

P. Spelier

A geometric approach to linear Chabauty

Master thesis

May 14, 2020

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



Leiden University
Mathematical Institute

Todo list

Bas, wat vind je van het bestaan van dit hoofdstuk?	6
Bas, je had "category of top. rings" gemarkeerd, waarom?	12
Bas, dit is gelukt wat simpeler te maken, geen lelijke berekeningen meer :) 15	
give proof	17
Bas, ik begrijp het bewijs niet helemaal...	17
Bas, ik ben niet echt groot fan van dit hoofdstuk, voegt het iets toe denk je?	18
finish	18
See [Todo]	25
Make the complexity better	26
Bas, what do I do with my code?	28
Bas, do you agree?	29
This is true, right? Can't find reference	29

Contents

1 Introduction	4
1.1 Overview	5
2 Points on a smooth scheme over \mathbb{Z}_p	8
2.1 From $C(\mathbb{Z}_p)$ to $J(\mathbb{Z}_p)$	9
3 From $J(\mathbb{Z})$ to $J(\mathbb{Z}_p)$	10
3.1 From group schemes to formal groups	10
4 Computing the intersection	16
5 Complications and improvements	18
6 Implementations of linear Chabauty	19
6.1 Makdisis algorithms	20
6.1.1 Going from \mathbb{F}_p to $\mathbb{Z}/p^e\mathbb{Z}$	21
6.2 Implementing the Abel-Jacobi map and Mumford representa- tions	21
6.3 Parameters at J	25
6.4 Interpolating polynomials	26

6.5 Complexity	27
7 An explicit example	27
8 Quadratic Chabauty	28
References	33

1 Introduction

In mathematics a fundamental problem 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 C , a numerical invariant of a curve. 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 an often infinite group.

In this thesis, we look only at the case $g > 1$. It turns out that there are always only finitely many points; this result was originally conjectured by Mordell in 1922 and finally proven by Faltings in 1983.

Before it 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, which 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 points. Loosely said, this proof and all Chabauty related theorems, rely on choosing a prime p for which C has good reduction, and intersecting $J(\mathbb{Z})$ with $C(\mathbb{Z}_p)$ inside the bigger p -adic manifold $J(\mathbb{Z}_p)$; by properties of \mathbb{Z}_p , the subgroup $J(\mathbb{Z}_p)$, generated by r elements, lies within a p -adic manifold of dimension at most r , and $C(\mathbb{Z}_p)$ is a 1-dimensional p -adic manifold, and hence their intersection is expected to be discrete and – as $J(\mathbb{Z}_p)$ is compact – finite.

This was later made into an effective argument by Coleman in 1985. This was done by finding explicitly, as a power series, a differential form ω on $J_{\mathbb{Z}_p}$ whose Coleman integral vanishes on $J(\mathbb{Z})$. Pulling ω back to $C_{\mathbb{Z}_p}$ 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 $C(\mathbb{Z})$ 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 introductory article [MP12].

This Coleman-Chabauty method has been greatly generalised by Kim to so called non-abelian Chabauty. 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. Using quadratic Chabauty, the simplest case of non-abelian Chabauty, Balakrishnan, Dogra, Müller, Tuitman and Vonk famously calculated in May of 2019 all rational

points of the “cursed curve”, the modular curve $X_s^+(13)$. They use an endomorphism of the Jacobian, and do p -adic analysis on p -adic local heights to make quadratic Chabauty explicit.

Very recently, Edixhoven and Lido made available a preprint of their article “Geometric quadratic Chabauty” [EL19]. Their goal in this article is to make a more geometric approach to effective quadratic Chabauty, by working in a pullback T of the Poincaré torsor of the Jacobian. They also abandon the Coleman method for Chabauty; instead they parametrise the map $T(\mathbb{Z}) \rightarrow T(\mathbb{Z}_p)$ with power series, and pull back equations for the curve inside $T(\mathbb{Z}_p)$ along this map.

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 $J(\mathbb{Z})$ and $J(\mathbb{Z}_p)$. In this thesis, we go into more detail of what is happening throughout the process, including both theoretical and practical components. This new method of applying Chabauty leads to, when working modulo p , 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. Heuristics show that generally trying multiple primes p of good reduction will yield good results, and if $r < g - 1$ the conditions hold for most primes. The methods used to obtain Proposition 4.4 are also amenable to higher precision calculations. We also give a hyperelliptic example with $r = 1, g = 2$, where the bound from Proposition ?? indeed holds.

1.1 Overview

We first present the context in which we will perform Chabauty. Let $p > 2$ be a prime, and C be a scheme over \mathbb{Z} , proper, flat, regular with C smooth over $\mathbb{Z}_{(p)}$ and $C_{\mathbb{Q}}$ of dimension 1 and geometrically connected, of genus $g \geq 1$ and with the Jacobian J of C having Mordell-Weil rank $r < g$. Assume we have a \mathbb{Q} -point b in C , or equivalently a \mathbb{Z} -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 $J(\mathbb{Z})$.

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

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

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

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

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 $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}$, where $\overline{J(\mathbb{Z})_t}$ is the closure of $J(\mathbb{Z})_t$ 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 canonically in bijection with respectively \mathbb{Z}_p and \mathbb{Z}_p^g . We also discuss the resulting map $\mathbb{Z}_p \rightarrow \mathbb{Z}_p^g$.

In Section 3 we further look at the map $J(\mathbb{Z})_t \rightarrow J(\mathbb{Z}_p)_t$. This is a translation of the group morphism $J(\mathbb{Z})_0 \rightarrow J(\mathbb{Z}_p)_0$ between kernels of reduction; it turns out that for our choice of p , the subgroup $J(\mathbb{Z})_0$ is free of rank r . We study the properties of the resulting map $\mathbb{Z}^r \rightarrow \mathbb{Z}_p^g$, using the theory of formal groups to determine the group structure on \mathbb{Z}_p^g induced by the bijection $J(\mathbb{Z}_p)_t \rightarrow \mathbb{Z}_p^g$.

In Section 4, we put all of this information together, culminating in several methods to possibly compute upper bounds on $|C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}|$ with finite precision calculations.

These methods are not always guaranteed to prove finiteness of $C(\mathbb{Z})_P$. In Section 5 we treat several possible complications and improvements, partially with explicit examples. We also look at the specific case of calculations modulo p , i.e. in $J(\mathbb{Z}/p^2\mathbb{Z})_t$, in which the theory simplifies.

Next, in Section 6 we focus on how to perform these 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 [Mas18] by Mascot, and also give an original algorithm for explicitly computing the map $C(\mathbb{Z}_p)_P \rightarrow J(\mathbb{Z}_p)_t$ 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.

Bas,
wat
vind
je van
het
bestaan
van
dit
hoofd-
stuk?

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} to make geometric quadratic Chabauty make sense; and we explain some of the problems and solutions that working over \mathbb{Z} gives rise to.

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 $X(\mathbb{Z}_p)_x$ is 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 $X = \text{Spec } A$ is affine and that p, t_1, \dots, t_d generate the maximal ideal of $O_{X,x}$ with t_1, \dots, t_d elements of $O_X(X) = A$, also called *parameters* at x . By shrinking X even more, we may assume as X is smooth that $t = (t_1, \dots, t_d) : X \rightarrow \mathbb{A}_{\mathbb{Z}_p}^d$ is étale. Now consider the blowup $\tilde{X}_x \rightarrow X$ of X at x , and let \tilde{X}_x^p be the part where p generates the inverse image of the maximal ideal of $O_{X,x}$. Equivalently, that is the part where t_1, \dots, t_d are multiples of p , so informally it consists of the points that reduce to x modulo p .

There is an explicit description of the map $\tilde{X}_x^p \rightarrow X$; as t is étale, the ideal of X defining x is the pullback along t of the ideal of $\mathbb{A}_{\mathbb{Z}_p}^d$ defining the origin a over \mathbb{F}_p . That means that the blowup $\tilde{X}_x \rightarrow X$ is the pullback of the blowup $\hat{\mathbb{A}}_{\mathbb{Z}_p,a}^d \rightarrow \mathbb{A}_{\mathbb{Z}_p}^d$. Then the part \tilde{X}_x^p is the pullback of the corresponding part of $\hat{\mathbb{A}}_{\mathbb{Z}_p,a}^d$, i.e. $\text{Spec } \mathbb{Z}_p[\tilde{x}_1, \dots, \tilde{x}_d] = \text{Spec } \mathbb{Z}_p[x_1/p, \dots, x_d/p]$ with the morphism $\mathbb{Z}_p[x_1, \dots, x_d] \rightarrow \mathbb{Z}_p[\tilde{x}_1, \dots, \tilde{x}_d]$ given by $x_i \mapsto p\tilde{x}_i$. That implies that \tilde{X}_x^p is $\text{Spec } A[t_1/p, \dots, t_d/p]$, with the map $\tilde{X}_x^p \rightarrow X$ given by the inclusion $A \rightarrow \text{Spec } A[t_1/p, \dots, t_d/p]$ (remember that the t_i are elements of $O_X(X) = A$).

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

Lemma 2.1. *With X as above, there is a natural bijection $X(\mathbb{Z}_p)_x \rightarrow \tilde{X}_x^p(\mathbb{Z}_p)$,*

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 $\mathcal{O}_{S,s} \rightarrow \mathbb{Z}_p$. In our case, we find that $X(\mathbb{Z}_p)_x$ is naturally in bijection with $\text{Hom}_{\text{local}}(A_x, \mathbb{Z}_p)$. As the maximal ideal of A_x is generated by p, t_1, \dots, t_d , the locality property just means that the images of t_1, \dots, t_d are divisible by p , i.e. exactly those morphisms that extend to a morphism $A[t_1/p, \dots, t_d/p] \rightarrow \mathbb{Z}_p$, i.e. a \mathbb{Z}_p -point of \tilde{X}_x^p . Hence we find the natural bijection. \square

Lemma 2.2. *With X as above, 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 $O(\tilde{X}_x^p)^{\wedge p}$ and the completion $\mathbb{Z}_p\langle\tilde{x}_1, \dots, \tilde{x}_d\rangle$ of $\mathbb{Z}_p[\tilde{x}_1, \dots, \tilde{x}_d]$, with the latter completion being the ring of convergent power series, i.e.

$$\mathbb{Z}_p\langle\tilde{x}_1, \dots, \tilde{x}_d\rangle = \{f \in \mathbb{Z}_p[[\tilde{x}_1, \dots, \tilde{x}_d]] \mid \forall n \geq 0, f \in \mathbb{Z}[\tilde{x}_1, \dots, \tilde{x}_d] + (p^n)\}.$$

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

$$\mathrm{Hom}(O(\tilde{X}_x^p), \mathbb{Z}_p) \rightarrow \mathrm{Hom}(\mathbb{Z}_p\langle\tilde{x}_1, \dots, \tilde{x}_d\rangle, \mathbb{Z}_p) = \mathbb{Z}_p^d.$$

Following all the bijections, we indeed get the bijection we wanted. \square

Remark 2.3. Note that this construction is functorial, as in the following sense: given two smooth schemes X, Y over \mathbb{Z}_p and two \mathbb{F}_p -points $x \in X(\mathbb{F}_p), y \in Y(\mathbb{F}_p)$, a map $f : Y \rightarrow X$ satisfying $f(y) = x$ gives rise to a morphism $\tilde{Y}_y^p \rightarrow \tilde{X}_x^p$. This is a direct consequence of II.7.15 of [Har77]

Remark 2.4. We look at the specific case of X being of relative dimension 1 over \mathbb{Z}_p . It then turns out that there is additionally a free transitive \mathbb{F}_p -action on $X(\mathbb{Z}/p^2\mathbb{Z})_x$, in the following way. We can parametrise $X(\mathbb{Z}/p^2\mathbb{Z})_x$ by $t = t_1 : X(\mathbb{Z}/p^2\mathbb{Z})_x \rightarrow p\mathbb{Z}/p^2\mathbb{Z}$; write P_λ for the point with t -value λp . Then as Cartier divisor, the point P_λ is defined by $t - \lambda p \in O(X_{\mathbb{Z}/p^2\mathbb{Z}})_x$, 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 $J(\mathbb{Z}_p)$

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 $\mathbb{Z}_p \rightarrow \mathbb{Z}_p^g$ is linear modulo p , i.e. by using that $\mathbb{Z}\langle z_1, \dots, z_g \rangle$ is p -adically complete there are power series $f_1, \dots, f_{g-1} \in \mathbb{Z}_p\langle z_1, \dots, z_g \rangle$ such that the image of $C(\mathbb{Z}_p)_P$ is exactly given by $V(f_1, \dots, f_{g-1})$, and all f_i are linear modulo p as a consequence of 2.4. 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, using Remark 2.3.

Remark 2.5. We can pick our parameters right such that $C(\mathbb{Z}_p)_P \rightarrow J(\mathbb{Z}_p)_t$ is given by $\mathbb{Z}_p \rightarrow \mathbb{Z}_p^g$, mapping \mathbb{Z}_p to the last coordinate. Then f_1, \dots, f_{g-1} are just the other parameters at t , so they are linear. This can be done by picking generators f_1, \dots, f_{g-1} for the ideal defining \tilde{C}_P^p inside \tilde{J}_t^p .

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

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

Theorem 3.1. *There are uniquely determined $\kappa_1, \dots, \kappa_g \in \mathbb{Z}_p\langle z_1, \dots, z_r \rangle$ such that for all $x \in \mathbb{Z}^r$ we have $\kappa(x) = (\kappa_1(x), \dots, \kappa_g(x))$ and the image $\overline{\kappa_i}$ of κ_i in $\mathbb{F}_p[z_1, \dots, z_r]$ 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 group 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. First we introduce some notation that will be used in this section. Let R be a commutative ring, and $x = (x_1, \dots, x_n)$ and sometimes y, z are vectors of variables. Then $R[[x]]$ denotes as usual the ring of formal powerseries in the x_i , and $R[[x]]_0$ denotes those power series with constant term 0. With $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_m)$, let $f \in R[[x]]^m$ and assume $f(0) = 0$. Then for $g \in R[[y]]^k$ for some $k \in \mathbb{Z}_{\geq 0}$, we can compose g and f to get $g \circ f := (g_1(f(x)), \dots, g_k(f(x))) \in R[[x]]^k$. This definition makes sense because f^i converges to 0, so for any $a \in R^{\mathbb{Z}_{\geq 0}}$ the sum $\sum_i a_i f^i$ always converges.

3.1 From group schemes to formal groups

We first recall the definition of a formal group. For this entire section, R is a ring, and x, y, z are vectors of variables.

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

Example 3.3. For any n , we can take $F(x, y) = x + y$, 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. This satisfies associativity as $F(F(x, y), z) = (1 + x)(1 + y)(1 + z) - 1 = F(x, F(y, z))$.

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

Lemma 3.5. *Let x, y have length n . Let $F \in R[[x, y]]_0^n$ such that $F \equiv Ax + By \pmod{(x, y)^2}$ with $B \in \text{GL}_n(R)$. Then there's a unique $\iota \in R[[x]]_0^n$ such that $F(x, \iota(x)) = 0$.*

Proof. If F is a polynomial, this is a special case of a multivariate version of Hensel's lemma, as in Corollaire 2 of [Bou98, III,4.5]: we work over $R[[x]]$ which is complete with respect to the ideal $\mathfrak{m} = (x)$, and the derivative matrix of $F(x, \iota)$ with respect to ι is B , which is invertible, and $\iota = 0$ gives a solution modulo \mathfrak{m} . Now for F any power series, let F_j be the polynomial consisting of all terms in F of degree at most j , and let ι_j be the unique power series in $R[[x]]_0^n$ such that $F_j(x, \iota_j) = 0$. Note that both ι_j and ι_{j+1} are solutions to $F_j(x, \iota) \equiv 0 \pmod{\mathfrak{m}^j}$, so by the uniqueness guaranteed by Hensel's lemma used over $R[[x]]/\mathfrak{m}^j$, these must be equal. Hence they converge to $\iota \in R[[x]]_0^n$, which is the unique solution of $F(x, \iota(x)) = 0$. \square

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

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

Proof. Let $F(x, y) = x - a(y)$. This satisfies the constraints of Lemma 3.5, so we find a unique b such that $a \circ b = x$. Applying Lemma 3.5 again gives a

unique c such that $b \circ c = x$. But then $a = a \circ (b \circ c) = (a \circ b) \circ c = c$ shows $a = c$ and hence we are done. \square

So a formal group F does by Lemma 3.5 indeed have a right inverse ι_F . Also, by $F(0, 0) = 0$ we have that $F(x, F(\iota_f, 0)) = 0$ so $F(\iota_f, 0)$ is in fact equal to ι_F ; as $\iota_F \equiv -x \pmod{(x)^2}$, it has a formal inverse and hence $F(x, 0) = x$, 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 gives $R[[x]]$, together with the (x) -adic topology, the structure of a group object in the category of topological rings; for two continuous morphisms f_1, f_2 from $R[[x]]$ to some ring A , given by sending x to a_1, a_2 respectively, we define $(f_1 \oplus f_2)(x) = F(a_1, a_2)$, and by our considerations this makes $\text{Hom}_{\text{cont}}(R[[x]], A)$ into a group, functorially in A .

Bas,
je had
"cat-
egory
of top.
rings"
gemar-
keerd,
waarom?

Given a smooth scheme G over \mathbb{Z}_p of relative dimension d , together with a \mathbb{Z}_p -point e , we can look at the completion $\hat{O}_{G,e}$ along the section e . By smoothness, after picking parameters, this is isomorphic as topological \mathbb{Z}_p -algebras to the ring of power series $\mathbb{Z}_p[[x_1, \dots, x_d]]$. This completion naturally gives rise to a formal scheme denoted $\text{Spf } \hat{O}_{G,e}$; in a categorical notion, this is a functor on finite length \mathbb{Z}_p -algebras sending A to $\text{Hom}_{\text{cont}}(\hat{O}_{G,e}, A)$, but we can also think of it as a locally ringed space with $\text{Spec } \mathbb{Z}_p$ as topological space, and sheaf of rings $\lim_n \hat{O}_{G,e}/m^n$ where m is the maximal ideal of $\hat{O}_{G,e}$. The global sections of these sheaf are simply $\hat{O}_{G,e}$.

If furthermore G is a group scheme over \mathbb{Z}_p , then this formal scheme promotes to a formal group scheme, i.e. for every finite \mathbb{Z}_p -algebra A the set $\text{Hom}_{\text{cont}}(\hat{O}_{G,e}, A)$ gets a group structure, functorially in A . By functoriality, this is the same as an continuous coproduct $\mu : \hat{O}_{G,e} \rightarrow (\hat{O}_{G,e})^{\hat{\otimes} 2}$. After choosing an isomorphism between $\hat{O}_{G,e}$ and $\mathbb{Z}_p[[x_1, \dots, x_d]]$, let $F_j \in \mathbb{Z}_p[[x, y]]$ denote $\mu(x_j)$. Then it is clear that $F_G = (F_1, \dots, F_d)$ is a d -dimensional formal group scheme, and commutative if G was commutative.

Example 3.4 (continued). Take $G = \mathbb{G}_m$ over \mathbb{Z}_p , i.e. $\mathbb{Z}_p[u, u^{-1}]$. Then the zero section e is the map sending u to 1, and we can identify the completion $\hat{O}_{G,e}$ 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 $\mathbb{Z}_p[[u - 1]] \rightarrow \mathbb{Z}_p[[u - 1, v - 1]]$, $u \mapsto uv$ 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_{G_m} corresponding to this group scheme is exactly the multiplicative formal group from Example 3.4.

This formal group tells us exactly how multiplication works on $G(\mathbb{Z}/p^e\mathbb{Z})_0$; if we let $t = (t_1, \dots, t_d)$ denote the formal parameters giving the isomorphism $\hat{O}_{G,e} \rightarrow \mathbb{Z}_p[[x_1, \dots, x_d]]$, 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 multiplication $p\mathbb{Z}/p^e\mathbb{Z} \times p\mathbb{Z}/p^e\mathbb{Z} \rightarrow p\mathbb{Z}/p^e\mathbb{Z}$ is exactly F . By taking limits, F also gives the multiplication on $G(\mathbb{Z}_p)_0$.

Now we will look at the theory of formal groups, and how that will help us. For a n -dimensional formal group F over a ring R , Proposition 1.1 of [HON70] gives us a canonical R -basis $\omega_1, \dots, \omega_n$ of the right invariant differentials; these are elements of $\bigoplus_{j=1}^n R[[x]] dx_j$. 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 $d\omega = \sum_{i=1}^n f_i dx_i$ 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 imbeds into $\mathbb{Q} \otimes R$ and, we can formally integrate ω , i.e. write it as df where $f \in (\mathbb{Q} \otimes R)[[x]]$. 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 $I = (I_1, \dots, I_n)$ we see that for all j we must have $I_j a_I \in R$ as $f_j = \frac{\partial f}{\partial x_j} \in R[[x]]$.

In particular, we write \log_i for the unique element of $(\mathbb{Q} \otimes R)[[x]]$ such that $d\log_i = \omega_i$. Together, these \log_i give an element $\log \in R[[x]]^n$, and by Theorem 1 of [HON70], this logarithm satisfies $\log(x) = x \bmod (x)^2$, and $\log(F(x, y)) = \log(x) + \log(y)$. By the first result, \log has an inverse which we will call \exp , also given by powerseries in $(\mathbb{Q} \otimes R)[[x]]$, and also satisfying $\exp(x) = x \bmod (x)^2$.

Example 3.4 (continued). Taking F the multiplicative 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 $\sum_{j \geq 0} (-x)^j$. The formal anti-derivative of this is $\log = \sum_{j \geq 1} \frac{-(-x)^j}{j} dx$, and Theorem 1 will tell us what we already know in the context of analysis $\log(x + y + xy) = \log(x) + \log(y)$. Then analysis will also explicitly tell us what \exp looks like: namely, $\exp(x) = \sum_{j \geq 1} \frac{x^j}{j!}$.

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 that we have a bijection $G(\mathbb{Z}_p)_0 \rightarrow p\mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$ given by evaluating at parameters $t = (t_1, \dots, t_d)$ 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 $\log \in \mathbb{Z}_p[[x]]^d$ denote the logarithm corresponding to F_G , and let \log_p denote the power series $\log(px)/p = (\log_1(px)/p, \dots, \log_d(px)/p)$. 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 :*

1. \log_p lies in $\mathbb{Z}_p\langle x_1, \dots, x_d \rangle^d$, the ring of convergent power series, and hence defines a map $\log_p : \mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$.
2. Letting \oplus denote the group structure on \mathbb{Z}_p^d coming from the bijection $G(\mathbb{Z}_p)_0 \rightarrow p\mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$, 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 $\mathbb{Z}_p\langle x_1, \dots, x_d \rangle_0^d$. Then this \exp_p is a two-sided inverse of \log_p , and hence $\log_p : \mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$ is a bijection.
4. Let $m \in \mathbb{Z}_{>0}$. For $p > m + 1$, the map \log_p and \exp_p are of degree at most m modulo p^m .

Proof. Write $\log_i = \sum_I a_{i,I} x^I$ and $\log_{p,i} = \sum_I a_{i,I} p^{|I|-1} x^I$ where I ranges over the multi indices. 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 $c_n := p^{n-1}/n$ lies in \mathbb{Z}_p and converges to 0, this means that

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

is indeed an element of $\mathbb{Z}_p\langle x_1, \dots, x_d \rangle^n$, and hence defines a map $\mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$. Hence all the $\log_{p,i}$ together give a map $\mathbb{Z}_p^d \rightarrow \mathbb{Z}_p^d$. By the equality of power series $\log(F(x, y)) = \log(x) + \log(y)$ from the definition of the logarithm, and the fact that all these powerseries 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 $\log_{p,i} = x_i \bmod (x)^2$, this means that for $p > 2$ we have

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

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

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 immediately for \exp_p , follows immediately from the consideration that the set

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

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

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

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 \bar{f} of polynomials $f \in \mathbb{Z}_p[x]_0^d$ such that there is a polynomial $\tilde{f} \in \mathbb{Z}_p[x]_0^d$ with $pf(x) = \tilde{f}(px)$. If we then take two elements $\bar{f}, \bar{g} \in S$, reductions of f, g respectively with \tilde{f}, \tilde{g} such that $pf(x) = \tilde{f}(px), pg(x) = \tilde{g}(px)$, we see that with $h = f \circ g, \tilde{h} = \tilde{f} \circ \tilde{g}$ that $ph(x) = \tilde{h}(px)$ and $h \equiv \bar{f} \circ \bar{g} \bmod p^m$, so indeed $\bar{f} \circ \bar{g}$ 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 $\exp_p \bmod p^m$. \square

This lemma makes the proof of Theorem 3.1 relatively easy.

Proof of Theorem 3.1. Write \log_p for the logarithm corresponding to the formal group corresponding to the The map $\kappa_0 : \mathbb{Z}^d \rightarrow \mathbb{Z}_p^g$ given by the inclusion $J(\mathbb{Z})_0$ 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

Bas,
dit is
gelukt
wat
sim-
peler
te
maken,
geen
lelijke
berekenin-
gen
meer
:)

Lemma 3.7 the map κ factors as in the diagram of groups

$$\begin{array}{ccc} (\mathbb{Z}^d, +) & \xrightarrow{\kappa} & (\mathbb{Z}_p^g, \oplus) \\ & \searrow \log_p \circ \kappa \quad \nearrow \exp_p & \\ & (\mathbb{Z}_p^g, +) & \end{array}$$

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 $m < p - 1$ \square

This immediately gives rise to the following corollary.

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

4 Computing the intersection

Clearly, as subsets of $J(\mathbb{Z}_p)_t$, we have the inclusion $C(\mathbb{Z})_P \subset C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})}_t$. 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 $\overline{J(\mathbb{Z})}_t$ to $C(\mathbb{Z}_p)_P$, we pull back equations for $C(\mathbb{Z}_p)_P$ to $\overline{J(\mathbb{Z})}_t$ to arrive at the following theorem.

Theorem 4.1. *Let C, J, p, P, t be as in the overview, let κ be as in Theorem 3.1 and let f_1, \dots, f_{g-1} be as in Subsection 2.1. Define $\lambda_1 = \kappa^* f_1, \dots, \lambda_{g-1} = \kappa^* f_{g-1}$ to be the pullbacks along κ of the f_i . Then κ induces a surjection from $Z(\lambda_1, \dots, \lambda_{g-1}) \subset \mathbb{Z}_p^r$ to $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})}_t$.*

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

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

Proof. We start by proving that A is p -adically complete. This follows from the more general fact of a quotient □

To utilise this theorem, we only need to calculate the λ_i modulo p . In our case, of all κ_i and f_i being linear modulo p , so are the λ_i , and we get as special case the following corollary.

Corollary 4.3. *If the linear system of equations $\forall i : \lambda_i \equiv 0 \pmod{p}$ has respectively no or one solution, there is respectively none or at most one point in $C(\mathbb{Z})_P$.*

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 defining $U(\mathbb{Z}_p)_P$ in $\overline{J(\mathbb{Z})}_P$ modulo p has at most one solution, we get the inequality*

$$|C(\mathbb{Z})| \leq |C(\mathbb{F}_p)|.$$

Remark 4.5. Note that in general a linear system of $n + k$ equations over a vector space of dimension n over a finite field of size p has more than one solution with probability at most $\frac{1}{(p-1)^{k+1}}$. By the Hasse-Weil bound, assuming $p = \Omega(g^2)$, and that all linear systems of Proposition 4.4 for all $P \in C(\mathbb{F}_p)$ are independent, we see that the conditions of these propositions have a high condition of being satisfied if $r < g - 1$, and may even work for the case $r = g - 1$ with probability around e^{-1} for p large enough. Hence trying a few small primes should generally be enough.

Of note are that this upper bound for $C(\mathbb{Z})$ does not even depend on the genus, and behaves agreeably when compared to the upper bound in Theorem 5.3 of [MP12], which tells us that $|C(\mathbb{Z})| \leq |C(\mathbb{F}_p)| + 2g - 2$ 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 consistency for being able to prove much sharper bounds.

In general, even if \bar{A}/\bar{I} is not finite, we see $\text{Hom}(A/I, \mathbb{Z}_p)$ factors through $A/(I : p)$ where $(I : p) = \{x \in A \mid \exists k \in \mathbb{Z}_{\geq 0} : p^k x \in I\}$. Then a higher

give
proof

Bas,
ik be-
grijp
het
bewijs
niet
hele-
maal...

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 powerseries, 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 4.6. 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 $2p(x - x^2) = 0 \bmod p^2$, or $x - x^2 = 0 \bmod p$. Now both Proposition 4.2 and Newton polygons give an upper bound of 2 for $C(\mathbb{Z})_P$.

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 section to real cases.

- Even if $r \geq g$, it might still be possible that $\overline{J(\mathbb{Z})}$ coincidentally has dimension r' smaller than r (for example, if $r > g$); then one can find a rank r' subgroup of $J(\mathbb{Z})$ 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 $J(\mathbb{Z})$ is open 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 $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})}_t$. It can and does however happen that this set is strictly bigger than $C(\mathbb{Z})_P$. For example, there might be a K -point Q where K is a quadratic field where p splits, such that $Q - b$ is non- p -torsion, and then $Q - b$ also lies in the closure of $J(\mathbb{Z})$. We refer to [BBCF⁺19] for further examples and explanations.
- An important part of doing these calculations, is working with the Mordell-Weil group $J(\mathbb{Z})$. In general, finding generators of $J(\mathbb{Z})$ is com-

Bas,
ik ben
niet
echt
groot
fan
van
dit
hoofd-
stuk,
voegt
het
iets
toe
denk
je?

finish

putationally out of reach, and one may need to assume the BSD conjecture to even find the rank r . However, note that one does not need to find all of $J(\mathbb{Z})$; if we can generate a subgroup of $J(\mathbb{Z})$ 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 feats are easier than finding all of $J(\mathbb{Z})$.

- Even 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 learned. For example, maybe the method tells us that we have found all points of $J(\mathbb{Z})$ stemming from $C(\mathbb{Z})$ except those in a certain fibre of the map $J(\mathbb{Z}) \rightarrow J(\mathbb{F}_p)$. We can then aggregate this information for different primes, by looking at the maps $J(\mathbb{Z}) \rightarrow \prod_{p \in S} J(\mathbb{F}_p)$ for some set S of primes of good reduction. See for example [BS10] for an introduction to the Mordell-Weil sieve.

6 Implementations of linear Chabauty

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

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

inside $\mathbb{P}(1, g+1, 1)$ 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; these coordinates do not behave nicely on the origin of the patch $D(Y)$. We mainly use the first chart; we call any point that lies on it an affine point of C . We will treat the case that f has degree $2g+2$ (this can be done 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 [Mas18], we briefly introduce his notation. This is a summary of section 2.1 in [Mas18].

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

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

We pick D_0 an effective divisor of degree $d_0 \geq 2g + 1$; in the case of hyperelliptic curves, this will be $(g + 1)(\infty_+ + \infty_-)$. 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 $V_5 \rightarrow k^Z$, 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 most importantly: checking equality. Important from a computational standpoint is the complexity; 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 matrix constant.

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, Mascots 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 by Hensel lifting 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 of \mathbb{F}_q . The corresponding notion of an extension of $\mathbb{Z}/p^e\mathbb{Z}$ is given by taking an irreducible polynomial $\bar{T} \in \mathbb{F}_p[t]$ with $\mathbb{F}_q \cong \mathbb{F}_p[t]/\bar{T}$, arbitrarily lifting \bar{T} to a polynomial $T \in \mathbb{Z}/p^e\mathbb{Z}$, 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 Mascots representation. Most of the times these divisors are sums of points over the ring we are working with, but sometimes they are given as a 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 $f - h^2$.

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

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

meaning that with additional calculations of the behaviour of $(y - h)$ 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 both how to explicitly compute the Abel-Jacobi embedding and divisors in Mumford representation in Makdisi's representation for the Jacobian. We start with the Abel-Jacobi embedding

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

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  $B = (b_1, \dots, b_{g+3}) \leftarrow$  a basis of  $\mathcal{L}(D_0);$ 
3 if  $(f^r)'(0) \neq 0$  then
4    $F \leftarrow x^{g+1} + y;$ 
5 else
6    $F \leftarrow x^{g+1} + x^g + y;$ 
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  $V \leftarrow \ker(\text{im } W \subset R^{n_Z+1} \rightarrow R)$ , the projection on the last
    coordinate.;
11  $U \leftarrow \text{im}(V \rightarrow R^{n_Z})$ , where the last map is the projection on the first
    coordinates.;
12 Return  $U;$ 
```

Proposition 6.3. *Algorithm 1 gives correct output.*

Before this proof, we start with a quick lemma.

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

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 ∞_{\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 doesn't vanish at both of ∞_{\pm} , we see that v is a uniformiser at both these points. That means that $v_{\infty_{\pm}}(x)$, the order of x at ∞_{\pm} , is equal to -1 .

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

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

again has the right poles. \square

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 $1, x, \dots, x^{g+1}, y$ 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 dimension to increase by at most 1, we have by that b_1, \dots, 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 $\mathcal{L}(D_0 + \infty_+) \rightarrow R$, 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 Mascots representation, so this represents $P - \infty_+$ in the Jacobian. \square

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 $D = D(a, b)$. 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 $\mathcal{L}(2D_0 - D_{\text{aff}})$. Both over \mathbb{Q}_p and over \mathbb{F}_p we have the equality

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

and then it should follow over \mathbb{Z}_p so over $\mathbb{Z}/p^k\mathbb{Z}$. [TODO: It is not necessarily true that a map that is an isomorphism when tensored with \mathbb{F}_p and \mathbb{Q}_p it is an isomorphism, but that is of course true if the map is between free modules, as I think it is here, right? As everything embeds into \mathbb{Z}_p^n by evaluating at points, and submodule of free is free]

See
[Todo]

For $\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+)$, we first inductively calculate $W_n := \mathcal{L}(2D_0 - n\infty_-)$. For W_1 we have a basis $1, x, \dots, x^{2g+1}, y, xy, \dots, x^g y, x^{g+1}y + x^{2g+2}$, 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 $\mathcal{L}((g+1+d)(\infty_+ + \infty_-))$, this allows us to calculate $\mathcal{L}((g+1)\infty_- + (g+1+d)\infty_+)$ and to finish the computation. \square

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 nice curve C over \mathbb{Z} , smooth over $\mathbb{Z}_{(p)}$, with a \mathbb{Z} -point b , we have a birational map from $C^{(g)}$, the g -fold symmetric product of C , to J , given on points by sending $[(P_1, \dots, P_g)]$ to $[\sum P_i - gb]$. This map is étale at $[(P_1, \dots, P_g)]$ if $H^0(P_1 + \dots + P_g)$ has dimension 1 as the fibre of $P_1 + \dots + P_g - gb$ is exactly $\mathbb{P}H^0(P_1 + \dots + P_g)$. Also, if all P_i are distinct, then the map $C^g \rightarrow C^{(g)}$ is étale at P_1, \dots, P_g as well. Then finding parameters t_1, \dots, 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 $C(\mathbb{Z}/p^k\mathbb{Z})_{P_i} \rightarrow p\mathbb{Z}/p^k\mathbb{Z}$; 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

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

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 $(t_1, \dots, t_g) : J(\mathbb{Z}/p^k\mathbb{Z})_Q \rightarrow (p\mathbb{Z}/p^k\mathbb{Z})^g$ 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 [?]. This algorithm computes a rational map $J \rightarrow \mathbb{P}V_2$, 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 take 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 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, \dots, f_{g-1} are as in Remark 2.5, 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 extrapolation, and the following lemma, an immediate consequence of Lagrange interpolation, tells us how.

Lemma 6.7. *Let R be a ring, and assume operations in R are $O(1)$, $f \in R[x]$ with $x = (x_1, \dots, x_n)$ a polynomial of degree at most m , and S a subset of R with $S - S \subset \{0\} \cup R^*$ and $|S| > m$. Then f is uniquely determinable in $O(nm^{n+1})$ by its values on S^n . There is a better complexity algorithm I think.*

Make
the
com-
plex-
ity
better

at least clearly so for $m = 1$. I have to work on this a bit more. For $m = 1$, clearly we only need $n + 1$ evaluations.

Proof. Both uniqueness and construction follow from the case with $n = 1$; uniqueness from the fact that the ideals $\{(x-s) \mid s \in S\}$ are pairwise coprime, and the construction is Lagrange interpolation. The complexity follows easily from induction on n and the formula for Lagrange interpolation. \square

Note that evaluating λ_i at a point in $J(\mathbb{Z})_t$ 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 $C(\mathbb{Z})_P$.

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

Then by Remark 6.5 and Lemma 6.7, we can compute $\lambda_i \bmod p$ in $O(r g^{\omega+1})$; then solving the linear system of equations $\forall i \lambda_i \equiv 0 \bmod p$ has complexity lower than that, and hence checking if $|C(\mathbb{Z})_P|$ is at most 1 can be done in $O(r g^{\omega+1})$. Repeating this for all \mathbb{F}_p -points, gives by the Hasse-Weil bound a complexity of $O((p + g\sqrt{p})r g^{\omega+1})$.

7 An explicit example

We treat the hyperelliptic curve C with first affine chart given by

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

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 $p = 5$. It turns out that $C(\mathbb{F}_5)$ has seven points; the reductions of the rational points, and $(1, 0)$. Again taking the map $C \rightarrow J$ to be subtraction of ∞_+ on points, all seven points in $C(\mathbb{F}_5)$ lie in the image of $J(\mathbb{Z})$.

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 $j_\theta : C \rightarrow J$ 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 $J(\mathbb{Z})_0$ with \mathbb{Z}^r , the image of $J(\mathbb{Z})_0$ in $J(\mathbb{Z}/p^2\mathbb{Z})_0$ can be given as a map $\mathbb{F}_p^r \rightarrow J(\mathbb{Z}/p^2\mathbb{Z})_0$. Choosing parameters by giving a local chart $J \rightarrow \mathbb{P}(V_2)$, we want to exactly show that the two maps $C(\mathbb{Z}/p^2\mathbb{Z})_\theta \rightarrow J(\mathbb{Z}/p^2\mathbb{Z})_0, \mathbb{F}_p^r \rightarrow J(\mathbb{Z}/p^2\mathbb{Z})_0$ together form a map $\mathbb{F}_p \oplus \mathbb{F}_p^r \rightarrow J(\mathbb{Z}_p^2\mathbb{Z})_0$ 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 $C(\mathbb{Z})$ 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 $C(\mathbb{Z})$ and has no fixed points, this means $|C(\mathbb{Z})| \leq 6$ so our list of rational points is complete.

Do I just paste it in at the end, give a link to the github page, or just not give it all?

Bas,
what
do I
do
with
my
code?

8 Quadratic Chabauty

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

We start with 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 $j_b : C_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}$. 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 in fact is isomorphic to $J_{\mathbb{Q}}$, taking as isomorphism for example the principal polarisation $\lambda : J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}^\wedge$. This dual parametrised degree 0 line bundles on $J_{\mathbb{Q}}$, and hence we get a universal degree 0 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 $P_{\mathbb{Q}} = O(\Delta - \{0\} \times C_{\mathbb{Q}} - C_{\mathbb{Q}} \times \{0\})$, indeed with the fibres $P|_{\mathbb{Q}, c \times E_{\mathbb{Q}}} \cong O(c-0)$ 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

$$P_{\mathbb{Q}}^{\times} = \text{Isom}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}}(O_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}}, P_{\mathbb{Q}});$$

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 O_S and $(P_{\mathbb{Q}})_S$, with a free, transitive action of $O_S(S)^{\times}$, i.e. a torsor of $O_S(S)^{\times}$ in the traditional group-theoretic sense (note that this torsor can be empty).

I don't want to explain the biextension structure.

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 $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge}$ given as $(\text{id}, \text{tr}_c \circ f)$ where $f : J_{\mathbb{Q}} \rightarrow J_{\mathbb{Q}}^{\wedge}$ is a morphism of group schemes. We denote the pullback of $P_{\mathbb{Q}}^{\times}$ 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

Bas,
do you
agree?

$$\begin{array}{ccccc} & & T_{\mathbb{Q}} & \longrightarrow & P_{\mathbb{Q}}^{\times} \\ & \nearrow \tilde{j}_b & \downarrow & & \downarrow \\ C_{\mathbb{Q}} & \xrightarrow{j_b} & J_{\mathbb{Q}} & \xrightarrow{(\text{id}, \text{tr}_c \circ f)} & J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\wedge} \end{array}$$

where \tilde{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 $\text{Hom}^+(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\wedge})$, 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 in general that is the best we can do, as generically the rank of $\text{Hom}^+(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\wedge})$, also called the Néron-Severi rank ρ , is 1. But in many interesting cases, this rank is non-zero. Using the isomorphism λ , this rank is also the rank of the endomorphism ring of $J_{\mathbb{Q}}$, and hence a family of examples is given by modular curves, where the endomorphism ring is the Hecke algebra and the Néron-Severi rank turns out to be equal to the genus.

This is
true,
right?
Can't
find
refer-
ence

In general, we can pick a basis $f_1, \dots, f_{\rho-1}$ of the trace 0 subgroup of $\text{Hom}^+(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\wedge})$ and elements $c_1, \dots, c_{\rho-1} \in J_{\mathbb{Q}}^{\wedge}$ with $j_b^*(\text{id}, \text{tr}_{c_i} \circ f_i)^* P_{\mathbb{Q}}^{\times}$ 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 \tilde{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, and hence we cannot easily upper bound the dimension of $\overline{T_{\mathbb{Q}}(\mathbb{Q})}$ inside $T_{\mathbb{Q}}(\mathbb{Q}_p)$.

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 fiber $C_{\mathbb{Q}}$. 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 structure of the Poincaré torsor intact, we can only extend to $P \rightarrow J \times J^{\wedge 0}$ where $J^{\wedge 0}$ is the connected component of J^{\wedge} containing 0; the component group $J/J^{\wedge 0}$ 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 $J/J^{\wedge 0}$. We can then make a similar diagram as before

$$\begin{array}{ccccc} & & T & \longrightarrow & P^{\times} \\ & \nearrow \tilde{j}_b & \downarrow & & \downarrow \\ C & \xrightarrow{j_b} & J & \xrightarrow{(\text{id}, \text{motr}_{c_i} \circ f)} & J \times J^{\wedge 0} \end{array}$$

Where this time f is an 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 then the lift exists and is unique up to the action of \mathbb{Q}^{\times} . For q prime for which C_q has only one component, we can multiply by a suitable power of q to make the fibre of $j_b^* T$ over p trivial, however we cannot always do this if C_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 $C(\mathbb{Z}) = C^{\text{sm}}(\mathbb{Z})$, it is enough to compute $U_i(\mathbb{Z})$ for every U_i . Then the map $j_{b,i} : U_i \rightarrow J$ does

lift as in the following diagram:

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

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 $\text{Hom}(J, J^\wedge)^+$. Taking a specific such U with a lift $\tilde{j}_b : U \rightarrow T$, for every prime p , the set $\tilde{j}_b(U(\mathbb{Z}))$ is a subset of the intersection, inside the p -adic manifold $T(\mathbb{Z}_p)$, of $\tilde{j}_b(U(\mathbb{Z}_p))$ and the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$. As the dimension of T 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 $T(\mathbb{Z})$ is a $\pm 11^{\rho-1}$ -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 of 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 $\mathbb{Z}^r \rightarrow J(\mathbb{Z}_p)_0 \cong \mathbb{Z}_p^g$ 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 $\kappa : \mathbb{Z}^r \rightarrow T(\mathbb{Z}_p)_t \cong \mathbb{Z}_p^{g+\rho-1}$ such that $\text{im } \kappa = \overline{T(\mathbb{Z})}$ and κ is given by convergent power series. When the parameters at t are chosen nicely, the first g coming from J , it turns out that $\kappa_1, \dots, \kappa_g$ are linear modulo p , and $\kappa_{g+1}, \dots, \kappa_{g+\rho-1}$ 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 $(\text{id}, m \circ \text{tr}_c \circ f)$ being a quadratic like map, as the product of id and $m \circ \text{tr}_c \circ f$, two linear maps. Also, one can again find equations $g_1, \dots, g_{r+\rho-2}$ for 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 $\tilde{j}_b : U \rightarrow T$. 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 $C \rightarrow J \times J^{\wedge 0}$, and this map factors through the diagonal map $C \times C \times C$. As described in Section 7 of the paper, it turns out that giving such a map $f : J \rightarrow J^\wedge$ and $c \in J^\wedge$ 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 $\text{pr}_2 : (C \times C)_\mathbb{Q} \rightarrow C_\mathbb{Q}$ are degree 0, and the pullback $\text{diag}^* \mathcal{L}$ is trivial on $C_\mathbb{Q}$. This turns the problem of describing a map $J \rightarrow J^\wedge$ in useful terms of th 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 lies in describing Hecke operators explicitly as correspondences on $C \times C$, and computations with these correspondences over \mathbb{Z} .

References

- [BBCF⁺19] Jennifer S. Balakrishnan, Francesca Bianchi, Victoria Cantoral-Farfán, Mirela Çiperiani, and Anastassia Etropolski. Chabauty–coleman experiments for genus 3 hyperelliptic curves. In Jennifer S. Balakrishnan, Amanda Folsom, Matilde Lalín, and Michelle Manes, editors, *Research Directions in Number Theory*, pages 67–90, Cham, 2019. Springer International Publishing.
- [Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). 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, 2019.
- [GD71] A. Grothendieck and J. A. Dieudonné. *Eléments de géométrie algébrique. I*, volume 166 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1971.
- [Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [has] 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.
- [KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.
- [Mas18] Nicolas Mascot. Hensel-lifting torsion points on jacobians and galois representations, 2018.

- [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.