Coleman's effective Chabauty

Corijn Rudrum

June 2023[1]

Abstract

We give an introduction to Coleman's effective version of Chabauty's method following his original papers [Col85a] and [Col85b]. This method can be used to bound the number of rational points on curves for which the rank of their Jacobian is less than their genus. Moreover, it presents a way of explicitly computing these rational points. We will use the theory of rigid analytic spaces, of which we present the basics in the first section. Rigid analytic geometry can be seen as an analogue for complex analytic geometry for spaces over non-archimedean fields. We also recall the notion of Coleman integration on such rigid analytic spaces.

Contents

[1] Version: 17/07/23

1 Introduction

Now over a century ago, Mordell conjectured in 1922 that a curve over $\mathbb{Q}$ of genus $g \geq 2$ has only finitely many rational points [Mor22]. This conjecture is now a theorem, proven by Faltings in 1983 [Fal83]. In fact, he proved the statement for curves over arbitrary number fields. Although a very powerful statement, the proof given by Faltings lacks effectivity. We know that the number of rational points is finite but we have no idea how big it might be, nor do we know how "big" the solutions might be. Before Faltings came with a full proof, Chabauty proved in 1941 that Mordell's conjecture is true if the genus of the curve is strictly bigger than the rank r of its Jacobian. Although this result is now strictly included in Faltings theorem, the way Chabauty proved his result is still of interest. The main reason for this is Coleman's 1985 paper in which he shows how to obtain effective statements from a variation on Chabauty's arguments. In particular, he proved an explicit upper bound for the number of rational points on a curve satisfying $r < g$ [Col85b]. A particularly elegant version of this bound is the following:

Theorem 1.1 (Corollary 4.6 below)**.** *Let X be a smooth curve of genus $g \geq 2$ over $\mathbb{Q}$ with good reduction at p. Denote its Jacobian by J, and let r be the rank of the Mordell–Weil group $J(\mathbb{Q})$. If $r < g < p/2$, then*

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + (2g - 2).$$

To get an idea of the general picture of the Chabauty–Coleman method, consider the following diagram of inclusions:

$$\begin{array}{ccc} X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ J(\mathbb{Q}) & \hookrightarrow & J(\mathbb{Q}_p). \end{array}$$

Then the rational points $X(\mathbb{Q})$ are contained in the intersection $J(\mathbb{Q}) \cap X(\mathbb{Q}_p) \subset J(\mathbb{Q}_p)$. The idea of the Chabauty–Coleman method is to construct a map $\eta : J(\mathbb{Q}_p) \to \mathbb{Q}_p$ that vanishes on this intersection and whose zeroes we can compute. Then the number of zeroes of η gives an upper bound on $\#X(\mathbb{Q})$. To define the map η, Coleman used the integrals on rigid spaces he defined in [Col85a]. Therefore, we start off these notes with an introduction to the theory of rigid analytic geometry and Coleman integrals.

Since Coleman made Chabauty's arguments effective, there have been many variations on their method. For instance, in [Sto17], Stoll describes a method similar to that of Chabauty and Coleman that does not need full knowledge of the Jacobian of the curve. Instead, he extracts the necessary information by passing through the p-Selmer group of the Jacobian, which is often much easier to compute. The power of this method is shown in [PS14], where he and Poonen show that almost all odd degree hyperelliptic curves have only one rational point. An interesting fact about this method is that its description in [Sto17] does not seem to need any rigid analytic geometry or Coleman integration at all. Instead, one considers p-division points for points on the Jacobian.

1.1 Outline

In Section 2 we give a relatively quick overview of the main definitions in the theory of rigid analytic geometry. The theory of rigid spaces can be seen as an analog of that of complex analytic spaces for spaces over non-archimedean fields. As we will see, the main difficulty of working with non-archimedean fields is that the topology they induce on geometric spaces is totally disconnected. This makes it significantly more complicated to define a sheaf of "analytic functions" on such a space. The spaces are called *rigid*, just because the naive way of constructing such a space yields something that is very much the opposite of rigid and not suitable as analogue for a complex analytic space. The spaces obtained in this way are sometimes called *wobbly*.

Section 3 is concerned with Coleman integrals. These were developed by Coleman in [Col85a] to give a theory of integration on varieties over discretely valued subfields of $\mathbb{C}_p$ that admit a smooth model over the ring of integers of K. On abelian varieties, these integrals coincide with the Bourbaki logarithms described in [Bou98, §III.7.6].

Lastly, in Section 4 we give an overview of Coleman's effective version of Chabauty's method following his original paper [Col85b].

1.2 Acknowledgements

It is a pleasure to thank Netan Dogra for his enthusiastic supervision on the mini-project that led to these notes.

2 Rigid analytic geometry

To prepare for the definition of a Coleman integral we start by giving an overview of the basics of rigid analytic geometry. Rigid analytic spaces were introduced by Tate while studying elliptic curves with bad reduction. For an introduction to the subject we recommend [Sch98] or [Har03, §4], for details we refer the reader to [BGR84] and [FvdP04].

In this section K denotes a field that is complete with respect to a non-archimedean absolute value $|\cdot|$. We fix an algebraic closure $\overline{K}$ of K and write $\hat{\overline{K}}$ its completion (which is again algebraically closed). The absolute value $|\cdot|$ extends uniquely to an absolute value of $\hat{\overline{K}}$. The most important example for us will be $K = \mathbb{Q}_p$, in which case we denote $\hat{\overline{K}}$ as $\mathbb{C}_p$. The aim of Sections 2.1 and 2.2 is to define a class of geometric spaces over K together with the analytic functions on such a space. We want to do this in such a way that the behaviour of these rigid analytic spaces is similar to that of complex manifolds (or complex analytic spaces when allowing singularities) and their holomorphic functions. Afterwards, in Section 2.3, we will see how we can associate a rigid analytic space to certain schemes. Lastly, in Section 2.4 we introduce rigid differentials.

2.1 The unit polydisk

Let us start with an informal discussion on what analytic functions on ultrametric spaces might look like. The absolute value on K defines a totally disconnected topology on (subspaces of) K^n via the associated metric. Inspired by the complex case, our first attempt at defining an analytic function on K^n might be to say that a function is analytic if it is locally given by a convergent power series. However, since the topology of K^n is totally disconnected this definition is not very restrictive. There is a wide variety even of locally constant functions on K^n. For example, on the affine K-line, the characteristic function f_D of the open unit disk $D = \{z \in \mathbb{A}_K \mid |z| < 1\}$ is continuous and locally given by a power series. This amount of freedom in the analytic functions is not suitable for doing geometry. Instead, we want the behaviour of our functions to be more *rigid*.

The first step towards a rigid definition of analytic functions is to consider them locally on *closed* (poly)disks instead of open ones, and have them agree on overlapping boundaries. Note that such boundaries in the non-archimedean metric are open (and rather "thick"), so closed disks are also open. With this in mind, the closed unit polydisk in K^n defined as

$$B^n(K) = \{(z_1, \ldots, z_n) \in K^n \mid \max |z_i| \leq 1\}$$

will play a very important role in our theory of rigid analytic spaces, so let us think about analytic functions on B^n. We define the subalgebra of power series

$$T^n(K) = \{f \in K[\![x_1, \ldots, x_n]\!] \mid f \text{ converges on } B^n(K)\}.$$

We may also write T^n and B^n when the field K is clear from the context. The K-algebra T^n is also commonly denoted as $K\langle x_1, \ldots, x_n\rangle$. Note that a power series

$$f = \sum_{k_i \geq 0} a_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$$

is in T^n if and only if $|a_{k_1,\ldots,k_n}| \to 0$ as $k_1 + \ldots + k_n \to \infty$. Certainly, a definition of analytic functions on $B^n(K)$ should include the functions $B^n(K) \to K$ represented by elements of $T^n(K)$. The following proposition shows how we can think of $T^n(K)$ as an algebra of $\overline{K}$-valued functions on $B^n(\overline{K})$.

Proposition 2.1 ([BGR84, §5.1.4])**.** *The elements of $T^n(K)$ correspond one-to-one with the functions $f : B^n(\overline{K}) \to \overline{K}$ which*

(i) *have a power series expansion over $\overline{K}$ converging on all of $B^n(\overline{K})$ and*

(ii) *map $B^n(K)$ into K.*

We will take $T^n(\overline{K})$ as the set of analytic functions on $B^n(\overline{K})$. While it does not justify the fact that we do not allow for a larger class of analytic functions on $B^n(\overline{K})$, the following analogy with the complex case at least hints that we are thinking in the right direction:

Proposition 2.2 (Maximum modulus principle)**.** *Taking $|f| := \max |a_{k_1,\ldots,k_n}|$ defines a norm on $T^n(K)$ for which*

$$|f| = \max_{z \in B^n(\overline{K})} |f(z)|.$$

The pair $(B^n(\overline{K}), T^n(\overline{K}))$ is our first and main example of an analytic space over an non-archimedean field. In the next section we will see that it belongs to a class of spaces called *affinoid varieties*, except that those spaces will be defined in more scheme-like language.

2.2 Rigid spaces

For any maximal ideal $\mathfrak{m} \subset T^n(K)$ the residue field $T^n(K)/\mathfrak{m}$ is a finite extension of K, and can therefore be embedded in $\overline{K}$. Not specifying an embedding, the image of an element in $T^n(K)/\mathfrak{m}$ is well-defined as an element of $\overline{K}/G_K$, the set of G_K-orbits in $\overline{K}$. Then, interpreting $f \in T^n(K)$ as the map that sends $\mathfrak{m} \subset T^n(K)$ to the image of $\widetilde{f} \in T^n(K)/\mathfrak{m}$ in $\overline{K}/G_K$, we can view $T^n(K)$ as an algebra of functions on $\operatorname{SpecMax} T^n(K)$, the set of maximal ideals of $T^n(K)$. For $z \in B^n(\overline{K})$ the set

$$\mathfrak{m}_z = \{f \in T^n(K) \mid f(z) = 0\}$$

is a maximal ideal of $T^n(K)$, allowing us to define a map

$$\begin{aligned} \tau : B^n(\overline{K}) &\longrightarrow \operatorname{SpecMax} T^n(K) \\ z &\longmapsto \mathfrak{m}_z. \end{aligned}$$

Proposition 2.3 ([BGR84, §7.1.1]). *For any $f \in T^n(K)$, the square*

$$\begin{tikzcd} B^n(\overline{K}) \arrow[r, "f"] \arrow[d, "\tau"'] & \overline{K} \arrow[d] \\ \operatorname{SpecMax} T^n(K) \arrow[r, "f"] & \overline{K}/G_K \end{tikzcd}$$

commutes. Further, the map τ is surjective with finite fibres and induces a bijection

$$B^n(\overline{K})/G_K \xrightarrow{\sim} \operatorname{SpecMax} T^n(K). \tag{2.1}$$

This shows that, up to Galois action, there is essentially no difference between viewing elements of $T^n(K)$ as functions on $B^n(\overline{K})$ or on $\operatorname{SpecMax} T^n(K)$. Note also that G_K acts *isometrically* on $B^n(\overline{K})$ [BGR84, §7.1.1], which basically means that the metric on $B^n(\overline{K})$ descends nicely to the set of Galois orbits. Therefore the identification (2.1) induces a topology on $\operatorname{SpecMax} T^n(K)$, called the *canonical toppology.* In particular the canonical topology is Hausdorff and totally disconnected.

The upshot of all this is that, encouraged by the success of schemes in algebraic geometry, we can view the space $(\operatorname{SpecMax} T^n(\overline{K}), T^n(\overline{K}))$ as an algebraically defined geometric model for the analytic space $(B^n(\overline{K}), T^n(\overline{K}))$. From now on, this will be the viewpoint we adopt. Our construction of rigid analytic spaces will be very similar to that of schemes. We start with so-called affinoid varieties, which, as the name suggests, are rigid analytic analogues of affine schemes.

Definition 2.4 (Tate/affinoid algebra). A K-algebra A is called *affinoid* if there exist an $n \in \mathbb{N}$ and an ideal $\mathfrak{a} \subset T^n(K)$ such that $A \cong T^n(K)/\mathfrak{a}$. Such A are also called *Tate algebras*[2].

Similar to the case of T^n, we can view elements of an affinoid algebra A as functions $\operatorname{SpecMax} A \to \overline{K}$.

Definition 2.5 (Affinoid space). We define an *affinoid space* as a pair $(\operatorname{SpecMax} A, A)$ where A is an affinoid algebra.

Example 2.6. From the above definition we see that the rigid analytic analogue of $\mathbb{A}^n_K$ is the *unit polydisk over K* defined as

$$\mathbb{B}^n(K) = (\operatorname{SpecMax} T^n(K), T^n(K)).$$

For algebraically closed K, we have seen that the spaces $\mathbb{B}^n(K)$ and $(B^n(K), T^n(K))$ are essentially the same. Note, however, that generally this is not the case, as an be seen from the fact that if K is not algebraically closed then the map in (2.1) does not define a bijection between $B^n(K)$ and $\operatorname{SpecMax}(T^n(K))$ ♢

Keeping up the analogy with schemes, we would like to be able to study analytic functions on affinoid varieties *locally*, even on $\mathbb{B}^n(K)$ itself. In other words, we want to replace the function algebra A with a sheaf of analytic functions on $\operatorname{SpecMax} A$ such that affinoid varieties become ringed spaces (in fact they will be locally ringed spaces). For an affinoid algebra $A = T^n(K)/(f_1, \ldots, f_r)$, the bijection given in (2.1) generalises as

$$\{z \in B^n(\overline{K}) \mid f_i(z) = 0\}/G_K \xrightarrow{\sim} \operatorname{SpecMax} A.$$

[2]Note that some authors reserve the name Tate algebra for the rings T^n themselves, like in [BGR84].

Similar to before this induces a *canonical topology* on $\operatorname{SpecMax} A$ that is Hausdorff and totally disconnected. This disconnectedness gives problems when trying to define a sheaf of analytic functions on an affinoid space, e.g. because, as we saw in Section 2.1, even locally constant functions on a totally disconnected space can have wild global behaviour. Furthermore, it turns out that when proceeding to define such a sheaf for the canonical topology in a natural way, not every morphism of such locally K-ringed spaces will be induced by a K-algebra homomorphism between the corresponding affinoid algebras [Har03, p. 64]. The analytic K-spaces obtained in this way are called "wobbly". Note that, instead of the canonical topology, we could consider the Zariski topology on $\operatorname{SpecMax} A \subset \operatorname{Spec} A$. In fact every Zariski open set is also open in the canonical topology. It turns out, however, that the Zariski topology is too extreme in the other direction. It is too course to give a useful theory of K-analytic spaces. So in order to *rigidify* the theory of wobbly spaces we have to go somewhere in between the two.

Definition 2.7 (G-topology [FvdP04, Definition 2.4.1])**.** Let X be a set. A *G-topology* on X consists of

(i) a family $\mathcal{F}$ of subsets of X such that $\emptyset, X \in \mathcal{F}$ and if $U, V \in \mathcal{F}$ then $U \cap V \in \mathcal{F}$, and

(ii) for each $U \in \mathcal{F}$ a set $\operatorname{Cov}(U)$ of coverings of U by elements of $\mathcal{F}$, satisfying the following properties:

- $\{U\} \in \operatorname{Cov}(U)$.
- If $V \in \mathcal{F}$ with $V \subset U$ and $\mathscr{U} \in \operatorname{Cov}(U)$ then the covering

$$\mathscr{U} \cap V := \{U' \cap V \mid U' \in \mathscr{U}\}$$

belongs to $\operatorname{Cov}(V)$.

- For a covering $\{U_i\}_{i \in I} \in \operatorname{Cov}(U)$ and a family of coverings $\mathscr{U}_i \in \operatorname{Cov}(U_i)$, the union

$$\bigcup_{i \in I} \mathscr{U}_i := \{U' \mid U' \in \mathscr{U}_i \text{ for some } i \in I\}$$

belongs to $\operatorname{Cov}(U)$.

Elements of $\mathcal{F}$ are called *admissible* or *G-open* subsets of X. For an admissible subset $U \subset X$ the elements of $\operatorname{Cov}(U)$ are called *admissible coverings*.

The G in G-topology stands for Grothendieck, as they are a special kind of *Grothendieck topologies* (which we will not define here). Note that the admissible subsets of a set X can not, in general, be viewed as the open sets of a topology on X, because arbitrary unions of admissible subsets are not necessarily again admissible in X. In these notes, we will always assume that a G-topology further satisfies the following two axioms:

(G_1) A subset $V \subset U$ of an admissible open U is admissible if and only if there exists an admissible covering $\{U_i\}_{i \in I} \in \operatorname{Cov}(U)$ such that $U_i \cap V$ is admissible for all $i \in I$.

(G_2) Let $\mathscr{U} = \{U_i\}_{i \in I}$ be a covering of an admissible subset U such that U_i is admissible for all $i \in I$. If $\mathscr{U}$ has a refinement that is admissible, then $\mathscr{U}$ is admissible.

For an affinoid algebra A, there exists a G-topology on $X = \operatorname{SpecMax} A$ called the *strong G-topology* on X. Here we will forgo its definition, but the curious reader can find it for example in [BGR84]. Even though the strong G-topology on X is not really a topology, it satisfies our requirements in the following sense:

- All admissible subsets $U \subset X$ are open in the canonical topology, and all Zariski open sets are admissible.
- The strong G-topology provides just enough structure to work with sheaves on X.

The fact that we can define sheaves on G-topological spaces allows us to consider (locally) G-ringed spaces.

Definition 2.8. A *G-ringed space* is a pair $(X, \mathscr{O}_X)$ where X is a G-topological space and $\mathscr{O}_X$ is a sheaf of rings with respect to the G-topology on X. If further for every $x \in X$ the stalk $\mathscr{O}_{X,x}$ is a local ring we call $(X, \mathscr{O}_X)$ a *locally G-ringed space*.

A *morphism of G-ringed spaces* $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is a pair (f, f^*) where

- $f : X \to Y$ is *G-continuous*, meaning that for every admissible $U \subset Y$ the preimage $f^{-1}(U)$ is admissible in X and for every admissible covering $\{U_i\}_{i \in I} \in \mathrm{Cov}(U)$ the set $\{f^{-1}(U_i)\}_{i \in I}$ is an admissible covering of $f^{-1}(U)$,
- f^* is a collection of ring homomorphisms

$$f_V^* : \mathscr{O}_Y(V) \to \mathscr{O}_X(f^{-1}(V)),$$

  one for each admissible subset $V \subset Y$, such that they are compatible with the restriction homomorphisms.

A *morphism of locally G-ringed spaces* has the further requirement that for every $x \in X$ the induced ring homomorphism $f_x^* : \mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ on the corresponding stalks is *local*, meaning that it maps the maximal ideal of $\mathscr{O}_{Y,f(x)}$ into that of $\mathscr{O}_{X,x}$.

If $\mathscr{O}_X$ is a sheaf of R-algebras for a fixed ring R then we call $(X, \mathscr{O}_X)$ a *(locally) G-ringed space over R*. Morphisms between such spaces are called *R-morphisms* and have the extra requirement that the homomorphisms f_V^* are R-algebra homomorphisms.

Let $X = \operatorname{SpecMax} A$ for some affinoid K-algebra A, equipped with the strong G-topology. For admissible subsets $U \subset X$ we define a set of analytic functions on U. This can be done in a natural way such that one obtains a sheaf of K-algebras $\mathscr{O}_X$ on X that in certain ways behaves similar to the structure sheaf of an affine scheme [Ach20, §6.2]. Note that the K-algebras $\mathscr{O}_X(U)$ are not, in general, affinoid algebras. Of course, the sheaf of analytic functions is consistent with our previous discussion in the sense that $\mathscr{O}_X(X) = A$. The stalks of $\mathscr{O}_X$ are in fact local rings, making X into a locally G-ringed space over K. From now on, we will view an affinoid space as a locally G-ringed space $(X, \mathscr{O}_X)$ where $X = \operatorname{SpecMax} A$ for some affinoid algebra A and $\mathscr{O}_X$ is its sheaf of analytic functions. The affinoid space corresponding to the affinoid algebra A is also denoted $\operatorname{Sp} A$.

Definition 2.9 (Rigid analytic space)**.** A *rigid analytic space X over K* is a locally G-ringed space $(X, \mathscr{O}_X)$ over K admitting an admissible covering $\{U_i\}_{i \in I}$ where $(U_i, \mathscr{O}_X|_{U_i})$ is an affinoid space for every $i \in I$.

A *morphism of rigid spaces over K* is simply any K-morphism of locally G-ringed spaces over K between two rigid analytic spaces.

As we do with schemes, we may write just X instead of $(X, \mathscr{O}_X)$.

Remark 2.10. We say $(X, \mathscr{O}_X)$ is a (locally) G-ringed space over another (locally) G-ringed space $(Y, \mathscr{O}_X)$ if we have specified a morphism of (locally) G-ringed spaces $(X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$. In this way, given a rigid analytic space X, we can work with rigid analytic spaces over X and define morphisms between them analogous to how this works for S-schemes. This way, the property of being a rigid analytic space over K in the sense of Definition 2.8 becomes equivalent to being a rigid analytic space over the one-point space $\operatorname{Sp} K = \operatorname{Spec} K$ [Ach20, p. 74]. $\diamondsuit$

A common way for constructing rigid analytic spaces is by *glueing* (or *pasting*) together a set of affinoid spaces. The following proposition explains this procedure.

Proposition 2.11 ([FvdP04, §4.3]). *Suppose that we have the following data:*

- *a family $\{X_i\}_{i \in I}$ of affinoid spaces over K, and*
- *for every pair $(i, j) \in I^2$ a rigid analytic subspace $X_{i,j} \subset X_i$ and an isomorphism $\varphi_{j,i} : X_{i,j} \to X_{j,i}$ of rigid spaces over K.*

Further assume these data to satisfy

(i) $X_{i,i} = X_i$ *and* $\varphi_{i,i} = \mathrm{id}$ *for all* i*,*

(ii) $\varphi_{i,j}$ *is inverse to* $\varphi_{j,i}$ *for all* $(i, j) \in I^2$*,*

(iii) *For all* $(i, j, k) \in I^3$ *we have* $\varphi_{j,i}(X_{i,j} \cap X_{i,k}) = X_{j,i} \cap X_{j,k}$ *and on* $X_{i,j} \cap X_{i,k}$ *it holds that* $\varphi_{k,i} = \varphi_{k,j} \circ \varphi_{j,i}$*.*

Then there exists a unique rigid analytic space Y over K with an admissible covering $\{Y_i\}$, such that each Y_i is an affinoid space over K provided with an isomorphism $\psi_i : X_i \to Y_i$ of rigid analytic spaces such that, for all $(i, j) \in I^2$, the restriction $\psi_i|_{X_{i,j}}$ is an isomorphism from $X_{i,j}$ to $Y_i \cap Y_j$. Moreover, then $\psi_i|_{X_{i,j}} = \psi_k|_{X_{j,i}} \circ \varphi_{j,i}$. The G-topology on Y is characterised by the facts that a subset $U \subset Y$ is admissible if and only if $U \cap X_i$ is admissible in X_i for all i, and for such U a covering $\{U_l\}_{l \in \ell}$ of U by admissible subsets U_l is admissible if and only if $\{U_l \cap X_i\}$ is and admissible covering of $U \cap X_i$ for all i.

Note that in the above proposition a set $X_{i,j}$ is allowed to be empty, in which case $X_{j,i}$ is also empty and the morphisms $\varphi_{i,j}$ and $\varphi_{j,i}$ do not exist.

2.3 Rigid spaces of projective flat schemes over $\mathcal{O}_K$

In this subsection we will construct a specific class of rigid analytic spaces obtained from projective flat schemes over valuation rings following [FvdP04, Example 4.8.4]. First, we fix some notation. For this subsection the field K will be assumed to be discretely valued (in addition to the assumptions stated at the beginning of this section). Further, we write $\mathcal{O}_K$ for the valuation ring of K and fix a uniformizer π such that (π) is the unique maximal ideal of $\mathcal{O}_K$. The residue field $\mathcal{O}_K/(\pi)$ will be denoted as k.

Let X be a projective flat scheme over $\mathcal{O}_K$. Then there exists a graded $\mathcal{O}_K$-algebra $A = \oplus_{n \geq 0} A_n$ such that $X = \operatorname{Proj}(A)$, where A satisfies:

- $A_0 = \mathcal{O}_K$,
- for all $n \geq 0$, A_n is a free $\mathcal{O}_K$-module of finite rank,
- A is generated by A_1 over $\mathcal{O}_K$.

We write X_K for the generic fiber of X, which is given by

$$X_K = X \times_{\mathcal{O}_K} \operatorname{Spec} K = \operatorname{Proj}(A \otimes_{\mathcal{O}_K} K).$$

The generic fiber is an open subscheme of X and can be viewed as a scheme over K by its projection onto $\operatorname{Spec} K$. The special fiber of X is denoted X_s, and is given by

$$X_s = X \times_{\mathcal{O}_K} \operatorname{Spec} k = \operatorname{Proj}(A \otimes_{\mathcal{O}_K} k).$$

The special fiber is a closed subscheme of X and can be viewed as a scheme over k. In what follows we will assume that X_s is reduced, implying that X_K is also reduced.

Let X_K^0 the set of closed points in X_K. We define a reduction map $\rho_X : X_K^0 \to X_s$ on the level of sets as

$$\{\rho_X(x)\} = \overline{\{x\}} \cap X_s,$$

where $\overline{\{x\}}$ is the Zariski closure of $\{x\}$ in X. This map is well-defined in the sense that for a closed point $x \in X_K^0$ the intersection $\overline{\{x\}} \cap X_s$ contains exactly one point [FvdP04, p. 103]. Note that ρ_X is not a morphism, and not even continuous.

Proposition 2.12 ([FvdP04, p. 104])**.** *The reduction map ρ_X is surjective onto the closed points of X_s and a closed map (meaning it sends closed subsets to closed subsets).*

Now, we will associate a rigid analytic space to X. Let $e_1, \ldots, e_m$ be an $\mathcal{O}_K$-basis of A_1. Note that $A[\frac{1}{e_i}]$ is a graded $\mathcal{O}_K$-algebra for every i. Then the set $\{X(i)\}$ where $X(i) = \operatorname{Spec} A[\frac{1}{e_i}]_0$ forms an open affine covering of X. For each $i \in \{1, \ldots, m\}$ the scheme $X(i)$ is an affine scheme over $\mathcal{O}_K$, so we can take its special fiber $X(i)_K$. The set $\{X(i)_K\}$ forms an open affine covering of X_K. For each i we consider the π-adic completion

$$B_i = \varprojlim A[\tfrac{1}{e_i}]_0/(\pi^n).$$

Then the ring

$$A_i = B_i \otimes_{\mathcal{O}_K} K$$

is an affinoid algebra over K for every $i \in \{1, \ldots, m\}$ [FvdP04, p. 104].

Definition 2.13. We define the rigid analytic space X_K^{an} associated to the projective flat scheme X over $\mathcal{O}_K$ as the space obtained by glueing[3] the affinoid spaces $\{\operatorname{Sp} A_i\}_{1 \le i \le m}$.

On the level of sets, we can think of X_K^{an} as the closed points on the generic fiber X_K of X. Then ρ_X defines a map

$$\rho_X : X_K^{\mathrm{an}} \to X_s$$

that is surjective onto the closed points of X_s.

2.4 Rigid differentials

Before defining differentials on an affinoid space, let us first recall the notion of *relative differentials* from algebraic geometry (see e.g. [Liu02, §6.1]).

Let A be a ring, B an A-algebra, and M a B-module. An *A-derivation of B into M* is an A-linear map $d : B \to M$ satisfying the Leibniz rule

$$d(b_1 b_2) = b_1 db_2 + b_2 db_1, \qquad \text{for } b_1, b_2 \in B,$$

and such $da = 0$ for all $a \in A$. Note that the latter automatically follows from the Leibniz rule and the A-linearity of d. The set of all A-derivations of B into M is denoted $\operatorname{Der}_A(B, M)$.

[3] This still needs a description of the $X_{i,j}$ as in Proposition 2.11

Definition 2.14. The *module of relative differential forms of B over A* is the B-module $\Omega^1_{B/A}$ endowed with an A-derivation $d : B \to \Omega^1_{B/A}$ having the following universal property:

> For every B-module M and every A-derivation $d' : B \to M$, there is a unique B-module homomorphism $\varphi : \Omega^1_{B/A} \to M$ such that the following diagram commutes:

$$\begin{tikzcd} B \arrow[r, "d'"] \arrow[d, "d"'] & M. \\ \Omega^1_{A/B} \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

This definition of course only makes sense if such a module actually exists, but fortunately that is the case.

Proposition 2.15. *The module $(\Omega^1_{A/B}, d)$ exists and is unique up to isomorphism.*

We can define differential forms on a scheme by glueing the modules of differential forms on its affine open subsets. For a morphism $f : X \to Y$ of schemes there exists a quasi-coherent sheaf $\Omega^1_{X/Y}$ called the *sheaf of relative differentials of degree* 1 *over* Y. If $Y = \operatorname{Spec} A$ we may also write $\Omega^1_{X/A}$, or just Ω^1_X if Y is clear from the context.

Now let us return to rigid spaces. We assume that K is perfect.

Definition 2.16. Let A be an affinoid algebra over K. We define the *universal finite differential module of A/K* as the A-module ${}_f\Omega^1_{A/K}$ equipped with a K-derivation $d = d_{A/K} : A \to {}_f\Omega^1_{A/K}$ having the following universal property:

> For every finitely generated A-module M and every K-derivation $d' : A \to M$ there is a unique A-module homomorphism $\varphi : {}_f\Omega^1_{A/K} \to M$ such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "d'"] \arrow[d, "d"'] & M. \\ {}_f\Omega^1_{A/K} \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Proposition 2.17 ([FvdP04, Theorem 3.6.1])**.** *The universal finite differential module exists.*

We also call ${}_f\Omega^1_{A/K}$ the *module of rigid differentials* on the affinoid space $\operatorname{Sp} A$. Note that most modern literature uses a slightly different definition of rigid differentials, see Remark 2.19 below. It is also important to note that ${}_f\Omega^1_{A/K}$ is in general not equal to $\Omega^1_{A/K}$, see e.g. [FvdP04, Remarks 3.6.2]. Following [Col85a, §I.3], we write ${}_f\Omega^i_{A/K}$ for the i'th exterior power of ${}_f\Omega^1_{A/K}$. We can naturally extend the derivation d to maps d^i to obtain a cochain complex

$$0 \longrightarrow A = {}_f\Omega^0_{A/K} \xrightarrow{d=d^0} {}_f\Omega^1_{A/K} \xrightarrow{d^1} {}_f\Omega^2_{A/K} \xrightarrow{d^2} \cdots.$$

Similar to how we defined $\Omega^1_{X/Y}$ for schemes $X \to Y$, for a general rigid space X over K the above construction can be used to define a complex $({}_f\Omega^\bullet_{X/K}, d)$ of sheaves with respect to the G-topology on X. Then, for an affinoid algebra A, the module ${}_f\Omega^1_{A/K}$ is equal to ${}_f\Omega^1_{X/K}(X)$ where $X = \operatorname{Sp} A$. We also consider the sheaf cohomology groups $H^j(X, {}_f\Omega^i_{X/K})$. Of particular interest for us will be the *differentials of the first kind*, or *holomorpic differentials*, which are the elements of $H^0(X, {}_f\Omega^1_{X/K}) \cong {}_f\Omega^1_{X/K}(X)$.

Example 2.18. The holomorphic differentials on the one-dimensional unit polydisk $\mathbb{B}^1(K) = \operatorname{Sp} K\langle z\rangle$ are given by

$$H^0(X, {}_f\Omega^1_{\mathbb{B}^1/K}) = {}_f\Omega^1_{\mathbb{B}^1/K}(\mathbb{B}^1) = K\langle z\rangle dz.$$

$\diamondsuit$

Remark 2.19. The definition of rigid differentials we give here is in some ways not a good analogue of differentials on complex analytic spaces. For example, since $\mathbb{B}^1$ is the rigid analytic analogue of $\mathbb{A}^1$, one would expect its first cohomology to be trivial. With our definition this is not the case, as explained by Besser in [Bes12, §1.3.2]. There he also shows how this can be remedied by replacing the affinoid algebras in Definition 2.16 by so-called *weakly complete finitely generated (wcfg) algebras*. These are often denoted with a dagger: $A^\dagger$.

Recall that the elements of T^n are the power series $f \in K[\![x_1, \dots, x_n]\!]$ converging on the closed unit polydisk B^n. For $r \in \mathbb{R}_{>0}$ we let B^n_r denote the closed polydisk of radius r. Then we define

$$(T^n)^\dagger = \{f \in \mathcal{O}_K[\![x_1, \dots, x_n]\!] \mid \exists r > 1 \text{ such that } f \text{ converges on } B^n_r(K)\}.$$

We see that the elements of $(T^n)^\dagger$ are *overconvergent* in the sense that they converge on a slightly larger polydisk than the unit polydisk. In general, an $\mathcal{O}_K$-algebra $A^\dagger$ is called wcfg if there exists a surjective algebra-homomorphism $(T^n)^\dagger \to A^\dagger$. To such an $\mathcal{O}_K$-algebra $A^\dagger$ we associate the K-algebra A obtained by completing $A^\dagger \otimes_{\mathcal{O}_K} K$ with respect to the quotient norm induced from $(T^n)^\dagger$. In particular, if $A^\dagger = (T^n)^\dagger/\mathfrak{a}$ then $A = T^n/\mathfrak{a}$, so A is affinoid.

Nowadays the standard definition of rigid differentials is with respect to wcfg algebras, which is more restrictive than the one in terms of affinoid algebras we gave above. However, in this document we stick to the latter because this is what Coleman used in [Col85b] when describing his effective version of Chabauty's method. $\diamondsuit$

3 Coleman integration

In this section we present (part of) a theory of integration on certain algebraic varieties over discretely valued complete subfields K of $\mathbb{C}_p$. This theory was developed by Coleman in [Col85a], and plays an important role in his effective version of Chabauty's method as described in [Col85b].

3.1 Models of curves and abelian varieties

We start this section by briefly recalling some definitions in the language of schemes relating to models and reductions of curves and abelian varieties. All scheme-theoretic language used in these notes comes directly from the book *Algebraic Geometry and Arithmetic Curves* by Qing Liu [Liu02]. In particular, we adopt the following terminology from [Liu02, Example 3.2.3]: for any field K, an *algebraic variety over K* is a scheme of finite type over $\operatorname{Spec} K$. An algebraic variety over K whose irreducible components are of dimension 1 is called an *algebraic curve (over K)*, or simply a *curve*.

Let S be a Dedekind scheme of dimension 1 with function field $K = K(S)$ and generic point η. In this subsection there are no further assumptions on the field K.

Definition 3.1 (Model)**.** Let X be a normal, connected, projective curve over K. A *model of X over S* consists of the following data:

- an integral, projective, flat S-scheme $\mathcal{X}$ of dimension 2 with generic fiber $\mathcal{X}_\eta$, and
- an isomorphism $\mathcal{X}_\eta \cong X$.

Generally speaking, we will say that a model $\mathcal{X}$ has a certain property if the structural morphism $\mathcal{X} \to S$ has that property, i.e. if it satisfies the property as an S-scheme.

Remark 3.2. In practice, we usually do not bother with specifying the isomorphism between $\mathcal{X}_\eta$ and X as it is rarely useful. $\diamondsuit$

Given a model $\mathcal{X} \to S$ of a curve X over K, for every closed point $s \in S$ we call the fiber $\mathcal{X}_s$ a *reduction of* X *at* s. In our case S will often be the spectrum of a Dedekind domain A. Then the point s corresponds to a maximal ideal $\mathfrak{p}$ of A, and we call $\mathcal{X}_s$ a *reduction of* C *modulo* $\mathfrak{p}$. In that case the fiber $\mathcal{X}_s$ has the structure of a scheme over the residue field $A/\mathfrak{p}$. Note that different models over S of C can give rise to very different reductions.

Definition 3.3 (Good reduction)**.** Let X be a normal, connected, projective curve over K. We say that X has *good reduction at* $s \in S$ if there exists a smooth model of X over $\operatorname{Spec} \mathscr{O}_{S,s}$. If this is not the case, we say that X has *bad reduction at* s.

Remark 3.4. Note that in order to have good reduction, X itself must be smooth. $\diamondsuit$

Now, we switch from curves to abelian varieties. To define all the notions involved would take us too far from the purpose of these notes, so for that we refer the reader to [Liu02] and [Lic11]. Let R be a discrete valuation ring with field of fractions K.

Definition 3.5. An abelian variety A over K is said to have *good reduction* if there exists an abelian scheme $\mathcal{A} \to \operatorname{Spec} R$ with generic fiber A.

For us, it is not too important what the above definition means exactly. We just note the similarity with Definition 3.3 (abelian schemes are smooth). Every abelian variety A over K admits a so-called *Néron model* $\mathcal{A} \to \operatorname{Spec} R$, which, in particular, is smooth, connected[4], separated and of finite type. The main results we will use are the following:

Proposition 3.6 ([Lic11, Corollary 2.2.7])**.** *If* A *has good reduction then its Néron model is an abelian scheme. In particular it is proper.*

In fact, since $\operatorname{Spec} R$ is normal, we can replace the word proper by projective in the above proposition (see e.g. [Dol14]).

Proposition 3.7 ([Mil08, Proposition IV.4.1])**.** *Let* X *be a curve over a number field* K*. If* X *has good reduction at a prime* $\mathfrak{p}$ *of* K*, then so does its Jacobian.*

3.2 The rigid space of a curve

Now, consider the results from the previous subsection in the case that K is as in Section 2.3. As before, we write $\mathcal{O}_K$ for the valuation ring of K. Note that $\mathcal{O}_K$ is a discrete valuation ring (and hence Dedekind), so $\operatorname{Spec} \mathcal{O}_K$ is a Dedekind scheme. If X is a normal, connected, projective curve over K, then a model over $\operatorname{Spec} \mathcal{O}_K$ of X is in particular a projective flat scheme over $\mathcal{O}_K$. Therefore, by Section 2.3, it has an associated rigid analytic space $\mathcal{X}_K^{\mathrm{an}}$. Recall that, as a set, we can view this rigid analytic space as the special fiber $\mathcal{X}_K$ of $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$, which is exactly the curve X.

[4]The reader, like the author, might be confused by seeing something like "connected component of the Néron model" written elsewhere. See `https://mathoverflow.net/questions/43054/basic-properties-of-neron-models` for clarification.

Definition 3.8. With notation as above, we call $\mathcal{X}_K^{\text{an}}$ the *rigid analytic space of the curve X*

Remark 3.9. Note that, at least a priori, this definition depends on the chosen model $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ of X. $\diamondsuit$

Similarly, since the Néron model $\mathcal{J} \to \operatorname{Spec} \mathcal{O}_K$ of the Jacobian $\mathcal{J}_K$ of such a curve is projective, we can use the same construction to define the rigid analytic space $\mathcal{J}_K^{\text{an}}$ of the Jacobian.

Remark 3.10. More generally, to any algebraic variety X over K we can associate a rigid analytic space X^{an}, see [BGR84, §9.3.4] for the construction. It even works for any scheme locally of finite type over K. $\diamondsuit$

Since $\mathcal{O}_K$ is local, the scheme $\operatorname{Spec} \mathcal{O}_K$ has exactly one closed point s corresponding to its maximal ideal (π). Therefore X has exactly one reduction $\mathcal{X}_s$. Recall that the reduction map

$$\rho_{\mathcal{X}} : \mathcal{X}_K^{\text{an}} \to \mathcal{X}_s$$

is surjective onto the closed points of $\mathcal{X}_s$.

Definition 3.11 (Residue disk)**.** For every closed point $t \in \mathcal{X}_s$, the preimage $\rho_{\mathcal{X}}^{-1}(t) \subset \mathcal{X}_K^{\text{an}}$ is called a *residue disk*. It is a rigid analytic subspace of $\mathcal{X}_K^{\text{an}}$ isomorphic to $\mathbb{B}^1(K)$ (hence the name *disk*).

In the next section where we describe Coleman's effective version of Chabauty's method, the residue field will be finite, meaning that $\mathcal{X}_K^{\text{an}}$ is covered by a finite set of (disjoint) residue disks. It will turn out to be convenient to consider things locally on each residue disk. In particular, a map $\mathcal{X}_K^{\text{an}} \to \overline{K}$ is called *locally analytic* if it's restriction to each residue disk (which is an affinoid space) is analytic. Note that this does certainly not imply that the function is analytic on the whole of $\mathcal{X}_K^{\text{an}}$. Further, we can consider a differential $\omega \in {}_f\Omega_{\mathcal{X}_K^{\text{an}}/K}(\mathcal{X}_K^{\text{an}})$ locally on each residue disk as a differential on that residue disk. Since the residue disks are isomorphic to $\mathbb{B}^1(K)$, this implies by Example 2.18 that there exists a *local parameter* or *local coordinate t* in the function field of the curve such that, on that residue disk, ω is of the form

$$\omega = \sum_{i \geq 0} a_i t^i dt, \qquad a_i \in K.$$

3.3 Coleman integration on curves

Note: This subsection is in a sense completely separate from the rest of this section. Please skip it, I only include it because it was part of the project I handed in.

We will define Coleman integrals on curves following [Bal11, §3.1]. Please note that for this section we need the definition of rigid differentials in terms of wcfg algebras mentioned in Remark 2.19. For this section we fix a prime number p and we let $K = \mathbb{C}_p$ with valuation ring $\mathcal{O} = \mathcal{O}_K$. We further fix a branch of the p-adic logarithm $\operatorname{Log} : \mathbb{C}_p^\times \to \mathbb{C}_p$, whose restriction to the disk $\{z \in \mathbb{C}_p : |z - 1| < 1\}$ is given by

$$\log x = -\sum_{i=1}^{\infty} \frac{(1-x)^i}{i}.$$

For an open subinterval I of $[0, +\infty)$ we let $A(I)$ denote the affinoid annulus (or disk) $\{z \in \mathbb{A}^1_{\mathbb{C}_p} \mid |z| \in I\}$. A differential $\omega \in {}_f\Omega^1_{A(I)/\mathbb{C}_p}(A(I))$ can be written as $\omega = \sum_{i \in \mathbb{Z}} c_i t^i dt$ for some local coordinate t in the function field of $\mathbb{P}^1_{\mathbb{C}_p}$.

Definition 3.12. For $P, Q \in A(I)$ and $\omega = \sum_{i\in\mathbb{Z}} c_i t^i dt \in {}_f\Omega^1_{A(I)/\mathbb{C}_p}(A(I))$ we define

$$\int_P^Q \omega = c_{-1}\operatorname{Log}(Q/P) + \sum_{i\neq -1} \frac{c_i}{i+1}(Q^{i+1} - P^{i+1}).$$

This is independent of the choice of local coordinate t for $A(I)$.

Let $\mathcal{X} \to \operatorname{Spec}\mathcal{O}$ be a smooth connected model of a normal, connected, projective curve X over $\mathbb{C}_p$. Using the above definition, we can compute integrals on residue disks on $\mathcal{X}^{\mathrm{an}}_{\mathbb{C}_p}$ by mapping the disk into some $A(I)$. Although $\mathcal{X}^{\mathrm{an}}_{\mathbb{C}_p}$ is covered by residue disks, the disks are also pairwise disjoint. This makes is hard to define integrals between points in different residue disks, as we cannot use the trick of taking an intermediate point on the overlap of two disks two divide the integral in two parts, both contained in a single residue disk. What Coleman discovered is that this can be fixed by requiring that the integrals behave nicely with respect to Frobenius action on the differentials. This is called Dwork's principle of continuation along the Frobenius. We also need to restrict to *wide open subspaces* on $\mathcal{X}^{\mathrm{an}}_{\mathbb{C}_p}$.

Definition 3.13. We call the affinoid space given as a set by $\{z \in \mathbb{C}_p \mid |z| \leq r\}$ the *closed disk of radius* r. A *diskoid* is an affinoid space isomorphic to a finite union of closed disks with radii < 1. We call an affinoid subspace of $\mathcal{X}^{\mathrm{an}}_K$ a *wide open subspace* if it is isomorphic to the complement of a diskoid subspace of $\mathcal{X}^{\mathrm{an}}_K$.

Let W be a wide open subspace of $\mathcal{X}^{\mathrm{an}}_{\mathbb{C}_p}$. We denote by $\operatorname{Div}(W)$ the free abelian group generated by the points on W, and we let $\operatorname{Div}^0(W)$ denote the kernel of the homomorphism $\deg : \operatorname{Div}(W) \to \mathbb{Z}$ sending each point on W to 1.

Theorem 3.14 (Coleman, [Bal11, Theorem 3.1.5])**.** *There is a unique map*

$$\mu_W : \operatorname{Div}^0(W) \times {}_f\Omega^1_{W/\mathbb{C}_p}(W) \to \mathbb{C}_p$$

such that

(i) *(Linearity) The map μ_W is linear on $\operatorname{Div}^0(W)$ and $\mathbb{C}_p$-linear on ${}_f\Omega^1_{W/\mathbb{C}_p}(W)$.*

(ii) *(Compatibility) For every residue disk $D \subset X$ and any choice of isomorphism $\psi : W \cap D \to A(I)$ for some interval I, the restriction of μ_W to $\operatorname{Div}^0(W \cap D) \times {}_f\Omega^1_{W/\mathbb{C}_p}(W)$ is compatible with Definition 3.12.*

(iii) *(Change of variables) Suppose that W' is another wide open subspace of another curve $\mathcal{X}' \to \mathcal{O}$, and suppose that $\psi : W \to W'$ is a morphism of rigid spaces corresponding to a continuous automorphism of $\mathbb{C}_p$. Then*

$$\mu'_W(\psi(\cdot), \cdot) = \mu_W(\cdot, \psi^*(\cdot)).$$

(iv) *(Fundamental theorem of calculus) For any divisor $D = \sum_i c_i P^i \in \operatorname{Div}^0(W)$ and any analytic function $f \in \mathscr{O}_W(W)$ we have*

$$\mu_W(D, df) = \sum_i c_i f(P_i).$$

One should think of the map μ_W as integration on W, where the divisor argument specifies the begin and endpoints of integration and the differential is the function being integrated.

3.4 Coleman's original integration

We fix a rational prime p, and we let K be a complete discretely valued subfield of $\mathbb{C}_p$ with valuation ring $\mathcal{O}_K$ and residue field k. In this section we define a theory of integration for varieties over K with smooth proper models over $\mathcal{O}_K$, following [Col85a, §II]. However, for the sake of simplicity and because it is all we need to follow effective Chabauty in [Col85b], we restrict ourselves to just the integration of differentials of the first kind.

Let $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ be a smooth, proper and connected scheme. Further, let ω be a differential of the first kind on $\mathcal{X}$, meaning $\omega \in H^0(\mathcal{X}_K^{\mathrm{an}}, {}_f\Omega^1_{\mathcal{X}_K^{\mathrm{an}}/K})$. Coleman showed that in that case there exists a locally analytic function $f_\omega : \mathcal{X}_K(\mathbb{C}_p) \to \mathbb{C}_p$ such that $df_\omega = \omega$. Here we identify points in $\mathcal{X}_K(\mathbb{C}_p)$ with points on $\mathcal{X}_{\mathbb{C}_p}^{\mathrm{an}}$. Further, by adding an extra requirement on f_ω relating to Dwork's principle of continuation along the Frobenius, the function will in fact be uniquely determined. For points $P, Q \in \mathcal{X}_K(\mathbb{C}_p)$ we set

$$\int_P^Q \omega = f_\omega(Q) - f_\omega(P).$$

Proposition 3.15 ([Col85a, Prop. 2.4])**.**

(i) *(Additivity) For two differentials $\omega, \omega' \in H^0(\mathcal{X}_K^{\mathrm{an}}, {}_f\Omega^1_{\mathcal{X}_K^{\mathrm{an}}/K})$ we have*

$$\int_P^Q \omega + \omega' = \int_P^Q \omega + \int_P^Q \omega'.$$

(ii) *(Fundamental theorem of calculus) If $\omega = df$ for some analytic function on $\mathcal{X}_{\mathbb{C}_p}^{\mathrm{an}}$ then*

$$\int_P^Q \omega = f(Q) - f(P).$$

(iii) *(Change of variables) Let $g : \mathcal{Y} \to \mathcal{X}$ be a morphism of smooth proper schemes over $\mathcal{O}_K$ on which Frobenius acts properly. Then*

$$\int_P^Q g^*\omega = \int_{g(P)}^{g(Q)} \omega.$$

We will not define here the meaning of the words "on which Frobenius acts properly". The only thing we will say about it is that we have the following result.

Proposition 3.16 ([Col85a, Theorem 1.4])**.** *Frobenius acts properly on every smooth projective scheme over $\mathcal{O}_K$.*

In addition to Proposition 3.15(iii), given a morphism $g : \mathcal{Y}_K \to \mathcal{X}_K$ between the generic fibers of $\mathcal{X}$ and $\mathcal{Y}$ it holds that

$$\int_P^Q g^*\omega = \int_{g(P)}^{g(Q)} \omega. \tag{3.1}$$

4 Coleman's effective Chabauty

With the results from the previous sections we are finally ready to look at Coleman's effective version of Chabauty's method. Our main reference will be Coleman's original paper [Col85b]. Another good introductory reference is [MP12], but there the theory of integration on curves and Jacobians over p-adic fields is phrased in a completely different language. Instead of rigid geometry and Coleman integration, the authors think in terms of p-adic Lie groups.

4.1 Setting the scene

Let X be a curve over a number field K of genus $g \geq 2$. Our ultimate goal is to completely determine the (finite!) set of rational points $X(K)$ on X. The first step is to search for points using a computer. In practice, this often already yields the complete set of rational points. The hard part, however, is to actually prove that they are indeed all. This is where the method of Chabauty and Coleman comes in.

If we know at least one point $O \in X(K)$, then we can embed X into its Jacobian J with the *Abel-Jacobi map* that sends a point $P \in X(K)$ to the divisor $[P - O]$. This defines a closed immersion $X \hookrightarrow J$ of schemes over K, so we can view X as a subvariety of J. The Mordell–Weil group $J(K)$ of the Jacobian is not necessarily finite, but it is a finitely generated abelian group. In general it is quite hard to find explicit generators for $J(K)$, but for now we will restrict to the case that it can be done. Then the problem we are left with is to determine which points in $J(K)$ lie on X.

Let $K_{\mathfrak{p}}$ be the completion of K at a prime $\mathfrak{p}$. Because K is a subfield of $K_{\mathfrak{p}}$, we have an inclusion $X(K) \subset X(K_{\mathfrak{p}})$ of sets of rational points. Doing the same for the Jacobian J of X we get a diagram of inclusions

$$\begin{tikzcd} X(K) \arrow[r, hook] \arrow[d, hook] & X(K_{\mathfrak{p}}) \arrow[d, hook] \\ J(K) \arrow[r, hook] & J(K_{\mathfrak{p}}). \end{tikzcd}$$

This shows that the rational points on X are contained in the intersection $X(K_{\mathfrak{p}}) \cap J(K)$ inside $J(K_{\mathfrak{p}})$. The general idea of the method of Chabauty and Coleman is to define a function $\eta : J(K_{\mathfrak{p}}) \to K_{\mathfrak{p}}$ that vanishes on this intersection, and whose zeroes are effectively computable. Then the number of zeroes of η gives an upper bound for $\#X(K)$. Further, we can go through this list of zeroes and check for each if they lie on X, thereby determining $X(K)$ completely. Of course, a crucial requirement for this method to work is that the number of zeroes of η is finite.

4.2 Chabauty's finiteness result

Let X be a curve of genus $g \geq 2$ over a number field K with good reduction at a prime $\mathfrak{p}$ of K. Let p be the rational prime lying under $\mathfrak{p}$. Then the completion of K at $\mathfrak{p}$ is a discretely valued complete subfield $K_{\mathfrak{p}} \subset \mathbb{C}_p$. Its valuation ring $\mathcal{O}_{K_{\mathfrak{p}}}$ has a unique maximal ideal $\mathfrak{P}$, and we write $k = \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{P}$ for the residue field. The Dedekind scheme $S = \operatorname{Spec} \mathcal{O}_{K_{\mathfrak{p}}}$ has exactly one closed point s corresponding to $\mathfrak{P}$, and the stalk $\mathscr{O}_{S,s}$ is isomorphic to $\mathcal{O}_{K_{\mathfrak{p}}}$ itself. Therefore, the fact that X has good reduction at $\mathfrak{p}$ implies that X is smooth and admits a smooth model $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_{K_{\mathfrak{p}}}$. We write $J_{K_{\mathfrak{p}}}$ for the Jacobian variety of X over $K_{\mathfrak{p}}$, and $\mathcal{J} \to \operatorname{Spec} \mathcal{O}_{K_{\mathfrak{p}}}$ for its Néron model. Recall from Section 3.1 that then $\mathcal{J}$ is in particular connected and projective.

The set of differentials of the first kind $H^0(J^{\mathrm{an}}_{K_{\mathfrak{p}}}, {}_f\Omega^1_{J^{\mathrm{an}}_{K_{\mathfrak{p}}}/K_{\mathfrak{p}}})$ forms a g-dimensional $K_{\mathfrak{p}}$-vector space[5]. For such a differential ω we define $\lambda_\omega : J_{K_{\mathfrak{p}}}(\mathbb{C}_p) \to \mathbb{C}_p$ as

$$\lambda_\omega(P) = f_\omega(P) - f_\omega(O),$$

where f_ω is as in Section 3.4 and $O \in J_{K_{\mathfrak{p}}}(K)$ is the origin. Then λ_ω is a group homomorphism from $J_{K_{\mathfrak{p}}}(\mathbb{C}_p)$ into $\mathbb{C}_p$ ([Col85a, Theorem 2.8(i)]).

[5] This needs a reference.

Remark 4.1. We use here that every differential of the first kind on $J_{K_\mathfrak{p}}^{\mathrm{an}}$ is invariant w.r.t. translation on the Jacobian. For holomorphic differentials on the Jacobian (not defined in these notes), this is indeed the case, see e.g. [Fre93, p. 248]. The fact that it is also true for rigid differentials on the analytic space of the Jacobian should follow from a rigid version of Serre's GAGA theorem ([Ked04, Theorem 3]). The author is still quite unfamiliar with the statement of GAGA, let alone its rigid analogue, so let us just assume that the differentials are invariant and march on in good faith. $\diamondsuit$

We define the set

$$V = \{\omega \in H^0(J_{K_\mathfrak{p}}^{\mathrm{an}}, {}_f\Omega^1_{J_{K_\mathfrak{p}}^{\mathrm{an}}/K_\mathfrak{p}}) \mid \lambda_\omega(x) = 0,\, \forall x \in J(K)\}.$$

Note that the fact that λ_ω is a group homomorphism implies that it always vanishes at torsion points of $J(K)$. From Proposition 3.15(i) it follows that for any $a \in K_\mathfrak{p}$ we have $\lambda_{\omega+a\omega'} = \lambda_\omega + a\lambda_{\omega'}$. Therefore, for any $x \in J(K)$ the subset of differentials ω for which $\lambda_\omega(x) = 0$ forms a subspace of $H^0(J_{K_\mathfrak{p}}^{\mathrm{an}}, {}_f\Omega^1_{J_{K_\mathfrak{p}}^{\mathrm{an}}/K_\mathfrak{p}})$. Then V is an intersection of subspaces and therefore also a subspace. Further, if $J(K)$ has rank r, then the dimension of V should be at least $g - r$. In particular V contains a non-trivial differential when $r < g$.

Proposition 4.2. *Let $P_0 \in X_{K_\mathfrak{p}}(K_\mathfrak{p})$ be the point mapped to $O \in J_{K_\mathfrak{p}}(K_\mathfrak{p})$ under the Abel–Jacobi embedding f. Then the intersection $X(K_\mathfrak{p}) \cap J(K)$ inside $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ is contained in the set*

$$Z = \{P \in X_{K_\mathfrak{p}}(K_\mathfrak{p}) \subset J_{K_\mathfrak{p}}(K_\mathfrak{p}) \mid \lambda_\omega(P) = 0,\, \forall \omega \in f^*V\}. \tag{4.1}$$

In the notation of Section 3.4 the set Z consists of the points $P \in X_{K_\mathfrak{p}}(K_\mathfrak{p})$ satisfying

$$\int_{P_0}^{P} \omega = 0, \qquad \textit{for all } \omega \in f^*V.$$

Proof. Since Frobenius acts properly on the Néron model $\mathcal{J}$, this follows immediately from Equation (3.1). $\square$

Theorem 4.3 (Chabauty)**.** *If V contains a non-trivial differential then the set Z is finite.*

We have already seen that V contains a non-trivial differential when $r < g$, so Chabauty's theorem tells us that in that case the intersection $X(K_\mathfrak{p}) \cap J(K)$ inside $J_{K_\mathfrak{p}}(K_\mathfrak{p})$ is finite. This proves Mordell's conjecture for curves whose genus is larger than the rank of their Jacobian.

4.3 Explicit bounds

Let us sketch the general strategy Coleman used to obtain explicit upper bounds for the number of elements in the intersection $X(K_\mathfrak{p}) \cap J(K)$. Note that since K is a number field, its completion $K_\mathfrak{p}$ is a finite extension of $\mathbb{Q}_p$. In particular, this means that the residue field k is finite.

A differential $\omega \in f^*V$ as in (4.1) is in particular an element of $H^0(X_{K_\mathfrak{p}}^{\mathrm{an}}, {}_f\Omega^1_{X_{K_\mathfrak{p}}^{\mathrm{an}}/K_\mathfrak{p}})$. Therefore, if we can bound the number of zeroes on $X_{K_\mathfrak{p}}(K_\mathfrak{p})$ of the function

$$g_\omega : P \mapsto f_\omega(P) - f_\omega(P_0)$$

for all differentials ω of the first kind on $X_{K_\mathfrak{p}}^{\mathrm{an}}$, then this gives a bound for the number of elements in the set Z given in (4.1). Recall that $X_{K_\mathfrak{p}}(K_\mathfrak{p})$ is covered by residue disks, and since the residue field k is finite there are only finitely many residue disks. The idea is to give an upper bound for the number of zeroes of g_ω for a (non-zero) differential on a single residue disk, and then add these to get a bound for the total number of zeroes. If we do this for an arbitrary differential of the first kind this yields an upper bound for $\#Z$ and therefore for $\#X(K)$.

Recall from Section 3.2 that on a residue disk D we can write a holomorphic differential as

$$\omega = \sum_{i\geq 0} c_i t^i, \qquad c_i \in K_{\mathfrak{p}}, \tag{4.2}$$

for some local coordinate t on the residue disk. Without changing the zeroes of g_ω, we can scale ω by an element in $K_{\mathfrak{p}}$ such that the reduction $\widetilde{\omega}$ obtained by reducing the coefficients c_i is non-zero. We define $\mathrm{ord}_D(\widetilde{\omega})$ as the degree of the first non-vanishing term in the expansion of $\widetilde{\omega}$. Similarly, there exists an expansion like in (4.2) for g_ω. The core of Coleman's proof is to bound the number of zeroes of this power series. He then uses this result to derive the following theorem:

Theorem 4.4 ([Col85b, Theorem 4])**.** *Let ω be a differential of the first kind on $X^{\mathrm{an}}_{K_{\mathfrak{p}}}$, scaled such that $\widetilde{\omega} \neq 0$. Then the number of zeroes of g_ω in $X_{K_{\mathfrak{p}}}(K_{\mathfrak{p}})$ is at most*

$$\sum_{D\in X_k(k)} n(\mathrm{ord}_D(\widetilde{\omega}) + 1, |p|^{1/e}), \tag{4.3}$$

where we identified a rational point on the reduced curve with its residue disk, e is the ramification index of $K_{\mathfrak{p}}$ over $\mathbb{Q}_p$, $|\cdot|$ denotes the absolute value on $K_{\mathfrak{p}}$, and

$$n(a, b) = \max\left\{ n \mid \frac{s^n}{|n|} \geq \frac{s^k}{|k|} \right\} \qquad \textit{for } s < 1.$$

Now assume that the rank r of $J(K)$ is strictly less than g. In that case f^*V as in (4.1) contains at least one non-zero differential, giving the following result:

Theorem 4.5. *If $r < g$, then the expression in* (4.3) *gives an upper bound for the number of rational points in $X_K(K)$.*

The following corollary gives an elegant bound in the case that $K = \mathbb{Q}$ and the prime p is large enough.

Corollary 4.6 ([MP12, Theorem 5.3b])**.** *If $r < g$ and $p > 2g$, then*

$$\#X_Q(\mathbb{Q}) \leq \#X_{\mathbb{F}_p}(\mathbb{F}_p) + (2g - 2).$$

Sketch of proof. To prove this one has to show that, counting multiplicities, the total number of zeroes of $\widetilde{\omega}$ on $X_{\mathbb{F}_p}(\mathbb{F}_p)$ is $2g - g$. The requirement that $p > 2g$ ensures that the function n in (4.3) always returns $\mathrm{ord}_D(\widetilde{\omega})$. □

References

[Ach20] Piotr Achinger. Introduction to non-Archimedean Geometry. `https://achinger.impan.pl/rigid/notes.pdf`, 2020. Version: January 28, 2021.

[Bal11] Jennifer Balakrishnan. Coleman integration for hyperelliptic curves: algorithms and applications. `https://dspace.mit.edu/handle/1721.1/67785`, 2011. Thesis (PhD)—Massachusetts Institute of Technology, Dept. of Mathematics.

[Bes12] Amnon Besser. Heidelberg lectures on Coleman integration. In *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contrib. Math. Comput. Sci.*, pages 3–52. Springer, Heidelberg, 2012.

[BGR84] S. Bosch, U. Güntzer, and R. Remmert. *Non-Archimedean analysis*, volume 261 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry.

[Bou98] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Col85a] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[Col85b] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Dol14] Igor V. Dolgachev. Abelian scheme. *Encyclopedia of Mathematics*. `https://encyclopediaofmath.org/wiki/Abelian_scheme`, 2014.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Fre93] Margaret N. Freije. The formal group of the jacobian of an algebraic curve. *Pacific Journal of Mathematics*, 157:241–255, 1993.

[FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004.

[Har03] David Harbater. Patching and Galois theory. In *Galois groups and fundamental groups*, volume 41 of *Math. Sci. Res. Inst. Publ.*, pages 313–424. Cambridge Univ. Press, Cambridge, 2003.

[Ked04] Kiran S. Kedlaya. Kiehl's finiteness theorems. `https://kskedlaya.org/18.727/kiehl.pdf`, 2004. Lecture notes for the MIT course 18.727 *Topics in Algebraic Geometry (Introduction to Rigid Analytic Geometry)*, offered during fall 2004.

[Lic11] Sam Lichtenstein. Néron models. `http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L11.pdf`, 2011. Notes for lecture 11 in the number theory learning seminar 2010-2011 at Stanford.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at `www.jmilne.org/math/`.

[Mor22] Louis Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Phil. Soc.*, 21:179–192, 1922.

[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.

[PS14] Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.

[Sch98] Peter Schneider. Basic notions of rigid analytic geometry. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 369–378. Cambridge Univ. Press, Cambridge, 1998.

[Sto17] Michael Stoll. Chabauty without the Mordell-Weil group. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 623–663. Springer, Cham, 2017.