to J$ denote the $\mathbb{G}_m$-torsor $(\mathrm{id},\alpha_f)^*\mathcal{M}^\times$ over J. The trivialization of $j_b^*(\mathrm{id}, m\cdot\circ\mathrm{tr}_c\circ f)^*\mathcal{M}^\times$ then gives us a morphism $\widetilde{j_{b,f}}\colon U \to T_f$ of schemes over J.

Remark 6.3.12. If f is identically zero, then T_f is isomorphic to the trivial $\mathbb{G}_m$-torsor over J. If $r < g$ this reduces to the geometric linear Chabauty case, see [Spe20, HS22a] for more details, but when $r = g$ this trivial torsor contains no information.

As discussed in the overview, we work on the curve residue disk by residue disk, and hence we will describe the residue disks of T_f, culminating in Lemma 6.3.20. Throughout the rest of this section, fix a $\overline{t} \in T_f(\mathbb{F}_p)$. We work inside the residue disk $T_f(\mathbb{Z}_p)_{\overline{t}}$. Since T_f is trivial on fibers, the residue disk $T_f(\mathbb{Z}_p)_{\overline{t}}$ is isomorphic to $J(\mathbb{Z}_p)_{\xi_f(\overline{t})} \times \mathbb{G}_m(\mathbb{Z}_p)_u$ for some unit $u \in \mathbb{F}_p$. We would like to parametrize this residue disk.

Definition 6.3.13. Let Y be a smooth scheme over $\mathbb{Z}_p$ of relative dimension d, and let $y \in Y(\mathbb{F}_p)$. We say $t_1,\dots,t_d$ are *parameters* of Y at y if they are elements of the local ring $\mathcal{O}_{Y,y}$ such that the maximal ideal is given by $(p,t_1,\dots,t_d)$.

Define $t_i' \coloneqq t_i/p$. Then evaluation of t', the vector $(t_1',\dots,t_d')$, gives a bijection $t'\colon Y(\mathbb{Z}_p)_y \to \mathbb{Z}_p^d$. We call t' a *parametrization* given by parameters t_i.

Example 6.3.14. Take $Y = \mathbb{G}_m = \operatorname{Spec}\mathbb{Z}_p[x,x^{-1}]$ over $\mathbb{Z}_p$; this is of relative dimension 1. Let $y = 1 \in \mathbb{G}_m(\mathbb{F}_p)$. Then $x-1$ is a parameter at y; it induces

a parametrization $\theta\colon \mathbb{G}_m(\mathbb{Z}_p)_y \to \mathbb{Z}_p$ given by $u \mapsto (u-1)/p$. Note that the map log, defined by its power series $\mathsf{log}(1+x) = x - \frac{x^2}{2} + \cdots$ also induces a bijection $\varphi = \mathsf{log}/p\colon \mathbb{G}_m(\mathbb{Z}_p)_y \to \mathbb{Z}_p$, but this is *not* a parametrization; it is not given by evaluating elements of the maximal ideal, and is not even fully algebraic in nature. However, there is a relation between φ and θ, in that $\theta \circ \varphi^{-1}$ is given by the power series $\frac{1}{p}\big(xp - \frac{(xp)^2}{2} + \cdots\big) \in \mathbb{Z}_p[[x]]$.

In [EL21, Lemma 6.6.8] the residue disk $T_f(\mathbb{Z}_p)_{\overline{t}}$ is parametrized using parameters at $\overline{t}$. However, this parametrization can be difficult to work with because it uses parameters in J. The group law of J expressed in these parameters is given by complicated converging power series. It is possible to use this parametrization in practice: see for example [Mas20], where the Khuri-Makdisi representation [KM04] is generalized in order to work with points of the Jacobian up to the required p-adic precision and compute parameters of them; however, with this representation other steps of the algorithm, like computing the image under an endomorphism, would be more difficult. Here, we opt to use the logarithm of J instead to give a bijection between the residue disk $T_f(\mathbb{Z}_p)_{\overline{t}}$ and $\mathbb{Z}_p^{g+1}$ that is not a parametrization in the sense of Definition 6.3.13. For a definition of this logarithm, see [Hon70]. To describe the relationship between this bijection and the parametrization of this residue disk we need the framework of convergent power series.

Definition 6.3.15. Let $n \in \mathbb{N}$. The *ring of convergent power series in n variables* is defined as

$$\mathbb{Q}_p\langle x_1, \ldots, x_n\rangle \coloneqq \{\sum_{I\in\mathbb{N}^n} a_I x^I \in \mathbb{Q}_p[[x_1,\ldots,x_n]] \mid \lim_{I\to\infty} |a_I| = 0\}$$

where $x = (x_1, \ldots, x_n)$ is the vector of variables. An element of this ring is called an *integral convergent power series* if it lies inside $\mathbb{Z}_p[[x_1,\ldots,x_n]]$. The convergent power series are those power series converging on all of $\mathbb{Z}_p^n$. Unlike formal power series, one can always compose two (integral) convergent power series, since by definition the resulting infinite sum inside the ring of (integral) convergent power series converges.

Remark 6.3.16. Let Y be a smooth scheme over $\mathbb{Z}_p$ of relative dimension d, let $y \in Y(\mathbb{F}_p)$, and let $\theta, \theta'\colon Y(\mathbb{Z}_p)_y \to \mathbb{Z}_p^d$ be two parametrizations. Then the composite $\theta' \circ \theta^{-1}\colon \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ is given by (multivariate) integral convergent power series that are linear modulo p, and in fact are of degree at most M modulo p^M.

Lemma 6.3.17. *Let G be a smooth, commutative group scheme over $\mathbb{Z}_p$ of relative dimension d. Let $G(\mathbb{Z}_p)_0$ be the residue disk containing the unit $0 \in$*

$G(\mathbb{Z}_p)$. Let $\theta\colon G(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^d$ be a parametrization, and let $\log\colon G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d$ be a choice of logarithm. Then $\log \circ \theta^{-1}\colon \mathbb{Z}_p^d \to p\mathbb{Z}_p^d$ is given by d integral convergent power series in d variables. For $n \geq 0$ the coefficient of a degree n monomial in one of these power series has valuation at least $\max(1, n - v_p(n))$.

Proof. By [Spe20, Lemma 3.7] the function $\log \circ \theta^{-1}$ is given by integral convergent power series. There the third author gives the vector-valued formula

$$\log = \sum_{I \in \mathbb{N}^d \setminus (0,\ldots,0)} a_I c_{|I|} x^I$$

where $x = (x_1, \ldots, x_d)$ is the vector of variables, the coefficients a_I lie in $\mathbb{Z}_p$, the notation $|I|$ means $i_1 + \cdots + i_d$ where $I = (i_1, \ldots, i_d)$, and $c_n = p^n/n$. (In this paper we do not divide by p in the log, unlike in [Spe20]). The result follows immediately from the observation that $v_p(c_{|I|}) = |I| - v_p(|I|)$. □

The following result establishes the analyticity of the map ψ on residue disks of $\mathcal{M}^\times$.

Lemma 6.3.18 ([EL21, Section 9.3])**.** *Let $\overline{z} \in \mathcal{M}^\times(\mathbb{F}_p)$. Let $\widetilde{z}$ be a lift of $\overline{z}$ to $\mathcal{M}^\times(\mathbb{Z}_p)$. Let $\Theta\colon \mathbb{Z}_p^{2g+1} \to \mathcal{M}^\times(\mathbb{Z}_p)_{\overline{z}}$ be a parametrization. Consider the map*

$$\begin{aligned} \psi_{\overline{z}}\colon \mathcal{M}^\times(\mathbb{Z}_p)_{\overline{z}} &\to \mathbb{Q}_p \\ z &\mapsto \frac{\psi(z) - \psi(\widetilde{z})}{p}. \end{aligned}$$

Then $\psi_{\overline{z}} \circ \Theta$ is given by a convergent power series.

As discussed above, we can now find a bijection between residue disks of T_f and $\mathbb{Z}_p^g \times \mathbb{Q}_p$. We use the logarithm of the Jacobian, which gives an isomorphism $\log\colon J(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^g$ by choosing a basis of $H^0(J_{\mathbb{Z}_p}, \Omega^1)$ as well as the map ψ defined in (6.3.3.1). For ease of notation, we suppress the monomorphism $T_f \to \mathcal{M}^\times$ in our notation, and apply ψ directly to $T_f(\mathbb{Z}_p)$.

Definition 6.3.19. Recall that we fixed a $\overline{t} \in T_f(\mathbb{F}_p)$. Choose $\widetilde{t} \in T_f(\mathbb{Z}_p)_{\overline{t}}$ to be a lift of $\overline{t}$. Let $\varphi_f\colon T_f(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p$ be defined by

$$\varphi_f(z) = ((\log \xi_f(z) - \log \xi_f(\widetilde{t}))/p, (\psi(z) - \psi(\widetilde{t}))/p)$$

where ψ is defined in (6.3.3.1) and the map $\xi_f\colon T_f \to J$ is the structure morphism of T_f.

We call φ_f a *pseudoparametrization* of the residue disk $T_f(\mathbb{Z}_p)_{\overline{t}}$.

Similarly to Example 6.3.14, this is not a parametrization; it shares some of the properties of a parametrization, notably the property in Remark 6.3.16, as the following lemma shows.

Lemma 6.3.20. *The pseudoparametrization φ_f is an injection, and for any parametrization $\theta\colon T_f(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^{g+1}$ the resulting map $\varphi_f \circ \theta^{-1}\colon \mathbb{Z}_p^{g+1} \to \mathbb{Z}_p^g \times \mathbb{Q}_p$ is given by $g+1$ convergent power series. The valuation of the coefficient of any degree n monomial occurring in one of the first g convergent power series is at least* $\max(0, n-1-v_p(n))$.

Proof. By Lemma 6.3.17 and Lemma 6.3.18 the pseudoparametrization is given by convergent power series and the valuations of the coefficients behave in the required way. It remains to prove that it is an injection. First, note that the maps $\frac{1}{p}\mathsf{log}\colon J(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^g$ and $\frac{1}{p}\mathsf{log}\colon \mathbb{G}_m(\mathbb{Z}_p)_1 \to \mathbb{Z}_p$ are bijections.

Let $[D], m(f([D]) + c) \in J(\mathbb{Z}_p)_0$ with disjoint representing divisors D and E, and let $\lambda_0, \lambda_1 \in \mathbb{G}_m(\mathbb{Z}_p)$ such that for $i = 0, 1$ we have $([D], [E], \lambda_i) \in T_f(\mathbb{Z}_p)_{\overline{t}}$. Assume that $\varphi_f(([D], [E], \lambda_0)) = \varphi_f(([D], [E], \lambda_1))$. Then we have that $\mathsf{log}\lambda + h_p(D, E) = \mathsf{log}\lambda' + h_p(D, E)$ so, because $\frac{1}{p}\mathsf{log}$ is injective on residue disks, then $\lambda = \lambda'$, and φ_f is injective.

By Lemma 6.3.17 the result follows. □

6.3.5 The torsor T

Let $f_1, \ldots, f_{\rho-1}$ be a basis for the trace zero endomorphisms of J. We simplify our notation by setting $c_i \coloneqq c_{f_i}$, $\alpha_i \coloneqq \alpha_{f_i}$, $T_i \coloneqq T_{f_i}$, and $\xi_i \coloneqq \xi_{f_i}\colon T_i \to J$.

Now we define $\xi\colon T \to J$ to be the $\mathbb{G}_m^{\rho-1}$-torsor given by the fiber product

$$T \coloneqq T_1 \times_J T_2 \times_J \cdots \times_J T_{\rho-1}.$$

Finally, let $\widetilde{j_b}\colon U \to T$ be a choice of morphism (well defined up to the choice of $\rho - 1$ signs) coming from the morphisms $\widetilde{j_{b,f_i}}\colon U \to T_i$.

As in Section 6.3.4, we can pseudoparametrize residue disks of T.

Definition 6.3.21. Recall that we fixed a $\overline{t} \in T(\mathbb{F}_p)$. We also fix

$$\widetilde{t} = (\widetilde{t}_1, \ldots, \widetilde{t}_{\rho-1}) \in T(\mathbb{Z}_p)_{\overline{t}}$$

a lift of $\overline{t}$. Let $\varphi\colon T(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ be defined by

$$\varphi(z_1, \ldots, z_{\rho-1}) = \\ ((\mathsf{log}\xi_1(z_1) - \mathsf{log}\xi_1(\widetilde{t}_1))/p, (\psi(z_1) - \psi(\widetilde{t}_1)/p), \ldots, (\psi(z_{\rho-1}) - \psi(\widetilde{t}_{\rho-1})/p))$$

where ψ is defined in (6.3.3.1). We call φ a *pseudoparametrization* of the residue disk $T(\mathbb{Z}_p)_{\overline{t}}$. (Recall that $\xi_i(z_i)$ and $\xi_i(\widetilde{t}_i)$ are independent of i, since T is a fibered product over J.)

Corollary 6.3.22. *The pseudoparametrization map φ is an injection, and for any parametrization $\theta\colon T(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^{g+\rho-1}$ the resulting map $\varphi\circ\theta^{-1}\colon \mathbb{Z}_p^{g+\rho-1} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by $g+\rho-1$ convergent power series. For any of the first g power series, the valuation of the coefficient of a degree n monomial is at least $n-1-v_p(n)$.*

Proof. This is a corollary of Lemma 6.3.20. □

The main advantage of this method is that for φ_f we need only to compute the map ψ defined in (6.3.3.1); it is this fact that allows to us to mainly work in $\mathcal{N}$ and only translate back to the image of the residue disk under φ when needed.

6.4 The line bundle

In this section we describe how to explicitly construct the nontrivial $\mathbb{G}_m$-torsor T and give a formula for the section $\widetilde{j_b}\colon U \to T$. For this, we work with endomorphisms of J. We make this explicit by considering correspondences on $X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ and extensions on $U \times X$. Recall that $p > 2$ is henceforth a prime of good reduction.

Remark 6.4.1. To work with divisors on U, X or $U \times X$ explicitly, we use equations for a projective regular model of X. There are multiple ways to do this. On a theoretical level, a regular model itself is projective over $\mathbb{Z}$ because it is a repeated blowup of the projective closure of its generic fiber. On a practical level, this process could embed the regular model in a high-dimensional projective space, and it is easier to work on affine patches. In this case we give divisors on each of the affine patches by Gröbner bases, compatible with the glueing data. For a practical implementation, we recommend this latter method. This is implemented in `Magma`, for example. The methods in the rest of the section are agnostic to the exact implementation. Throughout this section, we assume we can represent effective divisors on the regular model by a Gröbner basis, and we represent general divisors by a difference between two effective divisors.

As explained in Section 6.3.5, to construct the torsor T, we need $\rho - 1$ independent trace zero endomorphisms $(f_i)_{i=1}^{\rho-1}\colon J \to J$. (In general one only

needs n independent nontrivial trace zero endomorphisms where n is such that $r < g + n$, but one expects to obtain a smaller superset of p-adic points containing $X(\mathbb{Z})$ for higher n. In fact, if we use n nontrivial independent endomorphisms such that $r < g + n - 1$, then we expect to cut out $X(\mathbb{Z})$ exactly unless there is some geometric reason for extra points.) To work with any endomorphism $f\colon J \to J$ explicitly, we recall some facts about correspondences, as can be found in [Smi05]. A *correspondence* on $X \times X$ is a divisor D on $X \times X$.

Write $D = \sum_i n_i D_i$ as a sum of prime divisors. Denote by $\pi_1^{D_i}\colon D_i \to X$ the projection onto the first factor of $X \times X$ and similarly $\pi_2^{D_i}$ for projection onto the second factor. The correspondence D induces an endomorphism of the Jacobian $\xi_D = \sum_i n_i \pi_{2,*}^{D_i} \pi_1^{D_i,*}$. In particular, it sends the Jacobian point $[x - y]$ to $\mathcal{O}_X(D|_{x\times X} - D|_{y\times X})$.

Example 6.4.2. Consider negation $-1\cdot\colon J \to J$ on a hyperelliptic curve of the form $y^2 = h(x, z)$ in weighted projective space. If we give $X \times X$ the projective coordinates x, y, z, x', y', z', then a correspondence representing $-1\cdot$ is given by the homogeneous equation $y = -y'$.

The aim of this section is to describe, given correspondences for all f_i, how to calculate the morphism $\widetilde{j_b}\colon U \to T$. For this goal, we partially follow [EL21, Section 7].

In the case where $X_{\mathbb{Q}}$ is a classical modular curve we can construct many trace zero endomorphisms using the Hecke algebra. See for example the computation leading to (6.9.0.4) in Section 6.9.

We now focus on the computations for a single trace zero endomorphism $f\colon J \to J$. We can compute equations for a correspondence $D_{f,\mathbb{Q}} \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ inducing f using the code of Costa, Mascot, Sijsling, and Voight [CMSV19]. The input of that algorithm is the $g \times g$ matrix giving the representation of the morphism f on a basis of differential forms $H^0(X_{\mathbb{Q}}, \Omega^1)$.

Algorithm 6.4.3 (Compute A_α)**.**
Input: $D_{f,\mathbb{Q}} \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ *a divisor.*
Output: a divisor A_α *on* $X^{\mathrm{sm}} \times X$*.*

1. *Spread out* $D_{f,\mathbb{Q}}$ *to* D'_f *over* $X^{\mathrm{sm}} \times X$ *by clearing denominators of the generators of the Gröbner basis.*
2. *Set* $B \coloneqq D'_f|_{X^{\mathrm{sm}}\times b}$ *and* $C \coloneqq D'_f|_{\Delta_{X^{\mathrm{sm}}}}$*.*
3. *Set* $A_\alpha \coloneqq m\left(D'_f - B \times X + X^{\mathrm{sm}} \times B - X^{\mathrm{sm}} \times C\right)$ *(where* m *is defined*

in (6.2.0.1)).

4. *Return A_α, as a Gröbner basis over $\mathbb{Z}$.*

Lemma 6.4.4. *The divisor A_α on $X^{\mathrm{sm}} \times X$ given by Algorithm 6.4.3 is the unique divisor on $X^{\mathrm{sm}} \times X$ with the following properties:*

(a) the endomorphism of J induced by the correspondence A_α is $m \cdot \circ f$;

(b) $\mathcal{O}_{X^{\mathrm{sm}}}(A_\alpha|_{U\times b})$ is rigidified with trivializing section 1;

(c) $\mathcal{O}_{X^{\mathrm{sm}}}(A_\alpha|_\Delta)$ is rigidified, compatible with the previous rigidification;

(d) the degree of A_α restricted to fibers of the first projection is 0.

Proof. By [Smi05, Theorem 3.4.7], any divisor inducing the endomorphism $m \cdot \circ f$ is of the form $mD_f + F$ such that F is a sum of vertical or horizontal divisors, so then (a) holds. Conditions (b) and (c) force F to be $m(-B \times X + X^{\mathrm{sm}} \times B - X^{\mathrm{sm}} \times C)$. Finally, by [BL04, Proposition 11.5.2] and the important fact that the trace of f is zero we have that $\deg(A_\alpha|_{P\times X}) = 0$ and (d) holds. So A_α is the desired divisor. □

Remark 6.4.5. Conditions (b) and (d) are the other way from the order chosen in Edixhoven–Lido, in order to agree with the convention in [CMSV19]. (That is, in Edixhoven–Lido, they require that the fibers of the *second* projection are degree 0.)

This divisor A_α determines a line bundle $\mathcal{L}_\alpha = \mathcal{O}_{X^{\mathrm{sm}}\times X}(A_\alpha)$ on $X^{\mathrm{sm}} \times X$, rigidified on $X^{\mathrm{sm}} \times b$, of degree 0 on the fibers of the first projection, and such that $\Delta^*\mathcal{L}_\alpha$ is trivial. This induces the endomorphism $m \cdot \circ f$ by

$$[x - y] \mapsto (\mathcal{L}_\alpha)_{x\times X} \otimes (\mathcal{L}_\alpha)^{-1}_{y\times X}. \tag{6.4.0.1}$$

Corollary 6.4.6. *Let $c \coloneqq [(\mathcal{L}_{\alpha,\mathbb{Q}})_{b\times X}] \in J(\mathbb{Q}) = J(\mathbb{Z})$. Let $\alpha = m \cdot \circ \mathrm{tr}_c \circ f$ be the morphism $\alpha\colon J \to J^0$. Then $j_b^*(\mathrm{id}, \alpha)^*\mathcal{M}^\times$ is trivial over U.*

Proof. This follows directly from [EL21, Proposition 7.2] □

The rest of this section will be dedicated to computing α, and computing the trivialization of $j_b^*(\mathrm{id}, \alpha)^*\mathcal{M}^\times$.

Algorithm 6.4.7 (Compute c)**.**

Input: equations for a correspondence A_α output by Algorithm 6.4.3, inducing the morphism $m \cdot \circ f\colon J \to J$.
Output: a divisor representing $c = [(\mathcal{L}_\alpha)_{b\times X}] \in J(\mathbb{Q}) = J(\mathbb{Z})$.

1. *Set $A_f \coloneqq A_\alpha/m$ (recall that A_α was defined as m times a different correspondence, so this is well defined).*
2. *Compute the generic fiber $A_{f,\mathbb{Q}}$ of A_f.*
3. *Compute equations for the divisor $A_{f,\mathbb{Q}}|_{b\times X}$ by specializing the equations of $A_{f,\mathbb{Q}}$ to b in the first copy of X^{sm}.*
4. *Return a Gröbner basis for $A_{f,\mathbb{Q}}|_{b\times X}$ over $\mathbb{Q}$.*

Algorithm 6.4.8 (Compute f_*)**.**

Input: a morphism of projective schemes $f\colon X \to Y$ given as a graded ring morphism $f^*\colon S \to R$, where $X = \operatorname{Proj} R$ and $Y = \operatorname{Proj} S$; an irreducible subvariety Z of X given by a Gröbner basis for its defining ideal J in R.
Output: the pushforward $f_*([Z])$, given by a Gröbner basis.

1. *Let B be a set of generators of S.*
2. *Set $I \subset S \otimes R$ to be the ideal generated by $\{b \otimes 1 - 1 \otimes f^*(b) \mid b \in B\}$ and $1 \otimes J$.*
3. *Compute a Gröbner basis B for I with respect to the lexicographical ordering on $S \otimes R$.*
4. *Set $K \coloneqq I \cap S$ with Gröbner basis $B \cap S$.*
5. *Compute the degree $d \coloneqq \deg(f|_Z\colon \operatorname{Proj} R/J \to \operatorname{Proj} S/K)$.*
6. *Return a Gröbner basis for K^d.*

Proof. By construction, K is the defining ideal for the image of Z. The pushforward of Z is then exactly $(\deg f|_Z) \cdot [\operatorname{im} f|_Z]$. □

Remark 6.4.9. In Step 5, we need to compute the degree of a morphism between projective schemes. There are algorithms to compute the degree of a rational map between two projective schemes. See for example [Sta18b] for a discussion on an implementation in Macaulay2.

Algorithm 6.4.10 (Apply f)**.**

Input: a ring S and two effective divisors D_+ and D_- on X_S^{sm} of the same degree; the correspondence A_α from Algorithm 6.4.3 inducing the morphism $m \cdot f\colon J \to J$.

Output: the Jacobian point $m \cdot f([D_+ - D_-]) \in J(S)$.

1. *For $D \in \{D_+, D_-\}$ do:*

   (a) *Compute a Gröbner basis for* $A_\alpha|_{D\times X}$ *as a divisor on* $D \times X$.
   (b) *Write* $D = \sum_i n_i D_i$ *as a sum of irreducible components using primary decomposition.*
   (c) *Compute the Gröbner basis for the pushforward* $E(D_i) \coloneqq n_i f_*(D_i)$ *on* X *using Algorithm 6.4.8 for every* D_i.
   (d) *Set* $E(D) \coloneqq \sum_i E(D_i)$.
2. *Return* $E(D_+) - E(D_-)$.

Remark 6.4.11. In the case where one can write $[D_+ - D_-]$ as a sum $\left[\sum_{i=1}^k n_i P_i\right]$ of S-points, one can use the isomorphism $P_i \times X \simeq X$ to simply compute $A_\alpha|_{P_i\times X}$ on X and take the linear combination $\left[\sum_{i=1}^k n_i A_\alpha|_{P_i\times X}\right]$.

Finally, we discuss the section $\widetilde{j_b}\colon U \to T$ lying above the Abel–Jacobi map $j_b\colon U \to J$ with base point b. Let $\bar{z} \in X(\mathbb{F}_p)$. Since the pullback j_b^*T is trivial, there is a morphism $\widetilde{j_b}\colon U \to T$ embedding each residue disk $U(\mathbb{Z}_p)_{\overline{z}}$ into the $(g+\rho-1)$-dimensional residue disk $T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{z})}$. To compute this map, we follow [EL21, Section 7]. Let n be the product of all primes of bad reduction. We first need to compute the numbers W_q and V_q mentioned in [EL21, Proposition 7.8] for $q \mid n$. These numbers have an involved definition in general. Nevertheless, they can be explicitly computed in our case, and we explain their meaning below.

By Lemma 6.4.4 the line bundles $\Delta^*(\mathcal{L}_\alpha)$ and $(\mathrm{id}, b)^*(\mathcal{L}_\alpha)$ are trivial with trivializing sections $\ell = 1$. Then W_q is defined as the valuation of this section ℓ on $U_{\mathbb{F}_q}$. In our case, these are always 0. It remains to compute V_q. We recall the definition. Note that $\mathcal{L}_\alpha$ has degree 0 on the fibers of the projection $U \times X \to U$, but it might not have multidegree 0.

Definition 6.4.12. We define V to be the unique vertical divisor on $U \times X$ having support disjoint from $U \times b$ such that $\mathcal{L}_\alpha(V)$ has multidegree 0 on all fibers of the projection. Write $V_{\mathbb{F}_q}$ as a sum of irreducible components of $U_{\mathbb{F}_q} \times X_{\mathbb{F}_q}$, i.e., as a linear combination of $U_{\mathbb{F}_q} \times Y_{\mathbb{F}_q}$ where $Y_{\mathbb{F}_q}$ is an irreducible component of $X_{\mathbb{F}_q}$. For $q \mid n$ define $V_q \in \mathbb{Z}$ to be the coefficient of the component $(U_{\mathbb{F}_q} \times U_{\mathbb{F}_q})$ in $V_{\mathbb{F}_q}$.

Lemma 6.4.13. *The local height* $h_q(z - b, A_\alpha|_{z\times X})$ *is equal to* $-V_q \log q$ *for any* $z \in U(\mathbb{Z}_q)$.

Proof. Since V is the unique vertical divisor with $A_\alpha + V$ having multidegree 0 on all fibers of the projection, we have that $h_q(z - b, A_\alpha|_{z\times X})$ is equal to

$-((z-b)\cdot(A_\alpha+V)|_{z\times X})_q \log q$. By construction, the divisors $z-b$ and $A_{\alpha|_{z\times X}}$ are disjoint over $\mathbb{Z}$, hence it remains to show that $((z-b)\cdot V|_{z\times X})_q = V_q$. This follows from Definition 6.4.12 and the fact that V has support disjoint from $U \times b$. □

To compute these numbers, we give the following algorithm.

Algorithm 6.4.14 (Calculate V_q)**.**

Input: the curve X, a bad prime q dividing n, the open set U such that $U(\mathbb{F}_q) \neq \emptyset$, and the divisor A_α on $X \times X$.
Output: the integer V_q.

1. *Pick a point $\overline{Q} \in U(\mathbb{F}_q)$.*
2. *Compute $A_\alpha|_{\overline{Q}\times X}$.*
3. *Compute the multidegree of $A_\alpha|_{\overline{Q}\times X}$.*
4. *Compute the multidegree of the irreducible components of $X_{\mathbb{F}_q}$.*
5. *Compute the unique linear combination $D \subset X_{\mathbb{F}_q}$ of these irreducible components such that D does not meet $\overline{b}$ and such that $A_\alpha|_{\overline{Q}\times X} + D$ has multidegree 0 at the fiber over q.*
6. *Set V_q to be the coefficient of the irreducible component containing $U_{\mathbb{F}_q}$ in D.*
7. *Return V_q.*

Remark 6.4.15. If $U(\mathbb{F}_q)$ is empty for some prime q, we can discard U. Integer points reduce to smooth points, so $U(\mathbb{Z}) = \emptyset$ in this case.

Remark 6.4.16. These local heights can also be computed using harmonic analysis on the dual graph, see [BD20, Section 12]. Even though both the geometric method and the harmonic method can be realized as combinatorics on the dual graph, it is not clear how to compare the two computations of local heights.

Let R be a ring and $z \in U(R)$. By [EL21, Proposition 7.5] we have

$$\begin{aligned} T_f(j_b(z)) &= \mathcal{M}^\times(j_b(z), \alpha(j_b(z))) = z^*(z,\mathrm{id})^*(\mathcal{L}_\alpha)^\times \otimes b^*(z,\mathrm{id})^*(\mathcal{L}_\alpha)^{\times,-1} \\ &= (\mathcal{L}_\alpha)^\times(z,z) \otimes (\mathcal{L}_\alpha)^\times(z,b)^{-1} = (\mathcal{L}_\alpha)^\times(z,z). \end{aligned}$$

We apply [EL21, Proposition 7.8] to give a formula for $\widetilde{j_b}(z)$ when $R \subset \mathbb{Z}_p$.

We have that

$$\widetilde{j_b}(z) = \prod_{q|n} q^{-V_q}(z^*1) \otimes (b^*1)^{-1} = (z-b)^* \prod_{q|n} q^{-V_q} \in (z-b)^* \mathcal{O}_X(A_\alpha|_{z\times X}) \tag{6.4.0.2}$$

is a trivializing section over the curve. The image in $\mathcal{N}$ is given by

$$\psi(\widetilde{j_b}(z)) = h_p(z-b, A_\alpha|_{z\times X}) - \sum_{q|n} V_q \mathsf{log} q. \tag{6.4.0.3}$$

Corollary 6.4.17. *The function $\Psi \circ \widetilde{j_b} \colon U(\mathbb{Z}_p) \to \mathcal{N}$ is given by*

$$z \mapsto ([z-b], [A_\alpha|_{z\times X}], h_p(z-b, A_\alpha|_{z\times X}) - \sum_{q|n} V_q \mathsf{log} q).$$

6.5 Embedding the curve

We now describe how to compute the embedding of the curve into the torsor through the evaluation of the trivializing section $\widetilde{j_b}$ on a residue disk of the point $\overline{P} \in U(\mathbb{F}_p)$. Recall the pseudoparametrization $\varphi \colon T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ from Definition 6.3.21. Let ν be a local parameter in the residue disk of the curve above $\overline{P}$. We can parametrize this residue disk by evaluating

$$\mathbb{Z}_p \to U(\mathbb{Z}_p)_{\overline{P}}, \qquad \nu \mapsto P_\nu.$$

This is also a parametrization in finite precision, i.e. we have bijections $\mathbb{Z}/p^k\mathbb{Z} \to U(\mathbb{Z}/p^{k+1}\mathbb{Z})_{\overline{P}}$ for any integer $k \geq 1$. Define the map $\lambda \colon \mathbb{Z}_p \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to be the composite of this parametrization $\mathbb{Z}_p \to U(\mathbb{Z}_p)_{\overline{P}}$ and $\widetilde{j_b}$. In this section, we show how to apply the following proposition.

Proposition 6.5.1. *The map $\varphi \circ \lambda : \mathbb{Z}_p \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by convergent power series.*

The image $\mathrm{im}(\varphi \circ \lambda)$ *inside* $\mathrm{im}\,\varphi$ *is cut out by equations $g_1 = \cdots = g_{g+\rho-2} = 0$ where $g_1, \ldots, g_{g+\rho-2} \in \mathbb{Z}_p\langle x_1, \ldots, x_{g+\rho-1}\rangle$ are integral convergent power series.*

Proof. This follows from Corollary 6.3.22 and [Bou98, Corollary 2, III.4.5]. □

For actual calculations with the convergent power series $\varphi \circ \lambda$, we need to produce a lower bound for the valuation of the coefficients.

Proposition 6.5.2. *Consider the $g+\rho-1$ convergent power series in $\mathbb{Q}_p\langle\nu\rangle$ given by $\varphi\circ\lambda\colon \mathbb{Z}_p \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$. For any of the first g convergent power series, the valuation of the coefficient of ν^n is at least $n-1-v_p(n)$. For any of the last $\rho-1$ power series, the valuation of the coefficient is at least $n-1-2\lfloor \mathsf{log}_p n\rfloor + v$, where v is an explicit (possibly negative) constant.*

Proof. The result about the coefficients of the first g power series follows from Corollary 6.3.22.

Let $i \in \{1,\dots,\rho-1\}$. Then [BDM+21, Lemma 4.5] states that the Nekovář height $h_{i,p}^{\mathrm{Nek}} : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ corresponding to the trace zero endomorphism f_i is analytic on residue disks. Let $c = \min\{0, \min_j d_j(\eta)\}$ for the $d_j(\eta)$ defined in [BDM+21, Section 4]. Furthermore they show that the valuation of the coefficient of ν^n is at least $n-1-2\lfloor \mathsf{log}_p n\rfloor + v'$, where $v' \coloneqq \min(\mathrm{ord}_p(\gamma_{\mathrm{Fil}}), c+c_2)$, and γ_{Fil} and c_2 are explicit constants defined in [BDM+21, Section 4], depending on f_i among other things. (The valuation of the coefficients of ν^n stated in [BDM+21, Lemma 4.5] differs by n from the value given here, because our coordinates differ from theirs by a factor of p.)

In Section 6.8 we go more into detail about this Nekovář height. In particular, in Theorem 6.8.10 together with Proposition 6.8.11 we show that $h_{i,p}^{\mathrm{Nek}}(z)$ and $h_p(z-b, A_{\alpha_i}|_{z\times X})$ differ by a factor of $-m$. It follows from Corollary 6.4.17 that we can take $v \coloneqq v' + v_p(m)$. □

Remark 6.5.3. In the example of Section 6.9, we calculate that the constant v is 0 for the residue disk of the curve we consider there. We suspect that this constant can often be taken to be 0, at least in the cases $p > 2g-1$ and $p \nmid \#J(\mathbb{F}_p)$.

We first present a general algorithm to compute the trivializing section $\varphi\circ\lambda$. For example, if $p>3$ and $v=0$, to compute $\widetilde{j_b}(P_\nu)$ in $\mathcal{N}$ modulo p, it suffices to compute $\widetilde{j_b}$ on two values, for example $\widetilde{j_b}(P_0)$ and $\widetilde{j_b}(P_1)$. Since the embedding must be linear in ν on $U(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}$, we can interpolate between these values to determine the map. In general, to compute $\varphi\circ\lambda$ to finite precision, it is enough to determine the map on $\mathbb{Z}/p^k\mathbb{Z}$-points for some large enough k. We give an algorithm to compute $\widetilde{j_b}(P)$ when P is a $\mathbb{Z}/p^k\mathbb{Z}$-point.

Algorithm 6.5.4 (The trivializing section)**.**

Input: A point $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})_{\overline{P}}$.
Output: The value $\varphi\circ\lambda(\nu)$ to finite precision.

1. *Calculate the Coleman integral* $\mathsf{log}(P_\nu - b)$.

2. *Compute* $A_{\alpha_i}|_{P_\nu \times X}$ *for each* $i = 1, \dots, (\rho - 1)$ *using Algorithm 6.4.10.*
3. *Calculate all* $h_p(P_\nu - b, A_{\alpha_i}|_{P_\nu \times X})$.
4. *For each* A_{α_i}, *compute* $c_{U,i} \coloneqq -\sum_{q|n} V_q \mathsf{log} q$ *using Algorithm 6.4.14, where* n *is the product of the primes of bad reduction for* X.
5. *Return*

$$(\varphi \circ \lambda)(\nu) = (\mathsf{log}(P_\nu - P_0), h_p(P_\nu - b, A_{\alpha_1}|_{P_\nu \times X}) + c_{U,1}, \dots, h_p(P_\nu - b, A_{\alpha_{\rho-1}}|_{P_\nu \times X}) + c_{U,\rho-1}).$$

For the rest of this section, we describe a practical algorithm to do Step 3 of Algorithm 6.5.4 in the case where X is a hyperelliptic curve of the form $y^2 = H(x)$. For hyperelliptic curves where H has odd degree, there is an algorithm to compute the local Coleman–Gross height at p of two disjoint divisors given as a sum of points [BB12, Algorithm 5.7]. Recent work [GM23] extends this algorithm to even degree models.

For any $i = 1, \dots, (\rho - 1)$ since the divisor $A_{\alpha_i}|_{P_\nu \times X}$ on $X_{\mathbb{Q}_p}$ may not split as a sum of points, we instead consider multiples of this divisor $nA_{\alpha_i}|_{P_\nu \times X}$ for $n \in \mathbb{N}$. We can hope some large enough multiple splits as a sum of points. Therefore, we must explicitly describe arithmetic in the Jacobian. For hyperelliptic curves, this process can be done via Cantor's algorithm [Can87]. The main idea is to use the Mumford representations of divisors. We use the implementation of Cantor's algorithm done by Sutherland in [Sut19, Section 3]. The only extra step is to keep track of the function that realizes the linear equivalence with a Mumford representation of the sum. Even though Sutherland works with even degree models for hyperelliptic curves, the algorithms still apply to our odd degree model hyperelliptic curves (see [Sut19, p.433]).

Remark 6.5.5. In practice, we represent divisors with ideals of polynomial rings. We can translate from a Gröbner basis of an ideal to a Mumford representation in the following way. Let Y be a hyperelliptic curve over a field k given by $y^2 = H(x)$. Let $\pi \colon Y \to \mathbb{P}^1$ be the degree two morphism forgetting y. Let D be an effective divisor on the affine chart $k[x, y]/(y^2 - H(x))$ of Y, given by a Gröbner basis. We assume that D and $\iota(D)$ are disjoint. Then we can find a Mumford representation for D by simply taking a Gröbner basis with respect to the lexicographical ordering $y \leq x$. If D and ιD are not disjoint, one can explicitly compute an effective divisor E on $\mathbb{P}^1$ such that $D - \pi^* E$ is disjoint from $\iota(D - \pi^* E)$, and hence find a Mumford representation for $D - \pi^* E$.

We can now give a practical algorithm to compute the local heights at p in Step 3 of Algorithm 6.5.4. When X is a hyperelliptic curve of the form $y^2 = H(x)$, given $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})$ we can apply Algorithm 6.4.10 to obtain $A_{\alpha_i}|_{P_\nu \times X}$ as a divisor on $X_{\mathbb{Q}_p}$.

Algorithm 6.5.6 (Local heights for the trivializing section on a hyperelliptic curve)**.**

Input: A point $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})_{\overline{P}}$ on a hyperelliptic curve $Y\colon y^2 = H(x)$ and the Mumford representation of $A_{\alpha_i}|_{P_\nu \times Y}$ as a divisor on Y.
Output: The value $h_p(P_\nu - b, A_{\alpha_i}|_{P_\nu \times Y})$ to finite precision.

1. *Set $n \coloneqq 1$.*
2. *Use Cantor's Algorithm to compute a Mumford representation (u_n, v_n) and a rational function s_n such that $\mathsf{Div}(u_n, v_n) + \mathsf{Div}s_n = nA_{\alpha_i}|_{P_\nu \times Y}$ [Can87].*
3. *Check if u_n factors completely over $\mathbb{Q}_p$ into linear factors.*
4. *If yes, set x_j to be the roots of u_n for $j = 1, \ldots, \deg(u_n)$. If no, increase n by 1 and go back to Step 2.*
5. *Set $y_j \coloneqq v_n(x_j)$.*
6. *Set $Q_j \coloneqq (x_j, y_j) \in Y(\mathbb{Q}_p)$.*
7. *Compute $h_p(P_\nu - b, \sum_{j=1}^{\deg(u_n)} Q_j - \deg(u_n)\infty)$ using [BB12, Algorithm 5.7].*
8. *Return $(1/n)(h_p(P_\nu - b, \sum_{j=1}^{\deg(u_n)} Q_j - \deg(u_n)\infty) + \mathsf{log}(s_n(P_\nu - b)))$.*

Algorithm 6.5.6 does not always terminate; we cannot guarantee that eventually $nA_{\alpha_i}|_{P_\nu \times Y}$ splits completely into a sum of points over $\mathbb{Q}_p$. In theory, we can split any divisor as a sum of points over some finite extension of $\mathbb{Q}_p$. However, working with these field extensions of $\mathbb{Q}_p$ is often currently not possible in practice.

Remark 6.5.7. Algorithm 6.5.4 and Algorithm 6.5.6 take in a point P_ν of precision k, but their output can be of smaller precision. This depends on the precision loss in the computation of the p-adic height; see [BB12, Section 6.2].

6.6 Integer points of the torsor

Next we discuss the integer points of the torsor T. We give an algorithm to construct a map $\kappa\colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$.

In practice, to give an upper bound on $\#U(\mathbb{Z})_{\overline{P}}$, we only need to compute the image of the map κ in $T(\mathbb{Z}/p^2\mathbb{Z})_{\widetilde{j_b(\overline{P})}}$, because after composing with the pseudoparametrization φ from Definition 6.3.21 the map κ is given by convergent power series. In fact, in this section we will show that by virtue of our choice of pseudoparametrization, they are given by g homogeneous linear polynomials and $\rho - 1$ quadratic polynomials.

For now we restrict to a single trace zero endomorphism f and the corresponding torsor T_f. By iterating over the linearly independent trace zero endomorphisms $f_1, \dots, f_{\rho-1}$ we recover T and κ.

Note that if the residue disk $T_f(\mathbb{Z})_{\widetilde{j_b(\overline{P})}}$ is empty, then its p-adic closure is also empty, and therefore we do not need to consider $\overline{P}$. If the disk is not empty, then we can find $\widetilde{t} \in T_f(\mathbb{Z})_{\widetilde{j_b(\overline{P})}}$ by arithmetic in the Jacobian. It is enough to consider if the corresponding residue disk $J(\mathbb{Z})_{j_b(\overline{P})}$ is empty. This is an instance of the Mordell–Weil sieve at p.

As an intermediate step, we need to compute points Q_{ij} on $\mathcal{N}$, the trivial biextension, that are the image under Ψ (defined in Definition 6.3.8) of generating sections on certain fibers of $\mathcal{M}^{\times}(\mathbb{Z})$.

We construct points on $\mathcal{N}$ that are the image of generating sections of residue disks of $\mathcal{M}^{\times,\rho-1}(\mathbb{Z})$ following the method in Example 6.3.6.

Algorithm 6.6.1 (Compute the Q_{ij})**.** *Input: $G_1, \dots, G_{r'}$ a generating set of the Mordell–Weil group of J, a trace zero endomorphism $f\colon J \to J$.*
Output: Points Q_{ij} on $\mathcal{N}$ that are the image of the generating section of

$$\mathcal{M}^{\times}(G_i, f(G_j))(\mathbb{Z})$$

and Q_{i0} that are the image of the generating section of

$$\mathcal{M}^{\times}(G_i, c)(\mathbb{Z})$$

for $1 \le i, j \le r'$.

1. *Compute $E_1, \dots, E_{r'}$ representing divisors of $G_1, \dots, G_{r'}$.*
2. *For each G_i, use Algorithm 6.4.10 to compute representing divisors $D_1, \dots, D_{r'}$ of $f(G_i)$.*
3. *Use Algorithm 6.4.7 to compute a divisor D_0 whose class is the point $c \in J(\mathbb{Z})$.*
4. *Compute the local height $h_p(E_i, D_j)$ and $h_p(E_i, D_0)$ for $1 \le i, j \le r'$.*
5. *Using [vBHM20, Section 2], compute the height $h_\ell(E_i, D_j)$ at $\ell \neq p$ and $h_\ell(E_i, D_0)$ at $\ell \neq p$ for $1 \le i, j \le r'$.*

6. *Return* $Q_{ij} \coloneqq (G_i, f(G_j), \sum_{\ell \ prime} h_\ell(E_i, D_j))$ *and* $Q_{i0} \coloneqq (G_i, c, \sum_{\ell \ prime} h_\ell(E_i, D_0))$ *for* $1 \leq i, j \leq r'$.

Let $G_1, \ldots, G_{r'}$ be a generating set for the full Mordell–Weil group, with $r' \geq r$. Let $\widetilde{G_i}$ be a basis for the kernel of reduction $J(\mathbb{Z}) \to J(\mathbb{F}_p)$ for $i = 1, \ldots, r$. (Note that the reduction map is injective when restricted to the torsion of $J(\mathbb{Z})$, so the kernel of reduction is a free $\mathbb{Z}$-module of rank r.) Write

$$\widetilde{G_i} = \sum_{j=1}^{r'} e_{ij} G_j$$

for some $e_{ij} \in \mathbb{Z}$. Let $\widetilde{G_t}$ denote the projection of $\widetilde{t} \in T(\mathbb{Z})_{\widetilde{j_b(P)}}$ to $J_{j_b(\overline{P})}$. Write

$$\widetilde{G_t} = \sum_{i=1}^{r'} e_{0i} G_i$$

for some $e_{0i} \in \mathbb{Z}$. Using the biextension group laws and the points Q_{ij} we construct a series of points in $\mathcal{M}^\times(\mathbb{Z})$ living over certain points in $J \times J$ that are the image of generating sections of the corresponding residue disks in $\mathcal{M}^\times(\mathbb{Z})$.

A formula for the points P_{ij} over $(\widetilde{G_i}, f(m\widetilde{G_j}))$ is

$$P_{ij} \coloneqq \sum_{k=1}^{r'}{}_1 \, e_{ik} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{6.6.0.1}$$

Here, $\cdot_i$ and $\sum_i$ for $i = 1, 2$ denote the biextension group laws (6.3.2.4) and (6.3.2.3).

Next $R_{i\widetilde{t}}$ live over $(\widetilde{G_i}, \alpha(\widetilde{G_t}))$ and hence

$$R_{i\widetilde{t}} \coloneqq \sum_{k=1}^{r'}{}_1 \, e_{ik} \cdot_1 \left(m \cdot_2 Q_{k0} +_2 \sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{0\ell} \cdot_2 Q_{k\ell} \right). \tag{6.6.0.2}$$

Finally, $S_{\widetilde{t}j}$ live over $(\widetilde{G_t}, f(m\widetilde{G_j}))$ and so

$$S_{\widetilde{t}j} \coloneqq \sum_{k=1}^{r'}{}_1 \, e_{0k} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{6.6.0.3}$$

Remark 6.6.2. In $\mathcal{M}^\times(\mathbb{Z})$, these points are all unique up to sign. Since we are recording the image in $\mathcal{N}$, this sign does not matter.

For $n = (n_1, \dots, n_r) \in \mathbb{Z}^r$ we can now construct the points $A_{\widetilde{t}}(n)$, $B_{\widetilde{t}}(n)$, $C(n)$, and $D_{\widetilde{t}}(n)$ in $T(\mathbb{Z})$ given by [EL21, (4.2)-(4.4)]. The key property of this construction is that $D_{\widetilde{t}}(n)$ lies above the point $\widetilde{G_t} + \sum_i n_i \widetilde{G_i} \in J(\mathbb{Z})_{\widetilde{j_b(P)}}$. Furthermore, by [EL21, (4.6)-(4.9)], we have that $D_{\widetilde{t}}((p-1)n)$ is in the residue disk $T_f(\mathbb{Z})_{\widetilde{j_b(P)}}$, allowing us to explicitly construct the map

$$\kappa_{f,\mathbb{Z}} \colon \mathbb{Z}^r \to T_f(\mathbb{Z})_{\widetilde{j_b(P)}}, \qquad (n_1, \dots, n_r) \mapsto D_{\widetilde{t}}((p-1)n_1, \dots, (p-1)n_r), \tag{6.6.0.4}$$

Finally, by [EL21, Theorem 4.10], the map $\kappa_{f,\mathbb{Z}}$ extends uniquely to a continuous map

$$\kappa_f \colon \mathbb{Z}_p^r \to T_f(\mathbb{Z}_p)_{\widetilde{j_b(P)}}. \tag{6.6.0.5}$$

The image of κ_f is $\overline{T_f(\mathbb{Z})}_{\widetilde{j_b(P)}}$.

By iterating over the basis $f_1, \dots, f_{\rho-1}$ of trace zero endomorphisms, we obtain the map

$$\kappa_{\mathbb{Z}} \colon \mathbb{Z}^r \to T(\mathbb{Z}_p)_{\widetilde{j_b(P)}} \tag{6.6.0.6}$$

and its unique extension to a continuous map

$$\kappa \colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j_b(P)}}. \tag{6.6.0.7}$$

The map κ has image $\overline{T(\mathbb{Z})}_{\widetilde{j_b(P)}}$.

Recall the pseudoparametrization $\varphi \colon T(\mathbb{Z}_p)_{\widetilde{j_b(P)}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ from Definition 6.3.21.

Proposition 6.6.3. *The map $\varphi \circ \kappa \colon \mathbb{Z}_p^r \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by g homogeneous linear polynomials and $\rho - 1$ polynomials of degree at most 2.*

Proof. It is enough to show this for $\kappa_{\mathbb{Z}}$, since $\varphi \circ \kappa$ is continuous.

We make the identification $J(\mathbb{Z})_{\widetilde{j_b(P)}} = D_0 + J(\mathbb{Z})_0 \simeq D_0 + \mathbb{Z}^r \simeq \mathbb{Z}^r$ where $D_0 \in J(\mathbb{Z})_{\widetilde{j_b(P)}}$. Under this bijection, the map $\varphi \circ \kappa_{\mathbb{Z}} \colon J(\mathbb{Z})_{\widetilde{j_b(P)}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by

$$D \mapsto \mathsf{log}(D - D_0),$$

on the first g components. Since log is a group homomorphism, it follows the first g polynomials are homogeneous linear as desired.

Now we fix one of the $\rho-1$ trace zero endomorphisms $f\colon J \to J$. Let $\pi_f\colon \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1} \to \mathbb{Q}_p$ be the projection onto the coefficient corresponding to f. Consider the map $\tau \coloneqq \pi_f \circ \varphi \circ \kappa_{\mathbb{Z}}$. We write F for the affine linear map

$$\mathbb{Z}^r \simeq J(\mathbb{Z})_{j_b(\overline{P})} \xrightarrow{f} J(\mathbb{Z})_{\alpha(j_b(\overline{P}))} \simeq \mathbb{Z}^r$$

where we identify $J(\mathbb{Z})_{\alpha(j_b(\overline{P}))}$ with $\mathbb{Z}^r$ by subtracting $\alpha(D_0)$ and use $J(\mathbb{Z})_0 \simeq \mathbb{Z}^r$.

By [EL21, (4.2)-(4.4)] we have that $\tau(n_1, \dots, n_r)$ is a sum of a constant term, a linear function in the integers $n_1, \dots, n_r$, a linear function in Fn and a bilinear form evaluated in (n, Fn). Since F is linear, in total, this gives a function of degree at most 2 in n. □

6.7 The geometric quadratic Chabauty algorithm

In this section, we present the main algorithm of this paper for doing geometric quadratic Chabauty. This algorithm ties together the results of the previous sections.

Algorithm 6.7.1 (Geometric quadratic Chabauty in a single disk)**.**

Input:

- $X_{\mathbb{Q}}/\mathbb{Q}$ *a smooth, projective, geometrically irreducible curve over* $\mathbb{Q}$ *such that* $X_{\mathbb{Q}}(\mathbb{Q}) \neq \varnothing$ *with a regular model* X *of genus* g *and Mordell–Weil rank* r*, and with Jacobian of Néron–Severi rank* $\rho > 1$*, such that* $r < g + \rho - 1$*;*
- $\rho - 1$ *nontrivial independent trace zero endomorphisms represented by* $(g \times g)$*-matrices giving the action on the sheaf of differentials with respect to a fixed basis;*
- *an open set* $U \subset X^{\mathrm{sm}}$ *containing the smooth points of one geometrically irreducible component of* $X_{\mathbb{F}_q}$ *for all primes* q*;*
- *a prime* $p > 2$ *of good reduction for* X*;*
- *a precision* $k \in \mathbb{N}$*;*
- *a base point* $b \in X(\mathbb{Z})$*;*

- *a point* $\overline{P} \in U(\mathbb{F}_p)$*;*
- *a generating set* $G_1, \dots, G_{r'}$ *of the Mordell–Weil group of* J*.*

Output: $g + \rho - 2$ *integral convergent power series in* $\mathbb{Z}_p\langle z_1, \dots, z_r\rangle$ *up to precision* k*, defining* $\widetilde{j_b}(U(\mathbb{Z}_p)_{\overline{P}}) \cap \overline{T(\mathbb{Z})}$ *inside* $\overline{T(\mathbb{Z})}$*.*

For each of the given trace zero endomorphisms f *do Steps 2 through 5.*

1. *For each of the given trace zero endomorphisms* f *do the following.*
   (a) *Compute the correspondence* A_α *that induces the endomorphism* $m \cdot \circ f\colon J \to J$ *as given in Lemma 6.4.4.*
   (b) *Find the divisor representing* $c = [(\mathcal{L}_\alpha)_{b\times X}] \in J(\mathbb{Z})$ *using Algorithm 6.4.7.*
   (c) *Choose a local parameter* ν *to parametrize* $U(\mathbb{Z}_p)_{\overline{P}}$ *as* $\nu \mapsto P_\nu$*. By Proposition 6.5.2 the map* $\nu \mapsto \varphi \circ \lambda(\nu)$ *is modulo* p^k *given by a polynomial with bounded degree. By calculating enough values, interpolate to find the polynomial expression. In particular, when* $v = 0$ *and* $p > 3$*, for* $k = 1$*, the degree bound is* 1*. In this case, compute* $\varphi \circ \lambda(0), \varphi \circ \lambda(1)$ *and interpolate the resulting line.*
   (d) *With the generating set* $G_1, \dots, G_{r'}$*, use Algorithm 6.6.1 to compute points* $Q_{ij}, Q_{i0} \in \mathcal{N}$ *up to precision* k *that are the images of the generating sections of* $\mathcal{M}^\times(G_i, f(G_j))(\mathbb{Z})$ *and* $\mathcal{M}^\times(G_i, c)(\mathbb{Z})$ *for* $1 \le i, j \le r'$*.*
   (e) *Using the elements* Q_{ij}*, find the map* $\kappa_{f,\mathbb{Z}}\colon \mathbb{Z}^r \to T_f(\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$ *as in (6.6.0.4) and extend it to the map* $\kappa_f\colon \mathbb{Z}_p^r \to T_f(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$*.*
2. *Using the* κ_f *for* $f = f_1, \dots, f_{\rho-1}$ *constructed in Step 1e, construct* κ *as in (6.6.0.7).*
3. *Compose with the pseudoparametrization* φ *to compute the* g *homogeneous linear and* $\rho - 1$ *quadratic polynomials describing* $\varphi \circ \kappa\colon \mathbb{Z}_p^r \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$*, as guaranteed by Proposition 6.6.3, up to precision* k*.*
4. *Use Hensel lifting to compute the power series* $g_1, \dots, g_{g+\rho-2}$ *defined in Proposition 6.5.1 that cut out* $\operatorname{im}(\varphi \circ \lambda)$*, up to precision* k*.*
5. *Return* $g_i \circ (\varphi \circ \kappa)$ *for* $i = 1, \dots, g + \rho - 2$*.*

By iterating this over all simple opens U_i such that $(U_i(\mathbb{Z}))_{i\in I}$ covers $X(\mathbb{Z})$ (as in Section 6.2), and also iterating over all $\mathbb{F}_p$-points of U_i, we obtain multivariate power series up to precision k cutting out $X(\mathbb{Z}_p)_{\mathrm{Geo}}$.

Remark 6.7.2. By [EL21, Section 9.2], the power series in the output of Algorithm 6.7.1 have at most finitely many zeros in $\mathbb{Z}_p$. In practice, one can solve these power series up to enough precision by using a multivariate Hensel's lemma [Kuh11, Theorem 25]. This assumes that the Jacobian matrix of the sequence of power series is invertible over $\mathbb{Q}_p$. We expect this to always happen unless there is a geometric obstruction.

Often solving these power series modulo p is enough to determine $X(\mathbb{Z}_p)_{\mathrm{Geo}}$. See for example [EL21, Theorem 4.12], which we use in Section 6.9. Even if computations modulo p are not enough, one can increase the precision by considering the residue disks $U(\mathbb{Z}_p)_{\overline{P}}$, where $\overline{P} \in U(\mathbb{Z}/p^k\mathbb{Z})$ for some integer k. An example of the geometric Chabauty method with higher precision is given in Remark 6.9.9.

Remark 6.7.3. In practice, to run Algorithm 6.7.1 we need to be able to compute Coleman–Gross heights on the curve X. Currently, this has only been made algorithmic for hyperelliptic curves.

6.8 The comparison theorem

In this section we give a comparison theorem between the geometric method and cohomological quadratic Chabauty [BD18, BD21, BDM$^+$19, BDM$^+$21]. In Theorem 6.8.5, we show that the geometric method produces a refined set of points, as is the case for classical Chabauty–Coleman [HS22a].

For this section we assume that p is a prime of good reduction, that $r = g$, that $\rho > 1$, and further, that $\overline{J(\mathbb{Z})}$ has finite index in $J(\mathbb{Z}_p)$. The cohomological quadratic Chabauty set in [BD18] is defined under these assumptions. We do not require a semistable model for $X/\mathbb{Q}_q$, $q|n$ as is sometimes assumed; a semistable model can make explicit calculations of heights away from p easier, see [BD20] or [BDM$^+$21, Section 3.1]. By [Bet21, Lemma 6.1.1] the local heights away from p factor through the component set of the minimal regular model.

Let $Z_1, \dots, Z_{\rho-1}$ be a basis for $\ker(\mathrm{NS}(J) \to \mathrm{NS}(X))$. In the cohomological method, from the transpose $Z_i^\top$ of such a correspondence[1] we can construct a quadratic Chabauty function $\sigma_i \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ and a finite subset $\Omega_i \subset \mathbb{Q}_p$ described explicitly in terms of local heights at primes of bad reduction such

[1] Due to a difference of conventions of rigidifications for line bundles on $X \times X$, we have to take the transpose of Z_i for the methods to align perfectly. The transpose $Z_i^\top$ induces the same endomorphism of the Jacobian.

that $\sigma_i(z) \in \Omega_i$ for all $z \in X(\mathbb{Q})$. This finite subset Ω_i consists of one constant $c_{U,i}$ for every simple open U.

We describe the construction of σ_i and the set Ω_i in more detail after we present the main theorem. The divisor Z_i is the correspondence of a trace zero endomorphism $f_i \colon J \to J$ of the Jacobian. In the geometric method, we work with the endomorphism $\alpha_i \coloneqq m \cdot \circ \operatorname{tr}_{c_i} \circ f_i$. This multiplication with m will result in all the heights in the trivial biextension $\mathcal{N}$ to be a factor m larger than in the cohomological case.

Definition 6.8.1. Define $X(\mathbb{Q}_p)_{\mathrm{Coh}} \coloneqq \bigcup_U \{x \in X(\mathbb{Q}_p) \mid \sigma_i(x) = c_{U,i}, \text{ for } i = 1, \dots, \rho - 1\}$ where the union is over all simple opens U.

Remark 6.8.2. As far as we know, the existing literature does not explicitly define the quadratic Chabauty set in the case of multiple endomorphisms. In the case where one uses a single trace zero endomorphism, the set is defined in [BD18, Theorem 1.2]. One can see Definition 6.8.1 as a special case of the finite set implicitly defined in [Bet21, Theorem A], for the quotient of the fundamental group that is an extension of the abelianization by $\mathbb{Q}_p(1)^{\rho-1}$.

The alternative definition is $\bigcap_i \bigcup_U \{x \in X(\mathbb{Q}_p) \mid \sigma_i(x) = c_{U,i}\}$. Here the union and the intersection have been switched, and hence the resulting set can be bigger. The difference between the two sets consists exactly of points $x \in X(\mathbb{Q}_p)$ such that $\sigma_i(x) \in \Omega_i$ for every i, but such that there is no U with $\sigma_i(x) = c_{U,i}$ for every i. In particular, the points in the difference do not lie in any of the simple opens U, and hence are not rational points.

Recall the definition of $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ from Definition 6.2.3. Given a covering of $X(\mathbb{Z})$ by simple opens U we have that

$$X(\mathbb{Z}_p)_{\mathrm{Geo}} \coloneqq \bigcup_U \widetilde{j_b}^*(\widetilde{j_b}(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}) \subset \bigcup_U U(\mathbb{Z}_p) = X(\mathbb{Z}_p).$$

The following definitions give terminology for two of the cases where $X(\mathbb{Q}_p)_{\mathrm{Coh}}$ is strictly bigger than $X(\mathbb{Z}_p)_{\mathrm{Geo}}$.

Definition 6.8.3. We say that the Mordell–Weil group is *of good reduction* (modulo p) if the map $\overline{J(\mathbb{Z})}_0/p\overline{J(\mathbb{Z})}_0 \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ is injective. Otherwise, we say that it is *of bad reduction.*

The Mordell–Weil group being of good reduction is equivalent to the map $\overline{J(\mathbb{Z})}_0 \to J(\mathbb{Z}_p)_0$ being an isomorphism. On the level of abstract groups, this map is always an embedding $\mathbb{Z}_p^g \to \mathbb{Z}_p^g$ with image of index some power of p. Another equivalent way of stating this is that the *p-saturation of $\overline{J(\mathbb{Z})}_0$ in*

$J(\mathbb{Z}_p)_0$

$$\{x \in J(\mathbb{Z}_p)_0 \mid \exists k, p^k x \in \overline{J(\mathbb{Z})}_0\}$$

is always equal to $J(\mathbb{Z}_p)_0$, and the Mordell–Weil group is of bad reduction if and only if this p-saturation is bigger than $\overline{J(\mathbb{Z})}_0$.

Definition 6.8.4. For $Q \in X(\mathbb{F}_p)$, if $j_b(Q)$ is not in the image of the reduction map $J(\mathbb{Z}) \to J(\mathbb{F}_p)$, then we say Q *fails the Mordell–Weil sieve* (at p). In this case, the residue disk $X(\mathbb{Z}_p)_Q$ cannot contain a rational point. Otherwise, Q *passes the Mordell–Weil sieve* (at p).

Our main theorem is the following comparison theorem.

Theorem 6.8.5. *There is an inclusion $X(\mathbb{Q}) \subseteq X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}}$. For $P \in X(\mathbb{Q}_p)_{\mathrm{Coh}}$ we have $P \notin X(\mathbb{Z}_p)_{\mathrm{Geo}}$ if and only if one of the following conditions holds:*

1. *P fails the Mordell–Weil sieve at p;*
2. *the Mordell–Weil group is of bad reduction at p and $j_b(P)$ does not lie in the p-adic closure of the Mordell–Weil group, but only in its p-saturation.*

Remark 6.8.6. It follows immediately from the proof of Theorem 6.8.5 that the inclusion $X(\mathbb{Q}) \subseteq X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}}$ and comparison from Theorem 6.8.5 also hold when the sets $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ and $X(\mathbb{Q}_p)_{\mathrm{Coh}}$ are constructed using a fixed subset $Z_{i_1}, \ldots, Z_{i_k}$ of $1 \leq k < \rho - 1$ independent elements of $\ker(\mathrm{NS}(J) \to \mathrm{NS}(X))$, instead of a full basis.

Remark 6.8.7. In [HS22a], an analogous theorem is given for the comparison between the classical Chabauty–Coleman method, as in [Col85b, BBK10], and the geometric linear Chabauty, as developed in [Spe20] and [HS22a]. The comparison theorem [HS22a, Theorem 5.1] (Theorem 5.5.1) shows that the set of candidates found by the classical Chabauty–Coleman method contains the set found by geometric linear Chabauty method. Furthermore, the two sets differ by conditions analogous to conditions 1 and 2.

Let $1 \leq i \leq \rho(J) - 1$. We briefly recall the constructions of σ_i and Ω_i from [BDM$^+$21]. For more details, the reader can also consult [BD18, BDM$^+$19]. The cohomological method for quadratic Chabauty uses Nekovář's theory [Nek93] of p-adic heights of certain Galois representations to construct a global height $h_i^{\mathrm{Nek}} \colon X(\mathbb{Q}) \to \mathbb{Q}_p$ by attaching a family of Galois representations to $X(\mathbb{Q})$ and $X(\mathbb{Q}_p)$. The Galois representation depends on the choice of base point b as well as the correspondence Z_i. We suppress this dependence on b in our notation. The global height also depends on a choice of splitting of the Hodge filtration and idèle class character, which we choose to be compatible

with the choices made to construct the Coleman–Gross height h. In particular we choose the cyclotomic character. This global height h_i^{Nek} factors through $h^{\mathrm{Nek}}\colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$ [BDM+21, Section 2.3]. We can thus extend h^{Nek} on $J(\mathbb{Q}) \times J(\mathbb{Q})$ to a bilinear function on $J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \to \mathbb{Q}_p$ and evaluate it on elements of $X(\mathbb{Q}_p)$.

This global height decomposes as a sum of local heights over finite places

$$h_i^{\mathrm{Nek}} = \sum_v h_{i,v}^{\mathrm{Nek}}$$

where $h_{i,v}^{\mathrm{Nek}}\colon X(\mathbb{Q}_v) \to \mathbb{Q}_p$. Define the quadratic Chabauty function

$$\sigma_i(z) \coloneqq h_i^{\mathrm{Nek}}(z) - h_{i,p}^{\mathrm{Nek}}(z)$$

for $z \in X(\mathbb{Q}_p)$, recalling that the right hand side implicitly depends on Z_i. Then, for any $z \in X(\mathbb{Q})$, using the decomposition above we can write $h_i^{\mathrm{Nek}}(z) = h_{i,p}^{\mathrm{Nek}}(z) + \sum_{q \neq p} h_{i,q}^{\mathrm{Nek}}(z)$. The set $\Omega_i \subset \mathbb{Q}_p$ is defined by the local heights in the following way. Let

$$\Omega_{i,q} \coloneqq \{h_{i,q}^{\mathrm{Nek}}(z) \mid z \in X(\mathbb{Q}_q)\}.$$

If $X_{\mathbb{F}_q}$ is geometrically irreducible, then $\Omega_{i,q} = \{0\}$. We can therefore define the finite set

$$\Omega_i \coloneqq \{\sum_q w_q \mid w_q \in \Omega_{i,q}\}, \tag{6.8.0.1}$$

Hence, when $z \in X(\mathbb{Q})$, we have $\sigma_i(z) \in \Omega_i$ and so $X(\mathbb{Q}_p)_{\mathrm{Coh}} \supseteq X(\mathbb{Q})$.

Remark 6.8.8. The function $\sigma_i(z)$ is locally analytic [BDM+21, pp. 6, 10]. If X has sufficiently many rational points, then one can explicitly express the function $\sigma_i(z)$ as a power series in every residue disk, and for each $c \in \Omega_i$ and each residue disk of $X(\mathbb{Q}_p)$ find the roots of $\sigma_i(z) - c$ to explicitly solve for elements of $X(\mathbb{Q}_p)_{\mathrm{Coh}}$.

The following theorem relates the local height of the Galois representation associated to a point $P \in X(\mathbb{Q}_p)$ to a pairing with a divisor that is studied in [DRS12].

Definition 6.8.9. Let $z \neq b$ be a point in $X(\mathbb{Q}_p)$. Define $D_{Z_i^\top}(z, b)$ to be the degree zero divisor on X given by $D_{Z_i^\top}(z, b) \coloneqq Z_i|_\Delta - Z_i|_{X \times b} - Z_i|_{z \times X}$.

Theorem 6.8.10. *[BD18, Theorem 6.3] Let q be a prime and let $z \neq b$ be a point in $X(\mathbb{Q}_p)$. We have the equality of local heights $h_{i,q}^{\mathrm{Nek}}(z) = h_q(z - b, D_{Z_i^\top}(z, b))$ and moreover*

$$h_i^{\mathrm{Nek}}(z) = h(z - b, D_{Z_i^\top}(z, b))$$

where h is the Coleman–Gross height.

Proposition 6.8.11. *Let $z \in X(\mathbb{Z}_p)$ be such that $z \neq b$. We have*

$$-mD_{Z_i^\top}(z, b) = A_{\alpha_i}|_{z \times X}$$

and

$$-m[D_{Z_i^\top}(z, b)] = [\alpha_i(z - b)].$$

Proof. Write $B = Z_i|_{X \times b}$ and $C = Z_i|_{\Delta}$. Then

$$D_{Z_i^\top}(z, b) = C - B - Z_i|_{z \times X}.$$

Define $A = Z_i - B \times X + X \times B - X \times C$. Then we see $A|_{z \times X} = Z_i|_{z \times X} + B - C = -D_{Z_i^\top}(z, b)$. Then by Lemma 6.4.4, mA is equal to A_{α_i} and the proposition follows. □

Definition 6.8.12. Define $\rho_{\mathcal{N}} \colon \mathcal{N} \to \mathbb{Q}_p$ by $(D_1, D_2, x) \mapsto h(D_1, D_2) - x$.

Note that $\rho_{\mathcal{N}}$ does not depend on Z_i.

Lemma 6.8.13. *The function $\rho_{\mathcal{N}}$ vanishes on the image $\Psi(\mathcal{M}^\times(\mathbb{Z}))$ in $\mathcal{N}$, and in particular, on $\Psi(T_i(\mathbb{Z}))$.*

Proof. This follows from Proposition 6.3.11. □

In order to characterize the difference between $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ and $X(\mathbb{Q}_p)_{\mathrm{Coh}}$, we will use the following lemma.

Lemma 6.8.14. *The difference $Z(\rho_{\mathcal{N}}) \setminus \Psi(\overline{\mathcal{M}^\times(\mathbb{Z})})$ consists of all the points (D, E, x) with $D, E \in J(\mathbb{Z}_p)$ such that*

1. *D or E fail the Mordell–Weil sieve, or;*
2. *the Mordell–Weil group is of bad reduction, and at least one of D or E does not lie in the p-adic closure $\overline{J(\mathbb{Z})}$ of the Mordell–Weil group, and only lies in its p-saturation.*

Proof. Note that $Z(\rho_{\mathcal{N}})$ is in bijection with $J(\mathbb{Z}_p)\times J(\mathbb{Z}_p)$. In contrast, the set $\Psi(\mathcal{M}^{\times}(\mathbb{Z}))$ is in bijection with $J(\mathbb{Z})\times J(\mathbb{Z})$. By assumption, $\overline{J(\mathbb{Z})}_0 \subset J(\mathbb{Z}_p)_0$ is a finite index $\mathbb{Z}_p$-sub-module, and therefore has p-saturation $J(\mathbb{Z}_p)_0$. Hence $J(\mathbb{Z}_p)\backslash\overline{J(\mathbb{Z})}$ consists exactly of points failing the Mordell–Weil sieve and points that only lie in the p-saturation of $\overline{J(\mathbb{Z})}$ and not in $\overline{J(\mathbb{Z})}$ itself. This can only happen if $\overline{J(\mathbb{Z})_0}$ is a proper subgroup of $J(\mathbb{Z}_p)_0 \simeq \mathbb{Z}_p^g$. A finite index $\mathbb{Z}_p$-submodule $G \subset \mathbb{Z}_p^g$ is a proper subgroup if and only if after tensoring with $\mathbb{F}_p$ the induced map $G/pG \to \mathbb{F}_p^g$ is not an isomorphism. This is equivalent to $G/pG \to \mathbb{F}_p^g$ not being injective. So the second condition can only happen if the Mordell–Weil group is of bad reduction. □

Definition 6.8.15. Let $U \subset X^{\mathrm{sm}}$ be a simple open set of X^{sm}. Define $c_{U,i} \in \Omega_i \subset \mathbb{Q}_p$ to be $\sum_{q\neq p} h_q(z_q - b, D_{Z_i^{\top}}(z_q, b))$ for any $z_q \in U(\mathbb{Z}_q)$ with $z_q \neq b$.

Remark 6.8.16. By Lemma 6.4.13, this is well defined and by this lemma as well as Proposition 6.8.11 we have that $mc_{U,i}$ is equal to $\sum_q V_q \mathsf{log} q$, with V_q as defined in Definition 6.4.12. Hence by (6.4.0.3) we have that $\psi \circ \widetilde{j_b}\colon U(\mathbb{Z}_p) \to \mathbb{Q}_p$ is given by $z \mapsto h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i}$ and $(\Psi \circ \widetilde{j_b})(z) = (z-b, A_\alpha|_{z\times X}, h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i})$.

Lemma 6.8.17. *The function $-m(\sigma_i(z) - c_{U,i})$ is the pullback along*

$$\Psi \circ \widetilde{j_b}|_U\colon U(\mathbb{Z}_p) \to \mathcal{N}$$

of $\rho_{\mathcal{N}}$.

Proof. Let $z \in U(\mathbb{Z}_p) \subset X(\mathbb{Z}_p)$ with $z \neq b$. By Theorem 6.8.10 and Proposition 6.8.11 we have that

$$-mh_{i,q}^{\mathrm{Nek}}(z) = -mh_q(z-b, D_{Z_i^{\top}}(z,b)) = h_q(z-b, A_\alpha|_{z\times X}).$$

By Lemma 6.4.13,

$$h_q(z-b, A_\alpha|_{z\times X}) = -V_q \mathsf{log} q$$

.

Then

$$\begin{aligned} &-m(\sigma_i(z) - c_{U,i}) = -m(h^{\mathrm{Nek}}(z) - h_p^{\mathrm{Nek}}(z) - c_{U,i}) \\ &= h(z-b, A_\alpha|_{z\times X}) - h_p(z-b, A_\alpha|_{z\times X}) + mc_{U,i}. \end{aligned}$$

This is equal to

$$h(z-b, A_\alpha|_{z\times X}) - (h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i}) =$$
$$\rho_{\mathcal{N}}((z-b, A_\alpha|_{z\times X}, h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i})) = \rho_{\mathcal{N}}(\widetilde{j_b}(z)).$$

This last equality follows from Corollary 6.4.17. □

Proof of Theorem 6.8.5. Let $c \in \Omega_i$, and consider the function $\sigma_i - c$. By (6.8.0.1), Theorem 6.8.10, and Definition 6.8.15 there is a simple open $U \subset X$ such that $c = c_{U,i}$.

Let $\widetilde{j_{b,U,i}}$ denote the map $U \to T_i$. According to Lemma 6.8.17 we have that $-m(\sigma_i - c)\colon U(\mathbb{Z}_p) \to \mathbb{Q}_p$ is the composite

$$U(\mathbb{Z}_p) \xrightarrow{\widetilde{j_{b,U,i}}} T_i(\mathbb{Z}_p) \to \mathcal{M}^\times(\mathbb{Z}_p) \xrightarrow{\Psi} \mathcal{N} \xrightarrow{\rho_{\mathcal{N}}} \mathbb{Q}_p, \tag{6.8.0.2}$$

where $T_i(\mathbb{Z}_p) \to \mathcal{M}^\times(\mathbb{Z}_p)$ is the natural injective map. Define $g_{U,i} \coloneqq -m(\sigma_i - c)$. Note that the first three maps in (6.8.0.2) are injections.

With this formulation we have

$$X(\mathbb{Q}_p)_{\mathrm{Coh}} = \bigcup_U \bigcap_i Z(g_{U,i}).$$

Similarly, we can write

$$X(\mathbb{Z}_p)_{\mathrm{Geo}} = \bigcup_U \bigcap_i \widetilde{j_{b,U,i}}^*(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})}).$$

By Lemma 6.8.13, the set $Z(g_{U,i})$ contains

$$\widetilde{j_{b,U,i}}^*(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})}).$$

Therefore, we get the containment $X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}}$.

By Lemma 6.8.14 for fixed U, i the difference

$$Z(g_{U,i}) \setminus \widetilde{j_{b,U,i}}^*(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})})$$

consists exactly of points P that fail the Mordell–Weil sieve and points P such that $j_b(P)$ lies not in $\overline{J(\mathbb{Z})}$ but only in its p-saturation. We see that an element of $X(\mathbb{Q}_p)_{\mathrm{Coh}} \setminus X(\mathbb{Z}_p)_{\mathrm{Geo}}$ satisfies condition Item 1 or condition Item 2 of Theorem 6.8.5.

On the other hand, if $P \in X(\mathbb{Q}_p)_{\mathrm{Coh}}$ fails the Mordell–Weil sieve or $j_b(P) \notin \overline{J(\mathbb{Z})}$, then $P \notin X(\mathbb{Z}_p)_{\mathrm{Geo}}$. The theorem follows. □

6.9 Example

We give an example of the implementation on the modular curve $X_0(67)^+$ of the algorithms presented. The rational points on this curve have already been determined [BBB+21] using quadratic Chabauty and a Mordell–Weil sieve, but we can also use the methods presented here to show the following proposition about the rational points of the curve in one residue disk. `Magma` code that can be used to verify the computations here can be found in [DRHS]. Let X be a regular model for $X_0(67)^+$ over the integers given by the homogenization of $y^2 + (x^3 + x + 1)y = x^5 - x$ in the weighted projective plane $\mathbb{P}^2_{(1,3,1)}$. Then $X(\mathbb{Q}) = X(\mathbb{Z})$ and we show the following.

Theorem 6.9.1. *The integer points of $X(\mathbb{Z})$ that do not reduce to $(1, 4) \in X(\mathbb{F}_7)$ are contained in the set*

$$\{[0 : -1 : 1], [4 \cdot 7 + O(7^2) : 6 + 6 \cdot 7 + O(7^2) : 1], [0 : 0 : 1],$$
$$[4 \cdot 7 + O(7^2) : 3 \cdot 7 + O(7^2) : 1], [1 : 0 : 1], [1 + 2 \cdot 7 + O(7^2) : 5 \cdot 7 + O(7^2) : 1],$$
$$[1 : -3 : 1], [1 + 2 \cdot 7 + O(7^2) : 4 + O(7^2) : 1], [1 : -1 : 0],$$
$$[1 : 6 + 3 \cdot 7 + O(7^2) : 3 \cdot 7 + O(7^2)], [1 : 0 : 0], [1 : 4 \cdot 7 + O(7^2) : 4 \cdot 7 + O(7^2)]\}.$$

Remark 6.9.2. The residue disk above $(1, 4) \in X(\mathbb{F}_7)$ has at least two integer points, $[1 : -3 : 2]$ and $[1 : -10 : 2]$. Using geometric quadratic Chabauty modulo p^2, we cannot bound the size of this residue disk. After doing the necessary calculations, it turns out $\operatorname{im} \widetilde{j_b}(z) = \operatorname{im} \kappa(0, n_2)$. In this case, applying [EL21, Theorem 4.12], since the ring $\mathbb{F}_p[n_1, n_2]/(\overline{g_1}, \overline{g_2}) \simeq \mathbb{F}_p[n_2]$ is not finite, we cannot determine the solutions using calculations modulo p^2.

By increasing precision we are guaranteed a finite set of solutions in this residue disk. In practice, this requires computing heights of points that lie in residue disks at infinity which is not possible using current implementations of Coleman–Gross heights.

We present the computations in a single residue disk over $\overline{P} = (0, -1) \in X(\mathbb{F}_7)$ where we show the following.

Proposition 6.9.3. *The integer points of $X(\mathbb{Z})$ reducing to $(0, -1) \in X(\mathbb{F}_7)$ are contained in the set*

$$\{(0, -1), (4 \cdot 7 + O(7^2), 6 + O(7^2))\}.$$

We first list some facts about this curve that will be useful in our computations.

The curve X is a projective curve of genus 2 with Jacobian J. We recall some details about X and its Jacobian that are presented in [BBB+21, Section 6]. The Jacobian J has Mordell–Weil rank 2 and $J_{\mathbb{Q}}$ has Néron–Severi rank 2. In addition, the only prime of bad reduction of X is 67. At 67, the special fiber is geometrically irreducible: it has one component with two nodes defined over $\mathbb{F}_{67^2}$. Hence, there are only geometrically irreducible fibers over every prime.

Remark 6.9.4. For this example curve, all of the fibers are geometrically irreducible, leading to a simplification in the notation used in the example compared to the notation in the preceding sections. In general, one needs to consider a distinction between J and J^0, where J^0 is the fiberwise connected component of 0 in J. We also omit the constant m which is the least common multiple of the exponents of all $J/J^0(\overline{\mathbb{F}}_p)$, with p ranging over all primes. Since $J = J^0$, we have $m = 1$. Let X^{sm} denote the open subscheme of X consisting of points at which X is smooth over $\mathbb{Z}$. Above, we consider the simple open subschemes U of X^{sm}. In this example, there is only one simple open to consider: the scheme X^{sm} obtained by removing the two Galois conjugate nodes in the fiber over 67. Since X is regular, $X^{\mathrm{sm}}(\mathbb{Z}) = X(\mathbb{Z})$.

Let ι be the hyperelliptic involution of X. We list some rational points on the curve that will be used in our computations:

$$\begin{aligned} P &\coloneqq [0:-1:1], & \iota P &\coloneqq [0:0:1], \\ Q &\coloneqq [-1:0:1], & \iota Q &\coloneqq [-1:1:1], \\ b &\coloneqq [1:0:1], & \iota b &\coloneqq [1:-3:1], \\ R &\coloneqq [1:-3:2], & \iota R &\coloneqq [1:-10:2], \\ \infty_+ &\coloneqq [1:0:0], & \infty_- &\coloneqq [1:-1:0]. \end{aligned} \tag{6.9.0.1}$$

These points turn out to be the only rational points on X, as proven in [BBB+21, Theorem 6.3] by a combination of quadratic Chabauty and the Mordell–Weil sieve.

Let $p = 7$. We first perform some local computations. There are 9 points on $X(\mathbb{F}_p)$. For each $\mathbb{F}_p$-point x of X^{sm}, we need an element in $T(\mathbb{Z})_{\widetilde{j_b(x)}}$, or equivalently an element in $J(\mathbb{Z})_{j_b(x)}$. Every residue disk of $X(\mathbb{Z}_p)$ contains an integer point; only R and ιR reduce to the same point. Therefore, none of the residue disks $J(\mathbb{Z})_{j_b(x)}$ are empty. So we cannot rule out any residue disks of the torsor immediately; in fact, this calculation is a Mordell–Weil sieve at p, see [HS22a, Section 3.4] for more details.

This example presents the specific case of the residue disk corresponding to $X(\mathbb{Z})_{\overline{P}}$, where P is the point defined in (6.9.0.1). Because we can consider

residue disks up to the hyperelliptic involution, this also gives us the analogous result for the residue disk corresponding to ιP.

Let $j_b\colon X^{\mathrm{sm}} \to J$ denote the Abel–Jacobi map with base point b defined in (6.9.0.1). We also have a set of generators for the Mordell–Weil group $J(\mathbb{Z})$ from the LMFDB,

$$\begin{aligned} G_1 &\coloneqq [P - \iota P], \\ G_2 &\coloneqq [P + Q - 2 \cdot \iota P]. \end{aligned} \tag{6.9.0.2}$$

Since X is a modular curve, its Jacobian has an action by the Hecke algebra. To describe the Hecke action on J explicitly, we fix the following basis for $H^0(X_{\mathbb{Q}}, \Omega^1_{X_{\mathbb{Q}}})$:

$$\left\{ \frac{dx}{2y - x^3 - x - 1}, \ \frac{x dx}{2y - x^3 - x - 1} \right\}. \tag{6.9.0.3}$$

We focus on the endomorphism given by the action of the Hecke operator T_2 on 1-forms of X. The Kodaira–Spencer map gives an isomorphism between $H^0(X_{\mathbb{Q}}, \Omega^1_{X_{\mathbb{Q}}})$ and $S_2(67)^+$. We choose a basis for $S_2(67)^+$ that is given by q-expansions with rational coefficients, as follows:

$$\begin{aligned} g_1 &\coloneqq q - 3q^3 - 3q^4 - 3q^5 + q^6 + 4q^7 + 3q^8 + O(q^9), \\ g_2 &\coloneqq q^2 - q^3 - 3q^4 + 3q^7 + 4q^8 + O(q^9). \end{aligned}$$

Then we choose the model for X where $\frac{du}{v}$ corresponds to $g_1 \frac{dq}{q}$ and $u\frac{du}{v}$ corresponds to $g_2 \frac{dq}{q}$, by setting $u = \frac{g_2}{g_1}$ and $v = q\frac{du}{g_1 dq}$. This allows us to find q-expansions for the monomials $\{v^2, 1, u, u^2, \ldots, u^5, u^6\}$ and use linear algebra to get an explicit equation for the new model of X,

$$v^2 = 9u^6 - 14u^5 + 9u^4 - 6u^3 + 6u^2 - 4u + 1.$$

Writing down an explicit change of model to the regular model, we can find the q-expansion of the forms in (6.9.0.3) and compute the Hecke action on these q-expansions. This gives us the matrix representation of the Hecke operator T_2 with respect to the basis on (6.9.0.3). The trace of this matrix is nonzero, so we let $f \coloneqq 2T_2 + 3\,\mathrm{id}\colon J \to J$. The endomorphism f has trace zero and matrix representation

$$\begin{pmatrix} 1 & -2 \\ -2 & -1 \end{pmatrix} \tag{6.9.0.4}$$

with respect to the basis presented in ((6.9.0.3)). Using the work of [CMSV19], we can compute a divisor $D_f \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ inducing f. The equations that define this divisor are given in [DRHS23, Appendix A]. Then Algorithm 6.4.3 produces the divisor A_α that satisfies the properties of Lemma 6.4.4.

We now use Algorithm 6.4.10 to calculate $f(G_1)$ and $f(G_2)$, where G_1 and G_2 are the generators of the Mordell–Weil group of J as in (6.9.0.2).

Since $J(\mathbb{Z}) = J(\mathbb{Q})$, the divisor $f(G_i)$ only needs to be computed over the rationals for $i = 1, 2$. For example, applying (6.4.0.1) we get $f(G_1) = \mathcal{O}_X(D_f|_{P\times X} - D_f|_{\iota(P)\times X})$ and we can compute an explicit divisor $f(G_1)$ using the equations for D_f. We find that

$$f(G_1) = -G_1 + 2G_2 = [-(P - \iota P) + 2(P + Q - 2\iota P)] = [P + 2Q - 3\iota P], \tag{6.9.0.5}$$

$$f(G_2) = 2G_1 + G_2 = [2(P - \iota P) + 1(P + Q - 2\iota P)] = [3P + Q - 4\iota P].$$

Furthermore, we compute $c = [-11G_1 - 8G_2]$ using Algorithm 6.4.7.

We can parametrize the residue disk over $\overline{P}$ up to finite precision by

$$\mathbb{F}_p \to X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}, \qquad \nu \mapsto P_\nu \text{ such that } x(P_\nu)/p = \nu. \tag{6.9.0.6}$$

We now find the trivializing section $\varphi \circ \lambda$, following Section 6.5. By direct computation the constant v from Proposition 6.5.2 is 0, hence the pseudoparametrization φ has codomain $\mathbb{Z}_p^3$ (instead of $\mathbb{Z}_p^2 \times \mathbb{Q}_p$). This computation is done using code from the repository [BDM$^+$].

Since $p > 3$, by Proposition 6.5.2 the map $\varphi \circ \lambda : \mathbb{Z}_p \to \mathbb{Z}_p^3$ is linear modulo p. We will calculate $\widetilde{j_b}(P_0)$ and $\widetilde{j_b}(P_1)$ following Algorithm 6.5.4 and interpolate to determine the map. What the following computations show is that

$$\varphi \circ \lambda(\nu) \equiv (2\nu, 0, 6 - \nu) \mod p. \tag{6.9.0.7}$$

By Proposition 6.5.1, the image of the map $\varphi \circ \lambda$ is cut out by two convergent power series. Giving $\mathbb{Z}_p^3$ the coordinates (x_1, x_2, x_3), we see the image of $\varphi\circ\lambda$ is cut out by the equations $g_1 = 0, g_2 = 0$ with $g_1 \equiv x_2 \mod p$, $g_2 \equiv 2x_3 + x_1 + 2 \mod p$.

Algorithm 6.5.4 relies on being able to compute Coleman–Gross local heights at p and at primes of bad reduction. We first note that, since the special fiber of X at 67 is geometrically irreducible, the heights at $\ell \neq p$ are all trivial, and we only have to consider the heights at p. Balakrishnan [Bal] has implemented Coleman–Gross local heights $h_p(D, E)$ for disjoint divisors of degree 0 on a curve Y with a few requirements:

1. the hyperelliptic curve $Y\colon y^2 = H(x)$ is given by a monic odd degree model;
2. the divisors D and E split as a sum of points $D = \sum_i n_i P_i$, $E = \sum_j m_j Q_j$ with $P_i, Q_j \in Y(\mathbb{Q}_p)$.

Remark 6.9.5. Suppose that $D = \sum_i n_i P_i$ and $E = \operatorname{Div} r + E'$ where $E' = \sum_j m_j Q_j$ with $P_i, Q_j \in Y(\mathbb{Q}_p)$. Then

$$\begin{aligned} h_p(D,E) &= h_p(D, E' + \operatorname{Div} r) \\ &= h_p(D,E') + h_p(D, \operatorname{Div} r) \\ &= h_p(D,E') + \mathsf{log}(r(D)) \end{aligned}$$

so we can also compute $h_p(D,E)$.

Therefore we make a change of model when doing computations on $\mathcal{N}$. The even degree model of X is given by

$$y^2 = g(x) \coloneqq x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1,$$

where $g(x)$ has a 7-adic zero $\beta = 4 + 3\cdot 7 + 4\cdot 7^2 + O(7^3)$. We can construct a degree 5 model:

$$\beta^6 y'^2 = g(\beta x'/(x'-1)) \cdot (x'-1)^6.$$

Letting $c_0 = 5 + 3\cdot 7 + 3\cdot 7^2 + O(7^3)$ be a 5th root of the leading coefficient of $g(\beta x'/(x'-1))$ we obtain an odd degree model over $\mathbb{Q}_p$ given by the coordinate transformation from the even degree model

$$(x,y) \mapsto (c_0 \cdot x/(x-\beta), \beta^3 y/(x-\beta)^3). \tag{6.9.0.8}$$

Remark 6.9.6. Recent work of Gajović and Müller [GM23] gives a practical algorithm and code for computing Coleman–Gross local heights $h_p(D,E)$ on even degree hyperelliptic curves.

We now compute for P the local height $\psi(\widetilde{j_b}(P)) = h_p(P - b, A_\alpha|_{P\times X})$. Let B, C be the divisors on X defined in Algorithm 6.4.3. One can check that $B \cap P_\nu$ is empty over $\mathbb{Z}/p^2\mathbb{Z}$ for all $\nu \in \mathbb{F}_p$, so we have $A_\alpha|_{P_\nu\times X} = D_f|_{P_\nu\times X} + B - C$; we denote $A_\alpha|_{P_0\times X}$ by E_{P_0}. Over the rationals

$$E_{P_0} \sim [0:0:1] - [-1:1:1] + 2[-1:0:1] - 2[1:-3:1] =: E'_{P_0},$$

with $E_{P_0} = E'_{P_0} + \mathsf{Div} g_{P_0}$ where g_{P_0} is computed explicitly as an element of the function field and given in [DRHS23, Appendix A]. By Remark 6.9.5, we can

decompose $h_p(P-b, E_{P_0}) = h_p(P-b, E'_{P_0}) + h_p(P-b, \mathsf{Div} g_{P_0})$. We compute

$$h_p(P-b, \mathsf{Div} g_{P_0}) = \mathsf{log} g_{P_0}(P)/g_{P_0}(b) = \mathsf{log}(4/9) \equiv 7 \mod 49.$$

We also compute

$$h_p(P-b, E'_{P_0}) = 5\cdot 7 + 3\cdot 7^2 + 3\cdot 7^3 + 6\cdot 7^4 + \\ 7^5 + 5\cdot 7^6 + 2\cdot 7^7 + 6\cdot 7^8 + O(7^9).$$

So, $\psi(\widetilde{j_b}(P)) = 6\cdot 7 + O(7^2)$.

Unlike the P_0 case, the divisor $D_{P_1} \coloneqq D_f|_{P_1\times X}$ is not a sum of two p-adic points. Instead we use the explicit Cantor's algorithm [Can87, Sut19] to get a linearly equivalent multiple which does split as a sum of p-adic points.

Let (u_1, v_1) be the Mumford representation for D_{P_1}. Then using [Sut19, Algorithm Compose] we can compute (u_2, v_2), the Mumford representation for $2D_{P_1}$. Applying [Sut19, Algorithm Reduce] we obtain the Mumford representation (u_3, v_3) for the reduction of $2D_{P_1}$ along with $r = (y - v_2(x))/u_3(x)$, satisfying the relationship

$$2D_{P_1} = \mathrm{Div}(u_1, v_1) = \mathsf{Div}((y - v_2(x))/u_3(x)) + \mathrm{Div}(u_3, v_3). \tag{6.9.0.9}$$

Remark 6.9.7. Since the computations for D_{P_1} were done on the regular model, we need to change the equations to the odd degree model. The Mumford divisor for D_{P_1} is a sum of 2 points over a totally ramified extension of $\mathbb{Q}_p$. Using the equations (6.9.0.8) for the change of model we can map the points to two points $(x_1, y_1), (x_2, y_2)$ on the odd degree model and construct the corresponding degree 2 Mumford divisor (u_1, v_1) vanishing on the x-coordinates using interpolation: $u_1(x) = (x - x_1)(x - x_2)$ and $v_1(x) = y_2 \cdot (x - x_1)/(x_2 - x_1) + y_1 \cdot (x - x_2)/(x_1 - x_2)$.

Then $2D_{P_1}$ is linearly equivalent to a divisor that splits into a sum of two points over the odd degree model. The splitting is given by

$$\{Q_1, Q_2\} \coloneqq \{(469610\cdot 7 + O(7^9), -15018865 + O(7^9)), \\ (499647 + O(7^9), -14480684 + O(7^9))\}.$$

By (6.9.0.9) we have

$$2D_{P_1} = Q_1 + Q_2 + \mathsf{Div}((y - v_2(x))/u_3(x)) + 2\infty,$$

where

$$v_2(x) \coloneqq -(462222 + O(7^8))x^3 + (73804 + O(7^8))x^2 + (1999391 + O(7^8))x - 1649234 + O(7^8)$$

and

$$u_3(x) \coloneqq (1 + O(7^8))x^2 + (1977884 + O(7^8))x + 297368 \cdot 7 + O(7^8).$$

With the splitting in hand, we can compute $\widetilde{j_b}(P_1)$:

$$\frac{1}{2}h_p(P_1 - b, 2D_{P_1}) + h_p(P_1 - b, B - C) =$$
$$h_p(P_1 - b, B - C) + \frac{1}{2}h_p(P_1 - b, Q_1 + Q_2 + 2\infty) + \frac{1}{2}h_p(P_1 - b, \mathsf{Div}((y - v_2(x))/u_3(x))).$$

The divisor $B - C$ is not a sum of points, but we have that $B - C$ is equal to $4\infty_- - \iota b - 5\iota Q + \mathsf{Div}(g_{P_1})$, where g_{P_1} is given in [DRHS23, Appendix A]. Therefore $\psi(\widetilde{j_b}(P_1))$ is

$$\begin{aligned} &h_p(P_1 - b, D_{P_1} + B - C) \\ &= \frac{1}{2}h_p(P_1 - b, Q_1 + Q_2 + 2\infty + 2(4\infty_- - \iota b - 5\iota Q)) \\ &+ \frac{1}{2}\mathsf{log}((y - v_2)(P_1 - b)/u_3(P_1 - b)) + \mathsf{log}g_{P_1}(P_1 - b). \end{aligned}$$

Then

$$\begin{aligned} &\mathsf{log}g_{P_1}(P_1 - b) = 6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 2 \cdot 7^4 + O(7^5) \\ &\mathsf{log}(y - v_2)(P_1 - b)/u_3(P_1 - b)) = 7^2 + 3 \cdot 7^3 + 2 \cdot 7^4 + O(7^5)) \\ &h_p(P_1 - b, Q_1 + Q_2 + 2\infty + 2(4\infty_- - \iota b - 5\iota Q)) = 5 \cdot 7 + 7^2 + 4 \cdot 7^3 + O(7^4) \end{aligned}$$

So $\psi(\widetilde{j_b}(P_1)) = 5 \cdot 7 + O(7^2)$.

Now we can calculate $\widetilde{j_b}(P_1)$ in the map $\varphi\colon T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$ given in Definition 6.3.21. We can compute this using the logarithm, normalized by the logarithm at P:

$$\begin{aligned} &\mathsf{log}(P_0 - b) - \mathsf{log}(P_0 - b) = (0, 0), \\ &\mathsf{log}(P_1 - b) - \mathsf{log}(P_0 - b) = (2 \cdot 7 + O(7^2), O(7^2)). \end{aligned}$$

Hence we see $\varphi(\widetilde{j_b}(P_0)) = (0,0,6)$ and $\varphi(\widetilde{j_b}(P_1)) = (2,0,5)$. By interpolating these values we get (6.9.0.7).

We now discuss the map κ using formulas in Section 6.6. We will show that the map $\varphi \circ \kappa \colon \mathbb{Z}_p^2 \to \mathbb{Z}_p^3$, which is by Proposition 6.6.3 given by two homogeneous linear polynomials and one quadratic polynomial, is modulo p equal to

$$(n_1, n_2) \mapsto (n_1, -n_1 - 2n_2, -3n_1^2 - n_1 n_2 - n_1 + n_2 - 1). \tag{6.9.0.10}$$

Following Algorithm 6.6.1 we construct the points of $\mathcal{M}^\times(G_i, f(G_j))(\mathbb{Z})$ and $\mathcal{M}^\times(G_i, c)(\mathbb{Z})$ for $i, j = 1, 2$ as in [EL21, Section 8.3].

We work out the example $\mathcal{M}^\times(G_1, f(G_2))(\mathbb{Z})$ here in detail. Recall that by (6.9.0.5) we have $G_1 = [P - \iota P]$ and $f(G_2) = [3P + Q - 4\iota P]$. By (6.3.2.2), the $\mathbb{G}_m$-torsor $\mathcal{M}^\times(G_1, f(G_2))$ is $f(G_2)^* \mathcal{O}_X^\times(G_1)$. Since we want to work with the image in $\mathcal{N}$, and this representation of $f(G_2)$ is not disjoint from G_1 over $\mathbb{Q}$, we represent G_1 by the linearly equivalent divisor $\iota b - \infty_+ + \infty_- - Q$ and $f(G_2)$ by the linearly equivalent divisor $3(P - \iota P) + (P - \iota Q)$. These divisors are not disjoint over $\mathbb{Z}$ because $-\iota Q$ and ιb intersect over $\mathbb{Z}/2\mathbb{Z}$ so

$$\begin{aligned} h(P - \iota P, 3(P - \iota P) + (P - \iota Q)) = \\ h_p(\iota b - \infty_+ + \infty_- - Q, 3(P - \iota P) + (P - \iota Q)) + \mathsf{log}(2). \end{aligned}$$

We can compute

$$\begin{aligned} Q_{12} &= ([P - \iota P], [3(P - \iota P) + (P - \iota Q)], h(\iota b - \infty_+ + \infty_- - Q, 3(P - \iota P) + (P - \iota Q)) \\ &= (G_1, f(G_1), 5 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + O(7^4)). \end{aligned}$$

The remaining Q_{ij} are:

$$\begin{aligned} Q_{11} &= (G_1, f(G_1), 2 \cdot 7 + 5 \cdot 7^3 + O(7^4)), \\ Q_{21} &= (G_2, f(G_1), 4 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + O(7^4)), \\ Q_{22} &= (G_2, f(G_2), 3 \cdot 7^2 + 4 \cdot 7^3 + O(7^4)), \\ Q_{10} &= (G_1, c, 3 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + O(7^4)), \\ Q_{20} &= (G_2, c, 2 \cdot 7 + 2 \cdot 7^3 + O(7^4)). \end{aligned}$$

Remark 6.9.8. In practice, since we will need to add Q_{ij} in $\mathcal{N} \simeq J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \times \mathbb{Q}_p$ we use the map $\mathsf{log} \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p^g$ for $i, j = 1, 2$ and for $j = 0$, we store Q_{ij} as the vector $(\mathsf{log}(G_i), \mathsf{log}(f(G_j)), h(G_i, f(G_j)))$. This allows us to add in $\mathbb{Q}_p^g$ instead of $J(\mathbb{Q}_p)$.

We proceed to compute the bijection $\kappa\colon \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b(\overline{P})}}$ of the integral points of T modulo p^2, as in [EL21, Section 8.5]. The divisor $j_b(\overline{P}) \in J(\mathbb{F}_p)$ is equal to the image of

$$\widetilde{G_t} \coloneqq G_1 + 3G_2$$

in $J(\mathbb{F}_p)$ and correspondingly we define $e_{01} \coloneqq 1$ and $e_{02} \coloneqq 3$.

Let $\widetilde{G_1}$ and $\widetilde{G_2}$ be a basis for the kernel of reduction $J(\mathbb{Z}) \to J(\mathbb{F}_p)$. Since

$$\widetilde{G_1} = -3G_1 + 7G_2, \quad \widetilde{G_2} = 7G_1 + 4G_2$$

we define $e_{11} = -3, e_{12} = 7, e_{21} = 7, e_{22} = 4$.

The map $\kappa_{\mathbb{Z}}$ is given in coordinates in $\mathcal{N}$ by sending (n_1, n_2) to

$$\begin{aligned}
&((7 + 7^2 + 7^3 + O(7^4)) \cdot n_1 + (4 \cdot 7^3 + O(7^4)) \cdot n_2 + 5 \cdot 7 + 5 \cdot 7^2 + 7^3 + O(7^4),\\
&(6 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + O(7^4)) \cdot n_1 + (5 \cdot 7 + O(7^4)) \cdot n_2 + 5 \cdot 7^2 + 3 \cdot 7^3 + O(7^4)),\\
&((6 \cdot 7 + 5 \cdot 7^2 + 6 \cdot 7^3 + O(7^4)) \cdot n_1 + (2 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + O(7^4),\\
&(4 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + O(7^4)) \cdot n_1 + (3 \cdot 7 + 3 \cdot 7^2 + O(7^4)) \cdot n_2 + 4 \cdot 7 + 2 \cdot 7^3 + O(7^4)),\\
&(4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + O(7^4)) \cdot n_1^2 + (6 \cdot 7 + 7^2 + 4 \cdot 7^3 + O(7^4)) \cdot n_2^2 +\\
&(6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + O(7^4)) \cdot n_1 + (7 + 7^3 + O(7^4)) \cdot n_2 + 6 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + O(7^4))
\end{aligned}$$

where we apply the logarithm to the first two coordinates as in Remark 6.9.8.

Finally, by [EL21, Theorem 4.10], the map $\kappa_{\mathbb{Z}}$ extends to a bijection

$$\kappa\colon \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b(\overline{P})}} \tag{6.9.0.11}$$

with image $\overline{T(\mathbb{Z})}_{\widetilde{j_b(\overline{P})}}$. This map $\varphi \circ \kappa$ is polynomials $(\kappa_1, \kappa_2, \kappa_3) \in \mathbb{Q}_p[x_1, x_2]^3$, with κ_1, κ_2 homogeneous linear and κ_3 at worst quadratic. Applying Corollary 6.3.22, we obtain the formula for $\varphi \circ \kappa$ given in (6.9.0.10).

We now have the tools to prove the upper bound on the number of points in the residue disk $\#X(\mathbb{Z})_{\overline{P}}$. We define

$$\overline{p_1} \coloneqq (\varphi \circ \kappa)^* \overline{g_1} = -n_1 - 2n_2, \quad \overline{p_2} \coloneqq (\varphi \circ \kappa)^* \overline{g_2} = n_1^2 - 2n_1 n_2 - n_1 + 2n_2,$$

and $\overline{A} \coloneqq \mathbb{F}_p[n_1, n_2]/(\overline{p_1}, \overline{p_2})$. The ring $\overline{A}$ is isomorphic to $\mathbb{F}_p[n_2]/(n_2^2 - 3n_2) \simeq \mathbb{F}_p \times \mathbb{F}_p$, so by [EL21, Theorem 4.12] we have an upper bound of 2 on $\#X(\mathbb{Z})_{\overline{P}}$. Specifically, we see that there is at most one point reducing to P_0, namely P itself, and at most one point reducing to P_4 in $X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}$; the other P_ν have no rational points lying over them.

Remark 6.9.9. If we calculate κ and $\widetilde{j_b}$ with greater p-adic precision, we can compute the point reducing to P_4 with greater precision. This can be done by brute force, that is, trying all lifts of the found solution $n_1 = 1, n_2 = 3, \nu = 4$ and seeing when any of the calculated values of κ or $\widetilde{j_b}$ agree modulo the required precision. However, there is a more efficient way. We can look at the "higher residue disks" $X(\mathbb{Z}_p)_{P_4}$ and $T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$, consisting of points that reduce to a specified $\mathbb{Z}/p^2\mathbb{Z}$-point. We can parametrize $X(\mathbb{Z}_p)_{P_4}$ with the map $\mathbb{Z}_p \to X(\mathbb{Z}_p)_{P_4}$ sending μ to $P_{4+p\mu}$. With respect to our usual map $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$, we get a bijection of the higher residue disk of the torsor $T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)} \to (1,0,2) + p\mathbb{Z}_p^3$. Given these identifications, the inclusion $\widetilde{j_b} \colon X^{\mathrm{sm}}(\mathbb{Z}_p)_{P_4} \to T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$ is given by power series that are linear modulo p. Like in Section 6.5, these can be found by interpolation. Similarly, κ restricted to $(1+p\mathbb{Z}_p) \times (3+p\mathbb{Z}_p)$ gives the inclusion $\kappa \colon \overline{T(\mathbb{Z})}_{\widetilde{j_b}(P_4)} \to T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$. For these identifications, κ is actually homogeneous linear modulo p. Solving the resulting affine linear system of equations, we get that the only possible intersection of the image of κ and of $\widetilde{j_b}$ in the higher residue disk $T(\mathbb{Z}/p^3\mathbb{Z})_{\widetilde{j_b}(P_4)} \simeq \mathbb{F}_p^3$ is $(5,1,5)$, corresponding to $P_{4+p\mu}$ with $\mu = 4$. This is the point $P_{32} \in X(\mathbb{Z}/p^3\mathbb{Z})_{P_4}$.

In total, we can strengthen Proposition 6.9.3 to say the residue disk $X(\mathbb{Z})_{\overline{P}}$ is contained in the set

$$\{P, (4 \cdot 7 + 4 \cdot 7^2 + O(7^3), 6 + 6 \cdot 7 + 6 \cdot 7^2 + O(7^3))\}.$$

6.10 Acknowledgements

This project began at the 2020 Arizona Winter School on Nonabelian Chabauty. It is a pleasure to thank the project supervisors Bas Edixhoven, Guido Lido, and Jan Vonk for their help. We are also very thankful to Jennifer Balakrishnan, Steffen Müller, John Voight, David Holmes, Alexander Betts, Edgar Costa, Jeroen Sijsling, Andrew Sutherland and Amnon Besser for helpful correspondence or computational advice. We thank the anonymous referee for their careful feedback, especially regarding the proof of the main theorem.