P. Spelier

A geometric approach to linear Chabauty

Master thesis

July 6, 2020

Thesis supervisor: prof. dr. S.J. Edixhoven

Leiden University
Mathematical Institute

Contents

1 Introduction

A fundamental problem in mathematics is solving polynomial equations over the rationals, dating back to Diophantus. An important special case in algebraic geometry is that of curves. The behavior of the rational points of curves depends enormously on the *genus* g of the curve, a numerical invariant. For $g = 0$, there are either no or infinitely many solutions, and their behavior is well understood. For $g = 1$, we get either no point or an elliptic curve, whose set of rational points forms a finitely generated abelian group.

In this thesis, we look only at the case of a curve C with genus $g > 1$. It turns out that there are always only finitely many rational points. This result was originally conjectured by Mordell in 1922 and finally proven by Faltings in 1983 in [Fal83].

Before Faltings's theorem was proven, one of the major partial results was a theorem from Chabauty in 1941, phrased in terms of the rank r of the group of rational points on the Jacobian J of the curve, also called the Mordell-Weil rank; this rank is finite by the Mordell-Weil theorem. Chabauty proved, using p-adic methods, that if r is strictly smaller than the genus g, then C has only finitely many rational points. Loosely said, this proof and all Chabauty-related theorems, rely on choosing a prime p for which C has good reduction, and intersecting $J(\mathbb{Q})$ with $C(\mathbb{Q}_p)$ inside the bigger Lie group $J(\mathbb{Q}_p)$. By properties of $\mathbb{Q}_p$, the subgroup $J(\mathbb{Q})$, up to torsion generated by r elements, lies within a Lie subgroup of dimension at most r, and $C(\mathbb{Q}_p)$ is a 1-dimensional p-adic manifold, and hence this intersection can be proven to be discrete and – as $J(\mathbb{Q}_p)$ is compact – finite.

This was made into an effective argument by Coleman in 1985. This was done by finding explicitly, as a power series, a differential form ω on $J_{\mathbb{Q}_p}$ whose Coleman integral vanishes on $J(\mathbb{Q})$. Pulling ω back to $C_{\mathbb{Q}_p}$ and looking at the fibre of reduction to a single $\mathbb{F}_p$-point P, one can in certain cases give an upper bound for the number of points in $C(\mathbb{Q})$ reducing to P based only on finite-precision calculations of ω. Most well known is the generic upper bound $|C(\mathbb{Q})| \leq |C(\mathbb{F}_p)| + 2g - 2$ under the conditions $r < g, p > 2g$, as explained in the excellent introductory article [MP12].

This Coleman-Chabauty method has been greatly generalised by Kim to so-called non-abelian Chabauty in [Kim05] and [Kim09]. He interprets working in the Jacobian as dealing with the abelianised fundamental group of the curve C and works with larger, non-abelian quotients of the fundamental group. Then quadratic Chabauty, the simplest case of non-abelian Chabauty,

was developed by Kim, Balakrishnan, Besser, Dogra and Müller in the series of articles [BB15],[BBM17],[BD18], and further extended by Balakrishnan, Dogra, Müller, Tuitman and Vonk; in 2017 they famously calculated all rational points of the "cursed curve", the modular curve $X_s^+(13)$ [BDM$^+$19]. They use an endomorphism of the Jacobian and do p-adic analysis on p-adic local heights to make quadratic Chabauty explicit. Their methods are strong enough to prove finiteness of $C(\mathbb{Q})$ under the condition of $r < g + \rho - 1$, where ρ is the Néron-Severi rank of the Jacobian, even if finding $C(\mathbb{Q})$ can still be difficult in those cases.

Very recently, Edixhoven and Lido made available a preprint of their article "Geometric quadratic Chabauty" [EL19]. Their goal in this article is to create a more geometric approach to effective quadratic Chabauty, by working in a pullback T of the Poincaré torsor of the Jacobian spread out over $\mathbb{Z}$. They also abandon the Coleman method for Chabauty; instead, they parametrise the map $T(\mathbb{Z}) \to T(\mathbb{Z}_p)$ with power series and pull back equations for the curve inside $T(\mathbb{Z}_p)$ along this map. Again, a necessary condition is $r < g + \rho - 1$.

The purpose of this thesis is to make the work by Edixhoven and Lido more accessible by applying geometric Chabauty to the linear case, i.e. when working with $J(\mathbb{Q})$ and $J(\mathbb{Q}_p)$ and assuming $r < g$. In this thesis, we go into more detail on what is happening throughout the process, including both theoretical and practical components. This new method of applying Chabauty leads to, when working with single-digit p-adic precision, a conditional upper bound $|C(\mathbb{Q})| \leq |C(\mathbb{F}_p)|$, as obtained in Proposition 4.4. This upper bound compares favorably with classical Coleman-Chabauty, but unlike classical Coleman-Chabauty, we cannot say in general when the conditions of these propositions hold. We develop heuristics that suggest that generally, trying multiple primes p of good reduction will yield good results; these heuristics say that the conditional upper bound will hold for a set of primes of density 1, and if $r < g-1$ the upper bound can even often (in a set of primes of density at least e^{-1}) be improved to prove there are at most $|C(\mathbb{Q})|$ rational points, i.e., finding $C(\mathbb{Q})$ exactly. The methods used to obtain Proposition 4.4 are also amenable to higher precision calculations; indeed, in the case $r = g - 1$ one expects to need either higher precision calculations or the Mordell-Weil sieve to calculate $|C(\mathbb{Q})|$ exactly.

We also give a hyperelliptic example with $r = 1, g = 2$, where the bound from Proposition 4.4 indeed holds, and we are able to compute $C(\mathbb{Q})$.

1.1 Overview

We first present the context in which we will perform Chabauty. Let $C_{\mathbb{Q}}/\mathbb{Q}$ be a curve (i.e., a proper, smooth, geometrically connected variety of dimension 1) of genus $g \geq 2$ whose $\mathbb{Q}$-points we will attempt to find. Let $p > 2$ be a prime, and assume we have a scheme C over $\mathbb{Z}_{(p)}$, proper and smooth with generic fibre $C_{\mathbb{Q}}$; then we immediately have $C_{\mathbb{Q}}(\mathbb{Q}) = C(\mathbb{Q}) = C(\mathbb{Z}_{(p)})$ by the valuative criterion of properness. Let J be the relative Jacobian of C over $\mathbb{Z}_{(p)}$, i.e. with fibres $\operatorname{Jac} C_{\mathbb{Q}}$ and $\operatorname{Jac} C_{\mathbb{F}_p}$. We assume from now on that the Mordell-Weil rank of J is $r < g$. Assume we have a $\mathbb{Q}$-point b in C, or equivalently a $\mathbb{Z}_{(p)}$-point. We view C as a subscheme of J, using the map $Q \mapsto Q - b$ on points. Let $P \in C(\mathbb{F}_p)$ be a point such that $t := P - b \in J(\mathbb{F}_p)$ lies in the image of $J(\mathbb{Z}_{(p)})$.

Definition 1.1. Let S be a scheme, $T \to U$ a morphism of schemes and $x : T \to S$ a T-point. We define $S(U)_x$ as the morphisms from U to S that, after precomposing with $T \to U$, give x.

Example 1.2. If we have a proper variety X over $\mathbb{Z}_{(p)}$, then $X(\mathbb{Z}_{(p)})$ is naturally in bijection with $X(\mathbb{Q})$. The natural map $X(\mathbb{Z}_{(p)}) \to X(\mathbb{F}_p)$ reduces a point modulo p and for $x \in X(\mathbb{F}_p)$, the set $X(\mathbb{Z}_{(p)})_x$ consists of the residue disc of $\mathbb{Z}_{(p)}$-points reducing to x.

Geometric Chabauty works by finding an upper bound for the cardinality of $C(\mathbb{Z}_{(p)})_P$. For this, we use the following diagram.

$$\begin{array}{ccc} C(\mathbb{Z}_{(p)})_P & \longrightarrow & J(\mathbb{Z}_{(p)})_t \\ \downarrow & & \downarrow \\ C(\mathbb{Z}_p)_P & \longrightarrow & J(\mathbb{Z}_p)_t \end{array}$$

where the two vertical maps are inclusions, and the two horizontal maps are subtraction of b. We will in fact compute upper bounds for the larger set $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z}_{(p)})_t}$, where $\overline{J(\mathbb{Z}_{(p)})_t}$ is the closure of $J(\mathbb{Z}_{(p)})_t$ in $J(\mathbb{Z}_p)_t$.

In Section 2, we treat the structure of $C(\mathbb{Z}_p)_P$ and $J(\mathbb{Z}_p)_t$; we will show that, after choosing parameters, they are in bijection with respectively $\mathbb{Z}_p$ and $\mathbb{Z}_p^g$. We also discuss the resulting map $\mathbb{Z}_p \to \mathbb{Z}_p^g$.

In Section 3 we further look at the map $J(\mathbb{Z}_{(p)})_t \to J(\mathbb{Z}_p)_t$. This is a translation of the group morphism $J(\mathbb{Z}_{(p)})_0 \to J(\mathbb{Z}_p)_0$ between kernels of

reduction; it turns out that for our choice of p, the subgroup $J(\mathbb{Z}_{(p)})_0$ is free of rank r. We study the properties of the resulting map $\mathbb{Z}^r \to \mathbb{Z}_p^g$, using the theory of formal groups to determine the group structure on $\mathbb{Z}_p^g$ induced by the bijection $J(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^g$.

In Section 4, we put all of this information together, culminating in several methods to possibly compute upper bounds on $\left|C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z}_{(p)})_t}\right|$ with finite precision calculations. We also perform a heuristic analysis to show that a simple calculation of linear algebra modulo p is very likely to result in an upper bound of at most $|C(\mathbb{F}_p)|$ for $|C(\mathbb{Z}_{(p)})|$, and for $r < g - 1$ even in an upper bound of $|C(\mathbb{Q})|$.

The methods developed in the first four sections are not always guaranteed to prove finiteness of $C(\mathbb{Z}_{(p)})_P$. In Section 5 we treat several possible complications and improvements, referring to other work on Chabauty for further reading.

Next, in Section 6 we focus on how to perform the calculations happening in the Jacobian. Here, we use Makdisi's approach of representing a divisor by a subspace of a large Riemann-Roch space. We partially follow the article [Mas20] by Mascot, and also give an original algorithm for explicitly computing the map $C(\mathbb{Z}_p)_P \to J(\mathbb{Z}_p)_t$ in Makdisi's representation.

We end our discussion of linear geometric Chabauty with an explicit example in Section 7, a genus 2 curve whose Jacobian has Mordell-Weil rank 1. We use both Magma and Pari/GP to do our calculations, and end up with a complete list of all rational points of the curve.

Finally, we provide an introduction to geometric quadratic Chabauty in Section 8. Here, we aim to introduce all the different objects relevant to geometric quadratic Chabauty; we explain why we have to work over $\mathbb{Z}$ instead of over $\mathbb{Q}$ in order for geometric quadratic Chabauty to make sense; and we explain some of the problems and solutions that working over $\mathbb{Z}$ gives rise to.

1.2 Preliminaries

We expect the readers of this thesis to be familiar with algebraic geometry, e.g. master students with a specialisation in algebraic geometry. The introduction to geometric quadratic Chabauty in Section 8 contains some terms typically not treated in a master programme; while knowing them will help to put the material in context, this section is meant to be understandable for those that are not familiar with the terminology as well.

1.3 Acknowledgements

I would like to thank my supervisor Bas Edixhoven for his help — I have learnt a great deal since starting on this thesis, and he helped me do so. I would also like to thank my father, for all the support he has shown me.

2 Points on a smooth scheme over $\mathbb{Z}_p$

Let $X/\mathbb{Z}_p$ be a smooth scheme of relative dimension d, and let $x \in X(\mathbb{F}_p)$ be a point. Then we will show in this section that $X(\mathbb{Z}_p)_x$ is, up to a single choice, naturally in bijection with $\mathbb{Z}_p^d$. This bijection is given by choosing parameters at x; evaluating at $X(\mathbb{Z}_p)_x$ gives a bijection with $(p\mathbb{Z}_p)^d$, and then we divide by p. For putting up a nice framework to work in, we start with blowing up X at x.

Assume, by looking at a neighborhood of x, that $X = \operatorname{Spec} A$ is affine and that $p, t_1, \ldots, t_d$ generate the maximal ideal of $\mathcal{O}_{X,x}$ with $t_1, \ldots, t_d$ elements of $\mathcal{O}_X(X) = A$, also called *parameters* at x. By shrinking X even more, we may assume as X is smooth that $t = (t_1, \ldots, t_d) : X \to \mathbb{A}^d_{\mathbb{Z}_p}$ is étale and the fibre of the origin over $\mathbb{F}_p$ consists of just x. Now consider the blowup $\widetilde{X}_x \to X$ of X at x, and let $\widetilde{X}_x^p$ be the open subscheme where p generates the inverse image of the maximal ideal of $\mathcal{O}_{X,x}$. Equivalently, that is the part where $t_1, \ldots, t_d$ are multiples of p, so informally $\widetilde{X}_x^p$ consists of the points that reduce to x modulo p.

There is an explicit description of the map $\widetilde{X}_x^p \to X$; as t is étale, the ideal of X defining x is the pullback along t of the ideal of $\mathbb{A}^d_{\mathbb{Z}_p}$ defining the origin a over $\mathbb{F}_p$. That means that the blowup $\widetilde{X}_x \to X$ is the pullback of the blowup $\widetilde{\mathbb{A}}^d_{\mathbb{Z}_p,a} \to \mathbb{A}^d_{\mathbb{Z}_p}$. Then the open subscheme $\widetilde{X}_x^p$ is the pullback of the corresponding subscheme of $\widetilde{\mathbb{A}}^d_{\mathbb{Z}_p,a}$, i.e. $\operatorname{Spec} \mathbb{Z}_p[\widetilde{x_1}, \ldots, \widetilde{x_d}] = \operatorname{Spec} \mathbb{Z}_p[x_1/p, \ldots, x_d/p]$ with the morphism $\mathbb{Z}_p[x_1, \ldots, x_d] \to \mathbb{Z}_p[\widetilde{x_1}, \ldots, \widetilde{x_d}]$ given by $x_i \mapsto p\widetilde{x_i}$. That implies that $\widetilde{X}_x^p$ is $\operatorname{Spec} A[t_1/p, \ldots, t_d/p]$, with the map $\widetilde{X}_x^p \to X$ given by the inclusion $A \to \operatorname{Spec} A[t_1/p, \ldots, t_d/p]$ (remember that the t_i are elements of $\mathcal{O}_X(X) = A$).

This now enables us to characterise explicitly the $\mathbb{Z}_p$-points above x, as in the following two lemmas.

Lemma 2.1. *There is a natural bijection*

$$X(\mathbb{Z}_p)_x \to \widetilde{X}_x^p(\mathbb{Z}_p).$$

Proof. Note that by (I,2.4.4) of [GD71], a $\mathbb{Z}_p$-point of a scheme S is just an $\mathbb{F}_p$-point s together with a local morphism $\mathcal{O}_{S,s} \to \mathbb{Z}_p$. In our case, we find that $X(\mathbb{Z}_p)_x$ is naturally in bijection with $\operatorname{Hom}_{\text{local}}(A_x, \mathbb{Z}_p)$. As the maximal ideal of A_x is generated by $p, t_1, \ldots, t_d$, the morphism being local just means that the images of $t_1, \ldots, t_d$ are divisible by p. That exactly gives those

morphisms that extend to a morphism $A[t_1/p, \ldots, t_d/p] \to \mathbb{Z}_p$, i.e. a $\mathbb{Z}_p$-point of $\widetilde{X}_x^p$. Hence we find the natural bijection. □

Lemma 2.2. *Evaluating t at $X(\mathbb{Z}_p)_x$ gives a bijection to $(p\mathbb{Z}_p)^d$.*

Proof. As t is locally of finite type, by (IV,17.6.3) of [GD71] we have an isomorphism between the p-adic completion $\mathcal{O}(\widetilde{X}_x^p)^{\wedge p}$ and the completion $\mathbb{Z}_p\langle \widetilde{x_1}, \ldots, \widetilde{x_d}\rangle$ of $\mathbb{Z}_p[\widetilde{x_1}, \ldots, \widetilde{x_d}]$, with the latter completion being the ring of convergent power series, i.e.

$$\mathbb{Z}_p\langle \widetilde{x_1}, \ldots, \widetilde{x_d}\rangle = \{f \in \mathbb{Z}_p[[\widetilde{x_1}, \ldots, \widetilde{x_d}]] \mid \forall n \geq 0, f \in \mathbb{Z}[\widetilde{x_1}, \ldots, \widetilde{x_d}] + (p^n)\}.$$

By the universal property of completions, as t induces the isomorphism between completions, t also induces a bijection

$$\mathrm{Hom}(\mathcal{O}(\widetilde{X}_x^p), \mathbb{Z}_p) \to \mathrm{Hom}(\mathbb{Z}_p\langle \widetilde{x_1}, \ldots, \widetilde{x_d}\rangle, \mathbb{Z}_p) = \mathbb{Z}_p^d.$$

Following all the bijections, we indeed get the bijection we wanted. □

Remark 2.3. Note that this construction is functorial, in the following sense: let X, Y be two smooth schemes over $\mathbb{Z}_p$ and $x \in X(\mathbb{F}_p)$, $y \in Y(\mathbb{F}_p)$ be two $\mathbb{F}_p$-points, and let $f : Y \to X$ be a map satisfying $f(y) = x$. Then the inverse image along the map

$$\widetilde{Y}_y^p \to Y \to X$$

of the ideal sheaf defining x is the ideal generated by p. Hence by the universal property of blowups (II.7.14 of [Har77]), this factors through a unique morphism $\widetilde{Y}_y^p \to \widetilde{X}_x$, landing in $\widetilde{X}_x^p$, i.e. we get that there is a unique morphism $\widetilde{f} : \widetilde{Y}_y^p \to \widetilde{X}_x^p$ making the diagram

$$\begin{array}{ccc} \widetilde{Y}_y^p & \xrightarrow{\widetilde{f}} & \widetilde{X}_x^p \\ \downarrow & & \downarrow \\ Y & \xrightarrow{f} & X \end{array}$$

commute.

Remark 2.4. In actual calculations, we will be focusing on $X(\mathbb{Z}/p^2\mathbb{Z})_x$. This set is a natural torsor of the tangent space $T_x X_{\mathbb{F}_p}$ of $X_{\mathbb{F}_p}$ at x, which we will describe here. We write R for the local ring $\mathcal{O}_{X_{\mathbb{Z}/p^2\mathbb{Z}}, x}$ and $\mathfrak{m}$ for its

maximal ideal, and $\overline{R}$ and $\overline{\mathfrak{m}}$ for their reductions modulo p. Then an element in $X(\mathbb{Z}/p^2\mathbb{Z})_x$ is a local morphism $R \to \mathbb{Z}/p^2\mathbb{Z}$. As $R/\mathfrak{m} = \mathbb{F}_p$, giving such a local morphism is equivalent to giving a map $\mathfrak{m} \to p\mathbb{Z}/p^2\mathbb{Z}$ respecting multiplication and sending p to p. Such a map factors uniquely through $\mathfrak{m}/\mathfrak{m}^2 \to p\mathbb{Z}/p^2\mathbb{Z}$. We see that the set $X(\mathbb{Z}/p^2\mathbb{Z})_x$ is canonically in bijection with $\mathbb{F}_p$-linear maps $\mathfrak{m}/\mathfrak{m}^2 \to p\mathbb{Z}/p^2\mathbb{Z}$ sending p to p. Note that $\mathfrak{m}/\mathfrak{m}^2$ is a $(d+1)$-dimensional $\mathbb{F}_p$-vector space, and $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is a d-dimensional $\mathbb{F}_p$-vector space; the map $\mathfrak{m}/\mathfrak{m}^2 \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ is dividing out by p. Denoting $^\wedge$ to be $\mathrm{Hom}(\cdot, \mathbb{F}_p)$, the exact sequence

$$0 \to p\mathbb{Z}/p^2\mathbb{Z} \to \mathfrak{m}/\mathfrak{m}^2 \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \to 0$$

can be dualised to

$$0 \to (\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2)^\wedge \to (\mathfrak{m}/\mathfrak{m}^2)^\wedge \to (p\mathbb{Z}/p^2\mathbb{Z})^\wedge \to 0.$$

As $X(\mathbb{Z}/p^2\mathbb{Z})_x$ is exactly the subset of $(\mathfrak{m}/\mathfrak{m}^2)^\wedge$ that gets mapped to the function $p \mapsto 1 \in (p\mathbb{Z}/p^2\mathbb{Z})^\wedge$, we see this is naturally a torsor under the tangent space $(\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2)^\wedge = T_x X_{\mathbb{F}_p}$.

Note that this set does not have any more canonical structure; for example, with $X = \mathbb{A}^1_{\mathbb{Z}_p}$ and x the $\mathbb{F}_p$-point 1, the set $X(\mathbb{Z}/p^2\mathbb{Z})_x$ is $\{1+pi | i \in \mathbb{F}_p\}$, and we see we cannot upgrade the torsor structure. This is because even after choosing a parameter at x as a point of $X_{\mathbb{F}_p}$, a lift of such a parameter to $X_{\mathbb{Z}/p^2\mathbb{Z}}$ is not canonical, and can in fact differ up to translation. This is in contrast to the situation over $\mathbb{F}_p[\varepsilon]/(\varepsilon^2)$, where the $\mathbb{F}_p$-algebra structure gives rise to an isomorphism of $\mathbb{F}_p$-vector spaces between $X(\mathbb{F}_p[\varepsilon]/(\varepsilon^2))$ and $T_x X_{\mathbb{F}_p}$; indeed, this is an alternate definition of the tangent space.

Remark 2.5. We look at the specific case of X being of relative dimension 1 over $\mathbb{Z}_p$. Then the $T_x X_{\mathbb{F}_p}$-torsor structure on $X(\mathbb{Z}/p^2\mathbb{Z})_x$ translates into something more concrete. We can parametrise $X(\mathbb{Z}/p^2\mathbb{Z})_x$ by $t = t_1$ from $X(\mathbb{Z}/p^2\mathbb{Z})_x \to p\mathbb{Z}/p^2\mathbb{Z}$; write P_λ for the point with t-value λp. Then as a Cartier divisor, the point P_λ is defined by $t - \lambda p \in \mathcal{O}_{X_{\mathbb{Z}/p^2\mathbb{Z}}, x}$, so $P_\lambda + P_\mu$ is defined by $(t-\lambda p)(t-\mu p) = t^2 - (\lambda+\mu)tp$, which defines the same Cartier divisor as $P_{\lambda'} + P_{\mu'}$ if and only if $\lambda + \mu = \lambda' + \mu'$. In that case, as a Cartier divisor, $P_\lambda + P_\mu$ is in fact equal to $P_{\lambda'} + P_{\mu'}$.

2.1 From $C(\mathbb{Z}_p)$ to $J(\mathbb{Z}_p)$

Let p, C and J be as defined in the overview. We know that $C(\mathbb{Z}_p)_P$ is in bijection with $\mathbb{Z}_p$, again with the bijection given by evaluating a parameter and dividing by p. The resulting function $\mathbb{Z}_p \to \mathbb{Z}_p^g$ is linear modulo p, i.e. by using that $\mathbb{Z}\langle z_1, \ldots, z_g\rangle$ is p-adically complete there are power series $f_1, \ldots, f_{g-1} \in \mathbb{Z}_p\langle z_1, \ldots, z_g\rangle$ such that the image of $C(\mathbb{Z}_p)_P$ is exactly given by $Z(f_1, \ldots, f_{g-1})$, and all f_i are linear modulo p as a consequence of Remark 2.5. Another way to think of this, is as $C(\mathbb{Z}/p^2\mathbb{Z})_P$ being an affine line inside $J(\mathbb{Z}/p^2\mathbb{Z})_t$. That $C(\mathbb{Z}/p^2\mathbb{Z})_P$ is an affine line inside $J(\mathbb{Z}/p^2\mathbb{Z})_t$ can also be seen more easily: this map can be identified with the tangent map, using the structure of $X(\mathbb{Z}/p^2\mathbb{Z})_x$ as a torsor over the tangent space from Remark 2.5.

Remark 2.6. We can pick our parameters such that $C(\mathbb{Z}_p)_P \to J(\mathbb{Z}_p)_t$ is given by $\mathbb{Z}_p \to \mathbb{Z}_p^g$, mapping $\mathbb{Z}_p$ to the last coordinate. Then $f_1, \ldots, f_{g-1}$ are just the other parameters at t, so they are linear. This can be done by picking generators $f_1, \ldots, f_{g-1}$ for the ideal defining $\widetilde{C}_P^p$ inside $\widetilde{J}_t^p$.

3 From $J(\mathbb{Z}_{(p)})$ to $J(\mathbb{Z}_p)$

Let p, C, J be as in the overview. As $p > 2$, we know that the torsion of $J(\mathbb{Z}_{(p)})$ injects into $J(\mathbb{F}_p)$, by Proposition 2.3 of [Par00]. Hence for $0 \in J(\mathbb{F}_p)$, we know $J(\mathbb{Z}_{(p)})_0$ is as a group isomorphic to $\mathbb{Z}^r$ with r the Mordell-Weil rank. By assumption, we also know $J(\mathbb{Z}_{(p)})_t$ is in bijection with $J(\mathbb{Z}_{(p)})_0$, with the bijection giving by translating with a lift of t. By Section 2 we know $J(\mathbb{Z}_p)_t$ is in bijection with $\mathbb{Z}_p^g$, with the bijection given by evaluating parameters and dividing by p. Let $\kappa : \mathbb{Z}^r \to \mathbb{Z}_p^g$ be the map resulting from the inclusion $J(\mathbb{Z}_{(p)})_t \to J(\mathbb{Z}_p)_t$. In this section we will prove that κ turns out to have a special property.

Theorem 3.1. *There are uniquely determined $\kappa_1, \ldots, \kappa_g \in \mathbb{Z}_p\langle z_1, \ldots, z_r\rangle$ such that for all $\mathbf{x} \in \mathbb{Z}^r$ we have $\kappa(\mathbf{x}) = (\kappa_1(\mathbf{x}), \ldots, \kappa_g(\mathbf{x}))$ and the image $\overline{\kappa_i}$ of κ_i in $\mathbb{F}_p[z_1, \ldots, z_r]$ has degree at most 1; furthermore, for $m \in \mathbb{Z}_{>0}$ with $m < p - 1$, these κ_i are also of degree at most m modulo p^m.*

We will prove this using results about formal groups as defined in [Hon70]. To be able to use this theory, we first give some results about going from a group scheme over $\mathbb{Z}_p$ to a formal group. We introduce some notation that will

be used in this section. Let R be a commutative ring, and let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$ be vectors of variables. Then $R[[\mathbf{x}]]$ denotes as usual the ring of formal power series in the x_i, and $R[[\mathbf{x}]]_0$ denotes those power series with constant term 0. With $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_m)$, let $f \in R[[\mathbf{x}]]_0^m$. Then for $g \in R[[\mathbf{y}]]^k$ for some $k \in \mathbb{Z}_{\geq 0}$, we can compose g and f to get

$$g \circ f := (g_1(f(\mathbf{x})), \ldots, g_k(f(\mathbf{x}))) \in R[[\mathbf{x}]]^k.$$

This definition makes sense because f^i converges to 0 in the $(\mathbf{x})$-adic topology, so the infinite sum $g_j(f(\mathbf{x}))$ converges.

3.1 From group schemes to formal groups

We first recall the definition of a formal group.

Definition 3.2. Let n be a non-negative integer. Let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ be vectors of n variables. An n-dimensional formal group is an element $F = (F_1, \ldots, F_n)$ of $R[[\mathbf{x}, \mathbf{y}]]_0^n$ with $F \equiv \mathbf{x} + \mathbf{y} \bmod (\mathbf{x}, \mathbf{y})^2$ and $F(F(\mathbf{x}, \mathbf{y}), \mathbf{z}) = F(\mathbf{x}, F(\mathbf{y}, \mathbf{z}))$. If furthermore $F(\mathbf{x}, \mathbf{y}) = F(\mathbf{y}, \mathbf{x})$, this formal group is said to be commutative.

Example 3.3. For any n, we can take $F(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y}$, also known as the n-dimensional additive formal group.

Example 3.4. Take $n = 1$ and $F(x, y) = x + y + xy = (1 + x)(1 + y) - 1$, also known as the multiplicative formal group, as it is a translation of the natural multiplication on $1 + xR[x]$. This satisfies associativity by the formula

$$F(F(x, y), z) = (1 + x)(1 + y)(1 + z) - 1 = F(x, F(y, z)).$$

Note there is no mention of an inverse; the following lemma, a formal version of the implicit function theorem, tells us that the existence and uniqueness of the inverse follows automatically from the definitions.

Lemma 3.5. *Let $\mathbf{x}, \mathbf{y}$ be vectors of variables of length n. Let $F \in R[[\mathbf{x}, \mathbf{y}]]_0^n$ such that $F \equiv A\mathbf{x} + B\mathbf{y} \bmod (\mathbf{x}, \mathbf{y})^2$ with $A \in \mathrm{Mat}_n(R)$ and $B \in \mathrm{GL}_n(R)$. Then there is a unique $\iota \in R[[\mathbf{x}]]_0^n$ such that $F(\mathbf{x}, \iota(\mathbf{x})) = 0$.*

Proof. Note that $R[[\mathbf{x}]]$ is complete with respect to the ideal $\mathfrak{m} = (\mathbf{x})$, and the derivative matrix of $F(\mathbf{x}, \iota)$ with respect to ι is B, which is invertible, and

$\iota = 0$ gives a solution modulo $\mathfrak{m}$. If F is a polynomial, this means the existence and uniqueness of ι follow directly from the multivariate version of Hensel's lemma (Corollaire 2 of [Bou98, III,4.5]). Now for general $F \in R[[\mathbf{x}, \mathbf{y}]]_0^n$, let $F_j \in R[\mathbf{x}, \mathbf{y}]_0^n$ consist of all terms in F of degree at most j, and let ι_j be the unique power series in $R[[\mathbf{x}]]_0^n$ such that $F_j(\mathbf{x}, \iota_j) = 0$. Note that both ι_j and ι_{j+1} are solutions to $F_j(\mathbf{x}, \iota) \equiv 0 \bmod \mathfrak{m}^j$, so by the uniquess guaranteed by Hensel's lemma used over $R[[\mathbf{x}]]/\mathfrak{m}^j$, these must be equal. Hence they converge to $\iota \in R[[\mathbf{x}]]_0^n$, which is the unique solution of $F(\mathbf{x}, \iota(\mathbf{x})) = 0$. □

This has the following corollary about the inverse of a power series.

Corollary 3.6. *Let* $\mathbf{x}$ *have length* n. *Let* $a \in R[[\mathbf{x}]]_0^n$ *with* $a \equiv P\mathbf{x} \bmod (x)^2$ *for some matrix* $P \in \mathrm{GL}_n(R)$. *Then there is a unique* $b \in R[[\mathbf{x}]]_0^n$ *such that* $a \circ b = b \circ a = x$.

Proof. Let $F(\mathbf{x}, \mathbf{y}) = \mathbf{x} - a(\mathbf{y})$. This satisfies the conditions of Lemma 3.5, so we find a unique b such that $a \circ b = \mathbf{x}$. Applying Lemma 3.5 again gives a unique c such that $b \circ c = \mathbf{x}$. But then $a = a \circ (b \circ c) = (a \circ b) \circ c = c$ shows $a = c$ and hence we are done. □

So a formal group F does have a right inverse ι_F. Also, by $F(0, 0) = 0$ we have that $F(\mathbf{x}, F(\iota_F, 0)) = 0$ so $F(\iota_F, 0)$ is in fact equal to ι_F; as $\iota_F \equiv -\mathbf{x} \bmod (\mathbf{x})^2$, it has a formal inverse and hence $F(\mathbf{x}, 0) = \mathbf{x}$, so 0 is indeed a right unit. A standard argument now shows that ι_F is also a left inverse and 0 is also a right unit, so F is indeed a group law in the following sense. We consider the category of pairs of objects (A, I) where A is a topological R-algebra, complete with respect to I with the I-adic topology. We give $(R[[\mathbf{x}]], (\mathbf{x}))$, together with the $(\mathbf{x})$-adic topology, the structure of a group object in this category for two continuous morphisms f_1, f_2 from $(R[[\mathbf{x}]], (\mathbf{x}))$ to (A, I), given by sending $\mathbf{x}$ to $\mathbf{a}_1, \mathbf{a}_2 \in I^n$ respectively, we define $(f_1 \oplus f_2)(x) = F(\mathbf{a}_1, \mathbf{a}_2)$. By our considerations, this makes $\mathrm{Hom}((R[[\mathbf{x}]], (\mathbf{x})), (A, I))$ into a group, functorially in (A, I).

Given a smooth scheme G of relative dimension d over a ring R, together with a R-point e, we can look at the completion $\widehat{\mathcal{O}}_{G,e}$ along the section e. By smoothness, after picking parameters, this is isomorphic as a topological R-algebra to the ring of power series $R[[x_1, \ldots, x_d]]$. This completion naturally gives rise to a formal scheme denoted $\mathrm{Spf}\, \widehat{\mathcal{O}}_{G,e}$; in a categorical view, this is a functor on finite length R-algebras sending A to $\mathrm{Hom}_{\mathrm{cont}}(\widehat{\mathcal{O}}_{G,e}, A)$, but we can also think of it as a locally ringed space with $\mathrm{Spec}\, R$ as topological

space, and sheaf of rings the inverse limits of the sheaf of rings associated to the R-algebra $\mathcal{O}_{G,e}/I^n$, where I is the ideal of $\mathcal{O}_{G,e}$ defining e. The global sections of this sheaf are simply $\widehat{\mathcal{O}}_{G,e}$.

If furthermore G is a group scheme over R and e is the unit section, then this formal scheme promotes to a formal group scheme, i.e. for every finite R-algebra A the set $\mathrm{Hom}_{\mathrm{cont}}(\widehat{\mathcal{O}}_{G,e}, A)$ gets a group structure, functorially in A. By functoriality, this is the same as an continuous coproduct

$$\mu : \widehat{\mathcal{O}}_{G,e} \to \left(\widehat{\mathcal{O}}_{G,e}\right)^{\widehat{\otimes} 2}.$$

After choosing an isomorphism between $\widehat{\mathcal{O}}_{G,e}$ and $R[[x_1, \ldots, x_d]]$, let the power series $F_j \in R[[\mathbf{x}, \mathbf{y}]]$ denote $\mu(x_j)$. Then it is clear that

$$F_G = (F_1, \ldots, F_d)$$

is a d-dimensional formal group scheme, and is commutative if G is commutative.

Example 3.4 (continued)**.** Take $G = \mathbb{G}_m = \operatorname{Spec} \mathbb{Z}_p[u, u^{-1}]$ over $\mathbb{Z}_p$. Then the zero section e is the map sending u to 1, and we can identify the completion $\widehat{\mathcal{O}}_{G,e}$ with the power series ring $\mathbb{Z}_p[[u-1]] \cong \mathbb{Z}_p[[x]]$, sending $u - 1$ to x. The group structure on G then gives rise to the coproduct $\mathbb{Z}_p[[u-1]] \to \mathbb{Z}_p[[u-1, v-1]], u \mapsto uv$ so the coproduct on $\mathbb{Z}_p[[x]]$ sends x to $uv - 1 = (x+1)(y+1) - 1 = x + y + xy$. Hence the formal group $F_{\mathbb{G}_m}$ corresponding to this group scheme is exactly the multiplicative formal group from Example 3.4.

Note that if $R = \mathbb{Z}_p$, the formal group F_G tells us exactly how multiplication works on $G(\mathbb{Z}/p^e\mathbb{Z})_0$; if we let $t = (t_1, \ldots, t_d)$ denote the formal parameters giving the isomorphism $\widehat{\mathcal{O}}_{G,e} \to \mathbb{Z}_p[[x_1, \ldots, x_d]]$, and we represent a point P in $G(\mathbb{Z}/p^e\mathbb{Z})_0$ by their parameter values $t(P) \in p\mathbb{Z}/p^e\mathbb{Z}$, then the resulting multiplication on $p\mathbb{Z}/p^e\mathbb{Z}$ obtained from the group structure on $G(\mathbb{Z}/p^e\mathbb{Z})_0$, i.e. the map $p\mathbb{Z}/p^e\mathbb{Z} \times p\mathbb{Z}/p^e\mathbb{Z} \to p\mathbb{Z}/p^e\mathbb{Z}$, is exactly evaluating F_G. By taking limits, F_G also gives the multiplication on $G(\mathbb{Z}_p)_0$.

Now we will look at some standard results on formal groups. For an n-dimensional formal group F over a ring R, Proposition 1.1 of [Hon70] gives us a canonical R-basis $\omega_1, \ldots, \omega_n$ of the right invariant differentials; these are elements of $\bigoplus_{j=1}^n R[[\mathbf{x}]]\, \mathrm{d}x_j$. If the formal group is furthermore commutative,

then by Proposition 1.3 of [Hon70] these are closed, i.e. $d\omega_j = 0$. A 1-form $\omega = \sum_{i=1}^n f_i \, \mathrm{d}x_i$ being closed means exactly that $\frac{\partial f_i}{\partial x_j} = \frac{\partial f_j}{\partial x_i}$ for all i, j. From now on, assume R has no torsion; then R embeds into $\mathbb{Q} \otimes R$ and, we can formally integrate ω, i.e. write it as df where $f \in (\mathbb{Q} \otimes R)[[\mathbf{x}]]$. We make this unique by demanding that $f(0) = 0$. Writing this f as $\sum_{I \in \mathbb{N}^n} a_I x^I$ with I denoting a multi-index and $a_I \in \mathbb{Q} \otimes R$, we see that a_I, although itself not necessarily lying in R, is close: writing $I = (I_1, \ldots, I_n)$ we see that for all j we must have $I_j a_I \in R$ as $f_j = \frac{\partial f}{\partial x_j} \in R[[\mathbf{x}]]$.

In particular, we write $\log_i$ for the unique element of $(\mathbb{Q} \otimes R)[[\mathbf{x}]]_0$ such that $d \log_i = \omega_i$. Together, these $\log_i$ give an element $\log \in (\mathbb{Q} \otimes R)[[\mathbf{x}]]_0^n$, and by Theorem 1 of [Hon70], this logarithm satisfies $\log(\mathbf{x}) = \mathbf{x} \bmod (\mathbf{x})^2$, and $\log(F(\mathbf{x}, \mathbf{y})) = \log(\mathbf{x}) + \log(\mathbf{y})$. By the first result, log has an inverse which we will call exp, also given by power series in $(\mathbb{Q} \otimes R)[[\mathbf{x}]]_0^n$, and also satisfying $\exp(\mathbf{x}) = \mathbf{x} \bmod (\mathbf{x})^2$.

Example 3.4 (continued)**.** Taking F again the multiplicative formal group as in Example 3.4, Proposition 1.1 of [Hon70] gives us $\omega = \frac{1}{x+1} dx$; as a power series this is $\sum_{j \geq 0} (-x)^j dx$. The formal anti-derivative of this is

$$\log = \sum_{j \geq 1} \frac{-(-x)^j}{j}$$

(note this is a translate of the log from analysis), and Theorem 1 of [Hon70] will tell us what we already know in the context of analysis, namely the formula $\log(x + y + xy) = \log(x) + \log(y)$ (this formula is also a translate of the corresponding formula from analysis). Then analysis will also explicitly tell us what exp looks like: $\exp(x) = \sum_{j \geq 1} \frac{x^j}{j!}$.

Now we will see how we can use this formal logarithm in our case of the formal group F_G stemming from a d-dimensional smooth group scheme $G/\mathbb{Z}_p$. Recall from Section 2 that we have a bijection $G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d \to \mathbb{Z}_p^d$ given by evaluating at parameters $t = (t_1, \ldots, t_d)$ and then dividing by p; furthermore, recall that the group structure on $G(\mathbb{Z}_p)_0$ is the same as the group structure defined by F_G on $p\mathbb{Z}_p^d$. Let $\log \in \mathbb{Z}_p[[\mathbf{x}]]^d$ denote the logarithm corresponding to F_G, and let $\log_p$ denote the power series

$$\log(p\mathbf{x})/p = (\log_1(p\mathbf{x})/p, \ldots, \log_d(p\mathbf{x})/p).$$

We then have the following little lemma to bridge the gap between power series and maps.

Lemma 3.7. *With notation as above, we have the following statements about* $\log_p$*, the first two of which also hold for* $p = 2$*:*

1. $\log_p$ *lies in* $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle^d$*, the ring of convergent power series, and hence defines a map* $\log_p : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$*.*

2. *Letting* $\oplus$ *denote the group structure on* $\mathbb{Z}_p^d$ *coming from the bijection* $G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d \to \mathbb{Z}_p^d$*, the map* $\log_p$ *is a group morphism from* $(\mathbb{Z}_p^d, \oplus)$ *to* $(\mathbb{Z}_p^d, +)$*.*

3. *If* $p > 2$*, the map* $\log_{p,i}$ *reduces to* x_i *modulo* p *and hence* $\log_p$ *has an inverse* $\exp_p$*, which is also an element of* $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle_0^d$*. Then this* $\exp_p$ *is a two-sided inverse of* $\log_p$*, and hence* $\log_p : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ *is a bijection.*

4. *Let* $m \in \mathbb{Z}_{>0}$*. For* $p > m + 1$*, the maps* $\log_p$ *and* $\exp_p$ *are of degree at most* m *modulo* p^m*.*

Proof. Write $\log_i = \sum_I a_{i,I}\mathbf{x}^I$ and $\log_{p,i} = \sum_I a_{i,I}p^{|I|-1}\mathbf{x}^I$ where I ranges over the multi indices, and $|I| = \sum_{i=1}^d I_i$. Recall that $a_{i,0} = 0$. Also, recall that although a priori the coefficients a_I lie in $\mathbb{Q}_p$, we have $I_j a_{i,I} \in \mathbb{Z}_p$ for all I and i, j. For purposes of easy estimation, this also means $|I|a_{i,I} \in \mathbb{Z}_p$. As we have, with no constraint on p, for all $n \geq 1$ that $c_n \coloneqq p^{n-1}/n$ lies in $\mathbb{Z}_p$ and converges to 0, this means that

$$\log_{p,i} = \sum_I a_{i,I}p^{|I|-1}\mathbf{x}^I = \sum_I |I|a_{i,I}c_{|I|}\mathbf{x}^I$$

is indeed an element of $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle^n$, and hence defines a map $\mathbb{Z}_p^d \to \mathbb{Z}_p$. Hence all the $\log_{p,i}$ together give a map $\mathbb{Z}_p^d \to \mathbb{Z}_p^d$. By the equality of power series $\log(F(\mathbf{x}, \mathbf{y})) = \log(\mathbf{x}) + \log(\mathbf{y})$ from the definition of the logarithm, and the fact that all these power series converge on $p\mathbb{Z}_p^d$, this $\log_{p,i}$ is indeed a group morphism from $(\mathbb{Z}_p^d, \oplus)$ to $(\mathbb{Z}_p^d, +)$.

To study $\log_p$ modulo p, we note that if $n \geq 3$, then p actually divides c_n, and for $p > 2$ we even have $p|c_2$. As $\log_{p,i} = x_i \bmod (\mathbf{x})^2$, this means that for $p > 2$ we have

$$\log_{p,i} \equiv \sum_{|I|=1} |I|a_{i,I}c_{|I|}x^I \equiv x_i \bmod p.$$

Note that as $\log_p \equiv \mathbf{x} \bmod (\mathbf{x})^2$, by Lemma 3.6 it has an inverse $\exp_p$ that a priori lies just in $\mathbb{Z}_p[[\mathbf{x}]]_0^n$. Modulo p, this $\exp_p$ must be x, which lies in $\mathbb{Z}_p\langle\mathbf{x}\rangle_0^n$; as $\mathbb{Z}_p\langle\mathbf{x}\rangle$ is p-adically complete, using Hensel's lemma this shows $\exp_p$ is indeed in $\mathbb{Z}_p\langle\mathbf{x}\rangle_0^n$.

Finally, let $m \in \mathbb{Z}_{>0}$ with $p > m+1$. As c_n has p-adic valuation $n-1$ for $n < p$, and p-adic valuation at least $p-2 \geq m$ for $n \geq p$, indeed $\log_p$ has degree at most m modulo p^m. That the same holds for $\exp_p$, follows immediately from the consideration that the set

$$S \coloneqq \{f \in \mathbb{Z}/p^n\mathbb{Z}[\mathbf{x}]_0^d \mid f \equiv \mathbf{x} \bmod p, \forall m \deg(f \bmod p^m) \leq m\}$$

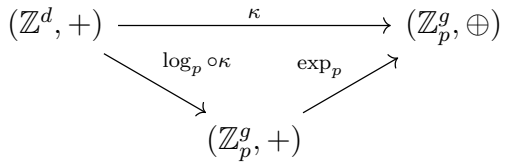
forms a group under composition, as we will now see. As $\mathbb{Z}_p\langle\mathbf{x}\rangle$ is complete, we know the superset of S

$$T \coloneqq \{f \in \mathbb{Z}/p^n\mathbb{Z}[\mathbf{x}]_0^d \mid f \equiv \mathbf{x} \bmod p\}$$

is a group. As S is finite and non-empty, all that remains to show is that S is closed under composition. We can also characterise S as consisting of images $\overline{f}$ of polynomials $f \in \mathbb{Z}_p[\mathbf{x}]_0^d$ such that there is a polynomial $\widetilde{f} \in \mathbb{Z}_p[\mathbf{x}]_0^d$ with $pf(\mathbf{x}) = \widetilde{f}(p\mathbf{x})$. If we then take two elements $\overline{f}, \overline{g} \in S$, reductions of f, g respectively with $\widetilde{f}, \widetilde{g}$ such that $pf(\mathbf{x}) = \widetilde{f}(p\mathbf{x}), pg(\mathbf{x}) = \widetilde{g}(p\mathbf{x})$, we see that with $h = f \circ g, \widetilde{h} = \widetilde{f} \circ \widetilde{g}$ that $ph(\mathbf{x}) = \widetilde{h}(p\mathbf{x})$ and $\overline{h} \equiv \overline{f} \circ \overline{g} \bmod p^m$, so indeed $\overline{f} \circ \overline{g}$ is also an element of S. Hence we see S is indeed a group, and as $\log_p \bmod p^m$ is an element of it, so is $\exp_p \bmod p^m$. □

This lemma makes the proof of Theorem 3.1 relatively easy.

Proof of Theorem 3.1. Write log for the logarithm corresponding to the formal group of J and $\log_p$ for $\log(p\mathbf{x})/p$ and $\exp_p$ for its inverse. Note that the map $\kappa_0 : \mathbb{Z}^d \to \mathbb{Z}_p^g$ given by the inclusion $J(\mathbb{Z}_{(p)})_0$ to $J(\mathbb{Z}_p)_0$ is a group morphism with the group structure on $\mathbb{Z}^d$ being addition and the group structure on $\mathbb{Z}_p^g$, denoted by $\oplus$, given by the bijection with $J(\mathbb{Z}_p)_0$ induced by choosing parameters at 0, and κ is $\kappa_0 \oplus t$. Then by Lemma 3.7 the map κ factors as in the diagram of groups



Then the arrow $\log_p \circ \kappa$ is just a linear map, and $\exp_p$ is a convergent power series that is of degree at most m modulo p^m for $m < p-1$, so their composite κ is also a convergent power series of degree at most m modulo p^m for $m < p-1$. □

This immediately gives rise to the following corollary.

Corollary 3.8. *The map $\kappa : \mathbb{Z}^r \to \mathbb{Z}_p^g$ extends uniquely to a continuous map $\kappa : \mathbb{Z}_p^r \to \mathbb{Z}_p^g$, given by the same power series, and the closure $\overline{J(\mathbb{Z}_{(p)})_t} \subset J(\mathbb{Z}_p)_t$ is given by the image of $\mathbb{Z}_p^r$ under κ.*

4 Computing the intersection

Let p, C and J be as defined in the overview. Clearly, as per the diagram

$$\begin{array}{ccc} C(\mathbb{Z}_{(p)})_P & \longrightarrow & J(\mathbb{Z}_{(p)})_t \\ \downarrow & & \downarrow \\ C(\mathbb{Z}_p)_P & \longrightarrow & J(\mathbb{Z}_p)_t \end{array}$$

we have, as subsets of $J(\mathbb{Z}_p)_t$, the inclusion

$$C(\mathbb{Z}_{(p)})_P \subset C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z}_{(p)})_t}.$$

The theory we have built so far enables the following method, which is in sharp contrast with Coleman's method; instead of pulling back equations for $\overline{J(\mathbb{Z}_{(p)})_t}$ to $C(\mathbb{Z}_p)_P$, we pull back equations for $C(\mathbb{Z}_p)_P$ to $\overline{J(\mathbb{Z}_{(p)})_t}$ to arrive at the following theorem.

Theorem 4.1. *Let $C, J, p, P \in C(\mathbb{F}_p), t \in J(\mathbb{F}_p)$ be as in the overview, let $\kappa : \mathbb{Z}_p^r \to \mathbb{Z}_p^g$ be as in Theorem 3.1 and let $f_1, \cdots, f_{g-1} \in \mathbb{Z}_p\langle x_1, \ldots, x_g\rangle$ be as in Subsection 2.1. Define*

$$\lambda_1 = \kappa^* f_1, \ldots, \lambda_{g-1} = \kappa^* f_{g-1}$$

to be the pullbacks along κ of the f_i. Then κ induces a surjection from $Z(\lambda_1, \ldots, \lambda_{g-1}) \subset \mathbb{Z}_p^r$ to $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z}_{(p)})_t}$.

Hence if we find an upper bound for the cardinality of $Z(\lambda_1, \ldots, \lambda_{g-1})$, this is also an upper bound for $C(\mathbb{Z}_{(p)})_P$. There are several, sometimes ad hoc, ways of proving finiteness. We start by looking simply at calculations modulo p. We let I denote the ideal inside $\mathbb{Z}_p\langle x_1, \ldots, x_r\rangle$ generated by $\lambda_1, \ldots, \lambda_{g-1}$, and A the quotient $\mathbb{Z}_p\langle x_1, \ldots, x_r\rangle / I$. Noting that $Z(\lambda_1, \ldots, \lambda_{g-1})$ is then exactly $\mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)$, we can use the following theorem, the statement and proof of which come from Theorem 4.12 of [EL19].

Proposition 4.2. *Let $\overline{A} = A/pA$. Assume $\overline{A}$ is finite. Then $\overline{A}$ is the product $\prod_{m \in \mathrm{MaxSpec}(\overline{A})} A_m$, and the sum of $\dim_{\mathbb{F}_p} \overline{A}_m$ over those $m \in \mathrm{MaxSpec}(\overline{A})$ with $\overline{A}/m = \mathbb{F}_p$ is an upper bound for $\mathrm{Hom}(A, \mathbb{Z}_p)$.*

Proof. We start by proving that A is p-adically complete. This follows from the following more general fact: let R be a Noetherian ring, and I, J two ideals of R such that R is J-adically complete. We will then prove that R/I is also J-adically complete. By Theorem 10.17 of [AM16], any module over a complete ring injects into its completion, i.e. the map $R/I \to \widehat{R/I}$ is injective. Furthermore, as completion is exact, the surjection $R \to R/I$ gives rise to a surjection $R \to \widehat{R/I}$. The kernel contains I, so the map $R/I \to \widehat{R/I}$ is surjective and hence an isomorphism. Then we observe that $\mathbb{Z}_p\langle x_1, \ldots, x_r\rangle$ is itself the p-adic completion of $\mathbb{Z}_p[x_1, \ldots, x_r]$ and hence is complete, so A is indeed p-adically complete.

Next, we use that $\overline{A}$ is a finite $\mathbb{Z}_p$-module, generated by the image of some finite set $S \subset A$. Using the series of exact sequences

$$0 \to \overline{A} \xrightarrow{\cdot p^{n-1}} A/p^n A \to A/p^{n-1}A \to 0,$$

we see by induction that S indeed generates $A/p^n A$ as a $\mathbb{Z}_p$-module and by completeness, S generates A as well. Hence A is a finite rank $\mathbb{Z}_p$-algebra.

Remember that a finite-dimensional algebra over a field is Artinian, and Artin rings are products of Artin local rings (Theorem 8.7 of [AM16]). So, we can write the $\mathbb{F}_p$-algebra $\overline{A}$ as a product of Artin local rings. As idempotents in $\overline{A}$ lift to A, we see this factorisation lifts, and we can decompose A as

$$A = \prod_{m \in \mathrm{MaxSpec}(\overline{A})} A_m.$$

Then any morphism $A \to \mathbb{Z}_p$ factors through one of the A_m. If we tensor A_m with $\mathbb{Q}_p$, we see that, after dividing out the nilradical, it is a product of

fields. Hence $\mathrm{Hom}(A_m, \mathbb{Z}_p)$ is of cardinality at most $\mathrm{rank}_{\mathbb{Z}_p}(A_m)$, and can be non-empty if and only if A/m is isomorphic to $\mathbb{F}_p$. We conclude that the sum of $\dim_{\mathbb{F}_p} \overline{A}_m$ over those $m \in \mathrm{MaxSpec}(\overline{A})$ with $\overline{A}/m = \mathbb{F}_p$ is an upper bound for $\mathrm{Hom}(A, \mathbb{Z}_p)$ □

To utilise this theorem, we only need to calculate the λ_i modulo p. In our case, as all κ_i and f_i being linear modulo p (as polynomials; they do not necessarily give linear maps), so are the λ_i, and we get as a special case the following corollary.

Corollary 4.3. *If the (not necessarily homogeneous) linear system of equations $\forall i : \lambda_i \equiv 0 \bmod p$ has respectively no or one solution, there is respectively none or at most one point in $C(\mathbb{Z}_{(p)})_P$.*

This leads to a now trivial proposition.

Proposition 4.4. *If for all points $P \in C(\mathbb{F}_p)$, the linear system of $g-1$ equations modulo p defining $C(\mathbb{Z}_p)_P \subset J(\mathbb{Z}_p)_t$ pulled back to $\overline{J(\mathbb{Z}_{(p)})_t}$ has $n_P \leq 1$ solutions, we get the inequality*

$$|C_{\mathbb{Q}}(\mathbb{Q})| = |C(\mathbb{Z}_{(p)})| \leq \sum_{P \in C(\mathbb{F}_p)} n_P \leq |C(\mathbb{F}_p)|.$$

Of note is that this upper bound for $|C(\mathbb{Z}_{(p)})|$ behaves agreeably when compared to the upper bound in Theorem 5.3 of [MP12], which tells us that $|C(\mathbb{Z}_{(p)})| \leq |C(\mathbb{F}_p)| + 2g - 2$ under the much lighter condition of $r < g, p > 2g$ where p is still a prime of good reduction. To summarise: in Proposition 4.4 we sacrifice certainty for being able to prove much sharper bounds. However, the loss of certainty is not too great; a simple heuristic analysis shows that the conditions are quite likely to be satisfied, as we shall see in the following lemma and proposition.

Lemma 4.5. *Let $\mathbb{F}_q$ be any finite field, let A be a random $(n+k) \times n$ matrix over $\mathbb{F}_q$, and b randomly chosen from $\mathbb{F}_q^{n+k}$. Then the probability that $Ax = 0$ has more than one solution is at most $\frac{1}{(q-1)q^k}$ and the probability that $Ax = b$ has more than one solution is at most $\frac{1}{(q-1)q^{2k+1}}$.*

Proof. Let A_i denote the columns of A, let the space V_i be the linear span of $A_1, \ldots, A_i$ with $V_0 = 0$, and let E_i denote the event that $A_i \in V_{i-1}$. Note that

$Ax = 0$ has more than one solution if and only if V_n is not n-dimensional, i.e. if and only if $E_1 \vee \cdots \vee E_n$ holds. As clearly for $1 \leq i \leq n$ we have $\dim V_{i-1} \leq i - 1$, we see that $\mathbb{P}(E_i)$, the probability of E_i occurring, is at most $q^{i-1-n-k}$. We then see

$$\begin{aligned}\mathbb{P}(E_1 \vee \cdots \vee E_n) &\leq \sum_{i=1}^{n} \mathbb{P}(E_i) \\ &\leq \sum_{i=1}^{n} q^{i-1-n-k} \\ &\leq \sum_{i=-\infty}^{n} q^{i-1-n-k} \\ &= \frac{1}{(q-1)q^k}.\end{aligned}$$

This shows that the probability of $Ax = 0$ having more than one solution is indeed at most $\frac{1}{(q-1)q^k}$. Furthermore, if $Ax = 0$ has more than one solution, then $\text{rank}A < n$ so there are at most q^{n-1} possible values of b such that $Ax = b$ has multiple solutions, hence the total probability is at most $\frac{1}{(q-1)q^{2k+1}}$. □

Remark 4.6. Using similar methods, one can show that $\mathbb{P}(E_1 \vee \cdots \vee E_n)$ is at least $\frac{1}{q^{k+1}}$, hence this lemma is asymptotically as sharp as possible.

We now want to use this lemma to say something about the number of solutions to the linear systems of Proposition 4.4. Note that for a point $P \in C(\mathbb{F}_p)$ coming from a $\mathbb{Z}_{(p)}$-point, we always know there is at least one solution to the linear system; and indeed, it turns out that with a translation, one can assume the linear system is homogeneous. For all other points of $C(\mathbb{F}_p)$, we might assume the linear system modulo p defining $C(\mathbb{Z}_p)_P$ pulled back to $\overline{J(\mathbb{Z}_{(p)})}$ is completely random. This motivates the assumptions of the following heuristic.

Proposition 4.7. *Assume that the map $C(\mathbb{Z}_{(p)}) \to C(\mathbb{F}_p)$ is injective. Assume that for points $P \in C(\mathbb{F}_p)$ coming from $C(\mathbb{Z}_{(p)})$ the linear system modulo p defining $C(\mathbb{Z}_p)_P$ pulled back to $\overline{J(\mathbb{Z}_{(p)})_t}$ is a random homogeneous linear system, and for all other points, it is a random not-necessarily-homogeneous*

linear system. Assume furthermore that all these linear systems are independently random. Then for p bigger than both $4g^2$ and $|C(\mathbb{Z}_{(p)})|$ the conditions of Proposition 4.4 are not satisfied with probability at most

$$(|C(\mathbb{Z}_{(p)})| + 2p^{-(g-r-1)})(p-1)^{-1}p^{-(g-r-1)}.$$

Hence for $r = g-1$ we expect a subset of primes with density 1 to show finiteness of $C_{\mathbb{Q}}(\mathbb{Q}) = C(\mathbb{Z}_{(p)})$, and for $r < g-1$ we expect all but a finite number to work. These expectations are uniform in g and $|C(\mathbb{Q})|$.

Proof. First note that our linear systems consist of $g-1$ equalities in r variables, i.e. we can use Lemma 4.5 with $k = g-1-r$. Let a denote $|C(\mathbb{Z}_{(p)})|$, and let b denote $|C(\mathbb{F}_p)| - a$. Under all our assumptions, the probability of none of the systems having more than one solutions is at least

$$\left(1 - \frac{1}{(p-1)p^k}\right)^a \left(1 - \frac{1}{(p-1)p^{2k+1}}\right)^b.$$

Using Bernoulli's inequality and the fact that $1 - a\frac{1}{(p-1)p^k}$ and $1 - b\frac{1}{(p-1)p^{2k+1}}$ are positive, this is at least

$$\left(1 - a\frac{1}{(p-1)p^k}\right)\left(1 - b\frac{1}{(p-1)p^{2k+1}}\right)$$

which is itself at least $1 - a\frac{1}{(p-1)p^k} - b\frac{1}{(p-1)p^{2k+1}}$. Using the Hasse-Weil bound, we can make the estimate $b \leq 2p$. Then we can lower bound this by

$$1 - a\frac{1}{(p-1)p^k} - 2\frac{1}{(p-1)p^{2k}} \geq 1 - (a + 2p^{-k})\frac{1}{(p-1)p^k}.$$

For $r = g-1$ we have $k = 0$, and the probability of one of the conditions not being satisfied is at most $(a+2)/(p-1)$, hence we indeed expect an infinite but density 0 subset of primes to fail. For $r < g-1$, we have $k > 0$; as $\sum_{p \text{ prime}} 1/p^2$ converges, one may expect a finite number of primes to fail. □

Remark 4.8. The author believes that this proposition gives a strong reason to expect the method of only computing modulo p to work in practice; and if it does not, one can just take the next prime.

Remark 4.9. Consider the case $r = g - 1$. As we expect a random $n \times n$-matrix to be invertible, we expect that if the conditions of Proposition 4.4 are satisfied, we generally find an upper bound for $|C(\mathbb{Q})|$ slightly lower than $|C(\mathbb{F}_p)|$. However, a not-necessarily-homogeneous linear system of dimension $(n+k) \times n$ is solvable with probability at most p^{-k}, as the dimension of the column space is at most n. Hence for $r = g - 2$ we can expect to find an upper bound for $|C(\mathbb{Q})|$ of approximately $|C(\mathbb{Q})| + 1$, and with probability approximately $(1 - \frac{1}{p})^{|C(\mathbb{F}_p)|} \approx (1 - \frac{1}{p})^p \approx e^{-1}$ even the optimal upper bound of $|C(\mathbb{Q})|$. For $r = g - 3$, we even expect to find an upper bound of $|C(\mathbb{Q})|$ for a set of primes of density 1; and for $r < g - 3$, for all but a finite set of primes.

Now we briefly discuss what can be done if for a specific prime p, the conditions of Proposition 4.4 are not satisfied. In general, even if $\overline{A}$ is not finite, we see $\mathrm{Hom}(A, \mathbb{Z}_p)$ factors through $\mathbb{Z}_p\langle x_1, \ldots, x_r\rangle / (I : p)$ where $(I : p)$ is the saturation

$$\{x \in \mathbb{Z}_p\langle x_1, \ldots, x_r\rangle \mid \exists k \in \mathbb{Z}_{\geq 0} : p^k x \in I\}.$$

Then a higher precision calculation of the λ_i can still lead to a succesful application of Proposition 4.2.

Another specific case is that of $r = 1$. In that case, we can use finite-precision approximations of λ_1 to deduce information about its Newton polygon and use that to bound the number of zeroes in $\mathbb{Z}_p$. We can even adapt this method if r is bigger than 1; sometimes it might be possible to use the implicit function theorem for power series, Lemma 3.5, to write one of the variables as a power series in the other variables, and then substitute it in the other equations.

Example 4.10. If $r = g - 1 = 2$ and

$$\lambda_1 \equiv px - py, \lambda_2 \equiv x + y + pxy \bmod p^2,$$

neither Proposition 4.2 nor Newton polygons are instantly applicable. However, substituting $y = -x + px^2 \bmod p^2$ into the first equation gives the equation $2p(x - x^2) = 0 \bmod p^2$, or $x - x^2 = 0 \bmod p$. Now both Proposition 4.2 and Newton polygons give an upper bound of 2 for $C(\mathbb{Z}_{(p)})_P$.

5 Complications and improvements

In this section, we quickly make some further remarks on how or when to apply the theory we have built up in previous sections to real cases.

- Even if $r \geq g$, it might still be possible that $\overline{J(\mathbb{Z}_{(p)})}$ coincidentally has dimension r' smaller than r (for example, if $r > g$); then one can find a rank r' subgroup of $J(\mathbb{Z}_{(p)})$ with the same closure inside $J(\mathbb{Z}_p)$, and do computations in this subgroup; we can expect this to work if $r' < g$. We can even use this to improve our calculations if we already have $r < g$, but r' is even smaller. On the other hand, if $J(\mathbb{Z}_{(p)})$ is dense in $J(\mathbb{Z}_p)$, there is no way to apply Chabauty's method to the curve.

- Note that in all of the discussion of the previous section, we are calculating upper bounds for the cardinality of $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z}_{(p)})}_t$. It can and does however happen that this set is strictly bigger than $C(\mathbb{Z}_{(p)})_P$, as shown in [BBCF$^+$19], where Coleman-Chabauty is used on a database of 16997 curves of genus 3 with Mordell-Weil rank of the Jacobian equal to 1. They treat several possible cases and examples where the set is bigger. One of the main families they have found can be given in the following way: let Q be a K-point where K is a quadratic number field where p splits. Embedding K into $\mathbb{Q}_p$, assume $Q - b$ lies in $J(\mathbb{Z}_p)_0$ and is torsion of order coprime to p in $J(\mathbb{Z}_p)_0/J(\mathbb{Z}_{(p)})_0$. Then, as $J(\mathbb{Z}_p)$ is isomorphic as continuous group to $\mathbb{Z}_p^g$, the point $Q - b$ lies in $\overline{J(\mathbb{Z}_{(p)})_0}$, and clearly also in $C(\mathbb{Z}_p)$.

- An important part of doing these calculations is working with the Mordell-Weil group $J(\mathbb{Z}_{(p)}) \cong J(\mathbb{Q})$. Finding generators of $J(\mathbb{Q})$ is as of yet a computationally difficult problem, and one may need to assume the Birch-Swinnerton-Dyer conjecture to even find the rank r. However, when one knows the rank, one does not necessarily need to find generators $J(\mathbb{Q})$; if we can generate a subgroup of $J(\mathbb{Q})$ of index finite and coprime to $p|J(\mathbb{F}_p)|$, it will have the same closure in $J(\mathbb{Z}_p)$. For this, we only need to generate sufficiently many independent points of the Jacobian and saturate subgroups with respect to some primes. Both of these tasks are easier than finding all of $J(\mathbb{Q})$.

- Even if this method does not work for a certain prime p, and neither for some other primes we tried, we can still use parts of the information

we have gathered. For example, maybe the method tells us that we have found all points of $J(\mathbb{Z}_{(p)})$ stemming from $C(\mathbb{Z}_{(p)})$ except those in a certain fibre of the map $J(\mathbb{Z}_{(p)}) \to J(\mathbb{F}_p)$. We can then aggregate this information for different primes, choosing a smooth model of C over for example $\mathbb{Z}[1/n]$ and lifting J as well, by looking at the maps $J(\mathbb{Z}[1/n]) \to \prod_{p \in S} J(\mathbb{F}_p)$ for some set S of primes of good reduction for $C_{\mathbb{Q}}$ not dividing n. This method is called the Mordell-Weil sieve, see for example [BS10] for an introduction.

6 Implementations of linear Chabauty

We now assume that our curve C is hyperelliptic, i.e. given by the degree $2g+2$ homogenisation of an equation of the form

$$y^2 = f(x)$$

inside the weighted projective space $\mathbb{P}(1, g+1, 1)$ where f is a monic polynomial of degree $2g+1$ or $2g+2$. An alternative way of defining such a curve, and the one we will be using mainly, is as a glueing of two affine charts: $y^2 = f(x)$, and $w^2 = f^r(v)$, where $f^r(v)$ is the polynomial $v^{2g+2}f(1/v)$, and a birational map between them is given by $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^{g+1}})$. We also have the coordinates X, Y, Z of $\mathbb{P}(1, g+1, 1)$, with

$$x = X/Z, y = Y/Z^{g+1}, v = Z/X, w = Y/X^{g+1},$$

but beware; $\mathbb{P}(1, g+1, 1)$ is not smooth and hence these coordinates do not behave nicely on all of $\mathbb{P}(1, g+1, 1)$. We mainly use the first chart; we call any point that lies on it an affine point of C. Again for ease of exposition, we will treat the case that f is monic of degree $2g+2$ (in general, one can demand f has degree $2g+2$ by translating f until the constant coefficient is non-zero, and then looking at f^r). In that case, near the line at infinity C looks like $Y^2 = X^{2g+2}$, i.e. $(Y - X^{g+1})(Y + X^{g+1}) = 0$, and we see there are two points $\infty_+ = (1 : 1 : 0)$ and $\infty_- = (1 : -1 : 0)$. Finally, we note that there is an involution on C given by $\sigma(x, y) = (x, -y)$ and $\sigma(v, w) = (v, -w)$.

6.1 Makdisi's algorithms

We work in the Jacobian using Makdisi's representations for divisors. As we are using and adding on to an implementation by Mascot [Mas20], we briefly introduce his notation. This is a summary of Section 2.1 in [Mas20].

We first look at representing $J(k)$ where k is a field. Given a divisor D on C, denote

$$\mathcal{L}(D) = \{f \in k(C)^\times : \mathrm{div}(f) + D \geq 0\} \sqcup \{0\}.$$

We pick an effective divisor D_0 of degree $d_0 \geq 2g+1$; in the case of hyperelliptic curves, we will choose $(g+1)(\infty_+ + \infty_-)$. We set $V_n = \mathcal{L}(nD_0)$. We let n_Z be an integer $\geq 5d_0+1$, and assume, if necessary passing to an extension of k, that we have a set Z of size n_Z of distinct points in $C(k)$ outside the support of D_0; in fact, this will consist of affine points in our case. We have an evaluation map $V_5 \to k^Z$, evaluating a rational function at Z. By our choice of n_Z, this is an injective map, i.e. we can represent rational functions in V_5 by their values in k^Z. In this representation, we can add, subtract, or, if the degree at infinity is not too large, even multiply rational functions, by respectively adding, subtracting, or multiplying the corresponding vectors in k^Z. It is now also possible to represent subspaces of V_5 by giving a basis in k^Z. (Instead of passing to an extension of k, one could also evaluate functions on infinitesimal neighborhoods of k-points, i.e. compute Taylor expansions near those points.)

We now explain the representation of $J(k)$. Note that for any $x \in J(k)$, we have that $x + [D_0]$ is a divisor class of degree at least $2g+1$ and hence is equivalent to an effective divisor $E \geq 0$ of degree d_0. Then we represent x by $\mathcal{L}(2D_0 - E)$ inside V_2; by Riemann-Roch this is a d_W-dimensional subspace of V_2 where $d_W = d_0 + 1 - g$, and in particular we can represent it as a $n_z \times d_W$ matrix, itself representing a subspace of k^Z. This representation is nowhere near unique; there are many different effective divisors E equivalent to $x + D_0$, and many bases for a subspace of k^Z.

As explained in Mascot's article, using this representation one can do all relevant computations in $J(k)$; adding, subtracting, finding the zero element, and very importantly: checking equality. Important from a computational standpoint is the complexity, which we write down in big O notation. As everything is simply linear algebra in spaces of dimensions $O(g)$, the complexity of all these operations, assuming calculations in the ground ring are $O(1)$, are all simply $O(g^\omega)$ where ω is the exponent of matrix multiplication.

6.1.1 Going from $\mathbb{F}_p$ to $\mathbb{Z}/p^e\mathbb{Z}$

We now know how to compute in $J(k)$ for k a field such that $C(k)$ is big enough. In practice, if we want to calculate in $J(\mathbb{F}_p)$, this means passing to

$J(\mathbb{F}_q)$ for some $q = p^a$ with a large enough; by the Hasse-Weil bound this will work. However, for Chabauty we want to compute inside $J(\mathbb{Z}/p^e\mathbb{Z})$. Luckily, Mascot's code takes care of this too, by passing from vector spaces over $\mathbb{F}_p$ to free R-submodules of R^n with $R = \mathbb{Z}/p^e\mathbb{Z}$; in fact, all submodules of R^n we will be seeing are free. That means all these submodules will have good reduction, i.e. they will remain free and of the same rank after tensoring with $\mathbb{F}_p$. If the maps between such modules also have good reduction, then all kernels, images, et cetera will also have these properties, and can first be calculated modulo p using linear algebra, and then Hensel lifted modulo higher powers of p.

The final trick we need is extensions of $\mathbb{Z}/p^e\mathbb{Z}$. As said before, we need n_Z affine points that are distinct modulo p, so we passed from $\mathbb{F}_p$ to an extension $\mathbb{F}_q$. The corresponding notion of an extension of $\mathbb{Z}/p^e\mathbb{Z}$ is given by taking an irreducible polynomial $\overline{T} \in \mathbb{F}_p[t]$ with $\mathbb{F}_q \cong \mathbb{F}_p[t]/\overline{T}$, arbitrarily lifting $\overline{T}$ to a polynomial $T \in \mathbb{Z}/p^e\mathbb{Z}[t]$, and looking at $R = (\mathbb{Z}/p^e\mathbb{Z}[t])/T$. Again, we will only be looking at free submodules of R^n, so we can again do normal linear algebra over $R \otimes \mathbb{F}_p = \mathbb{F}_q$, and using Hensel to lift.

6.2 Implementing the Abel-Jacobi map and Mumford representations

Now that we can do computations with elements in the Jacobian over $\mathbb{Z}/p^2\mathbb{Z}$, it only remains to construct elements in the Jacobian. Explicitly, we want to go from a degree zero divisor to an element in Mascot's representation. Most of the time these divisors are sums of points over the ring we are working with, but sometimes they are given as a so-called Mumford representation.

Definition 6.1. Let C be any (hyper)elliptic curve given by $y^2 = f(x)$ with f of degree $2g+2$ where g is the genus of C. A Mumford representation is a pair (a, b) with a, b polynomials in x, representing the degree 0 divisor $D(a, b)$ on C, given on the first affine chart by the equation $a(x) = 0, y = b(x)$ and on the line at infinity by $(-\deg a)\infty_+$. Such a pair a, b is required to satisfy that

1. the polynomial b is of degree at most $\deg a - 1$;
2. the polynomial a is monic of degree at most $g + 1$;
3. the polynomial a divides $b^2 - f$.

Remark 6.2. If b does not satisfy the first condition, we can reduce b modulo a. If a does not satisfy the second condition, we can use the formula that on the first affine chart, we have

$$D(a,b) + D\left(\frac{f-b^2}{a}, b\right) = (y-b)$$

meaning that with additional calculations of the behaviour of $(y-b)$ at infinity we can express $[D(a,b)]$ in the Jacobian in terms of $D(\frac{f-b^2}{a}, b)$, and if $\deg a$ is strictly bigger than $g+1$, the degree of $\frac{f-b^2}{a}$ is at most $\deg a - 2$.

We will treat how to explicitly compute both the Abel-Jacobi embedding and divisors in Mumford representation in Makdisi's representation for the Jacobian. We start with the Abel-Jacobi embedding

$$\begin{aligned} j_{\infty_+} : C &\to J \\ P &\mapsto P - \infty_+. \end{aligned}$$

We will only need $j_{\infty_+}(P)$ and $j_{\infty_-}(P)$ for affine points P; as the calculation of $j_{\infty_-}(P)$ is entirely similar to $j_{\infty_+}(P)$, we only focus on $j_{\infty_+}(P)$. For this, we present the following algorithm:

Algorithm 1: The Abel-Jacobi embedding

Data: C, J, an affine point $P \in C(R)$ where $R = \mathbb{Z}/p^e\mathbb{Z})$
Result: A space of the form $\mathcal{L}(2D_0 - E)$ where $E - D_0 = P - \infty_+$ as divisors and $E \geq 0$

1 $Z' \leftarrow Z \sqcup \{P\}$;
2 $B = (b_1, \ldots, b_{g+3}) \leftarrow$ a basis of $\mathcal{L}(D_0)$;
3 **if** $(f^r)'(0) \neq 0$ **then**
4 $\quad F \leftarrow x^{g+1} + y$;
5 **else**
6 $\quad F \leftarrow x^{g+1} + x^g + y$;
7 **end**
8 $b_{g+4} \leftarrow xF$;
9 $W \leftarrow$ a $(n_Z + 1) \times (g + 4)$ matrix with rows being the evaluations of $B \sqcup b_{g+4}$ on a point in Z'.;
10 $V \leftarrow \ker(\operatorname{im} W \subset R^{nz+1} \to R)$, the projection on the last coordinate.;
11 $U \leftarrow \operatorname{im}(V \to R^{nz})$, where the last map is the projection on the first coordinates.;
12 Return U;

Proposition 6.3. *Algorithm 1 gives correct output.*

Before proving this proposition, we start with a quick lemma.

Lemma 6.4. *The poles of F, as defined in line 4 or 6, are $g(\infty_+ + \infty_-) + \infty_+$.*

Proof. We start by recalling that at the other affine patch, the curve C is given by $w^2 = f^r(v)$ and by the assumption that f is monic of degree $2g + 2$ we have $f^r(0) = 1$. The points $\infty_\pm$ correspond to $(v, w) = (0, \pm 1)$ in this patch. Letting $g^r(v)$ be the polynomial $(f^r(v) - 1)/v$, we can rewrite the equation for C to $(w-1)(w+1) = vg^r(v)$. As the derivative of $(w-1)(w+1)$ to w does not vanish at both of $\infty_\pm$, we see that v is a uniformiser at both these points. That means that $v_{\infty_\pm}(x)$, the order of x at $\infty_\pm$, is equal to -1.

Now, if $g^r(0)$ is non-zero, then $w - \pm 1$ is also a uniformiser at $\infty_\pm$ and non-zero at $\infty_\mp$, so

$$(w+1)/v^{g+1} = y + x^{g+1}$$

has poles exactly $(g+1)(\infty_+ + \infty_-) - \infty_-$ as we wanted to show. And if $g^r(0)$ is zero, then $v_{\infty_\pm}(w - \pm 1)$ is at least 2 so $w - \pm 1 + v$ is a uniformiser at $\infty_\pm$ and non-zero at $\infty_\mp$, so

$$(w+1+v)/v^{g+1} = y + x^{g+1} + x^g$$

again has the right poles. □

Remark 6.5. Clearly, the complexity of Algorithm 1 is $O(g^\omega)$. For a point in the Jacobian that is represented as $\sum P_i - gb$, this gives an $O(g^{\omega+1})$ algorithm for computing it in Makdisi's representation.

Proof of Proposition 6.3. First note that by Riemann-Roch, the dimension of $\mathcal{L}(D_0)$ is $g+3$, and we also have by the proof of the previous lemma that $1, x, \ldots, x^{g+1}, y$ all lie in $\mathcal{L}(D_0)$ and hence form a basis, so we can indeed find B as in line 2. Note that by Lemma 6.4 the element b_{g+4} lies in $\mathcal{L}(D_0 + \infty_+)$ but not in $\mathcal{L}(D_0)$, so as adding a point to a divisor causes the the dimension to increase by at most 1, we have that $b_1, \ldots, b_{g+4}$ is a basis for $\mathcal{L}(D_0 + \infty_+)$; that it is in fact a basis is evident as this argument tells us it is a basis when tensored with $\mathbb{F}_p$.

Evaluating $\mathcal{L}(D_0 + \infty_+)$ on P gives a linear map $\mathcal{L}(D_0 + \infty_+) \to R$, and the kernel is exactly $\mathcal{L}(D_0 + \infty_+ - P)$; this is the resulting U in line 10. Furthermore we have the equality of divisors $P - \infty_+ = E - D_0$ where $E = P + D_0 - \infty_+ \geq 0$, so $\mathcal{L}(D_0 + \infty_+ - P)$ is as a subspace of V_2 equal to $\mathcal{L}(2D_0 - E)$. This last term is in fact in Mascot's representation, so this represents $P - \infty_+$ in the Jacobian. □

Now we move on to the Mumford representation. We present a way to go from the Mumford representation of a divisor to a Makdisi representation for the corresponding point on the Jacobian. This is based on private correspondence between Mascot and the author.

Algorithm/proof. Let (a, b) be the Mumford representation of a divisor D. Let $\deg a = d \leq g$, and denote D_{aff} for the affine part of D. Note that $E - D_0 = D$ for $E = D_0 + D_{\text{aff}} - d\infty_+$, an effective divisor, so $\mathcal{L}(2D_0 - E) = \mathcal{L}(D_0 - D)$ is a Makdisi representation for $[D]$.

Of course, we can rewrite $\mathcal{L}(D_0 - D)$ as

$$\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+ - D_{\text{aff}}) \\ = \mathcal{L}(2D_0 - D_{\text{aff}}) \cap \mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+).$$

We first calculate $\mathcal{L}(2D_0 - D_{\text{aff}})$. Over $\mathbb{F}_p$ we have the equality

$$\mathcal{L}(2D_0 - D_{\text{aff}}) \\ = a(x)\mathcal{L}((2g+2-d)(\infty_- + \infty_+)) + (y - b(x))\mathcal{L}((g+1)(\infty_- + \infty_+)).$$

Note all these Riemann-Roch spaces are of the form $H^0(C_{\mathbb{F}_p}, \mathcal{F}_{\mathbb{F}_p})$ where $\mathcal{F}$ is an invertible $\mathcal{O}_{C_{\mathbb{Z}/p^k\mathbb{Z}}}$-module on $C_{\mathbb{Z}/p^k\mathbb{Z}}$ of degree higher than $2g-2$. Hence by Serre duality, $h^1(C_{\mathbb{F}_p}, \mathcal{F}_{\mathbb{F}_p}) = 0$. That means the base change map

$$H^1(C_{\mathbb{Z}/p^k\mathbb{Z}}, \mathcal{F}) \otimes \mathbb{F}_p \to H^1(C_{\mathbb{F}_p}, \mathcal{F}_{\mathbb{F}_p}) = 0$$

is surjective, and by Theorem III.12.11 of [Har77] an isomorphism. Because $H^1(C_{\mathbb{Z}/p^k\mathbb{Z}}, \mathcal{F})$ is a $\mathbb{Z}/p^k\mathbb{Z}$-module, this means it is 0. Hence we can use Theorem III.12.11b of [Har77] to conclude that the base change map

$$H^0(C_{\mathbb{Z}/p^k\mathbb{Z}}, \mathcal{F}) \otimes \mathbb{F}_p \to H^0(C_{\mathbb{F}_p}, \mathcal{F}_{\mathbb{F}_p})$$

is also an isomorphism, and $H^0(C_{\mathbb{Z}/p^k\mathbb{Z}}, \mathcal{F})$ is a free $\mathbb{Z}/p^k\mathbb{Z}$-module. That means the equality

$$\mathcal{L}(2D_0 - D_{\text{aff}}) \\ = a(x)\mathcal{L}((2g+2-d)(\infty_- + \infty_+)) + (y - b(x))\mathcal{L}((g+1)(\infty_- + \infty_+)).$$

also holds over $\mathbb{Z}/p^k\mathbb{Z}$. Note that both the Riemann-Roch spaces on the right hand side can be easily calculated, as they are generated by the monomials in x, y of the right order at $\infty_\pm$.

For $\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+)$, we first inductively calculate the spaces $W_n := \mathcal{L}(2D_0 - n\infty_-)$. For W_1 we have a basis

$$1, x, \ldots, x^{2g+1}, y, xy, \ldots, x^g y, x^{g+1}y + x^{2g+2}$$

, and for $n \geq 0$ we have by a simple use of Lemma 2.2 of [KM04] that for $1 \leq n \leq g+1$ we have

$$W_n = \{s \in \mathcal{L}(2D_0) \mid s\mathcal{L}(2D_0) \in W_1 \cdot W_{n-1}\}.$$

This is a purely linear constraint, hence simple linear algebra allows us to calculate all W_n for $n \leq g+1$. Finally, we have

$$\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+) = \{s \in \mathcal{L}((g+1+d)(\infty_+ + \infty_-)) \mid sx^{g+1-d} \in W_d\}.$$

Once again noting that we can write down an explicit basis for the space $\mathcal{L}((g+1+d)(\infty_+ + \infty_-))$, we can now calculate $\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+)$ and finish the computation. □

6.3 Parameters at J

Being able to calculate in the Jacobian, we can move on to the final ingredient for explicit computations: parameters at points of J. For any proper, smooth curve C over $\mathbb{Z}_{(p)}$, with a $\mathbb{Z}_{(p)}$-point b, we have a birational map from $C^{(g)}$, the g-fold symmetric product of C, to J, given on points by sending $[(P_1, \ldots, P_g)]$ to $[\sum P_i - gb]$. This map is étale at $[(P_1, \ldots, P_g)]$ if $\mathcal{L}(P_1 + \cdots + P_g)$ has dimension 1 as the fibre of $P_1 + \cdots + P_g - gb$ is exactly $\mathbb{P}\mathcal{L}(P_1 + \cdots + P_g)$. Also, if all P_i are distinct, then the map $C^g \to C^{(g)}$ is étale at $P_1, \ldots, P_g$ as well. Then finding parameters $t_1, \ldots, t_g$ at $Q := [\sum_{i=1}^g P_i - gb]$ just comes down to finding parameters at each of the P_i. In our case of a hyperelliptic curve, this is just an easy computation; for a point (a, b) on the first affine chart, we can take $x - a$ if b is non-zero and y if a is zero. We can also compute the inverse of the map $C(\mathbb{Z}/p^k\mathbb{Z})_{P_i} \to p\mathbb{Z}/p^k\mathbb{Z}$; this is just a simple exercise in Hensel lifting.

This now means $J(\mathbb{Z}_p)_Q$ is parametrised as the product of $C(\mathbb{Z}_p)_{P_i}$. In particular, we have a bijection

$$\prod_{i=1}^{g} C(\mathbb{Z}/p^k\mathbb{Z})_{P_i} \to J(\mathbb{Z}/p^k\mathbb{Z})_Q.$$

As we are able to explicitly compute this map using the Abel-Jacobi map, and we are able to test equality in $J(\mathbb{Z}/p^k\mathbb{Z})$, we can compute the map $(t_1, \ldots, t_g) : J(\mathbb{Z}/p^k\mathbb{Z})_Q \to (p\mathbb{Z}/p^k\mathbb{Z})^g$ by first computing its inverse and storing all found values. This gives an algorithm for computing this map that consists of $O(p^{(k-1)g})$ operations in the Jacobian.

Remark 6.6. We can do this faster at the cost of consistency, by applying another algorithm by Mascot, Algorithm 7 in [Mas20]. This algorithm computes a rational map $J \to \mathbb{P}V_2$, dependent on the choice of some specific

degree effective divisors, with complexity $O(g^\omega)$. Of course, it is trivial to compute parameters in $\mathbb{P}V_2$, but the downside is that the rational map may not need to be defined where we want it to be. In that case, one can just make another choice of effective divisors and construct a different rational map; remember that we only need the map to be defined in our residue disc of choice.

6.4 Interpolating polynomials

The λ_i from Theorem 4.1 are in general not computationally available, as they are power series, but we can approximate them modulo powers of p. For example, we know that the λ_i are linear modulo p. And in particular, if $f_1, \ldots, f_{g-1}$ are as in Remark 2.6, then $\lambda_i = \kappa_i$ for $i \leq g-1$, so they are also of degree at most m modulo p^m for $m < p-1$. Knowing this, we can compute λ_i modulo powers of p by interpolation, and the following formula, coming from [Sal45]: if f is a polynomial over a ring R of degree m in n variables and $m!$ is a unit in R, then we have the equality of polynomials

$$f(x_1, \ldots, x_n) = \sum_{i_1+\cdots+i_n \leq m} f(i_1, \ldots, i_n) \binom{m - x_1 - \cdots - x_n}{m - i_1 - \cdots - i_n} \prod_{j=1}^{n} \binom{x_j}{i_j}.$$

Note that this formula requires evaluation of f at $\binom{m+n}{n}$ points; this is clearly optimal, as there are $\binom{m+n}{n}$ monomials of degree at most m. Also note that for $m = 1$, the complexity of calculating this formula is simply $O(n)$ applications of f, and $O(n)$ calculations in R.

Note that evaluating λ_i at a point in $J(\mathbb{Z}_{(p)})_t$ comes down to calculating the value of a parameter at that point, and this is something we can do. That means we can explicitly compute λ_i modulo p^m for $m < p-1$. Using Proposition 4.2 or another way, we can hope to find an upper bound on the number of common zeroes of the λ_i, and hence an upper bound on $C(\mathbb{Z}_{(p)})_P$.

This formula for interpolation unfortunately does not work for $m \geq p$; then the values of λ_i on $\mathbb{F}_p^n$ do not determine λ_i, and one needs to evaluate on extensions on $\mathbb{F}_q^n$ and look for more general interpolation formulas (e.g., Lagrange interpolation).

6.5 Complexity

We assume necessary data for the Mordell-Weil group of the Jacobian is given; that is, we have a set of generators for either $J(\mathbb{Z}_{(p)})$, or just a full

rank subgroup of index coprime to $p|J(\mathbb{F}_p)|$. We also assume that all relevant elements in $J(\mathbb{Z}_{(p)})$ and $J(\mathbb{F}_p)$ are in the subgroup generated by $C(\mathbb{Z}_{(p)})$ and $C(\mathbb{F}_p)$. Finally, we assume that we can find rational maps $J \to \mathbb{P}V_2$ as in Remark 6.6.

Then by Remark 6.5 and Section 6.4, we compute $\lambda_i \bmod p$ in $O(rg^{\omega+1})$; then solving the linear system of equations $\forall i \lambda_i \equiv 0 \bmod p$ has complexity lower than that, and hence checking if $|C(\mathbb{Z}_{(p)})_P|$ is at most 1 can be done in $O(rg^{\omega+1})$. Repeating this for all $\mathbb{F}_p$-points, gives by the Hasse-Weil bound a complexity of $O\left((p + g\sqrt{p})rg^{\omega+1}\right)$.

7 An explicit example

We treat the hyperelliptic curve $C_{\mathbb{Q}}/\mathbb{Q}$ with first affine chart given by

$$y^2 = f(x) = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1.$$

This curve has genus 2, and the Mordell-Weil group is isomorphic to $\mathbb{Z}$. This curve is also treated in Example 8.2 of [MP12].

We denote the standard involution on this curve by σ. It has six known rational points $\infty_+, \infty_- = \sigma(\infty_+)$ and $\theta = (0,1), \sigma(\theta), \eta = (-3,1), \sigma(\eta)$. We take $p = 5$, and use the same equation for the model C over $\mathbb{Z}_{(5)}$. It turns out that $C(\mathbb{F}_5)$ has seven points; the reductions of the rational points, and $(1,0)$. Again taking the map $C \to J$ to be subtraction of ∞_+ on points, all seven points in $C(\mathbb{F}_5)$ lie in the image of $J(\mathbb{Z}_{(p)})$.

We will first show there is at most one point in the same residue disc as θ. As we already know there is at least one point, namely θ, we can simplify the calculations by looking at the map $j_\theta : C \to J$ to be subtraction of θ. Letting θ_μ for $\mu \in \mathbb{F}_p$ denote the deformations of θ in $C(\mathbb{Z}/p^2\mathbb{Z})_\theta$, with $\theta_\mu \mapsto \mu$ being a parameter at θ, we see the image of $C(\mathbb{Z}/p^2\mathbb{Z})_\theta$ in $J(\mathbb{Z}/p^2\mathbb{Z})_0$ is $\{\theta_\mu - \theta \mid \mu \in \mathbb{F}_p\}$. Also, identifying $J(\mathbb{Z}_{(p)})_0$ with $\mathbb{Z}^r$, the image of $J(\mathbb{Z}_{(p)})_0$ in $J(\mathbb{Z}/p^2\mathbb{Z})_0$ can be given as a map $\mathbb{F}_p^r \to J(\mathbb{Z}/p^2\mathbb{Z})_0$. Choosing parameters by giving a local chart $J \to \mathbb{P}(V_2)$, we want to exactly show that the two maps $C(\mathbb{Z}/p^2\mathbb{Z})_\theta \to J(\mathbb{Z}/p^2\mathbb{Z})_0, \mathbb{F}_p^r \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ together form a map $\mathbb{F}_p \oplus \mathbb{F}_p^r \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ with kernel 0. Now that this is a statement in linear algebra, it can be verified easily, and it turns out that indeed the residue disc of $C(\mathbb{Z}_{(p)})$ containing θ contains only θ.

Similarly, it follows that all points in $C(\mathbb{F}_5)$ lift to at most one $\mathbb{Z}$-point. Noting that the group generated by σ acts on $C(\mathbb{Z}_{(p)})$ and has no fixed points, this means $|C(\mathbb{Z}_{(p)})| \leq 6$ so our list of rational points is complete.

Code for the calculations in this section can be found in [Spe20].

8 Quadratic Chabauty

In this section, we attempt to give an introduction to the article [EL19] aimed to introduce all the players in quadratic Chabauty at a slightly slower pace. We will omit all proofs. For further reading, see for example [HL], an in-progress cartoon guide to the article by Edixhoven and Lido.

We start by explaining the idea over $\mathbb{Q}$; we let $C_{\mathbb{Q}}$ be a projective, smooth curve over $\mathbb{Q}$ of genus at least 2, we let $J_{\mathbb{Q}}$ be its Jacobian. We again assume the existence of a rational point $b \in C_{\mathbb{Q}}(\mathbb{Q})$ and use it to construct an embedding $j_b : C_{\mathbb{Q}} \to J_{\mathbb{Q}}$. We wish to set up a similar situation to classic Chabauty, and for that, we introduce the Poincaré line bundle and Poincaré torsor. For this, we need $J_{\mathbb{Q}}^{\wedge}$, the dual of $J_{\mathbb{Q}}$, which is in fact isomorphic to $J_{\mathbb{Q}}$, taking as isomorphism for example the principal polarisation $\lambda : J_{\mathbb{Q}} \to J_{\mathbb{Q}}^{\wedge}$. This dual parametrises line bundles that are algebraically equivalent to 0 on $J_{\mathbb{Q}}$, and hence we get a universal such line bundle $P_{\mathbb{Q}}$ on $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}$, called the Poincaré line bundle $P_{\mathbb{Q}}$, which also satisfies that both $P_{\mathbb{Q}}|_{0 \times J_{\mathbb{Q}}^{\wedge}}$ and $P_{\mathbb{Q}}|_{J_{\mathbb{Q}} \times 0}$ are trivial.

Example 8.1. If $C_{\mathbb{Q}}$ is an elliptic curve then, identifying $C_{\mathbb{Q}}, J_{\mathbb{Q}}$ and $J_{\mathbb{Q}}^{\wedge}$, we get $P_{\mathbb{Q}} = \mathcal{O}(\Delta - \{0\} \times C_{\mathbb{Q}} - C_{\mathbb{Q}} \times \{0\})$, with the fibres $P_{\mathbb{Q}}|_{,c \times C_{\mathbb{Q}}} \cong \mathcal{O}(c - 0)$ being exactly the degree 0 line bundles on $C_{\mathbb{Q}}$ up to isomorphism.

The object we will be working with is the Poincaré torsor, the $\mathbb{G}_m$ torsor over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}$ defined by

$$P_{\mathbb{Q}}^{\times} = \mathrm{Isom}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}}(\mathcal{O}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}}, P_{\mathbb{Q}}).$$

We can also describe this in terms of its functor of points; for any scheme S over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}$, we have that $P_{\mathbb{Q}}^{\times}(S)$ is the set of isomorphisms between $\mathcal{O}_S$ and $(P_{\mathbb{Q}})_S$, with a free, transitive action of $\mathcal{O}_S(S)^{\times}$, i.e. a pseudotorsor of $\mathcal{O}_S(S)^{\times}$ in the traditional group-theoretic sense (note that this set can be empty).

Furthermore, this Poincaré torsor has a nice structure of a biextension; this means we can think of the fibres $P_{\mathbb{Q},(x,y)}^{\times}$ as being a $\mathbb{G}_m$ above the point

$x \times y$; this structure then gives multiplication maps

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

and similarly

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

This bilinear structure comes from interpreting $J^{\wedge}_{\mathbb{Q}}$ as $\mathrm{Ext}^1(J_{\mathbb{Q}}, \mathbb{G}_m)$; then $P^{\times}_{\mathbb{Q}}$ is the universal extension of $J_{\mathbb{Q}}$ by $\mathbb{G}_m$, indexed by $J^{\wedge}_{\mathbb{Q}}$, and by duality vice versa as well.

Instead of doing Chabauty in this Poincaré torsor, we will look at a pullback of this torsor to a $\mathbb{G}_m$-torsor over $J_{\mathbb{Q}}$. Our first attempt is pulling back along the map $J_{\mathbb{Q}}$ to $J_{\mathbb{Q}} \times J^{\wedge}_{\mathbb{Q}}$ given as $(\mathrm{id}, \mathrm{tr}_c \circ f)$ where $f : J_{\mathbb{Q}} \to J^{\wedge}_{\mathbb{Q}}$ is a morphism of group schemes and $\mathrm{tr}_c : J^{\wedge}_{\mathbb{Q}} \to J^{\wedge}_{\mathbb{Q}}$ is translation along $c \in J^{\wedge}_{\mathbb{Q}}(\mathbb{Q})$. We denote the pullback of $P^{\times}_{\mathbb{Q}}$ along this map by $T_{\mathbb{Q}}$, a $\mathbb{G}_m$-torsor over $J_{\mathbb{Q}}$. This $T_{\mathbb{Q}}$ has dimension $g + 1$. The general idea of geometric quadratic Chabauty, is to work with the following diagram

$$\begin{array}{ccccc} & & T_{\mathbb{Q}} & \longrightarrow & P^{\times}_{\mathbb{Q}} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ C_{\mathbb{Q}} & \xrightarrow{j_b} & J_{\mathbb{Q}} & \xrightarrow{(\mathrm{id},\mathrm{tr}_c \circ f)} & J_{\mathbb{Q}} \times J^{\wedge}_{\mathbb{Q}} \end{array}$$

where $\widetilde{j_b}$ is a lift of j_b. This lift will only exist if $j_b^* T$ is a trivial $\mathbb{G}_m$-torsor over $C_{\mathbb{Q}}$; for that, it turns out that we want f to be an element of $\mathrm{Hom}^+(J_{\mathbb{Q}}, J^{\wedge}_{\mathbb{Q}})_0$, the group of self dual homomorphisms of trace 0 (where this trace comes from identification with the Néron-Severi group); if we do that, it turns out that $j_b^* T$ will correspond to a degree 0 line bundle on $C_{\mathbb{Q}}$, and we only need to translate by a constant to make $j_b^* T$ trivial.

If f itself is already 0, then T is trivial and this will give no further information, and most of the time that is the best we can do, as generically the rank of $\mathrm{Hom}^+(J_{\mathbb{Q}}, J^{\wedge}_{\mathbb{Q}})$, also called the Néron-Severi rank ρ, is 1. But in many interesting cases, this rank is bigger than 1. Using the isomorphism λ, this rank is also the rank of a certain subgroup of the endomorphism ring of $J_{\mathbb{Q}}$, and it turns out a family of possible examples is given by modular curves; for example, normalisers of non-split Cartan curves $X^+_{\mathrm{ns}}(\ell)$ have Néron-Severi rank equal to the genus, and, according to the BSD conjecture, Mordell-Weil rank at least equal to the genus.

In general, we can pick a basis $f_1, \ldots, f_{\rho-1}$ of the trace 0 subgroup of $\mathrm{Hom}^+(J_{\mathbb{Q}}, J^\wedge_{\mathbb{Q}})$ and elements $c_1, \ldots, c_{\rho-1} \in J^\wedge_{\mathbb{Q}}$ with $j_b^*(\mathrm{id}, \mathrm{tr}_{c_i} \circ f_i)^* P^\times_{\mathbb{Q}}$ trivial, and take the product of all the resulting pullbacks over $J_{\mathbb{Q}}$, to get a $\mathbb{G}_m^{\rho-1}$-torsor T over $J_{\mathbb{Q}}$ that admits a morphism from $C_{\mathbb{Q}}$.

We then would like to intersect the rational points of $T_{\mathbb{Q}}$ with the p-adic points of $C_{\mathbb{Q}}$, mapped to $T_{\mathbb{Q}}$ under $\widetilde{j_b}$, inside the p-adic points of $T_{\mathbb{Q}}$. As in the case of classic Chabauty, one can conclude that the p-adic points of $T_{\mathbb{Q}}$ form a p-adic manifold of dimension $g + \rho - 1$, but there is a problem with the rational points of $T_{\mathbb{Q}}$; these are in bijection with $\mathbb{G}_m(\mathbb{Q})^{\rho-1} \times J_{\mathbb{Q}}(\mathbb{Q})$. The latter is a finitely generated group of rank r, the Mordell-Weil rank, but the former is an infinitely generated group. One can upper bound the dimension of $\overline{T_{\mathbb{Q}}(\mathbb{Q})}$ by $r + \rho - 1$, but it is clear that this will not lead to an improvement to classic Chabauty.

To combat this problem, the crucial insight is that while $\mathbb{Q}^\times$ is infinitely generated, $\mathbb{Z}^\times$ is finite, so we set everything to work over $\mathbb{Z}$ instead of over $\mathbb{Q}$. Our curve is now a surface C, of relative dimension 1 over $\mathbb{Z}$, proper, flat and regular with generic fibre $C_{\mathbb{Q}}$. We cannot expect C to be smooth over $\mathbb{Z}$, we only ask that C is smooth over $\mathbb{Z}[1/n]$ for some squarefree n consisting of bad primes. We let J be the Néron model over $\mathbb{Z}$ of the Jacobian of $C_{\mathbb{Q}}$, and $J^\wedge$ the Néron model of the dual of J. If we want to keep the essential biextension structure of the Poincaré torsor intact, we can only extend to $P \to J \times J^{\wedge 0}$ where $J^{\wedge 0}$ is the connected component of $J^\wedge$ containing 0; the component group $J^\wedge / J^{\wedge 0}$ is only supported on $\mathbb{Z}/n\mathbb{Z}$, i.e. on the bad primes. We let $m \in \mathbb{Z}_{>0}$ be the annihilator of $J^\wedge / J^{\wedge 0}$. We can then make a similar diagram as before

$$\begin{array}{ccccc} & & T & \longrightarrow & P^\times \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ C & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id}, \cdot m \circ \mathrm{tr}_c \circ f)} & J \times J^{\wedge 0} \end{array}$$

where this time f is an element of $\mathrm{Hom}^+(J, J^\wedge)$ of trace 0 and $c \in J^\wedge$ such that $j_b^*(\mathrm{id}, \mathrm{tr}_{c_i} \circ f_i)^* P^\times_{\mathbb{Q}}$ is trivial.

There is one problem: the lift of j_b from C to T only exists if $j_b^* T$ is trivial over C. We know this is true when base changed over $\mathbb{Q}$, and over $\mathbb{Q}$ the lift exists and is unique up to the action of $\mathbb{Q}^\times$. For q prime for which $C_{\mathbb{F}_q}$ has only one component, we can multiply a trivialising section over $C_{\mathbb{Q}}$ by a suitable power of q to make it a trivialising section over $C_{\mathbb{Z}_{(q)}}$. However, we cannot always do this if $C_{\mathbb{F}_q}$ has multiple components.

So instead we cover C^{sm} with multiple opens U_i, obtained by removing for each q dividing n all but one irreducible components. As $C(\mathbb{Z}) = C^{\mathrm{sm}}(\mathbb{Z})$, it is enough to compute $U_i(\mathbb{Z})$ for every U_i. Then the map $j_{b,i} : U_i \to J$ does lift as in the following diagram:

$$\begin{array}{ccccc} & & T & \longrightarrow & P^{\times} \\ & \widetilde{j_{b,i}} \nearrow & \downarrow & & \downarrow \\ U_i & \xrightarrow{j_{b,i}} & J & \xrightarrow{(\mathrm{id}, \cdot m \circ \mathrm{tr}_c \circ f)} & J \times J^{\wedge 0} \end{array}$$

and we can finalise the summary of quadratic Chabauty. Denote T now for the product of all $\rho - 1$ such pullbacks for f ranging over a basis of the trace 0 submodule of $\mathrm{Hom}^+(J, J^\wedge)$. Taking a specific such U with a lift $\widetilde{j_b} : U \to T$, for every prime p, the set $\widetilde{j_b}(U(\mathbb{Z}))$ is a subset of the intersection, inside the p-adic manifold $T(\mathbb{Z}_p)$, of $\widetilde{j_b}(U(\mathbb{Z}_p))$ and the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$. As the relative dimension of T over $\mathbb{Z}_p$ is $g + \rho - 1$ (it is a $\mathbb{G}_m^{\rho-1}$-torsor over J), we can as in Section 2 see that $T(\mathbb{Z}_p)$ has dimension $g + \rho - 1$; and as $\underline{T(\mathbb{Z})}$ is a $\{\pm 1\}^{\rho-1}$-torsor over the group $J(\mathbb{Z})$ of rank r, it will turn out $\overline{T(\mathbb{Z})}$ has dimension at most r. As $U(\mathbb{Z}_p)$ has dimension 1, we can hope that this intersection is dimension 0, and hence finite as $T(\mathbb{Z}_p)$ is compact, if $r < g + \rho - 1$, hence we have an improvement over classical Chabauty.

This argument can be made explicit when looking at residue discs; in short, just like we could parametrise $J(\mathbb{Z})_0$ with $\mathbb{Z}^r$ in Section 3 where the inclusion $\mathbb{Z}^r \to J(\mathbb{Z}_p)_0 \cong \mathbb{Z}_p^g$ is given by convergent power series, it turns out that for $t \in T(\mathbb{F}_p)$ that lift to $T(\mathbb{Z})$, there is a map $\kappa : \mathbb{Z}^r \to T(\mathbb{Z}_p)_t \cong \mathbb{Z}_p^{g+\rho-1}$ such that κ is given by convergent power series and extending the domain of κ to $\mathbb{Z}_p^r$ we have $\kappa(\mathbb{Z}_p^r) = \overline{T(\mathbb{Z})_t}$. This fact is a consequence of the biextension structure of $P^\wedge$; it allows us to quite explicitly move in the Poincaré torsor.

When the parameters at t are chosen nicely, the first g coming from J, it turns out that $\kappa_1, \ldots, \kappa_g$ are linear modulo p, and $\kappa_{g+1}, \ldots, \kappa_{g+\rho-1}$ are quadratic modulo p. The fact that these are quadratic is in fact related to this being called quadratic Chabauty; it has to do with the bilinear structure on $P^\times$, that when restricted to the image of $(\mathrm{id}, \cdot m \circ \mathrm{tr}_c \circ f)$ is a quadratic object, as both of id and $m \circ \mathrm{tr}_c \circ f$ are linear maps. This is analogous to how a bilinear form gives a quadratic form when evaluated at the diagonal. One can also again find equations $g_1, \cdots, g_{r+\rho-2}$ for the the image of $U(\mathbb{Z}_p)$ in $T(\mathbb{Z}_p)_t$, which will again be linear modulo p.

We end with a proposition we already know; Proposition 4.2 also holds in our case, and this once again can lead to giving an explicit upper bound

for the cardinality of residue discs of $U(\mathbb{Z})$ using finite precision calculations; repeating these calculations for the multiple opens U and their $\mathbb{F}_p$-points, finally gives an upper bound for $C(\mathbb{Z})$.

An important part of making the calculations work is forming the map $\widetilde{j_b} : U \to T$. For this, we need to be able to explicitly describe the trivialisation of the $\mathbb{G}_m$-torsor $j_b^* T$ restricted to U. Remember that $j_b^* T$ is also the pullback of $P^\times$ along the map $C \to J \times J^{\wedge 0}$, and this map factors through the diagonal map $C \to C \times C$. As described in Section 7 of the paper, it turns out that giving such a map $f : J \to J^\wedge$ and $c \in J^\wedge(\mathbb{Z})$ with $j_b^* T$ trivial over all opens U is equivalent to giving a line bundle $\mathcal{L}$ on $C \times C$ satisfying the following three properties: $\mathcal{L}$ is rigidified on $\{b\} \times C_\mathbb{Q}$, the fibres of $\mathrm{pr}_2 : (C \times C)_\mathbb{Q} \to C_\mathbb{Q}$ are degree 0, and the pullback $\mathrm{diag}^* \mathcal{L}$ is trivial on $C_\mathbb{Q}$. This turns the problem of describing a map $J \to J^\wedge$ in the sometimes more concrete problem of giving a line bundle on $C \times C$ satisfying some simple conditions.

These line bundles are crucial in doing actual computations. In the example in the Edixhoven-Lido paper, they use an involution of the curve to construct a correct line bundle. Right now, the focus is on doing a modular example, $X_0(73)^+$, a genus 2 curve with endomorphism ring of rank 2. Here, the extra information comes from the Hecke algebra working on the curve, and the problem at the time of writing lies in describing Hecke operators explicitly as correspondences on $C \times C$, and computations with these correspondences over $\mathbb{Z}$.

References

[AM16] Michael Atiyah and Ian Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016.

[BB15] Jennifer Balakrishnan and Amnon Besser. Coleman-Gross height pairings and the p-adic sigma function. *J. Reine Angew. Math.*, 698:89–104, 2015.

[BBCF+19] Jennifer Balakrishnan, Francesca Bianchi, Victoria Cantoral-Farfán, Mirela Çiperiani, and Anastassia Etropolski. Chabauty–Coleman experiments for genus 3 hyperelliptic curves. In *Research Directions in Number Theory*, pages 67–90, Cham, 2019.

[BBM17] Jennifer Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86(305):1403–1434, 2017.

[BD18] Jennifer Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller.

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics. Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[EL19] Bas Edixhoven and Guido Lido. Geometric quadratic Chabauty. *arXiv e-prints*, page arXiv:1910.10752, October 2019.

[Fal83] Gerd Faltings. Endlichkeitssatze fur abelsche Varietaten uber Zahlkorpern. *Invent. Math.*, 73(3):349–366, 1983.

[GD71] Alexander Grothendieck and Jean Dieudonné. *Eléments de géométrie algébrique. I*, volume 166 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1971.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[HL] Sachi Hashimoto and Hannah Larson. A cartoon guide to finding Q-points using geometric quadratic chabauty. `http://math.bu.edu/people/svh/cartoonguide.pdf`. Accessed: 03-04-2020.

[Hon70] Taira Honda. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22(2):213–246, 04 1970.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[Kim09] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.

[Mas20] Nicolas Mascot. Hensel-lifting torsion points on Jacobians and Galois representations. *Math. Comp.*, 89(323):1417–1455, 2020.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[Par00] Pierre Parent. Torsion des courbes elliptiques sur les corps cubiques. *Ann. Inst. Fourier (Grenoble)*, 50(3):723–749, 2000.

[Sal45] Herbert E. Salzer. Note on interpolation for function of several variables. *Bull. Amer. Math. Soc.*, 51:279–280, 1945.

[Spe20] Pim Spelier. Linear chabauty. `https://github.com/pimsp/lin-chabauty`, 2020.