P. Spelier

A geometric approach to linear and quadratic Chabauty

Master thesis

January 17, 2020

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

Leiden University
Mathematical Institute

Contents

1 Introduction

Say something about the problem, Faltings, et cetera

Say something about Chabauty's general idea

Mention Flynn, Coleman, Kim, Balakrishnan et al. and their way of doing quadratic Chabauty

Say something about linear Chabauty geometric style

Say something about quadratic Chabauty geometric style.

Say how much is borrowed from the article by Bas and Guido, but with a focus on the linear part, and more explanations.

2 Linear 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 Mordell-Weil rank $r < g$. Assume we have a $\mathbb{Q}$-point b in C, or equivalently a $\mathbb{Z}$-point. Let J be the Jacobian of $C_{\mathbb{Q}}$; 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 2.1. Let S be a scheme, $T \to U$ a morphism of schemes and $x : T \to S$ a T-point. We define $S(U)_x$ as the morphisms from U to S that, after precomposing with $T \to U$, give x.

We want to find an upper bound for the cardinality of $C(\mathbb{Z})_P$

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

As t is étale, the ideal of X defining x is the pullback along t of the ideal of $\mathrm{A}^d_{\mathbb{Z}_p}$ defining the origin a over $\mathbb{F}_p$. That means that the blowup $\tilde{X}_x \to X$ is the pullback of the blowup $\tilde{\mathrm{A}}^d_{\mathbb{Z}_p,a} \to \mathrm{A}^d$. Then the part $\tilde{X}_x^p$ is the pullback of the corresponding part of $\tilde{\mathrm{A}}^d_{\mathbb{Z}_p,a}$, i.e. $\operatorname{Spec} \mathbb{Z}_p[\tilde{x_1}, \ldots, \tilde{x_d/p}] = \operatorname{Spec} \mathbb{Z}_p[x_1/p, \ldots, x_d/p]$ with the morphism $\mathbb{Z}_p[x_1, \ldots, x_d] \to \mathbb{Z}_p[\tilde{x_1}, \ldots, \tilde{x_p}]$ given by $x_i \mapsto p\tilde{x_i}$. That implies that $\tilde{X}_x^p$ is $\operatorname{Spec} A[t_1/p, \ldots, t_d/p]$, with the map $\tilde{X}_x^p \to X$ given by the inclusion $A \to \operatorname{Spec} A[t_1/p, \ldots, t_d/p]$ (remember that the t_i are elements of $O_X(X) = A$). If furthermore t is locally of finite type, then by (IV,17.6.3) of [GD71] we have an isomorphism between the p-adic completion $O(\tilde{X}_x^p)$ and the completion $\mathbb{Z}_p\langle \tilde{x_1}, \ldots, \tilde{x_d} \rangle$ of $\mathbb{Z}_p[\tilde{x_1}, ..., \tilde{x_d}]$, with the latter completion being the ring of convergent power series, i.e.

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

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

Lemma 2.2. *Given two smooth schemes X, Y over $\mathbb{Z}_p$, two $\mathbb{F}_p$-point $x \in X(\mathbb{F}_p), y \in Y(\mathbb{F}_p)$, there is a natural bijection between maps $f : Y \to X$ satisfying $f(y) = x$, and morphisms $\tilde{Y}^p_y \to \tilde{X}^p_Y$.*

Proof. $\square$

Applying this lemma with $Y = \operatorname{Spec} \mathbb{Z}_p$ and y the origin over $\mathbb{F}_p$, we get a natural bijection between $X(\mathbb{Z}_p)_x$ and $\operatorname{Hom}(O(\tilde{x}^p_Y), \mathbb{Z}_p)$. As $\mathbb{Z}_p$ is p-adically complete, the map t gives an isomorphism between $\operatorname{Hom}(O(\tilde{x}^p_Y), \mathbb{Z}_p)$ and $\operatorname{Hom}(\mathbb{Z}_p\langle \tilde{x_1}, \ldots, \tilde{x_d}\rangle, \mathbb{Z}_p) \cong \mathbb{Z}_p^d$.

Conclude that $\tilde{X}^p_x(Z_p)$ is in bijection with $X(Z_p)_x$

Talk about the coordinate ring and its p-adic completion

Say something about functoriality

2.2 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 2.1 we know $J(\mathbb{Z}_p)_t$ is in bijection with $\mathbb{Z}_p^g$, with the bijection given by evaluating parameters and dividing by p. Let $\kappa : \mathbb{Z}^r \to \mathbb{Z}_p^g$ be the map resulting from the inclusion $J(\mathbb{Z})_t \to J(\mathbb{Z}_p)_t$. Then κ turns out to have a special property.

Theorem 2.3. *There are uniquely determined $\kappa_1, ..., \kappa_g \in \mathbb{Z}_p\langle z_1, ..., z_r\rangle$ such that for all $x \in \mathbb{Z}^r$ we have $\kappa(x) = (\kappa_1(x), ..., \kappa_g(x))$ and the image $\overline{\kappa_i}$ of κ_i in $\mathbb{F}_p[z_1, ..., z_r]$ has degree at most* 1.

TODO: give proof. Use formal group scheme by looking to 0.

Corollary 2.4. *The map κ extends uniquely to a continuous map $\kappa : \mathbb{Z}_p^r \to \mathbb{Z}_p^g$, given by the same power series, and the closure $\overline{J(\mathbb{Z})_t} \subset J(\mathbb{Z}_p)_t$ is given by the image of $\mathbb{Z}_p^r$ under κ.*

TODO: give proof

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

By Subsection 2.1, we also know that $C(\mathbb{Z}_p)_P$ is in bijection with $\mathbb{Z}_p$, again with the bijection given by evaluating a parameter and dividing by p. The resulting function $\mathbb{Z}_p \to \mathbb{Z}_p^g$ is linear and non-constant modulo p, i.e. there are power series $f_1, ..., f_{g-1} \in \mathbb{Z}_p\langle z_1, ..., z_g\rangle$ such that the image of $C(\mathbb{Z}_p)_P$ is exactly given by $V(f_1, ..., f_{g-1})$, 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 $J(\mathbb{Z}/p^2\mathbb{Z})_t$. TODO: give proof

2.4 Finding $C(\mathbb{Z})$

Clearly, as subsets of $J(\mathbb{Z}_p)_t$, we have the inclusion $C(\mathbb{Z})_P \subset C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}$. Let $\kappa^* f_1, ..., \kappa^* f_{g-1}$ be the pullbacks along κ of the f_i, and let I be the ideal they generate inside $A := \mathbb{Z}_p\langle z_1, ..., z_r\rangle$. Then $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}$ is in bijection with $\mathrm{Hom}(A/I, \mathbb{Z}_p)$. By Theorem 4.2 of Edixhoven-Lido, we just need to check whether $\overline{A}/\overline{I}$ is finite. As all $\overline{\kappa^* f_i}$ are linear, in fact, $\overline{A}/\overline{I}$ is always of the form 0 or $\mathbb{F}_p[w_1, ..., w_s]$ for some $s \leq r$, and $s = 0$ iff the system of linear equations $\overline{\kappa^* f_i} = 0, i \in \{1, ..., g-1\}$ has a unique solution. In general, we may expect an upper bound for $|C(\mathbb{Z})_P|$ of 1 if $r \leq g-1$. TODO: give proof of Theorem 4.2.

2.5 Calculations modulo p^2

Say something about how, for the right set of points $\{p_1, ..., p_g\}$, the map $C^g \to J$ is etale at that set of points. Then say something about what that implies about $J(\mathbb{Z}_p)_0$ (equal to $\sum q_i - p_i$ where $q_i \in C(\mathbb{Z}_p)_{p_i}$), and $J(\mathbb{Z}/p^2\mathbb{Z})_0$, which becomes isomorphic as vector spaces to $\mathbb{F}_p^g$, and how we can find κ by expressing elements of $J(\mathbb{Z})_0$ in that basis, and similarly $f_1, ..., f_{g-1}$ by finding $P_1 - P_2$ in that basis for some $Q_1, Q_2 \in C(\mathbb{Z}/p^2\mathbb{Z})_P$ not equal.

An important part of this, is that there is a parametrisation $P_\mu, \mu \in \mathbb{F}_p$ of the points in $C(\mathbb{Z}/p^2\mathbb{Z})_P$ such that $P_\mu + P_\nu = P_{\mu+\nu} + P_0$ as Cartier divisors.

3 Implementations of linear Chabauty and an explicit example

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, writing , 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 $\sigma(v, w) = (v, -w)$.

3.1 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

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

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 $V_5 \to k^Z$, evaluating a rational function at Z. By our choice of n_Z, this is an injective map, i.e. we can represent rational functions in V_5 by their values in k^Z. In this representation, we can even add, subtract, or multiply rational function, by respectively adding, subtracting or multiplying the correspondig vectors in k^Z. It is now also possible to represent subspaces of V_5 by giving a basis in k^Z.

We now explain the representation of $J(k)$. Note that for any $x \in J(k)$, we have that $x+D_0$ is of degree at least $2g+1$ and hence is equivalent to an effective divisor $E \geq 0$. 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 Mascots article, using this representation one can do all relevant computations in $J(k)$; adding, subtracting, finding the zero element, and most importantly: checking equality.

3.1.1 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 $R = Z/p^e\mathbb{Z}$; in fact, all submodules of R^n we will be seeing are free. That means all these submodules will have good reduction, i.e. the rank remains the same when 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 be calculated by Hensel lifting the kernels, images, et cetera of these maps modulo 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 $\overline{T} \in \mathbb{F}_p[t]$ with $\mathbb{F}_q \cong \mathbb{F}_p[t]/\overline{T}$, arbitrarily lifting $\overline{T}$ to a polynomial $T \in \mathbb{Z}/p^e\mathbb{Z}$, 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.

3.2 Implementing the Abel-Jacobi map

Say something about implementing the Abel-Jacobi map $C \to J, Q \mapsto Q - \infty_+$. Right now, information about this (the implementation and why it works) can be found in Hyper2RR.gp.

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. Since we can add elements in the Jacobian, for this it is enough to compute the Abel-Jacobi embedding

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

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

Algorithm 1: The Abel-Jacobi embedding

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

$Z' \leftarrow Z \sqcup \{P\}$;
$B = (b_1, \dots, b_{g+3}) \leftarrow$ a basis of $\mathcal{L}(D_0)$;
if $(f^r)'(0) \neq 0$ **then**
  $F \leftarrow x^{g+1} + y$;
else
  $F \leftarrow x^{g+1} + x^g + y$;
end
$b_{g+4} \leftarrow xF$;
$W \leftarrow$ a $(n_Z + 1) \times (g + 4)$ matrix with rows being the evaluations of $B \sqcup b_{g+4}$ on a point in Z'.;
$V \leftarrow \ker(\operatorname{im} W \subset R^{n_Z+1} \to R)$, the projection on the last coordinate.;
$U \leftarrow \operatorname{im}(R^{g+4} \xrightarrow{\cdot V} R^{n_Z+1} \to R^{n_Z})$, where the last map is the projection on the first coordinates.;
Evaluate the special function F (see Hyper2RR.gp) on Z;
Return $U \cdot \sigma(F)$;

Proposition 3.1. *Algorithm 1 gives correct output.*

Before this proof, we start with a quick lemma.

Lemma 3.2. *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 $\infty_\pm$ correspond to $(v,w) = (0, \pm 1)$ in this patch. Letting $g^r(v)$ be the polynomial $(f^r(v) - 1)/v$, we can rewrite the equation for C to $(w-1)(w+1) = vg^r(v)$. As the derivative of $(w-1)(w+1)$ to w doesn't vanish at both of $\infty_\pm$, we see that v is a uniformiser at both these points. That means that $v_{\infty_\pm}(x)$, the order of x at $\infty_\pm$, is equal to -1.

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

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

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

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

again has the right poles. □

Proof of Proposition **??**. First note that by Riemann-Roch, the dimension of $\mathcal{L}(D_0)$ is $g+3$, and we also have by the proof of the previous lemma that $1, x, \ldots, x^{g+1}, y$ all lie in $\mathcal{L}(D_0)$ and hence form a basis, so we can indeed find B as in line 2. Note that by Lemma 3.2 the element b_{g+4} lies in $\mathcal{L}(D_0 + \infty_+)$ but not in $\mathcal{L}(D_0)$, so as $\deg D_0 \geq 2g - 1$, we have by a dimensional argument that $b_1, \ldots, b_{g+4}$ is a basis for $\mathcal{L}(D_0 + \infty_+)$; that it is in fact a basis is evident as this argument tells us it is a basis when tensored with $\mathbb{F}_p$.

Evaluating $\mathcal{L}(D_0 + \infty_+)$ on P gives a linear map $\mathcal{L}(D_0 + \infty_+) \to R$, and the kernel is exactly $\mathcal{L}(D_0 + \infty_+ - P)$; this is the resulting V in line 10. Then. Finally, note that the poles of $\sigma(F)$ are, again by the previous lemma, $g(\infty_+ + \infty_-) + \infty_+$; write E for the divisor of zeroes of F; we see it has degree $2g+1$. Then we have the equality

$$\mathcal{L}(D_0 + \infty_+ - P) \cdot F = \mathcal{L}(2D_0 - E - P).$$

This last term is in fact in Mascots representation, and trivially $P - \infty_+ = P + E - D_0$, so this represents $P - \infty_+$ in the Jacobian. □

Say something about how with just this map and Mascots code, one can already find the $\overline{\kappa^* f_i}$ and compute an upper bound for $C(\mathbb{Z})_P$ using brute force.

3.3 Speeding up the calculations

Say something about how one express an element in $J(\mathbb{Z}/p^2\mathbb{Z})_0$ on the basis in something like $O(g)$ hopefully (ignoring the time for adding,multiplying, et cetera in the Jacobian), instead of the bruteforce $O(p^g)$. This is currently done using code from Mascot. Say what the final complexity is.

3.4 An explicit example

Treat the example in ExChabauty.gp.

4 The Poincare torsor

Define and cite theorems about the Poincare Torsor

5 Quadratic Chabauty using the Poincare torsor

Explain how to do Chabauty in the case $r < g + \rho - 1$, where ρ is the Néron-Severirank.

6 Implementations of quadratic Chabauty and an explicit example

Explain something about implementing quadratic Chabauty.

References

[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.

[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.