

P. Spelier

A geometric approach to linear Chabauty

Master thesis

February 28, 2020

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



Leiden University
Mathematical Institute

Todo list

Bas, is dit de goede samenvatting? Voornamelijk mijn vraag: is het nog steeds een specifiek geval van Coleman-Chabauty?	4
Bas, wat vind je van het bestaan van dit hoofdstuk?	6
give proof	8
maybe replace this by an action of the tangent space of $X_{\mathbb{F}_p}$ at x . . .	8
give proof	9
nicely LaTeX Example bla, continued	11
nicely LaTeX Example bla, continued	12
TODO This is clearly a Hensel like proof, and I would prefer to just outright use Hensels lemma in some way	14
give exact statement and proof	16
Write everything	16
Give more details, currently talking with Mascot about this.	23
find a reference for this	23
Explain how this can be improved in complexity	24
There is a better complexity algorithm I think, at least clearly so for $m = 1$	24
Refer back to complexity of calculations on the Jacobian ($J(\mathbb{Z})$ and so on)	24
Find complexity of operations in the Jacobian performed by Mascots code	24
Add computations	25

Contents

1 Introduction	4
1.1 Overview	5
2 Points on a smooth scheme over \mathbb{Z}_p	7
2.1 From $C(\mathbb{Z}_p)$ to $J(\mathbb{Z}_p)$	8
3 From $J(\mathbb{Z})$ to $J(\mathbb{Z}_p)$	9
3.1 From group schemes to formal groups	10
4 Computing the intersection	15

5	Complications and improvements	16
6	Implementations of linear Chabauty	17
6.1	Makdisis algorithms	18
6.1.1	Going from \mathbb{F}_p to $\mathbb{Z}/p^e\mathbb{Z}$	19
6.2	Implementing the Abel-Jacobi map and Mumford representations	19
6.3	Parameters at J	23
6.4	Interpolating polynomials	24
6.5	Complexity	24
7	An explicit example	25
8	Quadratic Chabauty	25
	References	26

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 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 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. Chabauty proved, using p -adic methods, that if r is strictly smaller than the genus g , then C has 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 .

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, a special case of non-abelian Chabauty, Balakrishnan, Dogra, Müller, Tuitman and Vonk famously miscalculated 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 non-abelian Chabauty explicit.

Very recently, Edixhoven and Lido made available a preprint of their article “Geometric quadratic Chabauty”. 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 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. We hope to provide the reader with a clear overview of geometric Chabauty, and a new way to do explicit computations.

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 $C_{\mathbb{Q}}$ having Mordell-Weil rank $r < g$. Assume we have a \mathbb{Q} -point b in C , or equivalently a \mathbb{Z} -point. We view $C_{\mathbb{Q}}$ 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 $C(\mathbb{Z}_p)_P \cup \overline{J(\mathbb{Z})}_t$, 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 $\left|C(\mathbb{Z}_p)_P \cup \overline{J(\mathbb{Z})}_t\right|$ 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 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.

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

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 $\tilde{\mathbb{A}}_{\mathbb{Z}_p,a}^d \rightarrow \mathbb{A}_{\mathbb{Z}_p}^d$. Then the part \tilde{X}_x^p is the pullback of the corresponding part of $\tilde{\mathbb{A}}_{\mathbb{Z}_p,a}^d$, 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.

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

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

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

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

Note that this construction is functorial, as in the following lemma:

Lemma 2.3. *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 $Y_y^p \rightarrow X_x^p$.*

Proof. \square

give proof

[TODO: add that the map $\tilde{Y}_y^p(\mathbb{Z}_p) \rightarrow \tilde{X}_x^p(\mathbb{Z}_p)$ is, after choosing parameters, given by convergent power series; are these in general linear modulo p ? And what happens modulo higher powers?]

Finally, 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 $X(\mathbb{Z}/p^2\mathbb{Z})_0$. We can parametrise $X(\mathbb{Z}/p^2\mathbb{Z})_0$ by $t = t_1 : X(\mathbb{Z}/p^2\mathbb{Z})_0 \rightarrow p\mathbb{Z}/p^2\mathbb{Z}$ 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 $(t - \lambda p)(t - \mu p) = t^2 - (\lambda + \mu)p$, which defines the same Cartier divisor as $P_{\lambda'} + P_{\mu'}$ if and only if $\lambda + \mu = \lambda' + \mu'$. So as a Cartier divisor, $P_\lambda + P_\mu$ is in fact equal to $P_{\lambda'} + P_{\mu'}$.

maybe re-
place
this
by an
action
of the
tan-
gent
space
of $X_{\mathbb{F}_p}$
at x

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 and non-constant modulo p , i.e. 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 . Another way to think of this, is as $C(\mathbb{Z}/p^2\mathbb{Z})_P$ being an affine line inside $J(\mathbb{Z}/p^2\mathbb{Z})_t$. This uses the functoriality of smooth \mathbb{Z}_p -points reducing to a point. 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 Lemma 2.3.

give
proof

Remark 2.4. 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.

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 $J(\mathbb{Z})_t \rightarrow J(\mathbb{Z}_p)_t$. Then 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 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 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. 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 $F(F(x, y), z) = (1 + x)(1 + y)(1 + z) - 1 = F(x, F(y, z))$.

Example 3.4. For any n , we can take $F(x, y) = x + y$, also known as the n -dimensional additive formal group.

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 Corrolaire 2 of [Bou98, III,4.5], over $R[[x]]$ with maximal ideal $\mathfrak{m} = (x)$, as 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 $A \in \text{GL}_n(R)$. Then there is a unique $b \in R[[x]]_0^n$ such that $a \circ b = b \circ a = x$.

Proof. Let $F(x, y) = x - a(x)$. 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 $R[[x]]$ 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 $\text{Hom}_{\text{cont}} R, A$ into a group, functorially in A .

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 $\hat{O}_{G,e}$.

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 [TODO: figure out why exactly? Probably just Yoneda] as an continuous coproduct $\mu : \hat{O}_{G,e} \rightarrow \left(\hat{O}_{G,e}\right)^{\otimes 2}$. 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 $\mu(x_i)$. 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 3.7. 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 $uv-1 = (x+1)(y+1)-1 = x+y+xy$.

nicely
La-
TeX
Ex-
ample
bla,
con-
tinued

Hence the formal group $F_{\mathbb{G}_m}$ corresponding to this group scheme is exactly the multiplicative formal group from Example 3.3.

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 , and then, if R has no torsion, 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 3.8. Taking F the multiplicative group as in Example 3.3, 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 $\log = \sum_{j \geq 1} \frac{-(-x)^j}{j}$, 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, $\exp(x) = \sum_{j \geq 0} \frac{x^j}{j!}$.

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

nicely
La-
TeX
Ex-
ample
3.8
con-
tinued

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 3.9. *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 $\mathbb{Z}_p\langle x_1, \dots, x_d \rangle$. 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 $n \geq$ 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 $\mathbb{Z}_p^d \rightarrow \mathbb{Z}_p$. 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 $\log_{p,i} = x_i \pmod{(x)^2}$, this means that for $p > 2$ we have

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

Note that as $\log_p \equiv x \pmod{(x)^2}$, 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 . Then we use induction to prove that \exp_p has degree at most m modulo p^m . This will follow immediately from the following considerations; firstly, for $f, g, g_m \in \mathbb{Z}/p^m\mathbb{Z}[x]_0^d$ satisfying $f(g(x)) = x \pmod{p^{m-1}}$, with f, g linear modulo p and f, g having as derivative at 0 invertible $d \times d$ -matrices C_f, C_g we have the formula

$$f(g(x) + p^{m-1}g_m(x)) + p^{m-1}f_m(g(x)) = f(g(x)) + p^{m-1}(C_f g_m(x))x^m$$

and as C_f is invertible, there is a unique value of $p^{m-1}g_m$ such that $f((g + p^{m-1}g_m)(x)) = x$, and then $p^{m-1}g_m$ has degree at most $\deg f(g(x))$. Secondly, if furthermore we can write f, g in the forms $f = \sum_{i=1}^m p^{i-1}a_i x^i, g = \sum_{i=1}^{m-1} p^{i-1}b_i x^i$ with $p^{i-1} \mid a_i, b_i$, then we have

$$\begin{aligned} f(g(x)) &= \sum_{i=1}^m p^{i-1}a_i g^i \\ &= \sum_{i=1}^m p^{i-1}a_i \sum_{I_1, \dots, I_i} \prod_{j=1}^i p^{I_j-1}b_{I_j} x^{I_j} \\ &= \sum_{i=1}^m \sum_n p^{n-1}x^n \left(\sum_{I_1 + \dots + I_i = n} a_i \prod_{j=1}^i b_{I_j} \right) \end{aligned}$$

which is clearly of degree at most m . In total, there is a unique $\tilde{g} \in \mathbb{Z}/p^m\mathbb{Z}[x]_0^d$ satisfying $\tilde{g} \equiv g \pmod{p^{m-1}}$ and $f(\tilde{g}(x)) = x$, and this \tilde{g} has degree at most m . This finishes the proof. [Is this doable? I think so... Maybe multiply g by p and divide coefficients of f by powers of p , and use that $\mathbb{Z}_p[[px]]$ is p -adically complete. Also, try to get rid of the calculation at the end.] \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

TODO
This is clearly a Hensel like proof, and I would prefer to just out-right use Hensels lemma

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 3.9 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 3.10. *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 $C(\mathbb{Z}_p)_P$. There are several, sometimes ad hoc, ways of proving finiteness. We let A denote $\mathbb{Z}_p\langle x_1, \dots, x_r \rangle$ and I the ideal generated by $\lambda_1, \dots, \lambda_{g-1}$. 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.

Proposition 4.2. *Let $\overline{A} = A/pA$ and $\overline{I} = I\overline{A}$. Assume $\overline{A}/\overline{I}$ is finite. Then*

...

Proof.

□

give
exact
state-
ment
and
proof

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 , we get as special case the following corollary.

Corollary 4.3. *If the 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 $C(\mathbb{Z})_P$.*

In general, even if $\overline{A}/\overline{I}$ is not finite, we see $\text{Hom}(A/I, \mathbb{Z}_p)$ factors through $A/(I : p)$ where $(I : p) = \{x \in A \mid \exists k \in \mathbb{Z}_{\geq 0} p^k x \in A\}$. Then a higher precision calculation of the λ_i can still lead to a successful 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 4.4. If $r = g - 1 = 2$ and $\lambda_1 \equiv px - py, \lambda_2 \equiv x + y + pxy \pmod{p^2}$, neither Proposition 4.2 nor Newton polygons are instantly applicable. However, substituting $y = -x + px^2 \pmod{p^2}$ into the first equation gives $2p(x - x^2) = 0 \pmod{p^2}$, or $x - x^2 = 0 \pmod{p}$. Now both Proposition 4.2 and Newton polygons give an upper bound of 2 for $C(\mathbb{Z})_P$.

5 Complications and improvements

- $\overline{J(\mathbb{Z})_0}$ open in $J(\mathbb{Z}_p)_0$.
- Calculations in $J(\mathbb{Z})$.

Write
every-
thing

- According to McCallum&Poonen, it can be that $J(\mathbb{Z})_0$ and $C(\mathbb{Z})_P$ are tangent as p -adic manifolds and then finite-precision calculations will never be enough. I don't see what's happening there. Maybe give an example?
- It is possible that $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})}_t$ is bigger than $C(\mathbb{Z})_P$; give an example. Refer to [BBCF⁺19].
- Explain Mordell-Weil sieve. Maybe "The Mordell-Weil sieve: Proving non-existence of rational points on curves" for a short explanation? Nice to also treat this in the final example.
- in general, generators of the Mordell-Weil group are computationally out of reach. But, if we only generate a subgroup of $J(\mathbb{Z})_0$ of index finite and coprime to p , then the closure of this in $J(\mathbb{Z}_p)_0$ will be the same. This happens in particular if we generate a subgroup of $J(\mathbb{Z})$ of index finite and coprime to $p|J(\mathbb{F}_p)|$. Preferably, find a source for this? Bas, do you have a reference for the complexity of such calculations?
- Fun case: if J splits up to isogeny as the product of an elliptic curve and an abelian surface of Mordell-Weil rank respectively 2 and 1, then we only need two elements of $J(\mathbb{Z})_0$ to generate $\overline{J(\mathbb{Z})}_0$ I think.

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 Makdisis algorithms

Say something about how Makdisis algorithms work (i.e., give an introduction to the terminology) [KM04].

As we are using and adding on 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.

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

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 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 $\mathbb{Z}/p^k\mathbb{Z}$.

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

Give more details, currently talking with Mas-ot about this.

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, and 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.

find a reference for this

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.

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 2.4, 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 6.5. *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 .*

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

Explain how this can be improved in complexity

There is a better complexity algorithm I think, at least clearly so for $m = 1$

Refer back to complexity of calculations on the Jacobian

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 residue disc of 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.

Bas, what do I do with my code? Do I just paste it in at the end, give a link to the github page, or just not give it all?

Add
com-
puta-
tions

8 Quadratic Chabauty

Maybe treat how the Poincare torsor fits into this context; perhaps give an overview? Not sure if I can say enough while keeping it interesting. I would like to give a simpler introduction to [EL19], saying a few things about the similarities and differences with linear Chabauty. I am not going to go in much detail, and am not going to do an example. Bas, do you think this would be useful?

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