Balakrishnan, J.S., and Dogra, N.. (0000) "Quadratic Chabauty and Rational Points II: Generalised Height Functions on Selmer Varieties," International Mathematics Research Notices, Vol. 0000, Article ID rnn000, 49 pages.
doi:10.1093/imrn/rnn000

Quadratic Chabauty and Rational Points II: Generalised Height Functions on Selmer Varieties

Jennifer S. Balakrishnan[1] **and Netan Dogra**[2]

[1]Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA and [2]Mathematical Institute, University of Oxford, Radcliffe Observatory Quarter,

Correspondence to be sent to: dogra@maths.ox.ac.uk

We give new instances where Chabauty–Kim sets can be proved to be finite, by developing a notion of "generalised height functions" on Selmer varieties. We also explain how to compute these generalised heights in terms of iterated integrals and give the first explicit nonabelian Chabauty result for a curve $X/\mathbb{Q}$ whose Jacobian has Mordell–Weil rank *larger than* its genus.

1 Introduction

Given a smooth projective curve X of genus $g \geq 2$ over a number field K, it is known by Faltings' theorem that the set $X(K)$ of its K-rational points is finite, but in general there is no known method to determine this set explicitly. When the Mordell–Weil rank of the Jacobian J of X is less than g, the method of Chabauty [15], made effective by Coleman [17], can determine explicit finite sets of $\mathfrak{p}$-adic points containing the set $X(K)$. In many cases, this can give a computationally feasible approach to determine the set of rational points [42].

In a series of papers [35, 34, 36], Kim proposed a generalisation of the Chabauty–Coleman method, which gives a nested sequence

$$X(K_{\mathfrak{p}})_1 \supset X(K_{\mathfrak{p}})_2 \supset \cdots \supset X(K)$$

of sets $X(K_{\mathfrak{p}})_n$ of $\mathfrak{p}$-adic points, each containing the set $X(K)$, such that the "depth 1" set $X(K_{\mathfrak{p}})_1$ is exactly the one arising from the Chabauty–Coleman method. Here $\mathfrak{p}$ is a prime of K lying above a prime p which splits completely and for which X has good reduction. When $K = \mathbb{Q}$, Kim [34] showed that the Bloch–Kato conjectures imply the finiteness of $X(\mathbb{Q}_p)_n$ for n sufficiently large. Coates and Kim [16] proved this eventual finiteness (again for $K = \mathbb{Q}$) in the case when J has complex multiplication. Recently, Ellenberg and Hast [23] extended this result to give a new proof of Faltings' theorem for curves $X/\mathbb{Q}$ which are solvable covers of $\mathbb{P}^1$.

In this paper, we consider two questions about the depth 2 set $X(K_{\mathfrak{p}})_2$, continuing our previous investigation [6]:

Question 1. *When can $X(K_{\mathfrak{p}})_2$ be proved to be finite?* □

Question 2. *When can $X(K_{\mathfrak{p}})_2$ be computed explicitly?* □

The key technical construction which we use to study these questions is presented in Section 3. We define the notion of *equivariant generalised p-adic heights*, inspired by Nekovář's construction of p-adic height functions [43]. We give a brief explanation of Nekovář's construction for divisors on X. Recall that the local height on X is usually defined to be a pairing on divisors of degree zero with disjoint support, and the global height is given by the sum of local heights, which only depends on the class of the divisors in the Picard group of X. In Nekovář's construction, local and global heights are constructed as functions on isomorphism classes of *mixed extensions*. Recall that the $\mathbb{Q}_p$-Kummer map allows us to associate to a divisor D in $\mathrm{Div}^0(X)$ a Galois cohomology class $\kappa(D) \in H^1(G_K, V)$, where $V := H^1_{\acute{e}t}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))$. Equivalently, we may think of $\kappa(D)$ as an isomorphism class of Galois representations of the form

$$\rho = \begin{pmatrix} 1 & 0 \\ * & \rho_V \end{pmatrix},$$

Received 1 Month 20XX; Revised 11 Month 20XX; Accepted 21 Month 20XX

where ρ_V is the Galois representation associated to V. Nekovář associates to a pair of divisors D_1, D_2 with disjoint support a Galois representation of the form

$$\rho = \begin{pmatrix} 1 & 0 & 0 \\ * & \rho_V & 0 \\ * & * & \chi \end{pmatrix}$$

where χ is the cyclotomic character. A Galois representation of this form is referred to as a *mixed extension* with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$. Nekovář's p-adic heights are functions on isomorphism classes of such mixed extensions (with some conditions at primes above p). For each prime v, Nekovář defines a local height function h_v on mixed extensions of G_v-representations. The global height is then the sum of the local heights, and class field theory implies this global height is bilinear in the two off-diagonal $H^1(G_K, V)$-classes.

From the point of view of the Chabauty–Kim method, the interesting feature of the p-adic height is that this bilinear structure gives a necessary condition for a collection M_v of mixed extensions of G_v-representations to come from a global G_K-representation. More precisely, in our previous work, we showed that if the Picard number of the Jacobian is bigger than 1, then the Chabauty–Kim method can be used to associate to each point x (over any extension $L|\mathbb{Q}$) a G_L-representation $A_Z(x)$ which is a mixed extension with graded pieces $\mathbb{Q}_p, V, \mathbb{Q}_p(1)$. We then obtain an obstruction to an adelic point $(x_v) \in \prod X(K_v)$ coming from a global point in $X(K)$: the associated mixed extensions $A_Z(x_v)$ must come from a global mixed extension, and hence there must be a 'bilinear relation' between the three $*$ entries (as the contributions from primes away from p are small, this can essentially be thought of as an obstruction to an element of $\prod_{v|p} X(K_v)$ coming from $X(K)$). This obstruction defines a subset intermediate between $X(K_{\mathfrak{p}})_1$ and $X(K_{\mathfrak{p}})_2$. Furthermore, by relating the mixed extensions $A_Z(x)$ to the ones arising in Nekovář's theory, we gave a formula for $h_v(A_Z(x))$ as a local height pairing $h_v(A_Z(x-b, D_Z(x-b))$ between divisors. This was inspired by earlier uses of p-adic heights to obtain quadratic Chabauty formulae for integral points on elliptic and hyperelliptic curves in papers of Kim [37] and of the first author with Kedlaya and Kim [8] and Besser and Müller [5].

To recover $X(K_{\mathfrak{p}})_2$, we need to consider more general mixed extensions (with graded pieces $\mathbb{Q}_p, V$ and W for W a quotient of $\wedge^2 V$). The key technical construction of this paper is the definition of a *generalised height* for such mixed extensions. As in the classical case, generalised heights give an obstruction to a collection of local mixed extensions to come from a global mixed extension (see Lemma 3.12 for a precise formulation). Via a twisting construction explained in Section 3.3, one may associate to each point z of $X(K)$ a mixed extension $A(b, z)$. This gives an explicit equation for $X(K_{\mathfrak{p}})_2$ (see Lemma 4.1), and in particular gives a necessary condition for an adelic point to come from a rational point. The relation between the approach of this paper (which we refer to below as "QC2") and previous related papers ("QC0" [5] and "QC1" [6]) may be summarised as follows:

	QC0	QC1	QC2
Scope (proof of finiteness of a superset)	$X(\mathbb{Z})$ for $X/\mathbb{Q}$ hyperelliptic with $r = g$	$X(K)$ for X/K with $r < g + \rho(J) - 1$, $K = \mathbb{Q}$ or im. quad.	$X(K)$ for X/K satisfying hypotheses of Theorems 1.1 or 1.2
Bilinear structure used	Coleman–Gross p-adic height [18]	Nekovář p-adic height [43] on $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, \mathbb{Q}_p(1))$	Generalised height functions (§3) on $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$, inspired by Nekovář
Local computation	$h_v(z-\infty, z-\infty)$	$h_v(z-b, D(b,z))$	$h_v(A(b,z))$

Here $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$ denotes the set of isomorphism classes of mixed extensions of $G_{K,T}$-representations with graded pieces $\mathbb{Q}_p, V, W$ which are crystalline at all primes above p. See Section 3 for a precise definition.

1.1 Main results

To address Question 1, in Section 2, we begin by recalling when, for $K = \mathbb{Q}$, finiteness of $X(\mathbb{Q}_p)_2$ is implied by the Bloch–Kato conjectures. We also note some elementary extensions of our previous results [6] on finiteness of $X(\mathbb{Q}_p)_2$ when the Néron–Severi group of its Jacobian is large. We then use generalised heights to prove new finiteness results when the curve X is hyperelliptic and satisfies "Manin–Demjanenko"-type conditions, i.e., that there are isogeny factors occurring in the Jacobian with large multiplicity. To state the first main theorem, let

$K = \mathbb{Q}$ or an imaginary quadratic field. We introduce the notational convention that, for an abelian variety A over K,

$$\rho_f(A) := \begin{cases} \operatorname{rk} \mathrm{NS}(A) + \operatorname{rk}(\mathrm{NS}(A_{\overline{\mathbb{Q}}})^{c=-1}) & \text{if } K = \mathbb{Q}, \\ \operatorname{rk} \mathrm{NS}(A) & \text{else,} \end{cases}$$

and

$$e(A) := \begin{cases} \operatorname{rk} \mathrm{End}^0(A) + \operatorname{rk}(\mathrm{End}(A_{\overline{\mathbb{Q}}})^{c=-1}) & \text{if } K = \mathbb{Q}, \\ \operatorname{rk} \mathrm{End}^0(A) & \text{else.} \end{cases}$$

Here $\mathrm{NS}(A)$ denotes the Néron–Severi group of A and $\mathrm{NS}(A_{\overline{\mathbb{Q}}})^{c=-1}$ the subspace of $\mathrm{NS}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ on which complex conjugation acts by -1. As usual, $\mathrm{End}^0(A) := \mathbb{Q} \otimes \mathrm{End}(A)$, where $\mathrm{End}(A)$ denotes endomorphisms of A defined over K.

Theorem 1.1. *Let X/K be a hyperelliptic curve and suppose J is isogenous to $A^d \times B$, where A is an abelian variety of rank r. If*

$$\rho_f(A)d + d(d-1)e(A)/2 - 1 > \min\{d(r - \dim(A)), r^2 - \dim(A)^2\},$$

then $X(K_{\mathfrak{p}})_2$ is finite. □

In Section 5.1, we give an example of a genus 5 curve $X/\mathbb{Q}(i)$ which satisfies the hypotheses of the theorem but does not satisfy the Chabauty–Coleman bound.

Theorem 1.1 is somewhat reminiscent of the following result, due to Demjanenko when A is an elliptic curve and Manin in general [41], [50, §5.2].

Theorem (Manin–Demjanenko)**.** *Let A be a simple abelian variety of rank r, with $\dim \mathrm{End}^0(A) = h$. If J is isogenous to $A^d \times B$, with $d > r/h$, then $X(\mathbb{Q})$ is finite and may be computed effectively.* □

To address Question 2, we use generalised heights to obtain equations for Selmer varieties at depth 2, and hence for the set $X(K_{\mathfrak{p}})_2$. The equations are given in terms of height functions on Selmer varieties in Proposition 4.1. To get from this proposition to an explicit computation, we need a way to compute the local generalised heights of the mixed extensions $A(b, z)$ arising from the twisting construction of Section 3. In this paper, we focus on the problem of describing the local heights at primes above p. This is done in Section 6 in three stages. The definition of the local heights is in terms of certain associated filtered ϕ-modules $D_{\mathrm{cr}}(A(b, z))$. First, one uses a p-adic comparison theorem due to Olsson [46] to relate this to a more tractable filtered ϕ-module $A^{\mathrm{dR}}(b, z)$, which is the fibre at z of a flat connection $\mathcal{A}^{\mathrm{dR}}$. The filtration on $A^{\mathrm{dR}}(b, z)$ is then computed in Section 6.5 by computing a filtration by sub-bundles on $\mathcal{A}^{\mathrm{dR}}$. Finally, the ϕ-action is computed in Section 6.7, when X is a hyperelliptic curve, in terms of iterated integrals. This is used to give equations for $X(K_{\mathfrak{p}})_2$ in terms of p-adic heights (see Proposition 6.4 for a more general result). We use this to give the first explicit nonabelian Chabauty result for a curve $X/\mathbb{Q}$ which has Mordell–Weil rank *larger than* its genus.

As an example, we consider the family of genus 2 curves

$$X = X_a : y^2 = x^6 + ax^4 + ax^2 + 1, \tag{1}$$

which was previously studied by Kulesz, Matera, and Schost [38]. We prove results controlling the set of K-rational points of X_a for $a \in K_0$, where $K_0 = \mathbb{Q}$ or a real quadratic field and K is a totally real extension of K_0. We consider the case where the Mordell–Weil rank over K of the associated elliptic curve

$$E = E_a : y^2 = x^3 + ax^2 + ax + 1 \tag{2}$$

is two. Consider the maps $X \to E$ given by $f_1 : (x, y) \mapsto (x^2, y)$ and $f_2 : (x, y) \mapsto (x^{-2}, yx^{-3})$. As the rank of E_t over the function field $\mathbb{Q}(t)$ is 1, generated by the point $b = (0, 1)$ [38, Prop. 1], for all but finitely many values of a, the specialisation E_a over K_0 has the point b of infinite order. By the conjectured equidistribution of parity, one expects to find many values of a for which $E_a(K)$ has rank 2.

Note that the Jacobian of X is isogenous to $E \times E$, and hence, when the rank of E is 2, the Chabauty–Coleman method does not apply. When the rank of E is 2, we show that $X(K_{\mathfrak{p}})_2$ is finite and give equations for a finite set containing it.

To state the theorem, let $\omega_i = \frac{x^i}{2y}dx$ and let w denote the hyperelliptic involution. Following Liu, we say that a genus 2 curve has *potential type V reduction* at v if, in an extension $L_w|K_v$ over which the curve acquires stable reduction, the special fibre of its stable model is isomorphic to two genus 1 curves meeting at a point. For simplicity, in the introduction we state a special case of the theorem, under a simplifying assumption on the reduction type of X. The general statement may be found in Section 7.

Theorem 1.2 (Special case)**.** *Let K_0 be $\mathbb{Q}$ or a real quadratic field. Let $K|K_0$ be a totally real extension. Let X/K_0 be a genus 2 curve in the family $y^2 = x^6 + ax^4 + ax^2 + 1$ whose Jacobian has Mordell–Weil rank 4 over K. Suppose p is a prime of $\mathbb{Q}$ such that*

- *The prime p splits completely in $K|\mathbb{Q}$.*
- *The curve X has good reduction at all primes above p, and the action of G_K on $E[p]$ is absolutely irreducible.*
- *If E has complex multiplication by a CM extension L, then L is not contained in $K(\mu_p)$.*

Suppose that X has no primes of potential type V reduction. Suppose z_0 is a point in $X(K)$ such that $f_1(z_0) \wedge f_2(z_0)$ is of infinite order in $\wedge^2 E(K)$. Then $X(K)$ is contained in the finite set of z in $X(K_{\mathfrak{p}})$ satisfying $G(z) = 0$, where

$$G(z) = F_1(z)F_2(z_0) - F_1(z_0)F_2(z),$$

with $b = (0, 1)$ and

$$F_1(z) = \int_b^z (\omega_0\omega_1 - \omega_1\omega_0) + \frac{1}{2}\int_b^z \omega_0 \int_{w(b)}^b \omega_1,$$
$$F_2(z) = 2\int_b^z (-\omega_0\omega_3 + a\omega_1\omega_2 + 2\omega_1\omega_4) - \frac{1}{2}x(z) - \int_b^z \omega_0 \int_{w(b)}^b \omega_3.$$

□

We briefly indicate the techniques used in the proof of the theorem (precise definitions may be found in subsequent sections). The isogeny gives an isomorphism

$$V = T_p \operatorname{Jac}(X) \otimes \mathbb{Q}_p \simeq V_E \oplus V_E,$$

where $V_E = T_p E \otimes \mathbb{Q}_p$. The quotient of the fundamental group of X used is an extension

$$1 \to \operatorname{Sym}^2 V_E \to U \to V \to 1.$$

The first step of the proof is to prove non-density of the localisation map

$$\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}(U) \to H^1_f(G_{\mathfrak{p}}, U)$$

from the Selmer variety of U to the local cohomology variety $H^1_f(G_{\mathfrak{p}}, U)$. In the case where $K = \mathbb{Q}$, the elliptic curve E does not have CM, and $p > 3$, we know $H^1_f(G_{K,T}, \operatorname{Sym}^2 V_E) = 0$ by Flach [24, Theorem 1] (see the remarks below Lemma 5.5 for an explanation of how this follows from Flach's theorem). In general, by Freitas, Le Hung, and Siksek [27] we know that E_a/K_0 is modular. Under our assumptions, the vanishing of the Selmer group of $\operatorname{Sym}^2 V_E$ follows from modularity lifting results [1, Theorem A]. This implies that the dimension of the global Selmer variety is 4. By p-adic Hodge theory, the local Selmer variety has the same dimension. Hence non-density cannot be proved by a dimension argument. Instead, it is deduced using the notion of a generalised height function which is equivariant with respect to the the action of $\mathrm{Mat}_2(\mathbb{Q}_p)$ on $V \simeq V_E \oplus V_E$.

1.2 Notation

We follow slightly different notational conventions to those used in [6], to make our notation more compatible with standard references such as [14]. Let X be a smooth projective curve over a number field K, with good reduction outside a set of primes T_0, and let p be a rational prime that splits completely in K and such that X has good reduction at all primes above p. We fix a prime $\mathfrak{p}$ above p, and define $T := T_0 \cup \{v|p\}$. For v a prime not above p, define $H^1_f(G_v, W)$ and $H^1_g(G_v, W)$ by

$$H^1_f(G_v, W) := \operatorname{Ker}(H^1(G_v, W) \to H^1(I_v, W)),$$
$$H^1_g(G_v, W) := H^1(G_v, W).$$

For $\mathfrak{p}$ a prime above p, define

$$H^1_f(G_{\mathfrak{p}}, W) := \operatorname{Ker}(H^1(G_{\mathfrak{p}}, W) \to H^1(G_{\mathfrak{p}}, W \otimes B_{\mathrm{cr}})),$$
$$H^1_g(G_{\mathfrak{p}}, W) := \operatorname{Ker}(H^1(G_{\mathfrak{p}}, W) \to H^1(G_{\mathfrak{p}}, W \otimes B_{\mathrm{dR}})).$$

We define the global versions

$$H^1_f(G_{K,T},W) := \{c \in H^1(G_{K,T},W) : \prod_{v\in T} \mathrm{loc}_v(c) \in \prod_{v\in T} H^1_f(G_v,W)\},$$
$$H^1_g(G_{K,T},W) := \{c \in H^1(G_{K,T},W) : \prod_{v\in T} \mathrm{loc}_v(c) \in \prod_{v\in T} H^1_g(G_v,W)\}.$$

More generally, for $S \subset T$ we may define global Galois cohomology groups with conditions intermediate between H^1_f and H^1_g:

$$H^1_{f,S}(G_{K,T},W) := \{c \in H^1(G_{K,T},W) : \prod_{v\in T} \mathrm{loc}_v(c) \in \prod_{v\in S} H^1_g(G_v,W) \times \prod_{v\in T-S} H^1_f(G_v,W)\}.$$

The reason for introducing these different conditions is that in the theory of Selmer varieties, we use cohomology classes which may be ramified at primes of bad reduction—and hence may not lie in H^1_f—but the dimensions of the Selmer varieties (which are of central importance in proving finiteness results) will be 'governed by' H^1_f (see Lemma 2.1 for a precise statement).

For finite-dimensional continuous $\mathbb{Q}_p$-representations W_1, W_2 of a topological group G, we identify the vector spaces $H^1(G, W_1^* \otimes W_2)$ and $\mathrm{Ext}^1(W_1, W_2)$ in the usual way. Via this identification, we define subspaces such as $\mathrm{Ext}^1_f(W_1, W_2)$.

If U is a unipotent group over $\mathbb{Q}_p$ with a continuous action of $G_{K,T}$ which is crystalline at all primes above p, we similarly define $H^1_f(G_{K,T}, U)$ as the set of isomorphism classes of $G_{K,T}$-equivariant U-torsors which are crystalline at all v above p and unramified at all v prime to p (and analogously for H^1_g and $H^1_{f,S}$).

We make repeated use of the twisting construction in nonabelian cohomology, as in [49, I.5.3]. For topological groups U and W, equipped with a continuous homomorphism $U \to \mathrm{Aut}(W)$ and a continuous left U-torsor P, we shall denote by $W^{(P)}$ the group obtained by twisting W by the U-torsor P:

$$W^{(P)} := W \times_U P. \tag{3}$$

Similarly if P is a continuous right U-torsor we define ${}^{(P)}W := P \times_U W$. For U a group with a continuous action of a topological group Γ, we let $H^1(\Gamma, U)$ denote the set of isomorphism classes of Γ-equivariant left U-torsors.

2 The Chabauty–Kim method

Let K be a number field, and X, T, T_0 as in Section 1.2. Given a rational point b in $X(K)$, let $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$ denote the unipotent $\mathbb{Q}_p$-étale fundamental group of $\overline{X} := X \times_K \overline{K}$ with basepoint b. Let

$$\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},b) \supset U^{(1)} = [\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},b), \pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},b)] \supset U^{(2)} = [U^{(1)}, \pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},b)] \supset \cdots$$

denote the central series filtration of $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$. Associated to this filtration we have the groups

$$U_n := U_n(b) := \pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X},b)/U^{(n)}, \qquad U[n] := \mathrm{Ker}(U_n \to U_{n-1}),$$

and the U_n-torsor

$$P_n(b,z) := \pi_1^{\acute{e}t}(\overline{X}; b, z) \times_{\pi_1^{\acute{e}t}(\overline{X},b)} U_n(b).$$

Then the assignment $z \mapsto [P_n(b,z)]$ defines a map

$$j_n : X(K) \to H^1(G_{K,T}, U_n(b)).$$

One of the fundamental insights of the theory of Selmer varieties is that the cohomology spaces $H^1(G, U_n(b))$ carry a much richer structure than merely that of a pointed set, and that this extra structure has Diophantine applications. For the following theorem we take G to be either G_v or $G_{K,T}$:

Theorem 2.1 (Kim [35, Proposition 2]). *Let U be a finite-dimensional unipotent group over $\mathbb{Q}_p$, admitting a continuous action of G. Let*

$$U = U^{(0)} \supset U^{(1)} \supset \cdots$$

denote the lower central series filtration of U. Suppose $H^0(G, U^{(i)}/U^{(i+1)})(\mathbb{Q}_p) = 0$ for all i. Then the functors

$$R \mapsto H^j(G, U(R)), j = 0, 1,$$

are represented by an affine algebraic variety over $\mathbb{Q}_p$, such that, for all i, the exact sequence

$$H^1(G, U^{(i)}/U^{(i+1)}) \to H^1(G, U/U^{(i+1)}) \to H^1(G, U/U^{(i)}) \tag{4}$$

is a diagram of schemes over $\mathbb{Q}_p$. □

In this paper, we will never distinguish between a cohomology variety and its $\mathbb{Q}_p$-points. We henceforth let U denote a Galois stable quotient of U_2 (i.e., such that the kernel of $U_2 \to U$ is Galois stable), whose abelianisation equals U_1. Since the abelianisation of $U(\mathbb{Q}_p)$ has weight -1, it satisfies the hypotheses of the theorem, and hence $H^1(G, U)$ has the structure of the $\mathbb{Q}_p$-points of an algebraic variety over $\mathbb{Q}_p$.

To go from the cohomology varieties $H^1(G_{K,T}, U)$ to Selmer varieties, one must add local conditions. Let $P(z)$ denote the pushout of $\pi_1^{\acute{e}t}(\overline{X}; b, z)$ along $\pi_1^{\acute{e}t}(\overline{X}, b) \to U$. Then for each v prime to p, there is a *local unipotent Kummer map*

$$j_v : X(K_v) \to H^1(G_v, U); \quad x \mapsto [P(x)]$$

which is trivial when v is a prime of good reduction and has finite image in general, by Kim and Tamagawa [36, Corollary 0.2]. For v above p, and x in $X(K_v)$, the torsor $P(x)$ is crystalline by Olsson (see Lemma 6.1), and we define j_v to be the map

$$j_v : X(K_v) \to H^1_f(G_v, U); \quad x \mapsto [P(x)].$$

There is then a commutative diagram

$$\begin{array}{ccc} X(K) & \xrightarrow{j} & H^1(G_{K,T}, U) \\ \downarrow & & \downarrow \prod \mathrm{loc}_v \\ \prod_{v\in T} X(K_v) & \xrightarrow{\prod j_v} & \prod_{v\in T} H^1(G_v, U) \end{array}$$

Kim [34, §4] also showed that the localisation morphisms are morphisms of varieties, and the set of crystalline cohomology classes has the structure of the $\mathbb{Q}_p$-points of a variety. Since, at any v prime to p, the image of $X(K_v)$ in $H^1(G_v, U)$ is finite by the Theorem of Kim and Tamagawa [36, Corollary 0.2], we may define a subvariety $\mathrm{Sel}(U)$ of $H^1(G_{K,T}, U)$ to be the set of cohomology classes c satisfying the following conditions:

- $\mathrm{loc}_v(c)$ comes from an element of $X(K_v)$ for all v prime to p,
- $\mathrm{loc}_v(c)$ is crystalline for all v above p, and
- the projection of c to $H^1(G_{K,T}, V)$ lies in the image of $\mathrm{Jac}(X)(K) \otimes \mathbb{Q}_p$.

For a prime $\mathfrak{p}$ above p, we define $X(K_\mathfrak{p})_U := j_\mathfrak{p}^{-1} \mathrm{loc}_\mathfrak{p} \mathrm{Sel}(U)$. We shall refer to this variety as the *Selmer variety* associated to U. We include the last condition, which is somewhat non-standard and perhaps in conflict with the "Selmer" prefix, so as to be able to make statements about relations between the set of weakly global points $X(K_\mathfrak{p})_U$ and the rank of the Jacobian of X which are not conditional on the finiteness of the p-part of the Shafarevich–Tate group. As explained in [6, Remark 2.3], $\mathrm{Sel}(U)$ is the reduced scheme associated to the fibre of zero under the algebraic map

$$\widetilde{\mathrm{Sel}}(U) \to H^1_f(G_{K,T}, V)/J(K) \otimes \mathbb{Q}_p,$$

where $\widetilde{\mathrm{Sel}}(U)$ is the subvariety of $H^1(G_{K,T}, U)$ obtained from only imposing the first two conditions above. Since $\mathrm{Sel}(U/U^{(i+1)})$ is then by definition the pre-image of $\mathrm{Sel}(U/U^{(i)})$ in $\widetilde{\mathrm{Sel}}(U/U^{(i+1)})$, we obtain an analogous exact sequence to (4).

It is often convenient to break up the Selmer variety by first fixing an element $\alpha = (\alpha_v) \in \prod_{v\in T_0} j_v(X(K_v))$, and defining $\mathrm{Sel}(U)_\alpha$ to be the subvariety of $\mathrm{Sel}(U)$ consisting of cohomology classes whose localisation at $v \in T_0$ is equal to α_v. We similarly write $X(K_\mathfrak{p})_\alpha$. We call the tuple α a *collection of local conditions*.

Lemma 2.1 ([6, Lemma 2.6])**.** Let $\beta_1, \ldots, \beta_N \in \mathrm{Sel}(U)$ be a set of representatives for the image of $\mathrm{Sel}(U)$ in $\prod_{v\in T_0} j_v(X(K_v))$. Let $\alpha_i = (\alpha_{v,i})$ denote the image of β_i in $\prod_{v\in T_0} j_v(X(K_v))$. Then

$$\mathrm{Sel}(U)_{\alpha_i} \simeq H^1_f(G_{K,T}, U^{(\beta_i)})',$$

where $H^1_f(G_{K,T}, U^{(\beta_i)})'$ denotes the subvariety of $H^1_f(G_{K,T}, U^{(\beta_i)})$ consisting of crystalline torsors whose image in $H^1_f(G_{K,T}, V)$ lies in the image of $J(K) \otimes \mathbb{Q}_p$, and $U^{(\beta_i)}$ denotes the twist of U by β_i as in (3). □

Lemma 2.2. Let U be a Galois stable quotient of U_2 which is an extension of V by W. Suppose

$$\dim D_{\mathrm{dR}}(W)/F^0 - \dim H^1_f(G_{K,T}, W) > r - g, \tag{5}$$

then $X(K_\mathfrak{p})_2$ is finite. □

Proof. By [34, Theorem 1], it is enough to prove that equation (5) implies

$$\dim D_{\mathrm{dR}}(U)/F^0 > \dim \mathrm{Sel}(U).$$

Since

$$\dim D_{\mathrm{dR}}(U)/F^0 = \dim D_{\mathrm{dR}}(V)/F^0 + \dim D_{\mathrm{dR}}(W)/F^0,$$

and $\dim(D_{\mathrm{dR}}(V)/F^0) = g$, to prove the lemma it will be enough to prove $\dim \mathrm{Sel}(U) \leq r + \dim H^1_f(G_{K,T}, W)$. By Lemma 2.1, it is enough to prove that, for all i,

$$\dim H^1_f(G_{K,T}, U^{(\beta_i)})' \leq r + \dim H^1_f(G_{K,T}, W).$$

We have a Galois equivariant exact sequence

$$1 \to W^{(\beta_i)} \to U^{(\beta_i)} \to V^{(\beta_i)} \to 1.$$

Since the action of U on itself by conjugation is unipotent, U acts trivially on V and W, we have Galois equivariant isomorphisms $V^{(\beta_i)} \simeq V$ and $W^{(\beta_i)} \simeq W$, inducing an exact sequence of pointed varieties

$$H^1_f(G_{K,T}, W) \to H^1(G_{K,T}, U^{(\beta_i)})' \to J(K) \otimes \mathbb{Q}_p.$$

Hence $\dim \mathrm{Sel}(U)_{\alpha_i} \leq \dim H^1_f(G_{K,T}, W) + \dim(J(K) \otimes \mathbb{Q}_p)$, as required. ∎

2.1 The context of the present work

We will always take U to be an intermediate quotient

$$U_2 \to U \xrightarrow{\pi} V.$$

The group U_2 is an extension of V by

$$\overline{\wedge^2 V} := \mathrm{Coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V),$$

hence such quotients are in correspondence with Galois-stable summands of $\wedge^2 V/\mathbb{Q}_p(1)$. This paper is concerned with the commutative diagram

$$\begin{array}{ccccc} X(K) & \xrightarrow{j} & \mathrm{Sel}(U) & & \\ \downarrow & & \downarrow{\scriptstyle \mathrm{loc}_{\mathfrak{p}}} & \searrow & \\ X(K_{\mathfrak{p}}) & \xrightarrow{j_{\mathfrak{p}}} & H^1_f(G_{\mathfrak{p}}, U) & \xrightarrow{\simeq} & D_{\mathrm{dR}}(U)/F^0 \end{array}$$

and in particular with identifying situations under which loc_p is not dominant and describing what $X(K_{\mathfrak{p}})_U$ looks like in this case.

2.2 Provable finiteness via the geometric Néron–Severi group

One piece of the weight -2 representation $[U_2, U_2]$ whose Selmer group we can understand unconditionally is the Artin–Tate part, equivalently the part coming from the geometric Néron–Severi group of J. In this subsection we restrict to the case $K = \mathbb{Q}$.

Lemma 2.3. For any representation of $G_{\mathbb{Q},T}$ on a finite-dimensional vector space V over a field $F \subset \mathbb{Q}_p$, which factors through a finite quotient $\mathrm{Gal}(L|\mathbb{Q})$ of $\mathrm{Gal}(\mathbb{Q})$, where $L|\mathbb{Q}$ is unramified at p, we have an isomorphism

$$H^1_f(G_{\mathbb{Q},T}, V \otimes_F \mathbb{Q}_p(1)) \simeq (V \otimes \mathbb{Q}_p)^{c=1}/(V \otimes \mathbb{Q}_p)^{\mathrm{Gal}(\mathbb{Q})},$$

where $c \in \mathrm{Gal}(\mathbb{Q})$ denotes complex conjugation. □

Proof. The crucial point is that, since $H^0(G_{L,T}, V \otimes \mathbb{Q}_p(1)) = 0$, the inflation-restriction exact sequence induces an isomorphism

$$H^1(G_{\mathbb{Q},T}, V \otimes_F \mathbb{Q}_p(1)) \simeq H^1(G_{L,T}, V \otimes_F \mathbb{Q}_p(1))^{\mathrm{Gal}(L|\mathbb{Q})},$$

and similarly we have isomorphisms

$$H^1(G_p, V \otimes_F \mathbb{Q}_p(1)) \simeq \oplus_{v|p} H^1(G_v, V \otimes_F \mathbb{Q}_p(1))^{\mathrm{Gal}(L|\mathbb{Q})},$$

which induce isomorphisms

$$H^1_f(G_p, V \otimes_F \mathbb{Q}_p(1)) \simeq \oplus_{v|p} H^1_f(G_v, V \otimes_F \mathbb{Q}_p(1))^{\mathrm{Gal}(L|\mathbb{Q})}.$$

This induces an isomorphism

$$H^1_f(G_{\mathbb{Q},T}, V \otimes_F \mathbb{Q}_p(1)) \simeq H^1_f(G_{L,T}, V \otimes_F \mathbb{Q}_p(1))^{\mathrm{Gal}(L|\mathbb{Q})}.$$

Given this, we observe

$$\begin{aligned} H^1_f(G_{L,T}, V \otimes_F \mathbb{Q}_p(1))^{\mathrm{Gal}(L|\mathbb{Q})} \simeq & (H^1_f(G_{L,T}, \mathbb{Q}_p(1)) \otimes_F V)^{\mathrm{Gal}(L|\mathbb{Q})} \\ \simeq & ((\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p) \otimes_F V)^{\mathrm{Gal}(L|\mathbb{Q})}. \end{aligned}$$

Now we use the description of $\mathcal{O}_L^\times \otimes \mathbb{Q}_p$ as a Galois module [44, §8.7.2]:

$$\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p \simeq \mathrm{Ind}_{\langle c \rangle}^{\mathrm{Gal}(L|\mathbb{Q})} \mathbb{Q}_p / \mathbb{Q}_p,$$

and finally, we have

$$\begin{aligned} ((\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p) \otimes_F V)^{\mathrm{Gal}(L|\mathbb{Q})} \simeq & \mathrm{Hom}_{\mathrm{Gal}(L|\mathbb{Q})}((\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p), V \otimes_F \mathbb{Q}_p) \\ \simeq & \mathrm{Ker}(\mathrm{Hom}_{\mathrm{Gal}(L|\mathbb{Q})}(\mathrm{Ind}_{\langle c \rangle}^{\mathrm{Gal}(L|\mathbb{Q})} \mathbb{Q}_p), V \otimes_F \mathbb{Q}_p) \to \mathrm{Hom}_{\mathrm{Gal}(L|\mathbb{Q})}(\mathbb{Q}_p), V \otimes_F \mathbb{Q}_p)) \\ \simeq & \mathrm{Ker}(\mathrm{Hom}_{\langle c \rangle}(\mathbb{Q}_p, V \otimes_F \mathbb{Q}_p) \to \mathrm{Hom}_{\mathrm{Gal}(L|\mathbb{Q})}(\mathbb{Q}_p, V \otimes \mathbb{Q}_p)) \\ \simeq & (V \otimes \mathbb{Q}_p)^{c=1} / (V \otimes \mathbb{Q}_p)^{\mathrm{Gal}(\mathbb{Q})}. \end{aligned}$$

■

We deduce the following corollary:

Proposition 2.2. *Let $K = \mathbb{Q}$, and define $\rho_f(J) = \mathrm{rk}\,\mathrm{NS}(J) + \mathrm{rk}(\mathrm{NS}(J_{\overline{\mathbb{Q}}})^{c=-1})$ as in the introduction. If*

$$\mathrm{rk}\, J < g - 1 + \rho_f(J),$$

then $X(\mathbb{Q}_p)_2$ is finite. □

Proof. Let

$$W := \varinjlim_L \left[\mathbb{Q}_p(1) \otimes \mathrm{Hom}_{G_L}(\mathbb{Q}_p(1), \overline{\wedge^2 V}) \right] \subset \overline{\wedge^2 V}$$

be the Artin–Tate part of $[U_2, U_2]$. Then we know that W contains (and is equal to by Faltings) the Artin–Tate representation $(\mathrm{NS}(J_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_p)/\mathbb{Q}_p(1)$. The proof that $X(\mathbb{Q}_p)_U$ is finite is as in [6, Lemma 2.6], with the only difference being a more general choice of W. To recall, we use the fact that it is enough to prove that

$$\dim \mathrm{Sel}(U) < \dim H^1_f(G_p, U).$$

It suffices to prove that $\dim \mathrm{Sel}(U)_\alpha < \dim H^1_f(G_p, U)$ for any collection of local conditions. By Lemma 2.1, we have

$$\dim \mathrm{Sel}(U)_\alpha \leq \dim H^1_f(G_{K,T}, W) + \dim H^1_f(G_{K,T}(V).$$

At p, we claim the sequence

$$1 \to H^1_f(G_p, W) \to H^1_f(G_p, U) \to H^1_f(G_p, V) \to 1,$$

is exact. One way to see this is that the non-abelian Dieudonné functor induces an isomorphism of schemes

$$H^1_f(G_p, U) \simeq D_{\mathrm{dR}}(U)/F^0.$$

In [34, §1], Kim proves that this map is algebraic. The map is given by sending a torsor P to a $D_{\mathrm{cr}}(U)$-torsor object $D_{\mathrm{cr}}(P)$ in the category of filtered ϕ-modules, and by proving that the set of isomorphism classes of such torsors is represented by $D_{\mathrm{dR}}(U)/F^0$. Although it is not explicitly stated in loc. cit. that this map is bijective, one can deduce it from the fact that the map has an inverse given by sending a $D_{\mathrm{cr}}(U)$-torsor P to the crystalline U-torsor $\mathrm{Spec}(F^0(\mathcal{O}(P) \otimes B_{\mathrm{cr}})^{\phi=1})$. Hence exactness follows from exactness of

$$1 \to D_{\mathrm{dR}}(W)/F^0 \to D_{\mathrm{dR}}(U)/F^0 \to D_{\mathrm{dR}}(V)/F^0 \to 1.$$

We deduce that $X(\mathbb{Q}_p)_2$ is finite whenever

$$\dim H^1_f(G_{\mathbb{Q},T}, W) + \mathrm{rk}\, J < \dim H^1_f(G_p, W) + g.$$

The proposition now follows from Lemma 2.3, since this implies

$$\dim H^1_f(G_p, W) - \dim H^1_f(G_{\mathbb{Q},T}, W) = \dim \mathrm{NS}(J) + \dim \mathrm{NS}(J_{\overline{\mathbb{Q}}})^{c=-1} - 1.$$

■

2.3 Finiteness assuming the Bloch–Kato conjectures

Here we describe situations when finiteness of $X(\mathbb{Q}_p)_2$ is implied by the Bloch–Kato conjectures. The Bloch–Kato conjectures relate the dimension of $H^1_f(G_{K,T}, W)$ to the rank of certain graded pieces of K-groups of algebraic varieties. Let Z be a smooth projective variety over $\mathbb{Q}$. For $i \in \mathbb{Z}$, let $K_i(Z)$ denote the ith algebraic K-group of Z in the sense of Quillen. The only fact we will use about $K_i(Z)$ is that it is zero when $i < 0$, and the action of Adams operators enables one to define a grading $K_i(Z) \otimes \mathbb{Q} = \oplus_{j \in \mathbb{Z}} K_i^{(j)}(Z)$ on the group tensored with $\mathbb{Q}$. The following is a special case of their conjectures.

Conjecture 2.3 (Bloch–Kato [14, Conjecture 5.3 (i)])**.** *Let Z be a smooth projective variety over $\mathbb{Q}$. Then for any $n > 0$ and $2r - 1 \neq n$, the map*

$$\mathrm{ch}_{n,r} : K^{(r)}_{2r-1-n}(Z) \otimes \mathbb{Q}_p \to H^1_f(G_{\mathbb{Q}}, H^n(Z_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(r))$$

is an isomorphism. □

Kim [34, Observation 1] showed that this conjecture implies that $X(\mathbb{Q}_p)_n$ is finite for all n sufficiently large, with no hypotheses on the rank of J. As we are interested in $X(\mathbb{Q}_p)_2$, we now work out the exact conditions on X for which Kim's argument can be used to show that Conjecture 2.3 implies finiteness of $X(\mathbb{Q}_p)_2$.

Lemma 2.4. Conjecture 2.3 implies $H^1_f(G_{\mathbb{Q},T}, \overline{\wedge^2 V}^*(1)) = 0$. □

Proof. As $\overline{\wedge^2 V}^*(1)$ is a direct summand of $H^2_{\acute{e}t}(X \times X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))$, it suffices to prove that

$$H^1_f(G_{\mathbb{Q},T}, H^2_{\acute{e}t}(X \times X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))) = 0.$$

This follows from Conjecture 2.3, since that implies

$$\dim H^1_f(G_{\mathbb{Q},T}, H^2_{\acute{e}t}(X \times X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))) \leq \dim H^1_g(G_{\mathbb{Q},T}, H^2_{\acute{e}t}(X \times X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))) \leq \dim K_{-1}(X \times X) \otimes \mathbb{Q} = 0.$$

■

Lemma 2.5. Conjecture 2.3 implies

$$\dim H^1_f(G_p, \overline{\wedge^2 V}) - \dim H^1_f(G_{\mathbb{Q},T}, \overline{\wedge^2 V}) \geq g(g-1).$$

□

Proof. Recall the following corollary of Poitou–Tate duality [26, Remark II.2.2.2]:

$$\dim_{\mathbb{Q}_p}(H^0(G_{\mathbb{Q},T},W)) - \dim_{\mathbb{Q}_p}(H^1_f(G_{\mathbb{Q},T},W)) + \dim_{\mathbb{Q}_p}(H^1_f(G_{\mathbb{Q},T},W^*(1)))$$
$$- \dim_{\mathbb{Q}_p}(H^0(G_{\mathbb{Q},T},W^*(1))) = -\dim_{\mathbb{Q}_p}(D_{\mathrm{dR}}(W)/F^0) + \dim_{\mathbb{Q}_p}(H^0(G_{\mathbb{R}},W)).$$

In this case of $W = \overline{\wedge^2 V}$, we have

$$\dim_{\mathbb{Q}_p}(H^0(G_{\mathbb{Q},T},W^*(1))) = \rho(J_X) - 1, \qquad D_{\mathrm{dR}}(W)/F^0 = H^1_f(G_p,W),$$
$$\dim_{\mathbb{Q}_p}(H^0(G_{\mathbb{R}},W)) = g(g-1), \qquad H^0(G_{\mathbb{Q},T},W) = 0,$$

hence the claim follows from Lemma 2.4. ∎

We thus deduce the following simple criterion for conjectural finiteness of $X(\mathbb{Q}_p)_2$.

Lemma 2.6. Suppose Conjecture 2.3. Let $X/\mathbb{Q}$ be a curve of genus $g \geq 2$. If $r = \mathrm{rk}\, J(\mathbb{Q}) < g^2$, then $X(\mathbb{Q}_p)_2$ is finite.

□

Proof. By the previous lemma, we have

$$\dim H^1_f(G_{\mathfrak{p}},U_2) - \dim \mathrm{Sel}(U_2) \geq \dim H^1_f(G_{\mathfrak{p}},W) - \dim H^1_f(G_{K,T},W) + g - \mathrm{rk}\, J(K)$$
$$> g(g-1) + g - g^2 = 0.$$

∎

3 Generalised height functions

We now return to considering a general finite extension $K|\mathbb{Q}$, with p a prime splitting completely in K and $\mathfrak{p}$ a prime of K lying above p. In [6], we used Nekovář's formalism of p-adic height functions on mixed extensions to describe Chabauty–Kim sets in terms of p-adic height pairings of cycles on X. Given a choice of global character $\chi \in H^1(G_{K,T},\mathbb{Q}_p)$, Nekovář's p-adic height functions associate to certain filtered Galois representations with graded pieces $\mathbb{Q}_p$, V, and $\mathbb{Q}_p(1)$, a collection of local cohomology classes with values in $\mathbb{Q}_p(1)$. We obtain a $\mathbb{Q}_p$-valued function by summing the cup products of these local classes with χ.

In this section, we describe a natural generalisation of Nekovář's formulation of the p-adic height pairing, resulting in a notion of generalised p-adic height functions. To do this, we essentially mimic his construction at every step, occasionally rephrasing some constructions in terms of nonabelian cohomology.

3.1 Mixed extensions

Following Nekovář, we construct generalised height functions as functions on equivalence classes of mixed Galois representations with fixed graded pieces. The most important examples will be the mixed extensions $A(b,z)$ constructed in the next subsection. Let $V := H^1_{\acute{e}t}(\overline{X},\mathbb{Q}_p)^*$, and let W be a direct summand of $V^{\otimes 2}$.

Definition 3.1. Define $\mathcal{M}_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$ to be the category whose objects are tuples $(M,(M_i)_{i=0,1,2,3},(\psi_i)_{i=0,1,2})$ where M is a $G_{K,T}$ representation which is crystalline at all primes above p, (M_i) is a Galois-stable filtration

$$M = M_0 \supset M_1 \supset M_2 \supset M_3 = 0,$$

and the ψ_i are isomorphisms

$$\psi_0 : \mathbb{Q}_p \to M_0/M_1, \qquad \psi_1 : V \to M_1/M_2, \qquad \psi_2 : W \to M_2/M_3$$

and whose morphisms are isomorphisms of Galois representations respecting the filtration and commuting with the ψ_i. An object of $\mathcal{M}_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$ will be referred to as a mixed extension with graded pieces $\mathbb{Q}_p, V$ and W. Define $M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$ to be the set $\pi_0(\mathcal{M}_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W))$ of isomorphism classes of mixed extensions. Similarly define $M(G_v;\mathbb{Q}_p,V,W)$ (resp. $M_f(G_v;\mathbb{Q}_p,V,W)$ for v above p) to be the set of isomorphism classes of corresponding categories of G_v representations (resp. crystalline representations). □

Given a mixed extension M in $\mathcal{M}_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$, we obtain extensions M/M_2 and M_1 of $\mathbb{Q}_p$ by V and of V by W respectively. As explained in Lemma 3.8 these extensions are automatically unramified at all primes of T_0, and hence lie in $H^1_f(G_{K,T},V)$ and $\mathrm{Ext}^1_f(V,W)$. We denote by π_{1*} and π_{2*} the natural maps

$$\pi_{1*}: M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\to H^1_f(G_{K,T},V),\qquad \pi_{2*}: M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\to \mathrm{Ext}^1_f(V,W).$$

Following Nekovář, we say that M is a mixed extension of $\pi_{1*}(M)$ and $\pi_{2*}(M)$. Given K-vector spaces V_1,V_2,V_3, define $U(V_1,V_2,V_3)$ to be the group of unipotent vector space isomorphisms of $V_1\oplus V_2\oplus V_3$, i.e., those which respect the filtration

$$V_1\oplus V_2\oplus V_3\supset V_2\oplus V_3\supset V_3,$$

and are the identity on the associated graded. We will mostly be interested in the case where $(V_1,V_2,V_3)=(\mathbb{Q}_p,V,W)$. Recall from [6, Lemma 4.7] that we have an isomorphism

$$M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\simeq H^1_{f,T_0}(G_{K,T},U(\mathbb{Q}_p,V,W)).$$

The maps π_{1*} and π_{2*} are induced from the exact sequence

$$0\to W\to U(\mathbb{Q}_p,V,W)\xrightarrow{(\pi_1,\pi_2)} V\oplus V^*\otimes W\to 0. \tag{6}$$

In fact, the proof in loc. cit. show more generally that, for any mixed extension M with graded pieces $\mathbb{Q}_p,V,W$, we have a bijection

$$H^1(G_{K,T};\mathrm{Aut}_{\mathrm{fil}}(M))\simeq M(G_{K,T};\mathbb{Q}_p,V,W) \tag{7}$$

between the set of mixed extensions with graded pieces $\mathbb{Q}_p,V,W$ and the set of $G_{K,T}$-equivariant $\mathrm{Aut}_{\mathrm{fil}}(M)$-torsors, where $\mathrm{Aut}_{\mathrm{fil}}(M)$ denotes the group of vector space automorphisms of M which are unipotent with respect to its filtration. The bijection is given by sending a mixed extension M' to the $\mathrm{Aut}_{\mathrm{fil}}(M)$-torsor of vector space isomorphisms $M\xrightarrow{\simeq}M'$ which are unipotent in the sense that they respect the filtrations, and induce the identity on $\mathrm{gr}_\bullet(M)\simeq\mathrm{gr}_\bullet(M')\simeq\mathbb{Q}_p\oplus V\oplus W$. Another way to say this is that, for any mixed extensions M and M', the cohomology sets $H^1(G_{K,T},\mathrm{Aut}_{\mathrm{fil}},(M))$ and $H^1(G_{K,T},\mathrm{Aut}_{\mathrm{fil}}(M'))$ are canonically isomorphic: this is a special case of [50, Proposition 35], since the set of unipotent isomorphisms $M\xrightarrow{\simeq}M'$ has the structure of a $G_{K,T}$-equivariant $(\mathrm{Aut}_{\mathrm{fil}}(M),\mathrm{Aut}_{\mathrm{fil}}(M'))$-bitorsor.

We now outline in broad strokes our generalisation of Nekovář's formulation of the p-adic height pairing. Although we could work in somewhat greater generality, we restrict attention to our case of interest. We take as input a tuple (V,W,j,s,χ), where V and W are as before. Let $s: D_{\mathrm{dR}}(V)\to F^0D_{\mathrm{dR}}(V)$ be a splitting of the Hodge filtration. Finally χ is a non-crystalline element of $H^1(G_{K,T},W^*(1))$. Note that the existence of such a χ is an assumption on W, and is equivalent, by exactness of (a part of) the Poitou–Tate exact sequence

$$H^1(G_{K,T},W^*(1))\xrightarrow{\oplus\mathrm{loc}_v}\oplus_{v\in T}H^1(G_v,W^*(1))\xrightarrow{\oplus\mathrm{loc}_v^*}H^1(G_{K,T},W)^*,$$

(see [26, II.1.2.1]) to the assumption that $\mathrm{loc}_p: H^1_f(G_{K,T},W)\to\oplus_{v|p}H^1_f(G_v,W)$ is not surjective.

Associated to this data, we will define, for each v prime to p, a local *pre-height* function

$$\widetilde{h}_v: M(G_v;\mathbb{Q}_p,V,W)\to H^1(G_v,W),$$

as well as a local pre-height at primes $\mathfrak{p}$

$$\widetilde{h}_{\mathfrak{p}}: M_f(G_{\mathfrak{p}};\mathbb{Q}_p,V,W)\to H^1_f(G_{\mathfrak{p}},W).$$

Using χ, we then define a global height

$$h: M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\to\mathbb{Q}_p,$$

such that $h(M)$ only depends on the image of M under

$$M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\to H^1_f(G_{K,T},V)\otimes H^1_f(G_{K,T},V^*\otimes W).$$

As in the classical set-up, the global height will be a sum of local heights h_v which are compositions of the map $\widetilde{h}_v$ with the character $\mathrm{loc}_v\,\chi$, thought of as an element of $H^1(G_v,W)^*$ via Tate duality. For the applications in this paper, we will only be interested in characters χ for which $h_{\mathfrak{q}}$ is trivial at all $\mathfrak{q}$ above p except $\mathfrak{p}$.

3.2 Twisting and mixed extensions

We now relate the construction of generalised heights to the Chabauty–Kim method. We construct compatible maps

$$\begin{aligned} H^1(G_{K,T}, U) &\to M(G_{K,T}; \mathbb{Q}_p, V, W) \\ H^1(G_{K_v}, U) &\to M(G_{K_v}; \mathbb{Q}_p, V, W) \\ H^1_f(G_{K_v}, U) &\to M_f(G_{K_v}; \mathbb{Q}_p, V, W) \text{ for } v|p, \end{aligned} \tag{8}$$

where U is a suitably chosen 2-unipotent quotient of (the $\mathbb{Q}_p$-completion of) the étale fundamental group of $\overline{X}$, and W is a suitably chosen quotient of $\overline{\wedge^2 V}$. To motivate the results of this subsection, we briefly recall how it fits with the goal of finding equations satisfied by $X(K_{\mathfrak{p}})_U$.

The basic idea of generalised p-adic heights is that, given a mixed extension M, they give some kind of algebraic relation between the projections $(\pi_{1*}(M), \pi_{2*}(M))$ and the localisations $(M_v)_{v\in T}$. To use these to obtain equations for $X(K_{\mathfrak{p}})_2$, we need to do two things. Firstly, we need an explicit description of each of the local maps

$$X(K_v) \to M(G_{K_v}; \mathbb{Q}_p, V, W).$$

Second, we need a description of the composite maps

$$H^1_f(G_{K,T}, U) \to M_f(G_{K,T}; \mathbb{Q}_p, V, W) \to H^1_f(G_{K,T}, V) \times H^1_f(G_{K,T}, V^* \otimes W).$$

To explain the construction of the map (8), recall from (7) that we have an identification of $M(G_{K,T}; \mathbb{Q}_p, V, W)$ with $H^1(G_{K,T}, \mathrm{Aut}_{\mathrm{fil}}(M))$, where M is any mixed extension with graded pieces $\mathbb{Q}_p, V$ and W, and $\mathrm{Aut}_{\mathrm{fil}}(M)$ denotes the group of automorphisms of M which are unipotent with respect to its filtration. Hence, a natural source of morphisms from Selmer varieties to sets of isomorphism classes of mixed extensions is to find a mixed extension which U acts on in a Galois-equivariant way. We find such a mixed extension as a quotient (which we denote $A(b)$) of the universal enveloping algebra of $\varprojlim \mathrm{Lie}(U_n)$. In fact, $A(b)$ is a quotient of the universal enveloping algebra by a two-sided ideal, and hence inherits the structure of an associative $\mathbb{Q}_p$-algebra. Roughly speaking, if P is a path torsor $\pi_1^{\acute{e}t}(\overline{X}; b, x)$, we can understand the mixed extension $A(b)^{(P)}$ if we can understand the mixed extension $A(b)$, and the action of U on $A(b)$ (which is the same as understanding the multiplicative structure of $A(b)$).

Lemma 3.2. Let $\mathcal{V}$ be a $\mathbb{Q}_p$-local system on $X_{\acute{e}t}$, and $b, x \in X(K)$. Let ρ denote the homomorphism

$$\pi_1^{\acute{e}t}(\overline{X}, b) \to \mathrm{Aut}(b^*\mathcal{V})$$

coming from viewing $b^*\mathcal{V}$ as a right $\pi_1^{\acute{e}t}(\overline{X}, b)$-module. Then there is an isomorphism of Galois representations

$$x^*\mathcal{V} \simeq (b^*\mathcal{V})^{(\rho_*[\pi_1^{\acute{e}t}(\overline{X}; b, x)])}.$$

□

Proof. By Lemma A.1, we have a canonical isomorphism of functors

$$x^* \simeq (b^*(.)) \times_{\pi_1^{\acute{e}t, \mathbb{Q}_p}(\overline{X}, b)} \pi_1^{\acute{e}t, \mathbb{Q}_p}(\overline{X}; b, z) \tag{9}$$

from the category of unipotent $\mathbb{Q}_p$-local systems on $X_{\overline{K}, \acute{e}t}$ to $\mathbb{Q}_p$-vector spaces. By definition, we have

$$(b^*\mathcal{V})^{(\rho_*[\pi_1^{\acute{e}t}(\overline{X}; b, x)])} \simeq b^*\mathcal{V} \times_{\pi_1^{\acute{e}t, \mathbb{Q}_p}(\overline{X}, b)} \pi_1^{\acute{e}t, \mathbb{Q}_p}(\overline{X}; b, z).$$

Since the identification of Lemma A.1 is functorial, the isomorphism (9) is Galois-equivariant. ■

We will be particularly interested in the case of $\mathbb{Q}_p$-local systems on $X_{\acute{e}t}$ with *unipotent geometric monodromy*, or equivalently representations of $\pi_1^{\acute{e}t}(X_K, b)$ whose restriction to $\pi_1^{\acute{e}t}(\overline{X}, b)$ is unipotent. For example, Lemma 3.2 implies the following.

Lemma 3.3. Suppose $\mathcal{V}$ is a $\mathbb{Q}_p$-local system on $X_{\acute{e}t}$ which is an extension

$$0 \to \mathcal{V}_2 \to \mathcal{V} \to \mathcal{V}_1 \to 0,$$

where the action of $\pi_1^{\acute{e}t}(\overline{X}, b)$ on $b^*\mathcal{V}_1$ and $b^*\mathcal{V}_2$ is trivial. Let ρ denote the corresponding homomorphism

$$\pi_1^{\acute{e}t}(\overline{X}, b) \to \mathrm{Hom}(b^*\mathcal{V}_1, b^*\mathcal{V}_2).$$

Then, in $H^1(G_K, b^*\mathcal{V}_1^* \otimes b^*\mathcal{V}_2)$, we have

$$[x^*\mathcal{V}] = [b^*\mathcal{V}] + \rho_*[\pi_1^{\acute{e}t}(\overline{X}; b, x)],$$

where

$$\rho_* : H^1(G_K, \pi_1^{\acute{e}t}(\overline{X}, b) \to H^1(G_K, \mathrm{Hom}(b^*\mathcal{V}_1, b^*\mathcal{V}_2)).$$

is the homomorphism induced by ρ. □

Proof. This is a special case of the previous lemma, since the action of $\pi_1(\overline{X}, b)$ on $b^*\mathcal{V}$ factors through the unipotent subgroup $1 + \mathrm{Hom}(b^*\mathcal{V}_1, b^*\mathcal{V}_2)$. ■

3.3 The Galois action on the enveloping algebra and related objects

In what follows, X is a smooth projective curve over K, $V = H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p)^*$, and W is a quotient of $\overline{\wedge^2 V} = \mathrm{Coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V)$. Our mixed extensions of interest are constructed as quotients of Galois representations associated to the path torsors $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}; b, z)$. None of the results of this subsection are original, but we include proofs when unable to find a precise reference.

Let $\mathbb{Z}_p[\![\pi_1^{\acute{e}t}(\overline{X}, b)]\!] := \varprojlim \mathbb{Z}_p[\pi_1^{\acute{e}t}(\overline{X}, b)/N]$, where the limit is over normal subgroups N such that $\pi_1^{\acute{e}t}(\overline{X}, b)/N$ is a finite p-group. Let I denote the kernel of the natural map

$$\mathbb{Q}_p \otimes \mathbb{Z}_p[\![\pi_1^{\acute{e}t}(\overline{X}, b)]\!] \to \mathbb{Q}_p.$$

Then define $A_n(b) := \mathbb{Q}_p \otimes \mathbb{Z}_p[\![\pi_1^{\acute{e}t}(\overline{X}, b)]\!]/I^{n+1}$.

The completed universal enveloping algebra of $\mathrm{Lie}(\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b))$ is given by $\varprojlim A_n(b)$ (see [16, §2]), giving $A_n(b)$ the structure of a $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$-module. The action of $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$ on $A_n(b)$ factors through $U_n(b)$, defining an injective group homomorphism

$$U_n(b) \hookrightarrow 1 + IA_n(b).$$

Via the logarithm, we similarly obtain an inclusion

$$L_n(b) \hookrightarrow IA_n(b).$$

Another way to describe $A_n(b)$ and $L_n(b)$ is in terms of the Malcev completion of $\pi_1^{\mathrm{top}}(X(\mathbb{C}), b)$. Namely, let L_n^{top} be the Lie algebra of the maximal n-unipotent quotient of the $\mathbb{Q}_p$ Malcev completion of $\pi_1^{\mathrm{top}}(X(\mathbb{C}), b)$. Then by [32, Theorem A.6], L_n^{top} is canonically isomorphic to $L_n(b)$ as a $\mathbb{Q}_p$-Lie algebra. In particular, this allows us to calculate the kernels of the surjections

$$V^{\otimes n} \to I^n/I^{n+1}$$

topologically. As we will only make use of $A_2(b)$ when $n \leq 2$, the only results we will use are that $A_1(b)$ is an extension

$$0 \to V \to A_1(b) \to \mathbb{Q}_p \to 0,$$

and $A_2(b)$ is an extension

$$0 \to \mathrm{Ker}(V^{\otimes 2} \xrightarrow{\cup} H^2_{\acute{e}t}(\overline{X}, \mathbb{Q}_p))^* \to A_2(b) \to A_1(b) \to 0.$$

This calculation can be reduced to working out a presentation for the graded Lie algebra, i.e., by showing that the graded Lie algebra $\varprojlim \mathrm{gr}^\bullet L_n^{\mathrm{top}}$ is isomorphic to the free completed Lie algebra on V modulo the ideal generated by $H^2(X(\mathbb{C}), \mathbb{Q}_p)^* \subset \wedge^2 V$. The proof of such a presentation is explained in [31, §3.1].

The Galois representation $\mathbb{Q}_p[\pi_1^{ét}(\overline{X}; b, z)]$ has the structure of an equivariant $(\mathbb{Q}_p[\pi_1^{ét}(\overline{X}, b)], \mathbb{Q}_p[\pi_1^{ét}(\overline{X}, z)])$-bimodule, allowing one to define a finite-dimensional $(A_2(b), A_2(z))$-bimodule

$$\begin{aligned} A_2(b,z) &:= \mathbb{Q}_p[\pi_1^{ét}(\overline{X}; b, z)] \otimes_{\mathbb{Q}_p[\pi_1^{ét}(\overline{X}, b)]} A_2(b) \\ &\simeq A_2(z) \otimes_{\mathbb{Q}_p[\pi_1^{ét}(\overline{X}, z)]} \mathbb{Q}_p[\pi_1^{ét}(\overline{X}; b, z)]. \end{aligned}$$

Equivalently, $A_2(b, z)$ is the twist of $A_2(b)$ by the path torsor $P_2(b, z)$ defined in Section 2.

As in [6], we define $A_2(b) \to A(b)$ to be the quotient of $A_2(b)$ by the kernel of the composite

$$I^2/I^3 \simeq \overline{\wedge^2 V} \oplus \mathrm{Sym}^2 V \to \overline{\wedge^2 V} \to W.$$

$A(b)$ is then an algebra with a faithful left action of $U(b) \subset A(b)^\times$. Given a U-torsor P, the induced twist of $A(b)$ by P, denoted $A(b)^{(P)}$, is an element of $\mathcal{M}(G_{K,T}; \mathbb{Q}_p, V, W)$. By Lemma 6.1, $A_2(b)$ is crystalline, and hence so is $A(b)$. If P is crystalline above p and unramified outside T, then $A(b)^{(P)}$ will also have these properties, inducing a morphism of varieties

$$\begin{aligned} H^1_{f,T_0}(G_{K,T}, U) &\to M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W), \\ P &\mapsto A(b)^{(P)}. \end{aligned}$$

The algebra $A(b)$ has a filtration $A(b) \supset IA(b) \supset I^2A(b) \supset I^3A(b) = 0$ by powers of the two-sided ideal I. Hence we obtain a product map $\wedge : IA(b) \times IA(b) \to I^2A(b)$, which factors through $IA(b)/I^2A(b) \times IA(b)/I^2A(b) \simeq V \times V$. Hence the product map on $IA(b)$ may be identified, via the surjection $IA(b) \to V$, with the following map.

Definition 3.4. Let $\tau : V \to \mathrm{Hom}(V, W)$ denote the map $v_1 \mapsto (v_2 \mapsto v_1 \wedge v_2)$. □

The following lemma is a special case of Lemma 3.3.

Lemma 3.5. $A^{(P)}$ is a mixed extension of $\pi_* P$ and $[IA(b)] + \tau_* \pi_* P$, where π_* is the map $H^1(G, U) \to H^1(G, V)$ induced by the projection $U \to V$. □

Proof. By Lemma 3.3, we can compute the extension classes $[A_1(b)^{(P)}] \in \mathrm{Ext}^1(\mathbb{Q}_p, V)$ and $[IA(b)^{(P)}] \in \mathrm{Ext}^1(V, W)$ by computing the classes $[A_1(b)]$ and $[IA(b)]$, and computing the action of $\pi_1^{ét}(\overline{X}, b)$ on $A_1(b)$ and $IA(b)$. Hence the lemma is implied by the statement that the extension class $[A_1(b)] \in \mathrm{Ext}^1(\mathbb{Q}_p, V)$ is trivial, which follows from the fact that the unit element of $A_1(b)$ gives a section of

$$0 \to V \to A_1(b) \to \mathbb{Q}_p \to 0.$$

■

In the case when P is the U-torsor of paths from b to z, we shall denote the corresponding element of $\mathcal{M}_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$ by $A(b, z)$. We obtain a map

$$H^1_{f,T_0}(G_{K,T}, U) \to M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W).$$

We define $A(b, z) := A(b)^{(P(b,z))}$; we have an isomorphism of mixed extensions

$$A(b)^{(P(b,z))} \simeq^{(P(z,b))} A(z).$$

The following lemma says that if we can describe the extension class $[IA(x_1, x_2)]$ for one specific choice of x_1 and x_2, then we can understand it for *any* choice of $[IA(x_1, x_2)]$ in terms of points on the Jacobian.

Lemma 3.6. For any x_1, x_2, z_1, z_2 in $X(K)$,

$$[IA(x_1, x_2)] = [IA(z_1, z_2)] + \tau_*(\kappa(x_1 + x_2 - z_1 - z_2)) \in \mathrm{Ext}^1(V, W), \tag{10}$$

where κ is the Kummer map $\mathrm{Pic}^0(X)(K) \to H^1(G_{K,T}, V)$. □

Proof. First suppose $x_1 = x_2$. Then $[IA(x_1, z_1)] = [IA(x_1, z_2)^{\kappa(z_1 - z_2)}]$, i.e., $IA(x_1, z_1)$ is the twist of $I(A_{x_1,z_1})$ via the natural action of V coming from the left action of $\pi_1(X_{\overline{\mathbb{Q}}}, z_1)$ on $IA(x_1, z_1)$. Hence, by definition of the twisting construction, $[IA(x_1, z_2)^{\kappa(z_1 - z_2)}] = [IA(x_1, z_2)] + \tau_*\kappa(z_1 - z_2)$. Similarly, $IA(x_1, z_1)$ is the twist of $IA(x_2, z_1)$ by $\kappa(x_2 - x_1)$ via the natural *right* action of $\pi_1(X_{\overline{\mathbb{Q}}}, x_2)$ on $IA(x_2, z_1)$. Since we are using the right action of $\pi_1(X_{\overline{\mathbb{Q}}}, x_2)$, the map $V \to \mathrm{Hom}(V, W)$ by which $\kappa(x_2 - x_1)$ acts on $IA(x_2, z_1)$ is given by $-\tau$, (since $v_1 \wedge v_2 = -v_2 \wedge v_1$), and hence $[IA(x_1, z_1)] = [^{\kappa(x_2 - x_1)}IA(x_2, z_1)] = [IA(x_2, z_1)^{\kappa(x_1 - x_2)}] = [IA(x_2, z_1)] + \tau_*\kappa(x_1 - x_2)$. ■

Note that, in general, the extension class of $IA(b)$ in $H^1(G, V^* \otimes W)$ will not lie in the image of τ_*. More specifically, we know that its class in $H^1(G, V^* \otimes W)/H^1(G, V)$ is related to the Abel–Jacobi class of the Gross–Kudla–Schoen cycle in $X \times X \times X$ corresponding to b, (see [19, Theorem 1], or [33]), which is generically non-trivial. One situation where the class of $IA(b)$ does lie in the image of τ_*, and furthermore can be described explicitly in terms of b, is when X is hyperelliptic; this is the reason for the restriction to hyperelliptic curves in Theorem 1.1. The argument, given below, is a straightforward generalisation of Lemma 1.1 of [37], and may be viewed as a special case of a slightly more general phenomenon where one reduces computations on $IA(b, z)$ to the case where $b = z$ is a Weierstrass point, at which point the computation becomes trivial. We refer to this as a *hyperelliptic splitting principle*.

Lemma 3.7. Let X be a hyperelliptic curve of genus g, with equation $y^2 = f(x)$, for f a degree $2g + 2$ polynomial. Let $\alpha_1, \ldots, \alpha_{2g+2}$ be the roots of f. Let Z denote the $\mathbb{Q}$-divisor $\frac{1}{g+1}\sum_i(\alpha_i, 0)$. Then

$$[IA(b, z)] = \tau_*(\kappa(b + z - Z)).$$

□

Proof. First note that it will be enough to prove that the two classes are equal in $H^1(G_{L,T}, V^* \otimes W)$, for L some finite extension of K, since the restriction map is injective. Let L be an extension containing all roots of f. For any i, j, the divisor $(\alpha_i, 0) - (\alpha_j, 0)$ is torsion, and so in particular

$$\kappa_L((\alpha_i, 0) - (\alpha_j, 0)) = 0.$$

Hence it is enough to show that the $H^1(G_{L,T}, V^* \otimes W)$ class obtained from $A_2(b, z)$ agrees with that of $z + b - 2(\alpha_i, 0)$ for some i. By Lemma 3.6, it is enough to prove this when $z = b = (\alpha_i, 0)$. In this case, the hyperelliptic involution gives an action of $\mathbb{Z}/2\mathbb{Z}$ on $A_2(b)$. This acts on the V-graded piece as -1 and on the W-graded piece as the identity, inducing a splitting of $A_2(b)$. ■

3.4 Definition of the local pre-height

We first describe the definition of the local pre-height when $v \neq p$. For this we need to recall some results on Galois cohomology of local fields. Let v be a prime of K, prime to p. Let $I_v \subset G_v$ be the inertia subgroup and $F_v \in G_v/I_v$ a generator. For any finite-dimensional $\mathbb{Q}_p$-representation of W, let $H^1_f(G_v, W) := W^{I_v}/(F_v - 1)W^{I_v}$. Then for any such W, by Tate duality, there is a short exact sequence

$$0 \to H^1_f(G_v, W) \to H^1(G_v, W) \to H^1_f(G_v, W^*(1))^* \to 0$$

(see e.g., [53, Lemma 1 and Theorem 1]).

Lemma 3.8. Let $V = H^1(\overline{X}, \mathbb{Q}_p)^*$, let $n \geq 0$, and let N be a direct summand of $V^{\otimes(2n+1)}(-n)$. Then $H^1(G_v, N) = 0$. □

Proof. As N is a direct summand, it is enough to prove this for $N = V^{\otimes(2n+1)}(-n)$. Since this representation is its own Tate dual, it is enough to prove that $H^1_f(G_v, N) = 0$, or equivalently $N^{G_v} = 0$. This follows directly from the weight-monodromy conjecture for curves [28, Exposé IX, Theorem 4.3(b) and Corollary 4.4]: let L be a finite extension of $\mathbb{Q}_v$ such that I_L acts unipotently on V (and hence W). If $V[i]$ and $N[i]$ denote the graded pieces of V and N of weight i, resp., then weight-monodromy implies that we have an equality $(1 - I_L)V[0] = V[-2]$, (and we know it is trivial on $V[-1]$), hence $(1 - I_L)V^{\otimes(2n+1)}[2n] = V^{\otimes(2n+1)}[2n - 2]$. Thus the kernel of $(1 - I_L)$ on the weight zero part of N is trivial, so $H^1_f(G_v, N) = H^1(G_v, N) = 0$. ■

We now define the local pre-height. When v is not in T, $\widetilde{h}_v$ is trivial. When v is in T_0, via the exact sequence (6) we get an isomorphism

$$M(G_v; \mathbb{Q}_p, V, W) \xrightarrow{\simeq} H^1(G_v, W).$$

We defined $\widetilde{h}_v$ to be this isomorphism and define h_v as the composite

$$M(G_v; \mathbb{Q}_p, V, W) \xrightarrow{\widetilde{h}_v \cup \chi} H^2(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

Finally for $v|p$, $\widetilde{h}_v$ and h_v are defined following [43, §§3-4]. As we restrict to global heights for which the only contribution from primes $v|p$ is at $\mathfrak{p}$, we will only describe $h_{\mathfrak{p}}$, but the description carries over verbatim to other primes above p.

The local height above p is described using Fontaine's functor D_{cr}, which gives an equivalence of categories between $\mathcal{M}_f(G_{\mathfrak{p}}; \mathbb{Q}_p, V, W)$ and the category $\mathcal{M}_{\mathrm{fil},\phi}(\mathbb{Q}_p, D_{\mathrm{cr}}(V), D_{\mathrm{cr}}(W))$ of mixed extensions of filtered ϕ-modules with graded pieces $\mathbb{Q}_p$, $D_{\mathrm{cr}}(V)$, $D_{\mathrm{cr}}(W)$. Similarly this induces a bijection between sets of isomorphism classes

$$M_f(G_{\mathfrak{p}}; \mathbb{Q}_p, V, W) \simeq M_{\mathrm{fil},\phi}(\mathbb{Q}_p, D_{\mathrm{cr}}(V), D_{\mathrm{cr}}(W)).$$

To ease notation, we henceforth write $D_{\mathrm{dR}}(V)$ and $D_{\mathrm{dR}}(W)$ as V_{dR} and W_{dR} respectively. As $K_{\mathfrak{p}}$ is an unramified extension of $\mathbb{Q}_p$, and V and W are crystalline, we also identify these with $D_{\mathrm{cr}}(V)$ and $D_{\mathrm{cr}}(W)$.

We identify $M_{\mathrm{fil},\phi}(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$ with $F^0\backslash U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$, where $F^0 := F^0U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$ is defined to be the subgroup of unipotent automorphisms of $\mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}}$ which preserve the Hodge filtration; more generally, $F^iU(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$ can be defined to be $\exp(F^i \log U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}))$, where

$$F^i \log U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}) := \log U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}) \cap F^i \operatorname{End}(\mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}}).$$

Given a mixed extension M, let $s^{\phi}, s^H : \mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}} \xrightarrow{\simeq} M$ be unipotent isomorphisms of filtered vector spaces which respect the Frobenius structure and Hodge filtration respectively. Then $(s^H)^{-1} \circ s^{\phi}$ defines an element of $U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$. The element s^{ϕ} is uniquely determined, and any different choice of the other isomorphism is of the form $s^H \circ u^H$, for some $u^H \in F^0U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$. This gives a bijective correspondence

$$M_{\mathrm{fil},\phi}(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}) \to F^0\backslash U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}), \tag{11}$$

which is furthermore an isomorphism of algebraic varieties.

We first define a section t of

$$M_f(G_{\mathfrak{p}}; \mathbb{Q}_p, V, W) \to H^1_f(G_{\mathfrak{p}}, V) \times H^1_f(G_{\mathfrak{p}}, V^* \otimes W)$$

as follows: given exact sequences of crystalline $G_{\mathfrak{p}}$-representations

$$0 \to V \to E_1 \to \mathbb{Q}_p \to 0$$
$$0 \to W \to E_2 \to V \to 0,$$

we have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_f(G_{\mathfrak{p}}, W) & \longrightarrow & H^1_f(G_{\mathfrak{p}}, E_2) & \longrightarrow & H^1_f(G_{\mathfrak{p}}, V) & \longrightarrow & 0 \\
 & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq & & \\
0 & \longrightarrow & D_{\mathrm{dR}}(W)/F^0 & \longrightarrow & D_{\mathrm{dR}}(E_2)/F^0 & \longrightarrow & D_{\mathrm{dR}}(V)/F^0 & \longrightarrow & 0
\end{array}$$

(exactness of the top row follows from the isomorphism with the bottom row). Define $\tau_{E_2} : D_{\mathrm{dR}}(V)/F^0 \to D_{\mathrm{dR}}(E_2)/F^0$ as follows. First, note that there is a unique ϕ-equivariant section of the surjection

$$r : D_{\mathrm{cr}}(E_2) \to D_{\mathrm{cr}}(V),$$

since by the Weil conjectures $D_{\mathrm{cr}}(V)$ and $D_{\mathrm{cr}}(W)$ do not have a common ϕ-eigenvalue. The define τ_{E_2} to be the composite

$$D_{\mathrm{dR}}(V)/F^0 \xrightarrow{s} D_{\mathrm{cr}}(V) \xrightarrow{r} D_{\mathrm{cr}}(E_2) \to D_{\mathrm{dR}}(E_2)/F^0$$

where s is the chosen splitting of the Hodge filtration, r is the Frobenius-equivariant section defined above and the third map is the projection. Then we define

$$t(E_1, E_2) := \tau_{E_2}(E_1).$$

For M in $\mathcal{M}_f(G_\mathfrak{p}; \mathbb{Q}_p, V, W)$, let E_1 and E_2 be M/M_2 and $\mathrm{Ker}(M \to M_0)$ respectively. Let $[M]$ denote the image of M in $H^1_f(G_\mathfrak{p}, E_2)$. Then we find that $[M]$ and $t(E_1, E_2)$ have the same image in $H^1_f(G_\mathfrak{p}, V)$, hence by the diagram above, $[M] - t(E_1, E_2)$ defines an element of $H^1_f(G_\mathfrak{p}, W)$, and we define

$$\widetilde{h}_\mathfrak{p}(M) := [M] - t(E_1, E_2) \in H^1_f(G_\mathfrak{p}, W).$$

The pre-height can be described explicitly as an algebraic function

$$F^0 \backslash U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}}) \to W_{\mathrm{dR}}/F^0.$$

Lemma 3.9. Let M be a mixed extension in $M_{\mathrm{fil},\phi}(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$ given by $1 + \alpha + \beta + \gamma \in U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$, where $\alpha \in V_{\mathrm{dR}}, \beta \in V^*_{\mathrm{dR}} \otimes W_{\mathrm{dR}}$, $\gamma \in W_{\mathrm{dR}}$. In block matrix notation, M is represented by

$$\begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \gamma & \beta & 1 \end{pmatrix}.$$

Then

$$\widetilde{h}_p(M) = \gamma - \beta(s_1(\alpha)),$$

where

$$s_1 : v \mapsto v - \iota \circ s(v)$$

is the projection onto the V_{dR}/F^0 summand induced by the splitting s. □

Proof. The class of the extension M in M_1/F^0 is given by $t^\phi - t^H$, where t^ϕ and t^H are isomorphisms of filtered vector spaces

$$\mathbb{Q}_p \oplus M_1 \xrightarrow{\simeq} M$$

respecting the Frobenius action and Hodge filtration respectively. Hence, in terms of s^ϕ and s^H, this class is given by $s^H(\alpha + \gamma)$. Then the extension class $t([\alpha])$ is given by $s^H(s_1(\alpha) + \beta(s_1(\alpha)))$. Hence the local height is given explicitly by

$$\widetilde{h}_p(M) = \gamma - \beta(s_1(\alpha)).$$

■

Lemma 3.10. For any choice of splitting of the Hodge filtration, the composite map

$$\pi_* \times \widetilde{h}_\mathfrak{p} : H^1_f(G_\mathfrak{p}, U) \to H^1_f(G_\mathfrak{p}, V) \times H^1_f(G_\mathfrak{p}, W)$$

is an isomorphism of algebraic varieties. □

Proof. The fact that the pre-height is algebraic follows from the explicit formula in Lemma 3.9. It is enough to prove that the corresponding map

$$D_{\mathrm{dR}}(U)/F^0 \to D_{\mathrm{dR}}(V)/F^0 \times D_{\mathrm{dR}}(W)/F^0$$

is an isomorphism. We have a commutative diagram

$$\begin{array}{ccc} D_{\mathrm{dR}}(U)/F^0 & \longrightarrow & D_{\mathrm{dR}}(V)/F^0 \times D_{\mathrm{dR}}(W)/F^0 \\ \downarrow & & \downarrow \\ D_{\mathrm{dR}}(U(\mathbb{Q}_p, V, W))/F^0 & \longrightarrow & D_{\mathrm{dR}}(V)/F^0 \times D_{\mathrm{dR}}(V^* \otimes W)/F^0 \times D_{\mathrm{dR}}(W)/F^0 \end{array}$$

where the righthand map sends (v, w) to $(v, [IA] + \tau_* v, w)$, and the lefthand map sends P to $A^{(P)}_{\mathrm{dR}}$. Both maps are closed immersions. We first construct an inverse to the bottom map. Given (v, α, w) in $D_{\mathrm{dR}}(V)/F^0 \times D_{\mathrm{dR}}(V^* \otimes W)/F^0 \times D_{\mathrm{dR}}(W)/F^0$, the mixed extension $t(v, \alpha)$ defines an element of $D_{\mathrm{dR}}(U(\mathbb{Q}_p, V, W))/F^0$, and we define $t(v, \alpha)^{(w)}$ to be the twist of $t(v, \alpha)$ by w. The map $(v, \alpha, w) \mapsto t(v, \alpha)^{(w)}$ gives the desired inverse. When we restrict this map to $D_{\mathrm{dR}}(W)/F^0$, it induces an inverse to the top map, as required. ■

One may view the above lemma as saying that the fact that $H^1_f(G_\mathfrak{p}, U)$ is non-canonically isomorphic to $H^1_f(G_\mathfrak{p}, V) \times H^1_f(G_\mathfrak{p}, W)$ is an analogue of the fact that the p-adic height pairing depends on a choice of splitting of the Hodge filtration.

3.5 Global height: definition and basic properties

Define $H^1_s(G_{K,T}, W^*(1)) := H^1(G_{K,T}, W^*(1))/H^1_f(G_{K,T}, W^*(1))$. Let χ be a nonzero element of $H^1_s(G_{K,T}, W^*(1))$, which is non-crystalline at $\mathfrak{p}$. Given χ and a collection of local pre-heights $(\widetilde{h}_v)$ as above we define the associated local height to be

$$h_v := \chi_v \cup \widetilde{h}_v : M(G_v; \mathbb{Q}_p, V, W) \to H^2(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

and the global height to be

$$h = \sum_v h_v : M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W) \to \mathbb{Q}_p,$$

where $v \in T_0 \cup \{\mathfrak{p}\}$. When we want to indicate the dependence on χ, we write $h_{v,\chi}$ and h_χ. Since h and h_v are linear in χ, we may define a *universal* height

$$\widetilde{h} : M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W) \to (H^1_s(G_{K,T}, W^*(1)))^*$$

by setting $\widetilde{h}(M)$ to be the functional $\chi \mapsto h_\chi(M)$.

Note that by construction, $\widetilde{h}_v$ is bi-additive in the same way that usual local heights are bi-additive (see e.g. [6, §4]). Namely, for $i = 1$ or 2, if M and N satisfy $\pi_{i*}(M) = \pi_{i*}(N)$, then we can form the sum $M +_{i,i} N$ in $M(G_v; \mathbb{Q}_p, V, W)$ (for example, when $i = 1$, this is the Baer sum of the extensions $[M], [N]$ in $\mathrm{Ext}^1(M/M_2, W)$), and its local pre-height will be equal to the sum of the local pre-heights of M and N. If $P = (P_v)_{v \in T} \in \prod_{v|p} M_f(G_v; \mathbb{Q}_p, V, W) \times \prod_{v \in T_0} M(G_v; \mathbb{Q}_p, V, W)$, then we similarly define $h(P)$ to be the sum of the local heights.

Lemma 3.11. The global height h factors as

$$M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W) \to H^1_f(G_{K,T}, V) \times H^1_f(G_{K,T}, V^* \otimes W) \to \mathbb{Q}_p,$$

where the first map is the projection and the second is bilinear. □

Proof. As remarked above, the global height is additive, so it is enough to show that it is invariant under the action of $H^1_f(G_{K,T}, W)$ on $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$. Invariance follows from Poitou–Tate duality: if a mixed extension M is twisted by $c \in H^1_f(G_{K,T}, W)$, then this will change h_v by $\chi_v \cup \mathrm{loc}_v\, c$, and $\sum \chi_v \cup \mathrm{loc}_v\, c = 0$. ■

Remark 1. Note that, unlike classical p-adic heights, it is not clear that this construction defines a pairing $H^1_f(G_{K,T}, V) \times H^1_f(G_{K,T}, V^* \otimes W) \to \mathbb{Q}_p$, as we do not know that given $[E_1]$ in $H^1_f(G_{K,T}, W)$ and $[E_2]$ in $\mathrm{Ext}^1_f(V, W)$, E_2 lifts to an element of $H^1_f(G_{K,T}, E_2)$. The existence of such a lifting is equivalent to the vanishing of $[E_1] \cup [E_2]$ in $H^2(G_{K,T}, W)$, and hence would be implied by injectivity of the localisation map $H^2(G_{K,T}, W) \to \oplus_{v \in T} H^2(G_v, W)$. By Poitou–Tate duality, this would be implied by injectivity of $H^1(G_{K,T}, W^*(1)) \to \oplus_{v \in T} H^1(G_v, W^*(1))$, and hence by Conjecture 2.3, as in Lemma 2.6. □

Given two different choices of splitting of the Hodge filtration $s^{(1)}$ and $s^{(2)}$, we obtain two different pre-heights $\widetilde{h}^{(1)}_p$ and $\widetilde{h}^{(2)}_p$. Their difference $\widetilde{h}^{(1)}_p - \widetilde{h}^{(2)}_p$ defines a map $M_f(G_\mathfrak{p}, \mathbb{Q}_p, V, W) \to D_{\mathrm{dR}}(W)/F^0$, which may easily be seen to factor as

$$M_f(G_\mathfrak{p}, \mathbb{Q}_p, V, W) \to D_{\mathrm{dR}}(V)/F^0 \times D_{\mathrm{dR}}(V^* \otimes W)/F^0 \to D_{\mathrm{dR}}(W)/F^0.$$

The latter map may be defined as follows. The difference $s^{(1)} - s^{(2)}$ gives a homomorphism $\overline{s} : D_{\mathrm{dR}}(V)/F^0 \times \to F^0 D_{\mathrm{dR}}(V)$. Given $v \in D_{\mathrm{dR}}(V)/F^0$ and $\alpha \in D_{\mathrm{dR}}(V^* \otimes W)/F^0$, choose a lift of α to $\widetilde{\alpha}$ in $D_{\mathrm{dR}}(V^* \otimes W)$. The lift $\widetilde{\alpha}(\overline{s}(v))$ gives an element of $D_{\mathrm{dR}}(W)$, which is independent of the choice of $\widetilde{\alpha}$ modulo $F^0 D_{\mathrm{dR}}(W)$.

Lemma 3.12. Suppose $[P] = ([P_v]) \in \prod_{v \in T_0 \cup \{\mathfrak{p}\}} M(G_v; \mathbb{Q}_p, V, W)$ satisfies

- $P_\mathfrak{p}$ is crystalline.
- $\pi_{1*}P \in H^1_f(G_\mathfrak{p}, V)$ is in the image of $H^1_f(G_{K,T}, V)$,
- $\pi_{2*}P \in H^1_f(G_\mathfrak{p}, V^* \otimes W)$ is in the image of $H^1_f(G_{K,T}, V^* \otimes W)$,
- there exist $P_1, \ldots P_n$ in $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$, and λ_i in $\mathbb{Q}_p$ such that

$$\pi_{1*}P \otimes \pi_{2*}P = \sum \lambda_i \pi_{1*}P_i \otimes \pi_{2*}P_i$$

in $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$ and for all φ in $H^1_s(G_{K,T}, \overline{\wedge^2 V}^*(1))$,

$$h_\varphi(P) = \sum \lambda_i h_\varphi(P_i).$$

Then P is in the image of $M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$. □

Proof. We have an exact sequence of unipotent groups with $G_{K,T}$-action

$$1 \to W \to U(\mathbb{Q}_p,V,W) \xrightarrow{\pi_1\oplus\pi_2} V\oplus V^*\otimes W \to 1.$$

The image of $H^1(G_{K,T},U(\mathbb{Q}_p,V,W))$ in $H^1(G_{K,T},V\oplus V^*\otimes W)$ is precisely equal to the kernel of the cup product map to $H^2(G_{K,T},W)$. Note that

$$\pi_{1*}P\cup\pi_{2*}P=\sum\lambda_i\pi_{1*}P_i\cup\pi_{2*}P_i=0,$$

and thus we conclude that there is a mixed extension P' whose image in $H^1_f(G_\mathfrak{p},V)\otimes H^1_f(G_\mathfrak{p},V^*\otimes W)$ is equal to that of P. Hence P is the twist of $\mathrm{loc}_\mathfrak{p}P'$ by some c in $H^1(G_\mathfrak{p},W)$, and the claim of the lemma is exactly that this c is in the image of $H^1_f(G_{K,T},W)$. By Poitou–Tate duality this is true if and only if for all φ in $H^1(G_{K,T},W^*(1))$ which are crystalline at all primes above p other than $\mathfrak{p}$, we have $\sum_v\varphi_v\,\mathrm{loc}_v\,c=0$. But, as in the proof of Lemma 3.11,

$$h_{v,\varphi}(P)=h_{v,\varphi}(P')+\varphi_v\,\mathrm{loc}_v(c).$$

■

4 Equations for Selmer varieties

In this section, we use the bilinear structure of generalised heights to obtain formulas for $X(\mathbb{Q}_p)_U$. More precisely, generalised heights allow us to describe explicit trivialisations

$$M_*(G_v;\mathbb{Q}_p,V,W)\simeq H^1_*(G_v,V)\times H^1_*(G_v,V^*\otimes W)\times H^1_*(G_v,W)$$

(where $*$ is f or g depending on whether or not $v|p$), and to describe the image of $M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)$ under the map

$$M_{f,T_0}(G_{K,T};\mathbb{Q}_p,V,W)\xrightarrow{(\pi_{1*},\pi_{2*},\mathrm{loc})}\begin{array}{c}H^1_f(G_{K,T},V)\times H^1_f(G_{K,T},V^*\otimes W)\\ \times\prod_{v|p}M_f(G_v;\mathbb{Q}_p,V,W)\times\prod_{v\in T_0}M(G_v;\mathbb{Q}_p,V,W).\end{array}$$

In Lemma 4.1, this is used to describe $X(K_\mathfrak{p})_\alpha$, by giving explicit quadratic relations between $\widetilde{h}_\mathfrak{p}(A(b,z))$ and $\kappa(b-z)$.

Fix a prime $\mathfrak{p}$ above p and a set of local conditions

$$\alpha\in\prod_{v\in T_0}j_v(X(\mathbb{Q}_v))\subset\prod_{v\in T_0}H^1(G_v,U).$$

For $\alpha=(\alpha_v)_{v\in T_0}$ in $\prod_{v\in T_0}H^1(G_v,W)$, let $M_f(G_{K,T};\mathbb{Q}_p,V,W)_\alpha$ denote the set of isomorphism classes of mixed extensions which are crystalline at p, and such that the localisation at $v\in T_0$ corresponds to $\alpha_v\in H^1(G_v,W)$ via the isomorphism $M(G_v;\mathbb{Q}_p,V,W)\simeq H^1(G_v,W)$. Then the twisting construction defines a map

$$\mathrm{Sel}(U)_\alpha\to M_f(G_{K,T};\mathbb{Q}_p,V,W)_\alpha.$$

Let m denote the codimension of $H^1_f(G_{K,T},W)$ in $H^1_f(G_\mathfrak{p},W)$. Suppose $P\in H^1_f(G_\mathfrak{p},U)$ comes from some P' in $\mathrm{Sel}(U)_\alpha$, and let Q denote the image of P' in $H^1_f(G_{K,T},V)$. Knowing π_*P gives g linear conditions on Q, and knowing $\widetilde{h}_p(P)$ gives m quadratic conditions on Q. Finding exact formulas for the subspace of $H^1_f(G_\mathfrak{p},U)$ where these $g+m$ equations have a solution is then a matter of elimination theory. Concretely, let H_α be the image of $\mathbb{Q}_p[\mathrm{Sel}(U)_\alpha]$ in $H^1_f(G_{K,T},V)\otimes H^1_f(G_{K,T},V^*\otimes W)$ under the map $P\mapsto\pi_{1*}(P)\otimes\pi_{2*}(P)$. Let S be a section of $\mathbb{Q}_p[\mathrm{Sel}(U)_\alpha]\to H_\alpha$. Let H be the image of $\mathrm{Sel}(U)_\alpha$ in $H^1_f(G_{K,T},V)$, and let T denote the map $H\to H_\alpha$ sending P to $P\otimes([IA(b)]+\tau_*(P))$. Then by the multilinearity of generalised heights we have

$$\widetilde{h}(P)=\widetilde{h}(S\circ T(\pi_*P)) \tag{12}$$

for all $P\in\mathrm{Sel}(U)_\alpha$. To use this to write down equations for $\mathrm{loc}_\mathfrak{p}(\mathrm{Sel}(U)_\alpha)$, we introduce some notation for resultants (see e.g. [39, §IX.3]). Given finite-dimensional vector spaces V_1,V_2,V_3 over a field K and a morphism of algebraic varieties $F:V_1\times V_2\to V_3$, we define the resultant $R_{V_2}(F)\subset\mathcal{O}(V_1)$ to be the ideal defining the

maximal subvariety of V_1 for which $F|_{R_{V_2}(F)\times V_2}$ is identically zero. By the fundamental theorem of elimination theory, this is of finite type over K. If $(\lambda_1, \dots \lambda_n)$ is a basis for V_2, we may also write this as $R_{\lambda_1,\dots,\lambda_n}(F)$, to indicate that the variables $\lambda_1, \dots, \lambda_n$ have been eliminated. In our case of interest,

$$V_1 = H^1_f(G_{\mathfrak{p}}, V) \oplus H^1_f(G_{\mathfrak{p}}, W), \qquad V_2 = H, \qquad V_3 = H^1_f(G_{\mathfrak{p}}, V) \oplus H^1_s(G_{K,T}, W^*(1)),$$

and the map

$$F : V_1 \times V_2 \to V_3$$

sends (v_1, v_2, v_3) in $H^1_f(G_{\mathfrak{p}}, V) \times H^1_f(G_{\mathfrak{p}}, W) \times H$ to

$$(\mathrm{loc}_{\mathfrak{p}}(v_3) - v_1, \widetilde{h}_{\mathfrak{p}}(v_2) + \sum_{v \in T_0} \widetilde{h}_v(\alpha_v) - \widetilde{h}(S \circ T(v_3)) \in H^1_f(G_{\mathfrak{p}}, V) \oplus H^1_s(G_{K,T}, W^*(1)).$$

Lemma 4.1. The image of $\mathrm{Sel}(U)_\alpha$ in $H^1_f(G_{\mathfrak{p}}, V) \times H^1_f(G_{\mathfrak{p}}, W)$ under the composite map $(\pi_*, \widetilde{h}_p) \circ \mathrm{loc}_{\mathfrak{p}}$ is equal to the zero set of $R_H(F)$. In particular

$$X(K_{\mathfrak{p}})_\alpha = \{z \in X(K_{\mathfrak{p}}) : \text{ for all } G \in R_H(F),\ G(\kappa_p(z), \widetilde{h}_p(j_{\mathfrak{p}}(z))) = 0\}.$$

□

Proof. Whenever P is in the image of $\mathrm{Sel}(U_2)_\alpha$, it satisfies the equations above. Conversely, by Lemma 4.2, there is a global U-torsor in $\mathrm{Sel}(U_2)_\alpha$ whose localisation at $\mathfrak{p}$ is given by P if and only if there is a mixed extension in $M_f(G_{K,T}; \mathbb{Q}_p, V, W)_\alpha$ whose localisation at $\mathfrak{p}$ is given by $A^{(P)}$. By Lemma 3.12, this happens if and only if there is an element Q of $H^1_f(G_{K,T}, V)$ which is a simultaneous solution to

$$\begin{cases} \mathrm{loc}_{\mathfrak{p}}(Q) & = \pi_* P \\ h_{\varphi,\mathfrak{p}}(P) + \sum_{v \in T_0} h_{\varphi,v}(\alpha_v) & = h_\varphi(S \circ T(Q)). \end{cases}$$

■

Lemma 4.2. The map

$$H^1_{f,T_0}(G_{K,T}, U) \to M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W); \qquad P \mapsto A(b)^{(P)}$$

is injective. □

Proof. As explained in [6, §5.1], this map may be described as the composite

$$H^1_{f,T_0}(G_{K,T}, U) \to H^1_{f,T_0}(G_{K,T}, \mathrm{Aut}(A(b))) \xrightarrow{\simeq} M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W),$$

where the first map is induced from the group homomorphism $U \to \mathrm{Aut}(A(b))$ and the second map is induced from the isomorphism

$$M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W) \simeq H^1_{f,T_0}(G_{K,T}; U(\mathbb{Q}_p, V, W))$$

together with the structure of $A(b)$ as an $(\mathrm{Aut}(A(b)), U(\mathbb{Q}_p, V, W))$-bitorsor. The upshot is that it suffices to check the first map is injective. By definition of the map, this is implied by injectivity of

$$H^1(G_{K,T}, U) \to H^1(G_{K,T}, \mathrm{Aut}(A(b))).$$

By the exact sequence

$$H^0(G_{K,T}, \mathrm{Aut}(A(b))/U) \to H^1(G_{K,T}, U) \to H^1(G_{K,T}, \mathrm{Aut}(A(b)))$$

(see e.g., [49, Proposition 36]), it is enough to show that the pointed $G_{K,T}$-set $\mathrm{Aut}(A(b))/U$ has no fixed points, which can be seen by noting that it is an extension of a weight -1 $G_{K,T}$-representation by a weight -2 $G_{K,T}$-representation. ■

Let $P_1, \dots, P_n$ be elements of $\mathrm{Sel}(U)_\alpha$ in $H^1_f(G_{K,T}, V)$ spanning H (recall that this is the image of $\mathbb{Q}_p[\mathrm{Sel}(U)_\alpha]$ in $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$ under the map $P \mapsto \pi_{1*}(A(b)^{(P)}) \otimes \pi_{2*}(A(b)^{(P)})$), and such that $P_1, \dots, P_r$ span the image of $\mathbb{Q}_p[\mathrm{Sel}(U)_\alpha]$ in $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$ under $P \mapsto \pi_* P \otimes [IA(b)]$. Suppose $m_{ijk}, m_{ik} \in \mathbb{Q}_p$ satisfy

$$\pi_* P_i \otimes \tau_* \pi_* P_j = \sum_{k=1}^{n} m_{ijk} (A(b)^{(P_k)}) \otimes \pi_{2*}(A(b)^{(P_k)}) \tag{13}$$

$$\pi_* P_i \otimes [IA(b)] = \sum_{k=1}^{r} m_{ik} (A(b)^{(P_k)}) \otimes \pi_{2*}(A(b)^{(P_k)}) \tag{14}$$

Let $z \in X(K_\mathfrak{p})$. Then if $j_\mathfrak{p}(z)$ is in the image of $\mathrm{loc}_\mathfrak{p}(\mathrm{Sel}(U)_\alpha)$, there are $\lambda_1, \dots, \lambda_r$ such that

$$\kappa_p(z) = \sum \lambda_i \, \mathrm{loc}_p \, \pi_* P_i$$

and for all $\varphi \in H^1_s(G_{K,T}, W^*(1))$,

$$h_{\mathfrak{p},\varphi}(j_\mathfrak{p}(z)) + \sum_{v \in T_0} h_{\mathfrak{p},\varphi}(\alpha_v) = \sum_{1 \le i \le r, 1 \le k \le r} \lambda_i m_{ik} h_\varphi(P_k) + \sum_{1 \le i,j \le r, 1 \le k \le n} \lambda_i \lambda_j m_{ijk} h_\varphi(P_k)$$

since if $j_\mathfrak{p}(z)$ comes from some $P \in \mathrm{Sel}(U)_\alpha$, then we must have

$$\pi_{1*}(A(b)^{(P)}) \otimes \pi_{2*}(A(b)^{(P)}) = \sum_{1 \le i \le r} \lambda_i \pi_*(P_i) \otimes ([IA(b)] + \sum_{1 \le j \le r} \lambda_j(P_j)),$$

in $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$, which is equal to the class of

$$\sum_{1 \le i \le r, 1 \le k \le r} \lambda_i m_{ik} \pi_{1*}(A(b)^{(P_k)}) \otimes \pi_{2*}(A(b)^{(P_k)}) + \sum_{1 \le i,j, \le r, 1 \le k \le n} \lambda_i \lambda_j m_{ijk} \pi_{1*}(A(b)^{(P_k)}) \otimes \pi_{2*}(A(b)^{(P_k)})$$

by assumption. This gives the following explicit version of Lemma 4.1.

Proposition 4.1. *Suppose the kernel of* $\mathrm{Div}^0(X(\mathbb{Q}))/P \otimes \mathbb{Q}_p \to J(K_\mathfrak{p})$ *has rank* k_1*, and that the codimension of* $H^1_f(G_{K,T}, W)$ *in* $H^1_f(G_\mathfrak{p}, W)$ *is* k_2*. Let* $k = k_2 - k_1$*. Then*

$$X(K_\mathfrak{p})_\alpha = \cap_{1 \le i \le k} \{ R_{\lambda_1, \dots, \lambda_{k_1}}(\mathcal{F}_z(\lambda_1, \dots, \lambda_{k_1}) = 0 \},$$

where

$$\mathcal{F}_z(\lambda_1, \dots, \lambda_{k_1}) = h_{p,\varphi}(j_p(z)) + \sum_{v \in T_0} h_{p,\varphi}(\alpha_v) - \sum \lambda_i m_{ik} h_\varphi(P_k) - \sum \lambda_i \lambda_j m_{ijk} h_\varphi(P_k),$$

and m_{ijk} *and* m_{ik} *are as in equation* (13). □

In particular, if the Mordell–Weil rank of the Jacobian of X is less than or equal to g, and the map $\mathrm{Div}^0(X(K))/P \otimes \mathbb{Q}_p \to J(K) \otimes \mathbb{Q}_p$ is injective, then

$$X(K_\mathfrak{p})_\alpha = \cap_i \{ h_{\mathfrak{p},\varphi_i}(z) + \sum h_{v,\varphi_i}(\alpha_v) - h_{v,\varphi_i}(S \circ T(j_\mathfrak{p}(z))) = 0 \},$$

where $\varphi_1, \dots, \varphi_r$ is a basis for $H^1_s(G_{K,T}, \overline{\wedge^2 V}^*(1))$.

4.1 Equivariant height pairings

For the Manin–Demjanenko type results in the next section, it will be crucial to consider the subset of height functions which are equivariant with respect to extra endomorphisms of J.

Definition 4.3. Let $\gamma \in H^0(G_{K,T}, GL(V))$. Then γ acts on $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$ by sending $(M, (M_i), (\psi)_i)$ to $(M, (M_i), (\psi_i'))$ where $\psi_1' = \psi_1 \circ \gamma$ and for $i = 0, 2$ $\psi_i' = \psi_i$. We denote this action by γ^*. □

Let $\mathrm{red}_{F^\bullet}$ denote the quotient map $W_{\mathrm{dR}} \to W_{\mathrm{dR}}/F^0$. The splitting s induces sections of $W_{\mathrm{dR}} \to W_{\mathrm{dR}}/F^0$ and $V^* \otimes W \to (V^* \otimes W)/F^0$ as follows: the isomorphism $V_{\mathrm{dR}} \simeq \mathrm{gr}_F V_{\mathrm{dR}}$ induces an isomorphism $\mathrm{gr}_F^\bullet(V_{\mathrm{dR}} \otimes V_{\mathrm{dR}}) \simeq V_{\mathrm{dR}} \otimes V_{\mathrm{dR}}$, and hence together with the surjection $V_{\mathrm{dR}} \otimes V_{\mathrm{dR}} \to W_{\mathrm{dR}}$, we get an isomorphism $W_{\mathrm{dR}} \simeq \mathrm{gr}_F W_{\mathrm{dR}}$. We denote the induced section of $V^* \otimes W \to (V^* \otimes W)/F^0$ by s.

Lemma 4.4. We have the following:

1. For $v \neq p$, and γ in $R^\times$, we have $h_v(M) = h_v(\gamma^* M)$.
2. The map $M \mapsto \widetilde{h}_{\mathfrak{p}}(M) - \widetilde{h}_{\mathfrak{p}}(\gamma M)$ factors as

$$M_f(G_{\mathfrak{p}}; \mathbb{Q}_p, V, W) \to V_{\mathrm{dR}}/F^0 \times (V_{\mathrm{dR}}^* \otimes W_{\mathrm{dR}})/F^0 \xrightarrow{\overline{h}_\gamma} W_{\mathrm{dR}}/F^0$$

   where $\overline{h}_\gamma$ is the bilinear map

$$(v, w) \mapsto \mathrm{red}_{F^\bullet}(s(w) \circ s)(v) - \mathrm{red}_{F^\bullet}(\gamma^* s(w)) \circ s(\gamma_* v).$$

3. If γ commutes with the splitting of the Hodge filtration, then $h_{\mathfrak{p}}(M) = h_{\mathfrak{p}}(\gamma M)$.

□

Proof. First note that for $v \neq p$, we have $h_v(M) = h_v(\gamma M)$, since the definition of h_v does not depend on a choice of isomorphism $M_2/W \simeq V$. For the second claim, note that by definition of $\widetilde{h}_{\mathfrak{p}}$ we have

$$h_{\mathfrak{p}}(M) - h_{\mathfrak{p}}(\gamma M) = t(M_1, M_2) - t(\gamma^* M_1, \gamma_* M_2),$$

as required. For the last part, note that if γ commutes with s we have

$$\mathrm{red}_{F^\bullet}(\gamma^* s(w)) \circ s \circ \gamma_*) = \mathrm{red}_{F^\bullet}((\gamma^* s(w)) \circ \gamma_* \circ s) = \mathrm{red}_{F^\bullet}(s(w) \circ s)$$

which by the above implies $h_{\mathfrak{p}}(M) = h_{\mathfrak{p}}(\gamma M)$. ■

As a result, the height h is R-equivariant if and only if for all γ in $R^\times$, $s(w) \circ s = (\gamma^* s(w)) \circ s \circ \gamma_*$ modulo $F^0 W$.

5 Generalised heights on hyperelliptic curves

In this section we prove Theorem 1.1 and the finiteness part of Theorem 1.2, using equivariant heights. In brief, the previous section explained how generalised heights provided non-trivial quadratic relations between $\widetilde{h}(A(b, z))$ and $\kappa(z - b)$. To prove finiteness of $X(K_{\mathfrak{p}})_U$, one would like to find non-trivial polynomial relations between $\widetilde{h}(A(b, z))$ and $\mathrm{loc}_{\mathfrak{p}}(\kappa(z - b))$. In general, the obstruction to doing this lives in $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$, in some sense. The idea of using equivariant heights on hyperelliptic curves is to try and replace this with a smaller obstruction space.

Definition 5.1. Define the *hyperelliptic subspace* of $H^1_f(G_{K,T}, V) \otimes H^1_f(G_{K,T}, V^* \otimes W)$ to be the image of $H^1_f(G_{K,T}, V)^{\otimes 2}$ under the map $1 \otimes \tau_*$, where τ is as in Definition 3.4. Define the *hyperelliptic subspace* of $M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$, denoted $M^h_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$, to be the subvariety of classes whose associated $H^1_f(G_{K,T}, V^* \otimes W)$ class is in the image of τ_*. □

The reason for the name is that, by Lemma 3.7, the image of the Selmer variety of a hyperelliptic curve lies in the hyperelliptic subspace.

Lemma 5.2. Let X be a hyperelliptic curve, b a rational point and U any quotient of $U_2(b)$. Then the natural map

$$H^1_{f,T_0}(G_{K,T}, U) \to M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W); P \mapsto A(b)^{(P)}$$

lands in the hyperelliptic subspace. □

One may straightforwardly extend this to equivariant heights.

Lemma 5.3. Suppose s is an R-equivariant splitting. Then

1. The generalised height
$$h : M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W) \to \mathbb{Q}_p$$
factors through $H^1(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V^* \otimes W)$.
2. The generalised height function, restricted to the hyperelliptic subspace, factors through $H^1_f(G_{K,T}, V) \otimes_{R,\tau} H^1_f(G_{K,T}, V)$.

□

Proof. By Lemma 3.11 and Lemma 5.2, we only need to prove R-equivariance. To prove this, it will be enough to prove that, for all $\gamma \in R^\times$, we have $h(\gamma^* E_1, E_2) = h(E_1, \gamma^* E_2)$. It suffices to prove this locally, i.e. to prove that for all mixed extensions M,
$$h_v(M) = h_v(\gamma^* M).$$
This follows from Lemma 4.4.

■

We now explain the application to finiteness of Chabauty–Kim sets.

Proposition 5.1. *Let X be a hyperelliptic curve. Let $R = \mathrm{End}^0_K(J)$. Suppose*
$$\dim(H^1_f(G_\mathfrak{p}, W)/\operatorname{loc}_\mathfrak{p} H^1_f(G_{K,T}, W)) - \dim(H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)) + \dim(H^1_f(G_\mathfrak{p}, V) \otimes_R H^1_f(G_\mathfrak{p}, V)) > 0.$$
Then $X(K_\mathfrak{p})_U$ is finite. □

Remark 2. Note that, given [6, Lemma 3.2], this result is only new when
$$\begin{aligned}\dim(H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)) - \dim(H^1_f(G_\mathfrak{p}, V) \otimes_R H^1_f(G_\mathfrak{p}, V))\\ < \dim H^1_f(G_{K,T}, V) - \dim H^1_f(G_\mathfrak{p}, V).\end{aligned}$$
This can only happen when there are simple abelian varieties which occur as isogeny factors of J with multiplicity greater than 1 (see the example below). □

Proof. By [34, Theorem 1], it is enough to prove that the localisation map
$$\mathrm{Sel}(U) \to H^1_f(G_\mathfrak{p}, U)$$
is not dominant. Writing $\mathrm{Sel}(U)$ as a disjoint union of $\mathrm{Sel}(U)_\alpha$, for α a collection of local conditions, we reduce to proving that, for all α, the localisation map
$$\mathrm{Sel}(U)_\alpha \to H^1_f(G_\mathfrak{p}, U)$$
is not dominant. Let
$$r = \dim(H^1_f(G_\mathfrak{p}, W)/\operatorname{loc}_\mathfrak{p} H^1_f(G_{K,T}, W)) + \dim(H^1_f(G_\mathfrak{p}, V) \otimes_R H^1_f(G_\mathfrak{p}, V)).$$
We show that the codimension of
$$(\operatorname{loc}_\mathfrak{p}, \pi_{1*} \otimes \pi_{2*}) : \mathrm{Sel}(U)_\alpha \to H^1_f(G_p, U) \times H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)$$
is greater than r, which proves the non-dominance of the localisation map by projecting. We first choose a (vector space) section t of the map
$$\mathbb{Q}_p[M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)^h] \to H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V).$$
Define a map
$$H^1_f(G_\mathfrak{p}, U) \times H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V) \to H^1_s(G_{K,T}, W^*(1))$$
by sending (c, d) to $\widetilde{h}_\mathfrak{p}(c) + \sum_{v \in T_0} \widetilde{h}_v(\alpha_v) - \widetilde{h}(t(d))$. Then by equation (12), the composite map
$$\mathrm{Sel}(U)_\alpha \to H^1_f(G_\mathfrak{p}, U) \times H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V) \to H^1_s(G_{K,T}, W^*(1))$$
is identically zero. Similarly the composite map
$$\begin{aligned}\mathrm{Sel}(U)_\alpha &\to H^1_f(G_\mathfrak{p}, U) \times H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)\\ &\xrightarrow{\pi_* \otimes \pi_* - \operatorname{loc}_\mathfrak{p} \otimes \operatorname{loc}_\mathfrak{p}} H^1_f(G_\mathfrak{p}, V) \otimes_R H^1_f(G_\mathfrak{p}, V)\end{aligned}$$
is identically zero. ■

Lemma 5.4. We have the following:

1. There is an R-equivariant pre-height.
2. The set of R-equivariant pre-heights is a $\mathrm{Hom}_{R\otimes\mathbb{Q}_p}(V/F^0, F^0V)$-torsor.

□

Proof. By Lemma 4.4, R-equivariant pre-heights correspond to R-equivariant splittings of the Hodge filtration. By functoriality, F^0V is an $R\otimes\mathbb{Q}_p$-submodule of V. Since R is semisimple, we deduce the existence of an R-equivariant splitting. ■

We now consider the setup of Theorem 1.1: $K=\mathbb{Q}$ or an imaginary quadratic field, the curve X/K is hyperelliptic, with Jacobian J isogenous to $A^d\times B$. Hence $R=\mathrm{Mat}_d(\mathbb{Q})$ is naturally a (non-unital) subalgebra of $\mathrm{End}^0(J)$. Let $V_A=T_p(A)\otimes\mathbb{Q}_p$ and $V_B=T_p(B)\otimes\mathbb{Q}_p$. Then $V\simeq V_A^{\oplus d}\oplus V_B$. To apply Proposition 5.1, note that

$$H^1_f(G_{K,T},V_A)^{\oplus d}\otimes_R H^1_f(G_{K,T},V_A)^{\oplus d}\simeq H^1_f(G_{K,T},V_A)\otimes_{\mathbb{Q}_p} H^1_f(G_{K,T},V_A).$$

We are now ready to give the proof of Theorem 1.1.

Proof of Theorem 1.1. Let $\overline{\wedge^2(V_A^{\oplus d})}$ be the quotient of $\wedge^2(V_A^d)$ by the image of

$$\mathrm{Ker}(\wedge^2V\to\overline{\wedge^2V})$$

under the projection from $\wedge^2V$ to $\wedge^2(V_A^d)$. First we prove that there is a quotient W of $\overline{\wedge^2V}$ such that the quotient map factors through $\overline{\wedge^2(V_A^{\oplus d})}$ and such that

$$\mathrm{codim}(\mathrm{loc}_{\mathfrak{p}}: H^1_f(G_{K,T},W)\to H^1_f(G_{\mathfrak{p}},W))=\rho_f(A)d+d(d-1)e(A)/2-1.$$

We have $\wedge^2(V_A^d)\simeq(\wedge^2V_A)^d\oplus(V_A^{\otimes 2})^{d(d-1)/2}$. Since $\mathrm{NS}(A_{\overline{K}})\otimes\mathbb{Q}_p(1)$ is a direct summand of $\wedge^2V_A$ and $\mathrm{End}^0(A_{\overline{K}})\otimes\mathbb{Q}_p(1)$ is a direct summand of $V_A^{\otimes 2}$, we have a Galois-equivariant surjection

$$\wedge^2V\to(\mathrm{NS}(A_{\overline{K}})\otimes\mathbb{Q}_p(1)))^d\oplus(\mathrm{End}^0(A_{\overline{K}}\otimes\mathbb{Q}_p(1)))^{d(d-1)/2}.$$

First suppose $K=\mathbb{Q}$. We take W to be the quotient of $\overline{\wedge^2V}$ corresponding to $(\mathrm{NS}(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}_p(1)))^d\oplus(\mathrm{End}^0(A_{\overline{\mathbb{Q}}}\otimes\mathbb{Q}_p(1)))^{d(d-1)/2}$. Then it is enough to prove

$$\dim H^1_f(G_{\mathfrak{p}},\mathrm{NS}(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}_p(1))-\dim H^1_f(G_{\mathbb{Q},T},\mathrm{NS}(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}_p(1))\geq\rho_f(A)$$

and

$$\dim H^1_f(G_{\mathfrak{p}},\mathrm{End}^0(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}_p(1))-\dim H^1_f(G_{\mathbb{Q},T},\mathrm{End}^0(A_{\overline{\mathbb{Q}}})\otimes\mathbb{Q}_p(1))\geq e(A),$$

which follows from Lemma 2.3. If K is imaginary quadratic, we have a surjection

$$\wedge^2V\to(\mathrm{NS}(A_K)\otimes\mathbb{Q}_p(1)))^d\oplus(\mathrm{End}^0(A_K\otimes\mathbb{Q}_p(1)))^{d(d-1)/2},$$

and we take W to be the corresponding quotient of $\overline{\wedge^2V}$. The result now follows from the fact that $H^1(G_{K,T},\mathbb{Q}_p(1))=0$.

We are now ready to complete the proof of Theorem 1.1. First suppose $\rho_f(A)d+d(d-1)e(A)/2-1>d(r-\dim(A))$. By Lemma 3.7, we have a Galois-stable quotient of U_2 (i.e. the kernel is Galois stable) which is an extension

$$1\to W\to U\to V_A^d\to 1$$

and we have

$$\dim H^1_f(G_{\mathfrak{p}},U)-\dim H^1_f(G_{K,T},U)\geq\rho_f(A)d+d(d-1)e(A)/2-1-d(r-\dim(A)).$$

Finally, if $\rho_f(A)d+d(d-1)e(A)/2-1>r^2-\dim(A)^2$, then we use Proposition 5.1. We take R, as above, to be $\mathrm{Mat}_d(\mathbb{Q})$, acting trivially on B and in the obvious way on A^d. Then

$$\mathrm{rk}(J(K)\otimes\mathbb{Q})\otimes_R(J(K)\otimes\mathbb{Q})=r^2\quad\text{and}$$

$$\dim H^1_f(G_{\mathfrak{p}},V)\otimes_{R\otimes\mathbb{Q}_p}\dim H^1_f(G_{\mathfrak{p}},V)=(\dim A)^2.$$

■

5.1 An example

Given the restrictive hypotheses of Theorem 1.1, it is perhaps worth demonstrating the existence of a hyperelliptic curve satisfying them which does not satisfy the Chabauty–Coleman bound. We use work of Paulhus [47, Table 2] and Shaska [51, §4] on a family of hyperelliptic curves X_t defined over $K = \mathbb{Q}(i)$ with Jacobian isogenous to $E_t^3 \times A_t$. Let X_t denote the genus 5 curve

$$y^2 = x^{12} - tx^{10} - 33x^8 + 2tx^6 - 33x^4 - tx^2 + 1.$$

For all but a finite number of t, we have a subgroup of $\mathrm{Aut}\, X_t$ isomorphic to A_4, generated by the automorphisms of order 2 and 3, respectively:

$$\tau : (x, y) \mapsto (-x, y), \qquad \sigma : (x, y) \mapsto \left(\frac{x - i}{x + i}, \frac{y}{(x + i)^6}\right).$$

Together with the hyperelliptic automorphism, this means that all but a finite number of curves in the family has $\mathbb{Z}/2\mathbb{Z} \times A_4$ as a subgroup of its automorphism group. The normalisation of the quotient of X by σ is the genus 1 curve

$$C : y^2 = x^4 + (-t + 12i)x^2 + ((2i - 2)t + 20i + 20)x + 2it + 21,$$

which has Jacobian

$$E_t : y^2 = x^3 - \frac{1}{4}(3t^2 - 70it - 411)x - \frac{1}{4}(t^3 - 30it^2 - 317t + 1180i).$$

Fix a prime p with $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K and such that X_t has good reduction at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$.

Corollary 5.2. *For all t such that $\mathrm{rk}_K\, E_t \leq 2$, and $\mathfrak{p}$ as above, $X(K_{\mathfrak{p}})_2$ is finite.* □

Proof. Let $V_E := T_p(E_t) \otimes \mathbb{Q}_p$, $V_A := T_p(A) \otimes \mathbb{Q}_p$. We have an isomorphism

$$\wedge^2 V \simeq \wedge^2(V_E^{\oplus 3}) \oplus V_E \otimes V_A \oplus \wedge^2 V_A.$$

Let $\overline{\wedge^2 V} \to \mathbb{Q}_p(1)^{\oplus 4}$ be the composite $\overline{\wedge^2 V} \to (\wedge^2(V_E^{\oplus 3}))/\mathbb{Q}_p(1) \to \mathbb{Q}_p(1)^{\oplus 4}$. Let U be the corresponding quotient of U_2. The result follows from Proposition 5.1. ■

Remark 3. Note that the dimension of the Selmer variety equals that of $H^1_f(G_{\mathfrak{p}}, U)$, so the multiplicities of isogeny factors are really used in an essential way. □

An explicit example of a value of t for which E_t has rank 2 is $t = 1$: the elliptic curve $y^2 = x^3 + (35/2i + 102)x + (-575/2i + 79)$ has two independent points $P_1 = (4i - 3, 14i + 4), P_2 = (-12i + 1, 11i + 9)$. Using SageMath [52], we verified linear independence (and a lower bound of 2 for the rank) by computing that the associated regulator of height pairings is approximately 6.501, and in particular, is nonzero. An upper bound of 2 on the rank was found by using Magma [13] to compute the rank of the 2-Selmer group to be 2.

5.2 The Kulesz–Matera–Schost family

Here we return to the family of genus 2 curves mentioned in the introduction. We show that for this family, one can use equivariant heights to prove stronger finiteness results than the ones above. Recall that X is a hyperelliptic curve of the form $y^2 = x^6 + ax^4 + ax^2 + 1$, and let E be the elliptic curve $y^2 = x^3 + ax^2 + ax + 1$. We assume E has rank 2. Define V_E to be $H^1(E_{\overline{K}}, \mathbb{Q}_p)^*$. The morphisms f_1, f_2 from X to E induce an isomorphism $V \simeq V_E \oplus V_E$, which induces a Galois-stable quotient U of U_2 with W taken to be $\mathrm{Sym}^2 V_E$, via the map

$$\wedge^2 V \to \mathrm{Sym}^2 V_E; (v_1, v_2) \wedge (v_3, v_4) \mapsto v_1 v_4 - v_2 v_3. \tag{15}$$

The aim of this subsection is to prove the following lemma:

Lemma 5.5. The localisation map $\mathrm{loc}_{\mathfrak{p}} : \mathrm{Sel}(U) \to H^1_f(G_{\mathfrak{p}}, U)$ is not dense. □

In fact we will prove an explicit form of this. The deep result underlying this non-density is the fact that $H^1_f(G_{K,T}, \mathrm{Sym}^2 V_E) = 0$. In the case when $K = \mathbb{Q}$, $p \geq 5$, and the map

$$\rho_{E[p]} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}(E[p])$$

is surjective, this is due to Flach [24, Theorem 1, and remarks below], who shows that $H^1_f(G_{K,T}, \mathrm{Sym}^2 T_pE \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ is finite, which implies triviality of $H^1_f(G_{K,T}, \mathrm{Sym}^2 V_E) = 0$. In general, the only known proof is via a Galois deformation argument, following Taylor–Wiles and Kisin. Namely, using Fontaine–Perrin-Riou's Euler characteristic formula [26, Remark II.2.2.2], we know that

$$\dim H^1_f(G_{K,T}, \mathrm{Sym}^2 V_E) = \dim H^1_f(G_{K,T}, \mathrm{ad}^0 V_E).$$

Under the assumptions above, it is known that $H^1_g(G_{K,T}, \mathrm{ad}^0 V_E) = 0$ (see Allen [1, Theorem A] for a more general result).

Let $R := \mathrm{Mat}_2(\mathbb{Q}_p)$. Then V has the structure of an R-module via the isomorphism $V \simeq V_E \oplus V_E$. Let $\Gamma : \mathbb{Q}_p[H^1_{f,T_0}(G_{K,T}, U)] \to \wedge^2 H^1_f(G_{K,T}, V_E)$ be the composite map

$$\begin{aligned}\mathbb{Q}_p[H^1_{f,T_0}(G_{K,T}, U)] &\to H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)\\ &\xrightarrow{\simeq} H^1_f(G_{K,T}, V_E) \otimes_{\mathbb{Q}_p} H^1_f(G_{K,T}, V_E) \to \wedge^2 H^1_f(G_{K,T}, V_E),\end{aligned}$$

where the first map sends P to the $H^1_f(G_{K,T}, V) \otimes_R H^1_f(G_{K,T}, V)$-class of $A(b)^{(P)}$, the second is the isomorphism

$$H^1_f(G_{K,T}, V_E^{\oplus 2}) \otimes_{\mathrm{Mat}_2(\mathbb{Q}_p)} H^1_f(G_{K,T}, V_E^{\oplus 2}) \xrightarrow{\simeq} H^1_f(G_{K,T}, V_E) \otimes_{\mathbb{Q}_p} H^1_f(G_{K,T}, V_E), \tag{16}$$

and the third is the usual projection of the tensor square onto the alternating product. By Lemma 3.7, and (15) when $P = P(b, z)$, we have that $\Gamma(P)$ is given by

$$f_{1*}\kappa(z-b) \wedge f_{2*}\kappa(z+b-D) - f_{2*}\kappa(z-b) f_{1*}(z+b-D),$$

which is equal to $2\kappa_E(f_1(z) - O) \wedge \kappa_E(f_2(z))$.

Definition 5.6. Given $[E_1], [E_2]$ in $H^1_f(G_{K,T}, V)$, define $[E_1, E_2] \in M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, W)$ to be the quotient of $E_1 \otimes E_2$ by $\wedge^2 V \subset V \otimes V \subset E_1 \otimes E_2$, viewed as a mixed extension with graded pieces $\mathbb{Q}_p, V$ and W via the isomorphism $V \simeq V_E^{\oplus 2}$. □

Lemma 5.7. Let $\mathfrak{p}$ be a prime above p.

1. The mixed extension $[E_1, E_2]$ lies in the hyperelliptic subspace, and its image in $H^1_f(G_{K,T}, V_E)^{\otimes 2}$ is given by $[E_1] \otimes [E_2] + [E_2] \otimes [E_1]$.
2. Let $[E_1] = f_{2*}\pi_* P$ and $[E_2] = -f_{1*}\kappa(2b - D)$. Let h be an R-equivariant height. Let $\alpha \in \prod_{v \in T_0} H^1(G_v, U)$ be a collection of local conditions. Then the map

$$\begin{aligned}\widetilde{h}' : H^1_f(G_{K,T}, U) &\to H^1_s(G_{K,T}, \mathrm{Sym}^2(V)(1))\\ P &\mapsto \widetilde{h}_{\mathfrak{p}}(A(b)^{(P)}) + \sum_{v \in T_0} \widetilde{h}_v(\alpha_v) - \frac{1}{2}\widetilde{h}([E_1, E_2])\end{aligned}$$

factors through $\wedge^2 H^1_f(G_{K,T}, V_E)$.

□

Proof. For the first part, the image of $[E_1, E_2]$ in $H^1(G_{K,T}, V) \otimes H^1(G_{K,T}, V^* \otimes W)$ is equal to $([E_1], [E_2]) \otimes ([E_2], [E_1])$, hence the claim follows from the explicit description of the isomorphism (16). For the second part, note by Lemma 3.7, $A(b)^{(P)}$ is a mixed extension of $\pi_* P$ and $\tau_*(\kappa(b - D) + \pi_* P)$. So under the decomposition

$$H^1_f(G_{K,T}, V_E) \otimes H^1_f(G_{K,T}, V_E) = \wedge^2 H^1_f(G_{K,T}, V_E) \oplus \mathrm{Sym}^2 H^1_f(G_{K,T}, V_E),$$

the image of $A(b)^{(P)}$ in $\mathrm{Sym}^2 H^1_f(G_{K,T}, V_E)$ is given by

$$\begin{aligned}&(f_{1*}\pi_* P)(f_{2*}(\kappa(2b - D) + \pi_* P) - (f_{2*}\pi_* P)(f_{1*}(\kappa(2b - D) + \pi_* P)\\ =&(f_{1*}\pi_* P) f_{2*}\kappa(2b - D) - (f_{2*}\pi_* P) f_{1*}(\kappa(2b - D)\\ =&-(f_{2*}\pi_* P)(f_{1*}\kappa(2b - D)),\end{aligned}$$

since $f_{2*}\kappa(2b - D)$ is zero. The image of $[E_1, E_2]$ in $\mathrm{Sym}^2 H^1_f(G_{K,T}, V_E)$ is given by

$$-(f_{2*}\pi_* P)(f_{1*}\kappa(2b - D)) - (f_{1*}\kappa(b - D))(2 f_{2*}\pi_* P).$$

Hence the class of $A(b)^{(P)} - \frac{1}{2}[E_1, E_2]$ in $H^1_f(G_{K,T}, V_E)^{\otimes 2}$ lies in $\wedge^2 H^1_f(G_{K,T}, V_E)$. ■

We are now ready to prove an explicit form of the non-dominance result for the localisation map.

Lemma 5.8. Let $\alpha \in \prod_{v\in T_0} H^1(G_v, \mathrm{Sym}^2_E)$ be a collection of local conditions.

1. Let
$$t : \wedge^2 H^1_f(G_{K,T}, V_E) \to \mathbb{Q}_p[H^1_f(G_{K,T}, U)]$$
be a section of Γ. Let w be a generator of $\wedge^2 H^1_f(G_{K,T}, V_E)$. Let P_0 be any element of $\mathrm{Sel}(U)_\alpha$. Then $\mathrm{loc}_\mathfrak{p}\,\mathrm{Sel}(U)_\alpha$ is contained within the kernel of
$$\begin{aligned} H^1_f(G_\mathfrak{p}, U) &\to \wedge^2 H^1_f(G_\mathfrak{p}, \mathrm{Sym}^2 V_E) \\ P &\mapsto (\widetilde{h}'_\mathfrak{p}(P) - \widetilde{h}'_\mathfrak{p}(P_0)) \wedge \widetilde{h}'_\mathfrak{p}(t(w)). \end{aligned}$$
2. Let b and z_0 be points of $X(K)$ satisfying $\Gamma(A(b, z_0)) \neq 0$. Then $X(K_\mathfrak{p})_U$ is in the kernel of
$$\begin{aligned} X(K_\mathfrak{p}) &\to \wedge^2(W_{\mathrm{dR}}/F^0) \\ z &\mapsto \widetilde{h}'_\mathfrak{p}(A(b, z)) \wedge \widetilde{h}'_\mathfrak{p}(A(b, z_0)). \end{aligned}$$

□

Note that part (1) of Lemma 5.8 implies Lemma 5.5, since by Lemma 3.10, the map $\widetilde{h}_\mathfrak{p} : H^1_f(G_\mathfrak{p}, U) \to H^1_f(G_\mathfrak{p}, W)$ is onto and hence the map in part (1) of the lemma is surjective.

Proof of Lemma 5.8. Choose a basis e_1, e_2 of $H^1_f(G_\mathfrak{p}, \mathrm{Sym}^2 V_E)$. Since we have $H^1_f(G_{K,T}, \mathrm{Sym}^2 V_E) = 0$, we can define cohomology classes χ_1, χ_2 in $H^1(G_{K,T}, \mathrm{ad}^0 V_E)$ which are crystalline at all primes above p other than $\mathfrak{p}$, and such that the image of $\mathrm{loc}_\mathfrak{p}(\chi_i)$ in $H^1(G_\mathfrak{p}, \mathrm{ad}^0 V_E)/H^1_f(G_\mathfrak{p}, \mathrm{ad}^0 V_E)$ is isomorphic to e_i^* via Tate duality. Let
$$h = (h_{\chi_1}, h_{\chi_2}) : M_{f,T_0}(G_{K,T}; \mathbb{Q}_p, V, \mathrm{Sym}^2 V_E) \to \mathrm{Sym}^2 V_{\mathrm{dR}}/F^0$$
be the corresponding sum of heights. Let h' denote the map
$$P \mapsto h(P) - \frac{1}{2}h([E_1, E_2])$$
as before. Part (1) follows from Lemma 5.7, since that implies that the image of $\mathrm{Sel}(U)$ in $H^1_f(G_\mathfrak{p}, \mathrm{Sym}^2 V_E)$ under h' has dimension at most 1. For part (2), by assumption, $\Gamma(A(b, z_0))$ is a generator of $\wedge^2 H^1_f(G_{K,T}, V_E)$, hence the result follows from part (1). ■

6 Explicit local methods

The goal of this section is to provide an explicit, algorithmic description of the composite map
$$X(K_\mathfrak{p}) \xrightarrow{j_\mathfrak{p}} H^1_f(G_\mathfrak{p}, U) \xrightarrow{\simeq} U^{\mathrm{dR}}/F^0 \xrightarrow{\widetilde{h}_\mathfrak{p}} W_{\mathrm{dR}}/F^0$$
which sends a $K_\mathfrak{p}$-point to the generalised pre-height of $A(b, z)$. As p splits completely in $K|\mathbb{Q}$, via a choice of embedding $K \hookrightarrow \mathbb{Q}_p$, we have that $K_\mathfrak{p}$ is isomorphic to $\mathbb{Q}_p$, and we henceforth write $\mathbb{Q}_p$ instead of $K_\mathfrak{p}$. Describing this map explicitly amounts to giving an explicit description of the structure of $D_{\mathrm{cr}}(A(b, z))$ as a filtered ϕ-module. As is explained below, by Olsson's comparison theorem [46, Theorem 1.4], this may be reduced to computing the Hodge filtration and Frobenius action on a de Rham path space $A^{\mathrm{dR}}(b, z)$ (see [35, §3]). The specific relation is stated in Section 6.2.

It turns out to be simplest to describe the Hodge filtration and Frobenius structure on $A^{\mathrm{dR}}(b, z)$ by understanding how it varies with z. More precisely, the vector space $A^{\mathrm{dR}}(b, z)$ is the fibre at z of a unipotent vector bundle with connection $\mathcal{A}^{\mathrm{dR}}$, which is a quotient of a universal bundle with connection $\mathcal{A}^{\mathrm{dR}}_n$. The filtration on $A^{\mathrm{dR}}(b, z)$ comes from a filtration by sub-bundles $F^i\mathcal{A}^{\mathrm{dR}} \subset \mathcal{A}^{\mathrm{dR}}$, and these sub-bundles are uniquely determined by certain universal properties. This rigidifying property means that, to compute $F^i\mathcal{A}^{\mathrm{dR}}(b, z)$ it is enough to find *any* filtration on $\mathcal{A}^{\mathrm{dR}}$ satisfying certain properties (see Lemma 6.4 and Corollary 6.2), giving an algorithm for computing $F^i A^{\mathrm{dR}}(b, z)$ (see Section 6.5).

To calculate Frobenius, one could employ a similar approach, by describing the Frobenius action on $A^{\mathrm{dR}}(b, z)$ as the pull-back along z of the Frobenius structure on $\mathcal{A}^{\mathrm{dR}}$. In Section 6.7 we take a slightly different approach, using the 'hyperelliptic splitting principle' in a similar manner to Lemma 3.7 to calculate the ϕ-action on $A^{\mathrm{dR}}(b, z)$ when b and z are Weierstrass points. Using Besser's Tannakian interpretation of Coleman integration, we can describe how the ϕ-action varies when we vary b and z in terms of iterated Coleman integrals.

6.1 The universal connection

First we recall some properties of the de Rham fundamental group and associated objects, as developed by Chen, Deligne, Hain and Wojtkowiak (see [20, 54, 30]). When describing $\mathcal{A}^{\mathrm{dR}}$, it is computationally convenient to restrict to a Zariski open $Y \subset X$, as on Y, unipotent vector bundles are trivial, making connections and morphisms between them easier to calculate. Another reason that the affine case is simpler is that the de Rham fundamental group of Y is a free pro-unipotent group, which makes it easier to write down elements of the fundamental group, or its enveloping algebra.

Let $Y \subset X$ be a non-empty Zariski open subset of X, with $X - Y$ of order r. Define $V_{\mathrm{dR}}(Y) = H^1_{\mathrm{dR}}(Y)^*$. Recall from Section 3 that $V_{\mathrm{dR}} := D_{\mathrm{cr}}(V) \simeq H^1_{\mathrm{dR}}(X)^*$. Denote by $\mathcal{C}^{\mathrm{dR}}(Y)$ the category of unipotent flat connections on Y, and $\mathcal{C}^{\mathrm{dR}}(X)$ the category of unipotent flat connections on X. Since X and Y are curves, all connections on them are flat, and hence this condition will henceforth not be mentioned. Given a connection $\mathcal{V}$ and a K-vector space W, we shall often refer to $W \otimes \mathcal{V}$ as a connection, in the natural way: the $\mathcal{U}$-sections of the vector bundle are just $W \otimes \mathcal{V}(\mathcal{U})$, and the connection morphism is $1_W \otimes \nabla$. Alternatively, if $\pi : Y \to \mathrm{Spec}(K)$ denotes the structure morphism, we can think of $W \otimes \mathcal{V}$ as being a tensor product of connections:

$$W \otimes \mathcal{V} := (\pi^* W, d) \otimes (\mathcal{V}, \nabla).$$

Let b be a K-point of Y. Then taking the fibre of the underlying bundle at b defines a fibre functor b^* from $\mathcal{C}^{\mathrm{dR}}(X)$ to K-vector spaces, giving $(\mathcal{C}^{\mathrm{dR}}(X), b^*)$ the structure of a neutral Tannakian category. Define $\pi_1^{\mathrm{dR}}(X, b)$ to be the corresponding K-group scheme. This group is pro-unipotent and is the inverse limit of the n-step unipotent quotients $U_n^{\mathrm{dR}}(b) = U_n^{\mathrm{dR}}(X)(b)$. Moreover,

$$P_n^{\mathrm{dR}}(X)(b, z) = P_n^{\mathrm{dR}}(b, z) = \pi_1^{\mathrm{dR}}(X; b, z) \times_{\pi_1^{\mathrm{dR}}(X,b)} U_n^{\mathrm{dR}}(b).$$

Similarly define $\pi_1^{\mathrm{dR}}(Y, b)$, $U_n^{\mathrm{dR}}(Y)(b)$, $P_n^{\mathrm{dR}}(Y)(b, z)$. Finally, in the notation of the appendix, define

$$\begin{array}{ll} \mathcal{A}_n^{\mathrm{dR}}(X)(b) := \mathcal{A}_n(\mathcal{C}^{\mathrm{dR}}(X), b^*), & \mathcal{A}_n^{\mathrm{dR}}(Y)(b) := \mathcal{A}_n(\mathcal{C}^{\mathrm{dR}}(Y), b^*), \\ A_n^{\mathrm{dR}}(X)(b, z) := A_n(\mathcal{C}^{\mathrm{dR}}(X); b^*, z^*), & A_n^{\mathrm{dR}}(Y)(b, z) := A_n(\mathcal{C}^{\mathrm{dR}}(Y); b^*, z^*), \\ \mathcal{A}_n^{\mathrm{dR}}(X) := \mathcal{A}_n^{\mathrm{dR}}(\mathcal{C}^{\mathrm{dR}}(X), b^*), & \mathcal{A}_n^{\mathrm{dR}}(Y) := \mathcal{A}_n^{\mathrm{dR}}(\mathcal{C}^{\mathrm{dR}}(Y), b^*). \end{array}$$

When there is no risk of confusion, we shall sometimes abbreviate $A_n^{\mathrm{dR}}(X)(b, z), A_n^{\mathrm{dR}}(X)(b), \mathcal{A}_n^{\mathrm{dR}}(X)$ to $A_n^{\mathrm{dR}}(b, z), A_n^{\mathrm{dR}}(b), \mathcal{A}_n^{\mathrm{dR}}$. As explained in the appendix, $A_n^{\mathrm{dR}}(X)(b)$ may equivalently be defined to be the quotient of the universal enveloping algebra of $\mathrm{Lie}(\pi_1^{\mathrm{dR}}(X, b))$ by the $(n+1)$th power of the kernel of the co-unit map. In particular, the vector spaces $A_n^{\mathrm{dR}}(X)(b) \simeq b^* \mathcal{A}_n^{\mathrm{dR}}(X)$ and $A_n^{\mathrm{dR}}(Y)(b) \simeq b^* \mathcal{A}_n^{\mathrm{dR}}(Y)$ each have the structure of associative algebras with unit elements that we will denote by e_n. As explained in the appendix, $\mathcal{A}_n^{\mathrm{dR}}(X)$ is a universal n-unipotent pointed object in $\mathcal{C}^{\mathrm{dR}}(X)^{b^*}$; i.e., for any n-unipotent connection $\mathcal{V}$ on X, and any $v \in b^* \mathcal{V}$, there exists a unique morphism of connections $f : \mathcal{A}_n^{\mathrm{dR}}(X) \to \mathcal{V}$ such that $b^*(f)(e_n) = v$. We shall refer to $\mathcal{A}_n^{\mathrm{dR}}(X)$ and $\mathcal{A}_n^{\mathrm{dR}}(Y)$ as *universal connections*. By Lemma A.1 and Lemma A.7, $A_n^{\mathrm{dR}}(X)(b, z)$ may equivalently be defined to be

$$A_n^{\mathrm{dR}}(X)(b) \times_{\pi_1^{\mathrm{dR}}(X,b)} \pi_1^{\mathrm{dR}}(X; b, z) \simeq A_n^{\mathrm{dR}}(X)(b) \times_{U_n(b)} P_n(b, z),$$

or to be $z^* \mathcal{A}_n^{\mathrm{dR}}(X)$, and similarly for $\mathcal{A}_n^{\mathrm{dR}}(Y), A_n^{\mathrm{dR}}(Y)(b, z)$. We denote by $I^k A_n^{\mathrm{dR}}(X)(b, z)$ the I-adic filtration on $A_n^{\mathrm{dR}}(X)(b, z)$, and similarly for $A_n^{\mathrm{dR}}(Y)(b, z)$.

In this paper we will only be interested in $U_n^{\mathrm{dR}}(b), P_n^{\mathrm{dR}}(b, z)$ and $A_n^{\mathrm{dR}}(b, z)$ in the cases $n = 1$ and 2. When $n = 1$ we have $U_1(b) \simeq V_{\mathrm{dR}}$ and an exact sequence

$$0 \to V_{\mathrm{dR}} \to A_1^{\mathrm{dR}}(b, z) \to K \to 0,$$

by Lemma A.8. When $n = 2$ we have exact sequences

$$\begin{aligned} &1 \to \overline{\wedge^2 V}_{\mathrm{dR}} \to U_2^{\mathrm{dR}} \to V_{\mathrm{dR}} \to 1, \\ &1 \to \wedge^2 V_{\mathrm{dR}}(Y) \to U_2^{\mathrm{dR}}(Y) \to V_{\mathrm{dR}}(Y) \to 1, \\ &0 \to \overline{V^{\otimes 2}}_{\mathrm{dR}} \to A_2^{\mathrm{dR}}(X)(b, z) \to A_1^{\mathrm{dR}}(X)(b, z) \to 0, \\ &0 \to V_{\mathrm{dR}}(Y)^{\otimes 2} \to A_2^{\mathrm{dR}}(Y)(b, z) \to A_1^{\mathrm{dR}}(Y)(b, z) \to 0, \end{aligned}$$

where $\overline{\wedge^2 V}_{\mathrm{dR}} := \mathrm{Coker}(H^2_{\mathrm{dR}}(X)^* \xrightarrow{\cup^*} \wedge^2 V_{\mathrm{dR}})$ and $\overline{V^{\otimes 2}}_{\mathrm{dR}} := \mathrm{Coker}(H^2_{\mathrm{dR}}(X)^* \xrightarrow{\cup^*} V_{\mathrm{dR}}^{\otimes 2})$. These exact sequences can be seen in various ways. They are a consequence of Lemma A.8 and Lemma A.10, since

$$\begin{aligned} &\mathrm{Ker}(H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X) \to \mathrm{Ext}^2_{\mathcal{C}^{\mathrm{dR}}(X)}(\mathbf{1}, \mathbf{1})) \\ \simeq &\mathrm{Ker}(H^1_{\mathrm{dR}}(X) \otimes H^1_{\mathrm{dR}}(X) \to H^2_{\mathrm{dR}}(X)). \end{aligned}$$

and similarly for Y. In words, the cup product of two classes in $H^1_{\mathrm{dR}}(X)$ is zero if and only if the Yoneda cup product of their corresponding extension classes in $\mathcal{C}^{\mathrm{dR}}(X)$; this can be checked at the level of cocycles, or by comparison with the corresponding statement for Betti cohomology or fundamental groups. The statements for U_2 can also be deduced from the Betti case, or from the result from A_2, using the fact that, for any 2-nilpotent Lie algebra L with enveloping algebra E, the inclusion $L \hookrightarrow E$ induces an isomorphism

$$L \simeq E/(I^3 + \mathrm{Sym}^2 L^{\mathrm{ab}}).$$

6.2 $A^{\mathbf{dR}}(b,z)$ and its relation to $A(b,z)$

Recall that the main goal of this section is to compute the generalised pre-height $\widetilde{h}_{\mathfrak{p}}(A(b,z))$, which amounts to describing the Frobenius action and Hodge filtration on $D_{\mathrm{cr}}(A(b,z))$. The vector spaces $A_n^{\mathrm{dR}}(b,z)$ have canonical Frobenius actions and Hodge filtration (described below), which are related to $A^{\mathrm{dR}}(b,z)$ by the following lemma (which is a special case of Olsson's theorem [46, Theorem 1.4]).

Lemma 6.1. For all primes $v|p$, the following hold.

1. The G_{K_v}-representation $A_n(b,z)$ is crystalline for all n and $b,z \in X(K_v)$, and
$$D_{\mathrm{cr}}(A_n(b,z)) = A_n^{\mathrm{dR}}(b,z). \tag{17}$$
2. The image of $j_{n,v}(X(K_v))$ in $H^1(G_{K_v}, U_n)$ lies in the subvariety $H^1_f(G_{K_v}, U_n)$ of crystalline torsors.
3. The extension $[IA_2(b)]$ in $\mathrm{Ext}^1_{G_{K_v}}(V,W)$ is crystalline.

□

Proof. As the statement of the lemma is slightly different from Olsson's theorem as stated in [46], we explain how to get from one to ther other. Let $\mathcal{O}(\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X};b,z))$ denote the coordinate ring of the $\mathbb{Q}_p$-unipotent étale torsor of paths from b to z. By [46, Theorem 1.11], this is an ind-crystalline representation (i.e. a direct limit of crystalline representations), and moreover there is an isomorphism of commutative algebras of ind-filtered ϕ-modules
$$D_{\mathrm{cr}}(\mathcal{O}(\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X};b,z))) \simeq \mathcal{O}(\pi_1^{\mathrm{dR}}(X;b,z)). \tag{18}$$
To prove that $A_n(b,z)$ is crystalline, it is enough to prove that $\varinjlim A_n(b,z)^*$ is ind-crystalline. This follows from Olsson's theorem via the Galois-equivariant isomorphism

$$\varinjlim A_n(b,z)^* \simeq \mathcal{O}(\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X};b,z)),$$

(see for example Hadian [29, 2.12] or Kim [34, §2]). This implies (1) and (3), since subquotients of crystalline representations are crystalline. The deduction of (2) from Olsson's work is explained in [34, §2]. ■

When $b = z$, the isomorphism (17) is an isomorphism of algebras (this follows from the statement that the isomorphism (18) is an isomorphism of Hopf algebras when $b = z$ [46, Theorem 1.8]), and hence on graded pieces is uniquely determined by the isomorphism

$$H^1_{\mathrm{dR}}(X_{\mathbb{Q}_p}) \simeq D_{\mathrm{cr}}(H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p)).$$

Since the associated gradeds of $A_n^{\mathrm{dR}}(b,z)$ are independent of z (i.e. are canonically isomorphic as z varies), and similarly for $A_n(b,z)$, from (17) we obtain a commutative diagram with exact rows whose vertical maps are isomorphisms

$$\begin{array}{ccccccccc}
0 & \longrightarrow & D_{\mathrm{cr}}(H^2_{\acute{e}t}(\overline{X},\mathbb{Q}_p)^*) & \xrightarrow{\cup^*} & D_{\mathrm{cr}}(V^{\otimes 2}) & \longrightarrow & D_{\mathrm{cr}}(A_2(b,z)) & \longrightarrow & D_{\mathrm{cr}}(A_1(b,z)) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^2_{\mathrm{dR}}(X_{K_{\mathfrak{p}}})^* & \xrightarrow{\cup^*} & V_{\mathrm{dR}}^{\otimes 2} & \longrightarrow & A_2^{\mathrm{dR}}(b,z) & \longrightarrow & A_1^{\mathrm{dR}}(b,z) & \longrightarrow & 0
\end{array}$$

Hence if we define $W_{\mathrm{dR}} := D_{\mathrm{dR}}(W)$, and

$$A^{\mathrm{dR}}(b,z) := A_2^{\mathrm{dR}}(b,z)/\operatorname{Ker}(\overline{V^{\otimes 2}}_{\mathrm{dR}} \to W_{\mathrm{dR}}),$$

then we obtain an isomorphism of filtered ϕ-modules $D_{\mathrm{cr}}(A(b,z)) \simeq A^{\mathrm{dR}}(b,z)$. When $b = z$, we have that $A^{\mathrm{dR}}(b,z)$ inherits the structure of an associative unital $\mathbb{Q}_p$-algebra from $A_2^{\mathrm{dR}}(b)$. Since the action of $\pi_1^{\mathrm{dR}}(X,b)$ on $I^2 A_n^{\mathrm{dR}}(b)$ is trivial, the kernel of

$$A_2^{\mathrm{dR}}(b) \to A^{\mathrm{dR}}(b)$$

is $\pi_1^{\mathrm{dR}}(X,b)$-stable, and hence there is a quotient

$$\mathcal{A}^{\mathrm{dR}} := \mathcal{A}_2^{\mathrm{dR}} / \operatorname{Ker}(\overline{V^{\otimes 2}}_{\mathrm{dR}} \to W_{\mathrm{dR}}) \otimes \mathcal{O}_X$$

in $\mathcal{C}^{\mathrm{dR}}(X)$, and a commutative diagram

$$\begin{array}{ccc} z^*\mathcal{A}_2^{\mathrm{dR}} & \xrightarrow{\simeq} & A_2^{\mathrm{dR}}(b,z) \\ \downarrow & & \downarrow \\ z^*\mathcal{A}^{\mathrm{dR}} & \xrightarrow{\simeq} & A^{\mathrm{dR}}(b,z) \end{array}$$

for all $z \in X(K)$. We similarly define

$$A^{\mathrm{dR}}(Y)(b,z) := A_2^{\mathrm{dR}}(Y)(b,z) / \operatorname{Ker}(V_{\mathrm{dR}}(Y)^{\otimes 2} \to W_{\mathrm{dR}})$$
$$\mathcal{A}^{\mathrm{dR}}(Y)(b,z) := \mathcal{A}_2^{\mathrm{dR}}(Y) / \operatorname{Ker}(V_{\mathrm{dR}}(Y)^{\otimes 2} \to W_{\mathrm{dR}}) \otimes \mathcal{O}_Y.$$

6.3 The Hodge filtration

In this section we recall Hadian's description of the Hodge filtration on $A_n^{\mathrm{dR}}(Y)(b,z)$ as the fibre at z of the Hodge filtration on the canonical extension of $\mathcal{A}_n^{\mathrm{dR}}(Y)$ to X.

Definition 6.2. By a filtered connection $\mathcal{V} = (\mathcal{V}, \nabla, F^\bullet)$ we shall mean a vector bundle $\mathcal{V}$ together with a connection ∇ and a decreasing, exhaustive, separated filtration $(F^i\mathcal{V})$ by sub-bundles, satisfying the *Griffiths transversality* condition

$$\nabla(F^i\mathcal{V}) \subset \Omega^1 \otimes F^{i-1}\mathcal{V}$$

for all i. We similarly define a filtered connection with log singularities. We sometimes write a filtered connection as $(\mathcal{V}, F^\bullet)$ and sometimes simply as $\mathcal{V}$. □

.

Definition 6.3. Given a unipotent connection $\mathcal{V}$ on Y, we shall denote by $\mathcal{V}^{\mathrm{can}}$ the canonical extension of $\mathcal{V}$ to a connection on X with log singularities along D, which exists and is functorial in $\mathcal{V}$ by Deligne [21, §II.5, Proposition 5.2] (although this construction is analytic, by GAGA it implies the corresponding algebraic result - alternatively see [2, I.4] for a purely algebraic proof). □

Proposition 6.1 (Hadian [29, Proposition 3.3])**.** *Let $\mathcal{E}$ and $\mathcal{F}$ be filtered connections on X with logarithmic singularities along D. Then the group of isomorphism classes of extensions of $\mathcal{E}$ by $\mathcal{F}$ (in the category of filtered connections on X with logarithmic singularities along D) is isomorphic to the first hypercohomology group of the complex*

$$F^0(\mathcal{E}^* \otimes \mathcal{F}) \xrightarrow{\nabla} \Omega^1 \otimes F^{-1}(\mathcal{E}^* \otimes \mathcal{F})$$

where ∇ denotes the associated connection on the internal Hom bundle $\mathcal{E}^* \otimes \mathcal{F}$. □

By computing these hypercohomology groups in the case $\mathcal{E} = \mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}$ and $\mathcal{F} = V_{\mathrm{dR}}(Y)^{\otimes n} \otimes \mathcal{O}_X$, Hadian proves the following lemma (note that in [29], $(X, Y, \mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}, V_{\mathrm{dR}}(Y))$ is written as $(C, X, \mathcal{P}_n^{\mathrm{dR}}, T_{\mathrm{dR}})$).

Lemma 6.4 (Hadian [29, Lemma 3.6])**.** There exists a filtration of $\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}$ by vector bundles $(F^i\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}})$ such that

1. For all n, the sequence of connections

$$0 \to \mathcal{O}_X \otimes V_{\mathrm{dR}}(Y)^{\otimes n} \to \mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}} \to \mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}} \to 0 \tag{19}$$

respects the filtrations, where $\mathcal{O}_X \otimes V_{\mathrm{dR}}(Y)^{\otimes n}$ is given the filtration induced by the Hodge filtration on $V_{\mathrm{dR}}(Y)^{\otimes n}$.

2. For all n, the filtration F^i satisfies Griffiths transversality, and hence gives $\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}$ the structure of a filtered connection for all n.
3. In the fibre at b, the unit element $e_n \in b^*\mathcal{A}_n^{\mathrm{dR}}(Y) \simeq A_n^{\mathrm{dR}}(Y)(b)$ lies in $b^*F^0\mathcal{A}_n^{\mathrm{dR}}(Y)$.

Moreover, a filtration F^i satisfying these properties is unique up to isomorphism of filtered connections. □

Remark 4. It is easy to see that the analogous theorem for the bundle $\mathcal{A}_n^{\mathrm{dR}}(Y)$ on Y is false: since every extension of vector bundles on Y admits a splitting, every unipotent vector bundle on Y is trivial. Hence there will be many ways to lift the Hodge filtration on the graded pieces and satisfy Griffiths transversality. Hence the content of computing the Hodge filtration on the $\mathcal{A}_n^{\mathrm{dR}}(Y)$ is contained in computing its canonical extension to X. □

Remark 5. There is a possible point of ambiguity in the statement of [29, Lemma 3.6]. It is not the case that there is a unique Hodge filtration on $\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}$ such that (19) is exact and Griffiths transversality (even for $\mathcal{A}_1^{\mathrm{dR}}(Y)^{\mathrm{can}}$). In loc. cit. the author proves uniqueness of the extension class of $\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}$ in the category of filtered connections, using injectivity of the map

$$\begin{aligned}&\mathrm{Ext}^1_{\mathrm{dR,fil}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, V_{\mathrm{dR}}(Y)^{\otimes n}\otimes\mathcal{O}_X)\\ \hookrightarrow\ &\mathrm{Ext}^1_{\mathrm{dR}}((\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, F^\bullet\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}), (V_{\mathrm{dR}}(Y)^{\otimes n}\otimes\mathcal{O}_X, F^\bullet V_{\mathrm{dR}}(Y)^{\otimes n}\otimes\mathcal{O}_X))\end{aligned}$$

To obtain uniqueness of the filtration itself, one must rigidify by imposing conditions on the filtration at the basepoint (this is already true when $n = 1$). Needless to say this distinction is not important in the context of Hadian's paper and does not affect the main results. □

The Hodge filtration on $A_n^{\mathrm{dR}}(Y)(b,z)$ is

$$F^iA_n^{\mathrm{dR}}(Y)(b,z) = z^*F^i\mathcal{A}_n^{\mathrm{dR}}(Y).$$

The Hodge filtration on $A_n^{\mathrm{dR}}(X)(b,z)$ is the filtration induced by the surjection $A_n^{\mathrm{dR}}(Y)(b,z) \to A_n^{\mathrm{dR}}(X)(b,z)$.

For our purposes, we will be interested in a mild generalisation of Lemma 6.4, where instead of considering $\mathcal{A}_n^{\mathrm{dR}}(Y)$, we consider sheaves coming from other quotients of the universal enveloping algebra. In the following corollary, we let W be any filtered quotient of $V_{\mathrm{dR}}(Y)^{\otimes n}$, and let $\mathcal{B}$ be the corresponding quotient of the connection $\mathcal{A}_n^{\mathrm{dR}}(Y)$. Hence the map $\mathcal{A}_n^{\mathrm{dR}}(Y) \to \mathcal{A}_{n-1}^{\mathrm{dR}}(Y)$ factors through $\mathcal{A}_n^{\mathrm{dR}}(Y) \to \mathcal{B}$, and $\mathcal{B}$ is an extension

$$0 \to W\otimes\mathcal{O}_Y \to \mathcal{B} \to \mathcal{A}_{n-1}^{\mathrm{dR}}(Y) \to 0.$$

Corollary 6.2. *There is a unique lift of the filtrations on $\mathcal{A}_{n-1}^{dR}(Y)^{\mathrm{can}}$ and $W\otimes\mathcal{O}_X$ to a filtered connection structure on $\mathcal{B}^{\mathrm{can}}$ such that in the fibre at b, 1 lies in $b^*F^0\mathcal{B}$.* □

Proof. The category of filtered K-vector spaces is semi-simple, so the quotient map $V_{\mathrm{dR}}^{\otimes n} \to W$ admits a filtered section, inducing an isomorphism $V_{\mathrm{dR}}(Y)^{\otimes n} \simeq W \oplus W'$. Hence

$$\mathrm{Ext}^1_{\mathrm{dR,fil}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, V_{\mathrm{dR}}(Y)^{\otimes n}\otimes\mathcal{O}_X) \simeq \mathrm{Ext}^1_{\mathrm{dR,fil}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, W\otimes\mathcal{O}_X) \oplus \mathrm{Ext}^1_{\mathrm{dR,fil}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, W'\otimes\mathcal{O}_X)$$

and

$$\mathrm{Ext}^1_{\mathrm{dR}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, V_{\mathrm{dR}}(Y)^{\otimes n}\otimes\mathcal{O}_X) \simeq \mathrm{Ext}^1_{\mathrm{dR}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, W\otimes\mathcal{O}_X) \oplus \mathrm{Ext}^1_{\mathrm{dR}}(\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}, W'\otimes\mathcal{O}_X).$$

Therefore uniqueness of the lift of the filtration on $\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}$ to $\mathcal{A}_n^{\mathrm{dR}}(Y)^{\mathrm{can}}$ given conditions on $b^*\mathcal{A}_n^{\mathrm{dR}}(Y)$ implies uniqueness of the lift of the filtration on $\mathcal{A}_{n-1}^{\mathrm{dR}}(Y)^{\mathrm{can}}$ to $\mathcal{B}^{\mathrm{can}}$ given conditions on $b^*\mathcal{B}$. ■

To compute the Hodge filtration on $\mathcal{A}_n^{\mathrm{dR}}(X)$ (i.e., to carry out the above for a projective curve), we may compute the Hodge filtration on the universal connection of an open affine Y, and then take the quotient to get the Hodge filtration on the universal connection on the projective curve X. This will be explained in more detail in the next section.

6.4 Universal pointed objects

Definition 6.5. For simplicity we assume that all the points of $X - Y$ are defined over K. Choose $\eta_0, \ldots, \eta_{2g+r-2} \in H^0(Y, \Omega^1)$ a set of differentials whose image in $H^1_{\mathrm{dR}}(Y)$ forms a basis. We will henceforth assume that this basis is chosen such that $\eta_0, \ldots, \eta_{g-1}$ is a basis of $H^0(X, \Omega^1)$, and $\eta_0, \ldots, \eta_{2g-1}$ form a basis of $H^1_{\mathrm{dR}}(X)$. Let $R = \oplus_{i\geq 0}V_{\mathrm{dR}}(Y)^{\otimes i}$ be the tensor algebra of $V_{\mathrm{dR}}(Y)$. Hence R may also be thought of as the free associative K algebra on $2g + r - 1$ generators $T_0, \ldots, T_{2g+r-2}$, where the T_i are the dual basis to the η_i.

Define R_n to be the quotient of R by the 2-sided ideal generated by $V_{\mathrm{dR}}(Y)^{\otimes(n+1)}$. Let $\mathcal{A}_n(Y) := R_n \otimes \mathcal{O}_Y$ be the corresponding trivial vector bundle, and define a connection ∇_n on $\mathcal{A}_n(Y)$:

$$\nabla : R_n \otimes \mathcal{O}_Y \to R_n \otimes \Omega^1_Y; w \otimes 1 \mapsto -\sum_{i=0}^{2g+r-2} T_i w \otimes \eta_i.$$

□

The following theorem of Kim says that $(\mathcal{A}_n(Y), 1)_n$ is a universal pointed pro-object in $(\mathcal{C}^{\mathrm{dR}}(Y), 1)$, and hence $(\mathcal{A}_n(Y), 1) \simeq (\mathcal{A}_n^{\mathrm{dR}}(Y), 1)$.

Theorem 6.3 (Kim [34, Lemma 3])**.** *For every n-unipotent pointed connection $(\mathcal{V}, v)$ there is a unique map $(\mathcal{A}_n(Y), 1) \mapsto (\mathcal{V}, v)$.* □

The isomorphism $\mathcal{A}_n^{\mathrm{dR}}(Y) \simeq \mathcal{A}_n(Y)$ gives a trivialisation

$$\mathcal{A}_n^{\mathrm{dR}}(Y) \simeq \oplus_{i=0}^n V_{\mathrm{dR}}(Y)^{\otimes i} \otimes \mathcal{O}_Y.$$

We shall refer to the bundle isomorphism $\mathcal{A}_n^{\mathrm{dR}}(Y) \simeq \oplus_{i=0}^n V_{\mathrm{dR}}(Y)^{\otimes i} \otimes \mathcal{O}_Y$, and the induced vector space isomorphism $A_n^{\mathrm{dR}}(Y)(b, z) \simeq \oplus_{i=0}^n V_{\mathrm{dR}}(Y)^{\otimes i}$ as the *affine trivialisation* of $\mathcal{A}_n$ (relative to the basis (η_i)).

6.5 Computation of the Hodge filtration

We now explain how to use this to algorithmically determine the Hodge filtration on the $\mathbb{Q}_p$-vector spaces $A^{\mathrm{dR}}(b, z)$. Unlike the computation of the Frobenius structure, this requires no particular ingenuity, as results of Kim and Hadian reduce the problem to elementary calculations in computational algebraic geometry.

Definition 6.6. Since W_{dR} is a quotient of $\wedge^2 V_{\mathrm{dR}}$, we have a surjection

$$\tau : V_{\mathrm{dR}}(Y) \otimes V_{\mathrm{dR}}(Y) \to W_{\mathrm{dR}}.$$

Let $S_1, \ldots, S_d$ be a basis of W_{dR}, and define $\tau_{ijk}, 0 \leq i, j \leq 2g + r - 2, 1 \leq k \leq d$, by

$$\tau(T_i \otimes T_j) = \sum_{k=1}^d \tau_{ijk} S_k.$$

By definition this map factors through $V_{\mathrm{dR}} \otimes V_{\mathrm{dR}}$, and hence by our choice of basis differentials, τ_{ijk} is zero whenever i or j are greater than $2g - 1$. Note that the condition that the map factors through $\overline{\wedge^2 V}_{\mathrm{dR}}$ is equivalent to the equations

$$\begin{aligned} \tau_{ijk} + \tau_{jik} &= 0, & 0 \leq i, j \leq 2g-1, 1 \leq k \leq d. \\ \sum_{0 \leq i < j \leq 2g-1} [\eta_i] \cup [\eta_j] \tau_{ijk} &= 0, & 1 \leq k \leq d. \end{aligned} \tag{20}$$

□

By Theorem 6.3, the connection on $\mathcal{A}^{\mathrm{dR}}(Y)$ is given as follows:

$$1 \mapsto -\sum_{i=0}^{2g+r-2} \eta_i \otimes T_i, \qquad T_i \mapsto +\sum_{j=0}^{2g+r-2} \sum_{k=1}^d \tau_{ijk} \eta_j \otimes S_k, \qquad S_k \mapsto 0.$$

The Hodge filtration on $\mathcal{A}^{\mathrm{dR}}(X)$ is computed in two stages:

1. Compute the maximal quotient $\mathcal{A}^{\mathrm{dR}}(X)|_Y$ of $\mathcal{A}^{\mathrm{dR}}(Y)$ whose canonical extension to X defines a connection without singularities.
2. Compute the Hodge filtration on $\mathcal{A}^{\mathrm{dR}}(X)$.

6.5.1 *Computing* $\mathcal{A}^{dR}(X)$

Lemma 6.7. The connection $\mathcal{A}^{\mathrm{dR}}(X)|_Y$ is the maximal quotient of $\mathcal{A}^{\mathrm{dR}}(Y)$ which extends to a connection on X without log singularities. □

Proof. By definition $\mathcal{A}^{\mathrm{dR}}(X)|_Y$ extends to X. By Tannaka duality, the claim is equivalent to the saying that $A^{\mathrm{dR}}(b)$ is the maximal quotient of $A^{\mathrm{dR}}(Y)(b)$ for which the action of $\pi_1^{\mathrm{dR}}(Y,b)$ factors through $\pi_1^{\mathrm{dR}}(X,b)$. Passing to enveloping algebras, this is equivalent to the action of $A_2^{\mathrm{dR}}(Y)(b)$ factoring through $A_2^{\mathrm{dR}}(X)(b)$, which implies the lemma. ■

We deduce that $\mathcal{A}^{\mathrm{dR}}(X)|_Y$ is the unique quotient of $\mathcal{A}^{\mathrm{dR}}(Y)$ which extends to a connection on the whole of X without log singularities and fits in a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_{\mathrm{dR}} \otimes \mathcal{O}_Y & \longrightarrow & \mathcal{A}^{\mathrm{dR}}(Y) & \longrightarrow & \mathcal{A}_1^{\mathrm{dR}}(Y) & \longrightarrow & 0 \\ & & \downarrow = & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & W_{\mathrm{dR}} \otimes \mathcal{O}_Y & \longrightarrow & \mathcal{A}^{\mathrm{dR}}(X)|_Y & \longrightarrow & \mathcal{A}_1^{\mathrm{dR}}(X)|_Y & \longrightarrow & 0. \end{array}$$

Let $C(Y/X) \subset \langle \eta_0, \ldots, \eta_{2g+r-1} \rangle$ be the subspace of $H^0(Y, \Omega)$ spanned by the differentials $\eta_{2g}, \ldots, \eta_{2g+r-2}$. We will show that there are unique $\xi_1, \ldots, \xi_d$ in $C(Y/X)$ such that

$$1 \mapsto -\sum_{i=0}^{2g-1} \eta_i T_i - \sum_{k=1}^{d} \xi_k S_k, \qquad T_i \mapsto + \sum_{0 \le j \le 2g-1, 1 \le k \le d} \tau_{ijk} \eta_j \otimes S_k, \qquad S_i \mapsto 0 \tag{21}$$

defines a connection on X, and give an algorithm for finding them. We solve for the ξ_k by computing the canonical extension for a general choice of ξ_k, and working out the condition for this extension to have no singularities.

For each $x \in D(K)$, let $t_x \in K(X)$ be a parameter at x. Let U_x be a Zariski neighbourhood of x such that t_x has no poles on U_x and $U_x \cap D = x$. To compute the canonical extension of $\mathcal{A}^{\mathrm{dR}}(Y)$, one has to find, for each $x \in (X - Y)(K)$, connections $(\mathcal{A}_x, \nabla_x)$ on U_x, with log singularities along x, and charts (i.2. isomorphisms of connections)

$$\psi_x : \mathcal{A}_x|_{U_x \cap Y} \xrightarrow{\simeq} \mathcal{A}^{\mathrm{dR}}(Y)|_{U_x \cap Y}.$$

Let S be the section of

$$K(\!(t)\!) \to K(\!(t)\!)/t^{-1}K[\![t]\!]$$

defined by sending the equivalence class of $\sum_i a_i t^i$ to $\sum_{i \le -2} a_i t^i$. Let I be the formal integration function

$$I : \oplus_{i<-1} K.t^i \to \oplus_{i<0} K.t^i; \qquad \sum a_i t^i \mapsto \sum \tfrac{a_i}{i+1} t^{i+1}.$$

For a global function $f \in K(X)$ or differential $\omega \in \Omega^1_{K(X)|K}$, let $\mathrm{loc}_x(f)$ or $\mathrm{loc}_x(\omega)$ denote its image in $K(\!(t_x)\!)$ or $K(\!(t_x)\!)dt_x$ respectively.

Lemma 6.8. Let $f_{i,x}, g_{k,x}$ and $h_{ik,x}$ be elements of $K(\!(t_x)\!)$ satisfying

$$f_{i,x} = I \circ S(\mathrm{loc}_x(\eta_i)),\ h_{ik,x} = \sum_{0 \le j \le 2g-1} \tau_{ijk} f_{j,x}.$$

$$g_{k,x} = -I \circ S\left(\sum_i (df_{i,x} - \mathrm{loc}_x(\eta_i)) h_{ik,x} - \sum_{0 \le j \le 2g-1} \tau_{ijk} f_{i,x} \mathrm{loc}_x(\eta_j) - \mathrm{loc}_x(\xi_k) \right).$$

Let $\mathcal{A}_x$ be a trivial bundle on $K[\![t_x]\!]$ with sections $1_x, T_{i,x} (0 \le i \le 2g+r-2), S_{k,x} (1 \le k \le d)$, and let ψ_x be the isomorphism

$$\psi_x : \mathcal{A}_x|_{U_x \cap Y} \xrightarrow{\simeq} \mathcal{A}^{\mathrm{dR}}(Y)|_{U_x \cap Y}.$$

given by

$$1_x \mapsto 1 + \sum_{i=0}^{2g+r-2} f_{i,x} T_i + \sum_{k=1}^{d} g_{k,x} S_k, \qquad T_{i,x} \mapsto T_i + \sum_{k=1}^{d} h_{ik,x} S_k, \qquad S_{k,x} \mapsto S_k; \tag{22}$$

Then there are unique connections ∇_x with log singularities on $(\mathcal{A}_x)_x$ such that $(\psi_x)_x$ form charts extending $\mathcal{A}^{\mathrm{dR}}(Y)$ to a connection with logarithmic singularities on $X - Y$. □

Proof. The connection ∇_x is unique if it is exists. Since ψ_x is an isomorphism of connections we deduce that the connection ∇_x must be given by

$$1_x \mapsto -\sum_{i=0}^{2g+r-2}(\eta_i - df_{i,x})T_{i,x} + \sum_{k=1}^{d}\left(dg_{k,x} - \sum_{i=0}^{2g+r-2}(df_{i,x}-\eta_i)h_{ik,x} - \sum_{j=0}^{2g+r-2}\tau_{ijk}f_{i,x}\eta_j\right)\otimes S_{k,x}$$

$$T_{i,x} \mapsto \sum_{k=1}^{d}\left(dh_{ik,x} + \sum_{j=0}^{2g+r-2}\tau_{ijk}\omega_j\right)S_{k,x}, \qquad S_{k,x}\mapsto 0.$$

It follows from the formulas for $f_{i,x}, g_{k,x}$ and $h_{ik,x}$ that this connection on $K(\!(t_x)\!)$ has poles of order at most one. ∎

In particular, this lemma implies that to compute $f_{i,x}, g_{k,x}$ and $h_{ik,x}$, it is enough to compute the t_x-adic expansion of the ω_i to sufficient accuracy.

Having determined the connection $(\mathcal{A}^{\mathrm{dR}}(Y)^{\mathrm{can}}, \nabla)$, we now determine the quotient connection without log singularities $(\mathcal{A}^{\mathrm{dR}}(X), d+\Lambda)$. Since we are looking for a quotient of $\mathcal{A}^{\mathrm{dR}}(Y)^{\mathrm{can}}$ of the form (21), the condition that $d+\Lambda$ extends to a connection without log singularities is exactly the condition that one can choose ξ_k such that, for all x,

$$\mathrm{Res}\left(\sum_{i=0}^{2g-1}(df_{i,x} - \mathrm{loc}_x(\eta_i)h_{ik,x} - \sum_{j=0}^{2g-1}\tau_{ijk}f_{i,x}\,\mathrm{loc}_x(\eta_j) - \mathrm{loc}_x(\xi_k)\right) = 0.$$

By the exact sequence

$$0 \to C(Y/X) \xrightarrow{\oplus_x \mathrm{Res}_x} \oplus_{x\in(X-Y)(K)}K \xrightarrow{\sum} K \to 0,$$

such ξ_k exist if and only if

$$\sum_{x\in D(K)}\mathrm{Res}\left(\sum_{i=0}^{2g-1}(df_{i,x} - \mathrm{loc}_x(\eta_i))h_{ik,x} + \sum_{j=0}^{2g-1}\tau_{ijk}f_{i,x}\,\mathrm{loc}_x(\eta_j)\right) = 0.$$

Since $\sum_{x\in D(K)}\mathrm{Res}_x(f_{i,x}\,\mathrm{loc}_x(\eta_j)) = [\eta_i]\cup[\eta_j]$ by Serre's cup product formula, we can solve for ξ_k by (20). Explicitly, the residue of ξ_k is equal to the residue of

$$dg_{k,x} - \sum_{i=0}^{2g-1}(df_{i,x}-\eta_i)h_{ik,x} - \sum_{j=0}^{2g-1}\tau_{ijk}f_{j,x}\eta_k. \tag{23}$$

By inspection, in order to compute these functions in practice, one simply needs to determine constants $\beta(i,j,x)\in K$ $(0\le i\le 2g+r-1, -m\le m)$ having the property that

$$\mathrm{loc}_x(\eta_i) - \sum_{j=-m}^{m-1}\beta(i,j,x)t_x^i dt_x \in t_x^m K[t_x]dt_x,$$

where m is the maximum over all i and x of the order of the pole of η_i at x.

6.5.2 *Computing the Hodge filtration*

To explain how to compute the Hodge filtration, we recall some elementary properties of differentials on curves.

Lemma 6.9. Suppose there is a function $g\in H^0(Y,\mathcal{O}_Y)$ and constants μ_i, $g\le i<2g$, such that for all $x\in D(K)$, the function $g-\sum\mu_i f_{i,x}$ has no pole at x. Then g is constant and all the μ_i are zero. □

Proof. For g and μ_i as in the lemma, we have that $dg-\sum_{i=g}^{2g-1}\mu_i\eta_i$ has no poles (recall $df_{i,x}=\eta_i$). Hence $dg-\sum_{i=0}^{g-1}\mu_i\eta_i$ defines an element of $H^0(X,\Omega^1)$. Since $[\eta_0],\ldots,[\eta_{2g-1}]$ is a basis of $H^1_{\mathrm{dR}}(X)$, the lemma follows. ∎

It follows that given any tuple $(w_x)_{x\in D(K)}\in\prod_{x\in D(K)}K(\!(t_x)\!)$, there is a unique choice of $g\in H^0(Y,\mathcal{O})$ and $\mu_i\in K$ $(g\le i<2g)$ such that $g(b)=0$ and for all x in $D(K)$, $w_x-\mathrm{loc}_x(g)-\sum_{i=g}^{2g-1}\mu_i f_{i,x}$ does not have a pole at x.

Definition 6.10. As above, let r denote the degree of D over K, and let m denote the maximum over all $x \in D(K)$ and $0 \leq i < 2g$ of the order of the pole of η_i at x. Denote by Π the rm-dimensional K-vector space

$$\prod_x t_x^{-m} K[t_x]dt_x / K[t_x]dt_x.$$

Define functions $r : \Pi \to H^0(Y, \mathcal{O})$ and $\underline{c} = (c_0, \dots c_{2g+r-1}) : \Pi \to K^{\oplus(2g+r)}$ by the property that for all π in Π,

$$\pi \equiv \mathrm{loc}_x(r(\pi)) + \sum c_i(\pi)\,\mathrm{loc}_x(\omega_i) \mod \prod t_x^{-1} K[t_x^{-1}] \tag{24}$$

and $r(\pi)(b) = 0$. □

By Lemma 6.4, $F^0\mathcal{A}^{\mathrm{dR}}$ is uniquely determined by the following properties:

- There is a commutative diagram of bundles

$$\begin{array}{ccccc} F^0\mathcal{I}^2\mathcal{A}^{\mathrm{dR}}(X) & \hookrightarrow & F^0\mathcal{I}\mathcal{A}^{\mathrm{dR}}(X) & \hookrightarrow & F^0\mathcal{A}^{\mathrm{dR}}(X) \\ \downarrow & & \downarrow & & \downarrow \\ W_{\mathrm{dR}} \otimes \mathcal{O}_X & \hookrightarrow & \mathcal{I}\mathcal{A}^{\mathrm{dR}}(X) & \hookrightarrow & \mathcal{A}^{\mathrm{dR}}(X) \end{array}$$

  where $\mathcal{I}\mathcal{A}^{\mathrm{dR}}(X)$ is the kernel of the surjective map of connections

$$\mathcal{A}^{\mathrm{dR}}(X) \to (\mathcal{O}_X, d).$$

  Passing to the associated map of gradeds defines an isomorphism

$$\mathrm{gr}\, F^0\mathcal{A}^{\mathrm{dR}} \simeq \mathcal{O}_X \oplus F^0 V_{\mathrm{dR}} \otimes \mathcal{O}_X \oplus F^0 W_{\mathrm{dR}} \otimes \mathcal{O}_X.$$

- In the fibre at b, $1 \in A_{\mathrm{dR}}(b)$ is in the image of $b^* F^0\mathcal{A}^{\mathrm{dR}}$.

An elementary calculation shows us that $H^0(Y, F^0\mathcal{A}_1^{\mathrm{dR}}(X))$ has basis of sections $1, T_g, \dots, T_{2g-1}$. To compute $F^0\mathcal{A}^{\mathrm{dR}}$, we need to lift these to determine the bundle $F^0\mathcal{A}^{\mathrm{dR}}$. Suppose they lift to sections $1 + \sum_{k=1}^d r_k^H \otimes S_k$ and $T_i + \sum_{k=1}^d c_{ik}^H \otimes S_k$. Then by the above computation of the charts defining the bundle $\mathcal{A}^{\mathrm{dR}}$, we find

Lemma 6.11. The functions r_k^H are given by $r_k^H = r((g_{k,x})_x)$. The functions c_{ik}^H are constant and are given by $c_{ik}^H = c_i((g_{k,x})_x)$. □

Proof. We need to check that the sub-bundle of $\mathcal{A}^{\mathrm{dR}}|_Y$ spanned by $1 + \sum_{k=1}^d r_k^H S_k$, $T_i + \sum_{k=1}^d c_{ik}^H S_k$ $(g \leq i < 2g)$, and S_k $(d_0 \leq k \leq d)$ extends to a sub-bundle of $\mathcal{A}^{\mathrm{dR}}$. Via the charts ψ_x, the corresponding sections of $\mathcal{A}_x^{\mathrm{dR}}|_{U_x - x}$ are given by

$$\begin{aligned} \psi_x^{-1}(1 + \sum_{k=1}^d r_k^H S_k) &= 1_x - \sum_{i=g}^{2g-1} f_{i,x} T_{i,x} + \sum_{k=1}^d (r_k^H - g_{k,x}) S_{k,x}, \\ \psi_x^{-1}(T_i + \sum_{k=1}^d c_{ik}^H S_k) &= X_{i,x} + \sum_{k=1}^d (c_{ik}^H - \sum_{j=0}^{2g-1} \tau_{ijk} f_{j,x}) S_{k,x}, \\ \psi_x^{-1}(S_k) &= S_{k,x}. \end{aligned}$$

For this $\mathcal{O}(U_x - x)$-module to be the localisation of an $\mathcal{O}(U_x)$-module, it is sufficient that there are functions $\theta_{i,x} (g \leq i < 2g)$ and $\chi_{k,x}$ $(1 \leq k \leq d)$ in $H^0(U_x - x, \mathcal{O})$ such that

$$\psi_x^{-1}(1 + \sum_{k=1}^d r_k^H S_k) + \sum_{i=0}^{2g-1} \theta_{i,x}(T_i + \sum_{k=1}^d c_{ik}^H S_k) + \sum_{k=1}^d \chi_{k,x} \phi_x^{-1} S_k \in H^0(U_x, \mathcal{A}^{\mathrm{dR}}(X)).$$

By examining T_i-coordinates, we find that $\theta_{i,x} \equiv f_{i,x} \mod H^0(U_x, \mathcal{O})$. For $k > d_0$ we take $\theta_k = g_{k,x}$. Hence the only non-trivial condition on the r_k^H and c_{ik}^H is that for $d - d_0 \leq k \leq d_0$,

$$g_{k,x} - \sum_{i=0}^{2g-1} c_{ik}^H f_{i,x} - r_k^H \in H^0(U_x, \mathcal{O}),$$

for all x, which hold by definition of the functions r and $\underline{c}$. ■

6.6 The universal connection of a hyperelliptic curve

In this subsection we use the hyperelliptic splitting to provide a simple description of the Hodge filtration on $A^{\mathrm{dR}}(b,z)$ when X is hyperelliptic. In general, given an automorphism σ of X, fixing the point b, by the universal property of $\mathcal{A}_n^{\mathrm{dR}}$, we obtain a unique morphism $\mathcal{A}_n^{\mathrm{dR}} \to \sigma^*\mathcal{A}_n^{\mathrm{dR}}$ sending 1 to σ^*1. The connection $\sigma^*\mathcal{A}_n^{\mathrm{dR}}$ is in a natural way isomorphic to $\mathcal{A}_n^{\mathrm{dR}}$. If $\sigma(Y) = Y$, then it will also be the case that $\sigma^*\mathcal{A}_n^{\mathrm{dR}}(Y)$ is isomorphic to $\mathcal{A}_n^{\mathrm{dR}}(Y)$. In this case the connection structure on $\sigma^*\mathcal{A}_n^{\mathrm{dR}}$ is given by

$$v \otimes 1 \mapsto -\sum_{i=0}^{2g+r-2} T_i v \otimes \sigma^*\omega_i.$$

Restricting to the fibre at b, we obtain an automorphism of the algebra $A_n^{\mathrm{dR}}(Y)(b)$. For example, suppose $X/\mathbb{Q}$ is hyperelliptic, given by

$$y^2 = f(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0,$$

$Y = X - \{\infty^{\pm}\}$, and $\omega_i = x^i dx/2y$. Then pulling back by the hyperelliptic involution w sends $\mathcal{A}_n^{\mathrm{dR}}(Y)$ to the connection $v \otimes 1 \mapsto \sum_{i=0}^{2g+r-2} T_i v \otimes \omega_i$. Hence we deduce that with respect to this affine trivialisation, at any Weierstrass point b, the automorphism on the algebra $A_n^{\mathrm{dR}}(Y)(b)$ induced by w is simply given by $T_i \mapsto -T_i$.

Definition 6.12. For an effective divisor D on X whose support has points $z_1, \ldots, z_n$ in an algebraic closure, we let $D[1]$ denote the divisor $D + \sum_{i=1}^n z_i$. □

Lemma 6.13. We have the following:

1. The constants c_{ik}^H are independent of basepoint.
2. Suppose X is hyperelliptic, with defining equation as above, and the η_i are taken to be a K-linear combination of the basis differentials $\omega_i = x^i dx/2y$. Then $c_{ik}^H(x)$ is zero for all i and k, and $\xi_k = 0$ for all $1 \leq k \leq d$.
3. Suppose $\eta_0, \ldots, \eta_{2g-1}$ are differentials in $H^0(X, \Omega(D))$, for some effective divisor D, and $\eta_0, \ldots, \eta_{g-1}$ are a basis of $H^0(X, \Omega)$. Then we have that for all $k < 2g-1$, $r_k^H \in H^0(X, D[1])$.

□

Proof. For part (1), we use the characterisation of c_{ik} from Lemma 6.11. By (24), changing the basepoint b changes r by a constant, but does not alter the $r_i(\pi)$.
For part (2), it suffices to prove this after a finite extension of the base field, and by part (1) we may assume that b is taken to be Weierstrass. As we did in the étale setting, we observe that w then induces an automorphism of the bundle $\mathcal{A}|_Y$. With respect to the affine trivialisation of $\mathcal{A}$ at b, w acts as -1 on the V_{dR} component, and acts as 1 on the W_{dR} component. By functoriality, the involution must respect w, and hence we conclude all the r_{ik}^H must be zero. Similarly, by the explicit description of ξ_k given in equation (23), we see that the residue of ξ_k is equal to the residue of a sum of differentials which are even with respect to the hyperelliptic involution, and hence zero. For part (3), this follows from the defining property (see (24)) of the function c used to define the c_{ik}^H. ■

We now explain how to carry out some of these calculations for a hyperelliptic curve. We consider X/K given by $y^2 = f(x) = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0$, and let $Y = X - \{\infty^{\pm}\}$ and $\omega_i = x^i dx/2y$. The set $\{\omega_0, \ldots, \omega_{2g}\}$ forms a basis of $H^1_{\mathrm{dR}}(Y)$, and the set $\{\omega_0, \ldots, \omega_{g-1}\}$ forms a basis of $H^0(X, \Omega^1)$. In general $\omega_0, \ldots, \omega_{2g-1}$ will not form a basis of $H^1_{\mathrm{dR}}(X)$, so we take $\eta_0, \ldots, \eta_{2g}$ in the K-span of $\omega_0, \ldots, \omega_{2g}$ forming a basis of $H^1_{\mathrm{dR}}(Y)$ such that $\eta_0, \ldots, \eta_{g-1}$ form a basis of $H^0(X, \Omega^1)$ and $\eta_0, \ldots, \eta_{2g-1}$ form a basis of $H^1_{\mathrm{dR}}(X)$. Let W_{dR} be any filtered quotient of $\overline{\wedge^2 V_{\mathrm{dR}}}$. By truncating the power series expansion of $x^{2g+2}\sqrt{f(x^{-1})}$, we find polynomials $f_{i,\infty^{\pm}}$ in $uK[u]$ such that

$$\omega_i - df_i \in u^{-1}K[u]du.$$

Similarly we find the functions $g_{i,\infty^{\pm}}$ and $h_{i,\infty^{\pm}}$.

In the notation of the previous section, $r = 2$, $m = g$, and for $x = \infty^{\pm}$, we may take the uniformiser t_x to be $u := x^{-1}$. The function

$$(c, r) : (u^{-g}K[u]/K[u]) \times (u^{-g}K[u]/K[u]) \to H^0(X, \mathcal{O}(g\infty)) \times K^g$$

is given as follows: let $s(x) = \sum_{i=1}^g s_i u^{-i}$ be a representative of an element of $u^{-g}K[u]/K[u]$. For any polynomial $s(x)$, we have $c(s(x), s(x)) = s(x)$ and $r(s(x)) = 0$. Define $B = (B_{ij})$ by $\mathrm{loc}_{\infty^+}(\omega_{i+g}) - \sum B_{ij}u^j du \in K[u]du$. Then $(c(s(x), -s(x)) = 0$ and $\underline{r}(s(x), -s(x)) = B^{-1}(\underline{s})$, where $\underline{s} := (s_1, \ldots, s_g)$.

6.7 Frobenius structure on the universal connection of a hyperelliptic curve

In order to complete the description of the filtered ϕ-module structure, we need to describe the Frobenius action on the fibres $A^{\mathrm{dR}}(b,z)$ of the connection $\mathcal{A}^{\mathrm{dR}}$. Although it will not be needed in this paper, for completeness we briefly outline how this computation might be carried out for a general curve.

Let $X_{\mathbb{F}_p}$ be the special fibre of a smooth model of X over $\mathbb{Z}_p$, and let ϕ be an overconvergent lift of the absolute Frobenius morphism to some wide open subspace in the rigid analytification of $X_{\mathbb{Q}_p}$. The analytifications of the pointed connections $(\mathcal{A}_n, 1)$ may be viewed as universal pointed objects $(\mathcal{A}_n^\dagger, 1)$ in the category of unipotent isocrystals on $X_{\mathbb{F}_p}$. The action of Frobenius on the category of unipotent isocrystals induces a Frobenius structure on $\mathcal{A}_n^\dagger$, and one may reduce the problem of computing the action of Frobenius on $A^{\mathrm{dR}}(b,z)$ to that of computing this Frobenius structure.

For a hyperelliptic curve, we use the hyperelliptic splitting principle to determine the filtered ϕ-module $A^{\mathrm{dR}}(b,z)$ when $b=z$ is a Weierstrass point. This gives a characterisation of the ϕ-module structure of $A^{\mathrm{dR}}(b,z)$ for general b and z in terms of Coleman integrals.

Lemma 6.14. 1. Let X be a hyperelliptic curve, and η_i as in Section 6.6. With respect to the affine trivialisation, the unipotent ϕ-equivariant isomorphism

$$\mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}} \xrightarrow{\simeq} A^{\mathrm{dR}}(b,z)$$

is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ \sum_{i=0}^{2g-1} T_i \int_b^z \eta_i & 1 & 0 \\ \sum_{1\le k\le d}\left(\sum_{0\le i,j\le 2g-1}\tau_{ijk}\int_b^z \eta_i\eta_j\right) S_k & \sum_{0\le i,j\le 2g-1,1\le k\le d} -\tau_{ijk} T_i^*\otimes S_k \int_{w(b)}^z \eta_j & 1 \end{pmatrix},$$

modulo $F^0\operatorname{Hom}(V_{\mathrm{dR}}, W_{\mathrm{dR}})$.

2. For general smooth projective X, there are constants c_{ik}^{ϕ}, independent of z, such that the ϕ-equivariant isomorphism is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ \sum_{i=0}^{2g-1} T_i \int_b^z \eta_i & 1 & 0 \\ \sum_{1\le k\le d}\left(\int_b^z \xi_k + \sum_{0\le i,j\le 2g-1}\tau_{ijk}\int_b^z \eta_i\eta_j\right) S_k & \sum_{0\le i<2g,1\le k\le d}(c_{ik}^{\phi} - \sum_{0\le j<2g}\tau_{ijk}\int_b^z \eta_j) T_i^*\otimes S_k & 1 \end{pmatrix}.$$

□

Proof. We compute the isomorphism as the composite of ϕ-equivariant isomorphisms

$$\mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}} \xrightarrow{\simeq} A^{\mathrm{dR}}(b) \xrightarrow{\simeq} A^{\mathrm{dR}}(b,z).$$

We compute the latter isomorphism first. By definition, such an isomorphism is given by iterated Coleman integrals, as in [10, Corollary 3.3]. More precisely, for all z_1, z_2, z_3 in $Y(\mathbb{Q}_p)$, the unipotent ϕ-equivariant isomorphism

$$A^{\mathrm{dR}}(z_1,z_2) \xrightarrow{\simeq} A^{\mathrm{dR}}(z_1,z_3)$$

is given by

$$\begin{aligned} 1 &\mapsto 1 + \sum_{i=0}^{2g-1}\int_{z_2}^{z_3}\eta_i\otimes T_i + \sum_{k=1}^{d}\Big(\int_{z_2}^{z_3}\xi_k + \sum_{0\le i<j\le 2g-1}\tau_{ijk}\int_{z_2}^{z_3}(\eta_i\eta_j - \eta_j\eta_i)\Big)S_k \\ T_i &\mapsto T_i - \sum_{0\le j\le 2g+r-2,1\le k\le d}\tau_{ijk}\int_{z_2}^{z_3}\eta_j\otimes S_k, \\ S_k &\mapsto S_k. \end{aligned}$$

This proves part (2). For part (1), we compute the other isomorphism. By Lemmas 3.6 and 3.7, we know that, modulo $F^0\operatorname{Hom}(V_{\mathrm{dR}}, W_{\mathrm{dR}})$, the ϕ-equivariant splitting is given by $T_i - \mapsto \sum_{j,k}\tau_{ijk}\int_{2b-D}\eta_j\otimes S_k$. Again, by the definition of Coleman integration we have

$$t(A_1^{\mathrm{dR}}(b,z), IA^{\mathrm{dR}}(b,z)) = \sum_{0\le i<g}\int_b^z \eta_i T_i - \sum\tau_{ijk}\left(\int_b^z\eta_i\right)\left(\int_{z+b-D}\eta_j\right)\otimes S_k$$

and for $i<g$, we have $\int_{w(b)}^z\eta_i = \int_b^z\eta_i + \int_{2b-D}\eta_i$. ■

Lemma 6.15. 1. Let X be a hyperelliptic curve, and η_i a basis of $H^1_{\mathrm{dR}}(Y)$ as in Section 6.6. Then the generalised pre-height of $A(b,z)$ is given by

$$\widetilde{h}_{\mathfrak{p}}(A(b,z)) = \sum_k \left(-r_k^H(z) + \sum_{0\leq i<j<2g} \tau_{ijk} \int_b^z (\eta_i\eta_j - \eta_j\eta_i) - \int_b^z \eta_i \int_{w(b)}^b \eta_j - \int_b^z \eta_j \int_{w(b)}^b \eta_i \right) S_k$$

2. Let X be a general smooth projective curve, $Y \subset X$ and (η_i) be as in Section 6.5 and ξ as in Section 6.5. Then

$$\widetilde{h}_{\mathfrak{p}}(A(b,z)) = \sum_k \left(-r_k^H(z) + \int_b^z \xi_k - \sum_{0\leq i<g} c_{ik}^{\phi} \int_b^z \eta_i + \sum_{0\leq i<j<2g} \int_b^z (\eta_i\eta_j - \eta_j\eta_i) - \sum_{g\leq i<2g} c_{ik}^H \int_b^z \eta_i \right) S_k.$$

□

Proof. Recall that Lemma 3.9 gives an explicit formula for the p-adic height of a mixed extension given a representative for its class in $F^0\backslash U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$. Recall from (11) that such a representative is given by $(s^H)^{-1} \circ s^{\phi}$, where s^{ϕ} and s^H are isomorphisms $\mathbb{Q}_p \oplus V_{\mathrm{dR}} \oplus W_{\mathrm{dR}}$ which commute with the Hodge filtration and Frobenius action respectively. Hence the result follows from Lemma 6.14 and from the definition of r_k^H and c_{ik}^H. ■

A corollary of Lemmas 6.13 and 6.15 is the following explicit general formula. Let $\eta_0, \ldots, \eta_{2g-1}$ be differentials of the second kind in $H^0(X, \Omega^1(D))$ for some effective divisor D. Let $|D|_{\mathbb{F}_p}$ denote the reduction mod p of the support of D, and let $\mathcal{W} \subset X_{\mathbb{Q}_p}$ denote the tube of p-adic points which are not congruent to $|D|$ mod p.

Proposition 6.4. *Suppose $m := \rho_f(J) - 1 > r - g$. Then there exist constants $a_{ijk}, b_{ijk}, c_{ijk}, b_{ik}, c_{ik}$, rational functions $s_k \in H^0(X, \mathcal{O}(D[1]))$, and differentials of the third kind ξ_k, such that*

$$X(\mathbb{Q}_p)_U \cap \mathcal{W} \subset \{z \in \mathcal{W} : R_{T_1,\ldots,T_{r-g}}(F_1, \ldots, F_m) = 0\},$$

$$F_k(T_1, \ldots, T_m, z) = \sum_{1\leq i,j\leq r-g} a_{ijk} T_i T_j + \sum_{1\leq i\leq r-g, 0\leq j<g} b_{ijk} T_i \int_b^z \eta_k + \sum_{1\leq i\leq r-g} b_{ik} T_i + \sum_{0\leq i,j<2g} c_{ijk} \int_b^z \eta_i\eta_j + \sum_{0\leq i<2g} c_{ik} \int_b^z \eta_i + \int_b^z \xi_k + s_k.$$

□

Proof. By Proposition 4.1, the set $X(\mathbb{Q}_p)_2$ is contained in the intersection of the zeroes of F_k. Using the identity $\int(\omega_i\omega_j + \omega_j\omega_i) = \int \omega_i \int \omega_j$, we can write the formula for the generalised pre-height as $\sum c_{ij} \int_b^z \omega_i\omega_j + \sum c_i \int_b^z \omega_i + \int_b^z \eta + s$. ■

7 Computing $X(K_{\mathfrak{p}})_U$

7.1 Theorem 1.2, general case

We now return to the setting of Section 5.2. Let X be a curve of the form

$$y^2 = x^6 + ax^4 + ax^2 + 1$$

with $a \in K_0$, where K_0 is $\mathbb{Q}$ or a real quadratic field, and the base field K is a totally real extension of K_0.

Let $T_{0,V}$ denote the set of primes of potential type V reduction. Let $L_w|K_v$ be a finite extension over which X acquires stable reduction. At each v in V_0 we choose an ordering of the two components of the special fibre of the stable model of X over $\mathcal{O}_{L_w}$. Over such an extension, the dual graph of a minimal regular model is then a "line", i.e., a graph with vertex set $\{v_0, \ldots, v_n\}$ and edge set $\{e_0, \ldots, e_{n-1}\}$ where e_i is an edge from v_i to v_{i+1}. Define $\pi_v : X(K_v) \to \mathbb{Q}$ to be the map sending a point x to i/n, where v_i is the unique vertex containing the reduction of x (note that the ratio i/n is independent of the choice of extension L_w). Finally, if α is a function from $T_{0,V}$ to $\mathbb{Q}$, we let $X(K)_{\alpha}$ denote the set of rational points for which $\pi_v(x) = \alpha(v)$ for all $v \in T_{0,V}$.

Theorem 1.2. *Let K_0 be $\mathbb{Q}$ or a real quadratic field. Let $K|K_0$ be a totally real extension. Let X/K_0 be a genus 2 curve in the family $y^2 = x^6 + ax^4 + ax^2 + 1$ whose Jacobian has Mordell–Weil rank 4 over K. Let $b \in X(K)$ denote the point $(0, 1)$. Assume that there is a prime p of $\mathbb{Q}$ such that*

- *The prime p splits completely in $K|\mathbb{Q}$.*
- *The curve X has good reduction at all primes above p, and the action of G_K on $E[p]$ is absolutely irreducible.*
- *If E has complex multiplication by a CM extension L, then L is not contained in $K(\mu_p)$.*

Then there exist constants $\lambda_v, \mu_v \in \mathbb{Q}_p$ for all $v \in T_{0,V}$ with the following property: Suppose z_0 is a point in $X(K)$ such that $f_1(z_0) \wedge f_2(z_0)$ is of infinite order in $\wedge^2 E(K)$. Then for all $\alpha : T_{0,V} \to \mathbb{Q}$, $X(K)_\alpha$ is contained in the finite set of z in $X(K_\mathfrak{p})$ satisfying $G(z) = 0$, where

- $$G(z) = \det \begin{pmatrix} F_1(z) + \sum_{v \in T_{0,V}} \lambda_v(\alpha(v) - \pi_v(b)) & F_2(z) + \sum_{v \in T_{0,V}} \mu_v(\alpha(v) - \pi_v(b)) \\ F_1(z_0) + \sum_{v \in T_{0,V}} \lambda_v(\pi_v(z_0) - \pi_v(b)) & F_2(z_0) + \sum_{v \in T_{0,V}} \mu_v(\pi_v(z_0) - \pi_v(b)) \end{pmatrix},$$
- $$F_1(z) = \int_b^z (\omega_0\omega_1 - \omega_1\omega_0) + \frac{1}{2}\int_b^z \omega_0 \int_{w(b)}^b \omega_1,$$
- $$F_2(z) = 2\int_b^z (-\omega_0\omega_3 + a\omega_1\omega_2 + 2\omega_1\omega_4) - \frac{1}{2}x(z) - \int_b^z \omega_0 \int_{w(b)}^b \omega_3.$$

□

7.2 Computing $(\underline{c}^H, \underline{r}^H)$ for the Kulesz–Matera–Schost family

To complete the proof of Theorem 1.2, by Lemma 5.8, it will be enough to show that, with respect to a suitable basis of W_{dR}/F^0, we have

$$\widetilde{h}_p(A(b,z)) - \frac{1}{2}\widetilde{h}_p([E_1, E_2]) = (F_1(z), -F_2(z)).$$

We shall prove this by explicitly determining the functions $f_{i,x}, g_{i,x}, h_{i,x}, \underline{c}^H$ and constants $\underline{r}^H$ from Section 6.

Let X be a hyperelliptic curve of the form $y^2 = x^6 + ax^4 + ax^2 + 1$. Denote by $\{\infty^+, \infty^-\}$ the points at infinity with respect to this model. Suppose b is a rational point of X and $U(b)$ is the quotient of the fundamental group defined in Section 1. Recall the maps f_1 and f_2 from the introduction. The set $\{\omega_0, \dots \omega_4\}$ forms a basis of $H^1_{\mathrm{dR}}(Y)$ and a basis of $H^1_{\mathrm{dR}}(X)$ is given by $\{\eta_0 = \omega_0, \eta_1 = \omega_1, \eta_2 = a\omega_2 + 2\omega_4, \eta_3 = \omega_3\}$. Let T_0, T_1, T_2, T_3 be the corresponding dual basis. For the quotient $\mathcal{A}^{\mathrm{dR}}(X)$, we find that all the ξ_k are zero, so that

$$1 \mapsto -\sum_{i=0}^{3} \eta_i \otimes T_i, \qquad T_j \mapsto -\sum_{0 \le j \le 3, 1 \le k \le 3} \eta_i \otimes (\tau_{ijk} S_k), \qquad S_k \mapsto 0$$

extends to a connection on X.

Let $\omega_E = dx/2y$ denote the canonical Weierstrass differential on E. Let $T_{E,1}$ and $T_{E,2}$ denote the basis of $H^1_{\mathrm{dR}}(E - O)$ dual to $[\omega_E], [x\omega_E]$. The set $\{S_0 = T_{E,0}T_{E,0}, S_1 = T_{E,0}T_{E,1}, S_2 = T_{E,1}T_{E,1}\}$ forms a basis of W_{dR}, and the set $\{S_0, S_1\}$ forms a basis of W_{dR}/F^0. Since the map τ factors through $\wedge^2 V_{\mathrm{dR}}$, it is enough to specify its values on the elements $T_i \wedge T_j$. These may be calculated by observing that

$$f_1^*[\omega_E] = [\eta_1], \qquad f_{2*}[\omega_E] = [\eta_0], \qquad f_1^*[x\omega_E] = [\eta_3], \qquad f_2^*[x\omega_E] = [\eta_2].$$

Hence we deduce by equation (15) that

$$\tau(T_0 \wedge T_1) = -S_0, \qquad \tau(T_0 \wedge T_3) = -\tau(T_1 \wedge T_2) = -S_1, \qquad \tau(T_2 \wedge T_3) = -S_2.$$

With respect to these bases, we find that $\underline{c}^H = 0$ and $\underline{r}^H = (0, \frac{1}{2}x(z) - \frac{1}{2}x(b))$.

7.3 Local constants at primes of bad reduction

We now explain how to compute local pre-heights at primes away from p, under the assumption of Hypothesis (H). First we explain why a non-trivial contribution at $v \in T_0$ can only arise when v is a prime of potential type V reduction.

Lemma 7.1. Suppose X has potential good reduction at v. Then j_v is trivial. □

Proof. Recall from [49, I.5.8] that, given a profinite group G, closed normal subgroup H, and G-group A, we get an exact sequence of pointed sets

$$H^1(G/H, A^H) \to H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A).$$

Applying this when $G = G_v$, $H = G_w$ is the Galois group of a finite extension L_w of K_v over which X acquires good reduction. The commutative diagram

$$\begin{array}{ccc} X(K_v) & \xrightarrow{j_v} & H^1(G_v, U) \\ \downarrow & & \downarrow \text{Res} \\ X(L_w) & \longrightarrow & H^1(G_w, U) \end{array}$$

implies that the composite $\text{Res} \circ j_v$ is trivial. Hence to prove the lemma it is enough to show that U^{G_w} is trivial, which may be seen from the fact that V and $\text{Sym}^2 V_E$ are pure of weight -1 and -2 respectively over L. ■

Lemma 7.2. Suppose E does not have potential good reduction at v. Then $H^1(G_v, U)$ is trivial. □

Proof. We have an exact sequence of pointed sets

$$H^1(G_v, \text{Sym}^2 V_E) \to H^1(G_v, U) \to H^1(G_v, V).$$

Applying Lemma 3.8 with $n = 0$, we see that $H^1(G_v, V) = 0$. Hence it is enough to show that $H^1(G_v, \text{Sym}^2 V_E) = 0$. This is well-known (see e.g. [24, Lemma 2.10]), but we recall the proof for the sake of completeness. Let L_w be a finite extension of K_v over which E acquires semi-stable reduction. Then $\text{Res}_{G_w} V_E$ is a non-trivial extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$. Hence $\text{Sym}^2 V_E$ is an extension

$$0 \to \mathbb{Q}_p(2) \to \text{Sym}^2 V_E \to (\text{Sym}^2 V_E)/\mathbb{Q}_p(2) \to 0,$$

and $(\text{Sym}^2 V_E)/\mathbb{Q}_p(2)$ is a non-trivial extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$. Then, arguing as in the proof of Lemma 3.8, we have $H^1_f(G_v, \text{Sym}^2 V_E/\mathbb{Q}_p(2)) = H^1_f(G_v, (\text{Sym}^2 V_E/\mathbb{Q}_p(2))^*(1)) = 0$, hence $H^1(G_v, \text{Sym}^2 V_E/\mathbb{Q}_p(2)) = 0$. Similarly $H^1(G_v, \mathbb{Q}_p(2)) = 0$ for weight reasons. ■

The only remaining case is where E has potential good reduction but X does not, which implies that X has potential type V reduction. Again using injectivity of the restriction map we can recover $j_{2,v}$ from its image in $H^1(G_L, \text{Sym}^2 V_E)$ which is determined (up to a scalar) by the following Lemma, whose proof will appear in [12].

Lemma 7.3. For all $v \in T_0$ of potential type V reduction, the map

$$j_v : X(K_v) \to H^1(G_v, U)$$

factors as $X(K_v) \to \mathbb{Q}_p \to H^1(G_v, U)$, where the first map sends z to $\pi_v(z) - \pi_v(b)$ and the second map is a vector space homomorphism. □

7.4 Completion of proof

We now explain how to use this explicit description of generalised heights on X to prove Theorem 1.2. This gives the following proposition.

Proposition 7.1. *With respect to the basis S_0, S_1 of $(\mathrm{Sym}^2 V_E^{dR})/F^0$, the local heights $\widetilde{h}_{\mathfrak{p}}(A(b,z))$ and $\widetilde{h}_{\mathfrak{p}}([E_1,E_2])$ are given by*

$$\widetilde{h}_{\mathfrak{p}}(A(b,z)) = (F_1(z) + \frac{1}{2}\int_b^z \omega_0 \int_{w(b)}^z \omega_1)S_0 - F_2(z)S_1, \qquad \widetilde{h}_{\mathfrak{p}}([E_1,E_2]) = \frac{1}{2}\int_b^z \omega_0 \int_{w(b)}^z \omega_1 S_0.$$

□

Proof. We have an isomorphism $H^1_f(G_{\mathfrak{p}}, V_E) \simeq \mathbb{Q}_p.T_{E,0}$ using the basis of $H^1_{\mathrm{dR}}(E)$ above, and given extensions $[E_1] = \lambda_1.T_{E,0}$ and $[E_2] = \lambda_2.T_{E,0}$. Then the class of $[E_1,E_2]$ in $F^0\backslash U(\mathbb{Q}_p, V_{\mathrm{dR}}, W_{\mathrm{dR}})$ is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ \lambda_1 T_{E,0} + \lambda_2 T_{E,1} & 1 & 0 \\ \lambda_1\lambda_2 S_0 & \lambda_2 T^*_{E,0}\otimes S_0 + \lambda_1 T^*_{E,0}\otimes S_0 & 1 \end{pmatrix}.$$

Hence the pre-height of $[E_1,E_2]$ is given by $-\lambda_1\lambda_2$, and the result follows from Lemma 5.7. ■

Hence we find

$$\widetilde{h}_{\mathfrak{p}}(A(b,z)) - \widetilde{h}_{\mathfrak{p}}([E_1,E_2]) = (F_1(z), F_2(z)).$$

7.5 Examples

In this section, we give three examples of our Theorem 1.2 applied to specific curves X. In the first two examples, we obtain a finite set of $\mathfrak{p}$-adic points containing $X(K)$. In general, if the codimension of $\mathrm{Sel}(U)$ in $H^1_f(G_{\mathfrak{p}}, U)$ is one, then $X(K_{\mathfrak{p}})_U$ will contain extra $\mathfrak{p}$-adic points that do not come from $X(K)$. In practice, one can often use the Mordell–Weil sieve in combination with the Chabauty–Kim method to determine $X(K)$ exactly ([48], [25], or [6] for an example in the context of the Chabauty–Kim method). Our `SageMath` code is available on Github [7].

7.5.1 *Example 1: $K = \mathbb{Q}$, $a = 31$, $p = 3$*

The curve E_{31} has rank 2 over $\mathbb{Q}$. To determine the local constants, we first need to find the primes of potential type V reduction. X has potential good reduction at all primes away from 2 and 7, which are both of potential type V reduction.

1. $v = 7$: modulo 7, the model $y^2 = x^6 + 31x^4 + 31x^2 + 1$ reduces to $y^2 = (x^2+1)^3$. In particular, with respect to this model, all $\mathbb{Q}_7$-points reduce to a smooth point of the special fibre, and lie on a common component. Hence all $\mathbb{Q}_7$-points reduce to a common component of the minimal regular model over $\mathbb{Z}_7$. Hence they reduce to a common component of the stable model of X over a finite extension of $\mathbb{Q}_7$, and so by (H) the contribution at 7 is zero.
2. $v = 2$: we observe $H^1(G_{\mathbb{Q}_2}, \mathrm{Sym}^2 V_E) = 0$, which implies that $H^1(G_{\mathbb{Q}_2}, U) = 0$. One way to see this is to note that for $H^1(\mathbb{Q}_2, \mathrm{Sym}^2 V_E)$ to be nonzero, it is necessarily the case that $\mathrm{Hom}_{G_{\mathbb{Q}_2}}(T_3E, T_3E)$ has rank bigger than 1, which means that the action of inertia at 2 must factor through an abelian subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. This does not happen at $a = 31$, because E does not acquire good reduction over any $(\mathbb{Z}/2)^2$ or degree 3 extension of $\mathbb{Q}_2$.

Hence our equation for rational points simplifies to $F_1(z)F_2(z_0) = F_1(z_0)F_2(z)$. The set of solutions is tabulated below. We find $X(\mathbb{Q}_3)_U$ appears to contain 8 non-rational points.

$\overline{z} \in X(\mathbb{F}_3)$	$x(z) \in \mathbb{Z}_p$	$z \in X(\mathbb{Q})$
$\overline{(0,\pm 1)}$	$O(3^7)$	$(0,\pm 1)$
	$2\cdot 3 + 2\cdot 3^3 + 2\cdot 3^5 + O(3^7)$	
	$3 + 2\cdot 3^2 + 2\cdot 3^4 + 2\cdot 3^6 + O(3^7)$	
$\overline{(1,\pm 2)}$	$1 + O(3^7)$	$(1,\pm 8)$
	$1 + 2\cdot 3 + O(3^7)$	$(7,\pm 440)$
	$1 + 3 + 2\cdot 3^3 + 3^4 + 2\cdot 3^5 + O(3^7)$	$(\frac{1}{7},\pm\frac{440}{343})$
$\overline{(2,\pm 2)}$	$2 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + O(3^7)$	$(-7,\pm 440)$
	$2 + 3 + 2\cdot 3^2 + 3^4 + 2\cdot 3^6 + O(3^7)$	$(-\frac{1}{7},\pm\frac{440}{343})$
	$2 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + O(3^7)$	$(-1,\pm 8)$
$\overline{\infty^{\pm}}$	$2\cdot 3^{-1} + 1 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + O(3^7)$	
	$3^{-1} + 1 + 2\cdot 3^5 + 2\cdot 3^6 + O(3^7)$	
	$\infty^{\pm}$	$\infty^{\pm}$

7.5.2 *Example 2:* $K = \mathbb{Q}(\sqrt{3})$, $a = 19$, $p = 11$, $\mathfrak{p} = (2\sqrt{3}+1)$

It follows from the functional equations satisfied by F_1 and F_2 that, for any z_0, the zero set of

$$F_2(z)F_1(z_0) - F_1(z)F_2(z_0)$$

is stable under $\mathrm{Aut}(X)$, and $F_i((\pm 1,\pm 1)) = 0$. Hence the fact that each of the known rational points z from Example 7.5.1 satisfied the identity $F_2(z)F_1(z_0) = F_1(z)F_2(z_0)$ is a trivial consequence of the above functional equations. It is natural to ask if one can find an example where Theorem 1.2 produces a non-trivial identity between the F_i evaluated on different rational points (analogous to 'motivic' identities between p-adic polylogarithms evaluated at S-units, or p-adic heights of integral points on elliptic curves). Numerical experiments suggest that it is rare for the formula in Theorem 1.2 to produce non-trivial identities (i.e. identities that cannot be explained by the functional equations) that the F_i satisfies on rational points, as when a curve has many rational points relative to its Mordell–Weil rank, it typically has many potential type V primes.

However, there are instances where the theorem produces non-trivial identities between the values of $F_i(z)$ on rational points. When $a = 19$ and $K = \mathbb{Q}(\sqrt{3})$, we find that $E(K)$ has rank 2, the prime above 2 is the only potential type V prime and the set $X(\mathbb{Q}(\sqrt{3}))$ has at least 28 points, coming from the $\mathrm{Aut}(X)$-orbits of $(0,1)$ together with the points

$$z_1 = (\sqrt{3}, 16), z_2 = (-\sqrt{3}+2, -24\sqrt{3}+40), z_3 = (-39\sqrt{3}/71 + 98/71, -2736216\sqrt{3}/357911 + 5551000/357911).$$

Local constants at v above 2: one can compute a semistable model of X over the totally ramified extension L of $\mathbb{Q}_2$ cut out by the polynomial

$$F(t) = t^8 + 32t^7 + 448t^6 + 3584t^5 + 16096t^4 + 28160t^3 - 18432t^2 - 6912$$

by first computing a smooth model of E over L, for example as described in [40, §10.2.3]. Let β be a root of F in L, and define $\gamma := \frac{1}{3}(\beta^2 + 8\beta)$. Using this model, we can show that the regular semistable model of X over $L(\sqrt{3})$ has 9 irreducible components, and that the map $\pi_v : X(K_v) \to \{a/8 : 0 \le a \le 8\}$ is given by

$$z \mapsto \begin{cases} 0 & v(x(z)-1) > 1, v(x(z)^2+1-\gamma) \ge 3 \\ (3 - v(x(z)^2+1-\gamma))/2 & v(x(z)-1) > 1, 2 \le v(x(z)^2+1-\gamma) \le 3 \\ 1/2 & v(x(z)^2+1-\gamma) \le 2 \\ (v(x(z)^2+1-\gamma)-1)/2 & v(x(z)-1) = 1, 2 \le v(x(z)^2+1-\gamma) \le 3 \\ 1 & v(x(z)-1) = 1, v(x(z)^2+1-\gamma) \ge 3 \end{cases}$$

where the valuation v is normalised so that $v(2) = 1$. For example, this tells us that $\pi_v(z_0) = 1/2$. For z_1, z_2 and z_3, we are in case 4, since

$$v(x(z_1)^2 - 1 + \gamma) = 5/2, v(x(z_2)^2 - 1 + \gamma) = 11/4, v(x(z_3)^2 - 1 + \gamma) = 11/4.$$

Hence $\pi_v(z_1) = 3/4$ and $\pi_v(z_2) = \pi_v(z_3) = 7/8$. We find that the divisor

$$3[z_2] + [z_3] - 6[z_1]$$

maps to zero in $\wedge^2 E(K) \otimes \mathbb{Q}$ and in $H^1(G_v, \mathrm{Sym}^2 V_E)$. Working at a prime above 11, we compute that

$$3F_1(z_2) + F_1(z_3) - 6F_1(z_1) = 3F_2(z_2) + F_2(z_3) - 6F_2(z_1) = O(11^{18}).$$

The vector space $E(K)\otimes\mathbb{Q}$ is generated by $P_1=(4\sqrt{3}+7,24\sqrt{3}+40)$ and $P_2=(1/3,16\sqrt{3}/9)$. With respect to these generators, we have $f_1(z_1)=(-1,-1)$, $f_2(z_1)=(1,0)$, $f_1(z_2)=(0,1)$, $f_2(z_2)=(-2,-1)$. Hence the images of z_1 and z_2 in $\wedge^2E(K)\otimes\mathbb{Q}$ are $P_1\wedge P_2$ and $2P_1\wedge P_2$ respectively. Thus we have

$$\lambda_v = 8(F_1(z_2)-2F_1(z_1)),$$
$$\mu_v = 8(F_2(z_2)-2F_2(z_1)).$$

We deduce that $X(\mathbb{Q}_{11})_2$ is contained in the zeroes of

$$\left(F_1(z)+\lambda_v\left(c-\frac{1}{2}\right)\right)\left(F_2(z_1)+\frac{\mu_v}{4}\right)-\left(F_2(z)+\mu_v\left(c-\frac{1}{2}\right)\right)\left(F_1(z_1)+\frac{\lambda_v}{4}\right),$$

$c\in\{0,1/8,\dots,7/8,1\}$. The $\mathbb{F}_{11}$-points of X are $\pm\infty,(0,\pm1),(\pm2,\pm4),(\pm3,\pm3),(\pm4,\pm5),(\pm5,\pm5)$. Because $X(\mathbb{Q}_{11})_U$ is stable under the automorphism group of X, we need only consider the residue disks corresponding to the $\mathbb{F}_{11}$-points $(0,1),(2,4),(3,3)$. We find the following points:

$\overline{z}\in X(\mathbb{F}_{11})$	$x(z)\in\mathbb{Z}_p$	$z\in X(\mathbb{Q})$
$\overline{(0,1)}$	$6\cdot11+6\cdot11^2+6\cdot11^3+7\cdot11^4+10\cdot11^6+O(11^7)$	
	$10\cdot11+3\cdot11^2+8\cdot11^4+5\cdot11^5+4\cdot11^6+O(11^7)$	
	$3\cdot11+5\cdot11^2+5\cdot11^3+9\cdot11^4+2\cdot11^5+3\cdot11^6+O(11^7)$	
	$7\cdot11+5\cdot11^2+10\cdot11^3+3\cdot11^4+5\cdot11^5+11^6+O(11^7)$	
	$O(11^7)$	$(0,1)$
	$4\cdot11+5\cdot11^2+7\cdot11^4+5\cdot11^5+9\cdot11^6+O(11^7)$	
	$8\cdot11+5\cdot11^2+5\cdot11^3+11^4+8\cdot11^5+7\cdot11^6+O(11^7)$	
	$11+7\cdot11^2+10\cdot11^3+2\cdot11^4+5\cdot11^5+6\cdot11^6+O(11^7)$	
	$5\cdot11+4\cdot11^2+4\cdot11^3+3\cdot11^4+10\cdot11^5+O(11^7)$	
$\overline{(3,3)}$	$3+3\cdot11+5\cdot11^2+3\cdot11^3+2\cdot11^4+6\cdot11^5+2\cdot11^6+O(11^7)$	
	$3+6\cdot11+7\cdot11^2+7\cdot11^3+7\cdot11^4+6\cdot11^6+O(11^7)$	$\left(\frac{-39\sqrt{3}-98}{71},\frac{-2736216\sqrt{3}-5551000}{357911}\right)$
	$3+9\cdot11+5\cdot11^2+5\cdot11^3+2\cdot11^4+11^5+11^6+O(11^7)$	
	$3+11+7\cdot11^2+4\cdot11^3+7\cdot11^4+4\cdot11^5+3\cdot11^6+O(11^7)$	
	$3+4\cdot11+7\cdot11^2+7\cdot11^4+5\cdot11^5+2\cdot11^6+O(11^7)$	
	$3+7\cdot11+2\cdot11^2+11^3+10\cdot11^4+8\cdot11^5+9\cdot11^6+O(11^7)$	
	$3+10\cdot11+10\cdot11^2+5\cdot11^3+11^4+8\cdot11^5+5\cdot11^6+O(11^7)$	
	$3+2\cdot11+6\cdot11^2+8\cdot11^3+11^4+9\cdot11^5+9\cdot11^6+O(11^7)$	$(\sqrt{3}-2,24\sqrt{3}-40)$
	$3+5\cdot11+6\cdot11^2+9\cdot11^3+7\cdot11^4+4\cdot11^5+6\cdot11^6+O(11^7)$	
$\overline{(2,4)}$	$2+7\cdot11+10\cdot11^2+5\cdot11^3+5\cdot11^4+8\cdot11^5+4\cdot11^6+O(11^7)$	
	$2+3\cdot11+6\cdot11^2+4\cdot11^3+3\cdot11^4+11^5+7\cdot11^6+O(11^7)$	
	$2+10\cdot11+8\cdot11^2+3\cdot11^4+4\cdot11^5+O(11^7)$	$\left(-\frac{1}{\sqrt{3}},\frac{19\sqrt{3}}{9}\right)$
	$2+6\cdot11+6\cdot11^2+2\cdot11^3+5\cdot11^6+O(11^7)$	
	$2+2\cdot11+9\cdot11^2+11^3+10\cdot11^4+4\cdot11^6+O(11^7)$	
	$2+9\cdot11+4\cdot11^2+10\cdot11^3+11^4+6\cdot11^5+O(11^7)$	
	$2+5\cdot11+3\cdot11^2+8\cdot11^3+3\cdot11^4+4\cdot11^5+2\cdot11^6+O(11^7)$	
	$2+11+4\cdot11^2+11^3+4\cdot11^4+10\cdot11^5+8\cdot11^6+O(11^7)$	
	$2+8\cdot11+5\cdot11^2+2\cdot11^3+9\cdot11^5+3\cdot11^6+O(11^7)$	

7.5.3 *Example 3:* $K_0=\mathbb{Q}(\sqrt{11}),K=K_0(\sqrt{2883589+3072\sqrt{11}}),a=-1-512\sqrt{11}$

In general, a major drawback to applying Theorem 1.2 is the need to have enough rational points to solve for the undetermined constants $\mu_v,\lambda_v,F_i(z_0)$. For example, this is illustrated by the case $K=\mathbb{Q}(\sqrt{2883589+3072\sqrt{11}})$, $a=-1-512\sqrt{11}$. The curve X has potential good reduction away from primes above $2,11,229$ and 787. Under GRH, the elliptic curve E has rank 1 over K_0 and rank 2 over K. The j-invariant of E is not integral at the prime above 2 (this is the reason for the choice of a) and the prime above 11, hence by Lemma 7.2 there are no local contributions at these primes. The reason for the obscure choice of K is that it is quite rare to find a totally real K for which E has rank two and X has non-trivial rational points. This particular K was constructed by computing the Mumford representation of the divisor $2(0,1)-2(0,-1)$.

The prime 787 splits in K_0. In the embedding $v_1:K_0\to\mathbb{Q}_{787}$ sending $\sqrt{11}$ to 621 modulo 787, the curve $X_{\mathbb{Q}_{787},v}$ has good reduction. In the embedding $v_2:K_0\to\mathbb{Q}_{787}$ sending $\sqrt{11}$ to 166 modulo 787, the factorization of f modulo 727 is $(x^2+1)^3$, hence the singular points of the original model are not $\mathbb{F}_{787}$-rational. The prime v_2 splits completely in K, hence we obtain two primes w_1 and w_2 of type V reduction, but in both cases the function π_{w_i} is constant on $X(K_{w_i})$.

The prime 229 splits in K_0. In the embedding $v_3 : K_0 \to \mathbb{Q}_{229}$ sending $\sqrt{11}$ to 34 modulo 229, $X_{\mathbb{Q}_{11},v}$ has good reduction. In the embedding $v_4 : K_0 \to \mathbb{Q}_{229}$ sending $\sqrt{11}$ to 195 modulo 229, $X_{\mathbb{Q}_{11},\overline{v}}$ has type V reduction. $\overline{v}$ splits in $K|K_0$, hence there are two primes w_3 and w_4 for which the function π_{w_i} is non-constant. Over $K_{w_i}(229^{1/6})$, X acquires semistable reduction, and one can show that the target of the maps π_{w_i} is $\{0, 1/2, 1\}$, with

$$\pi_{w_i}^{-1}(\{0,1\}) = \{z \in X(K_{w_i}) : \mathrm{val}_{w_i}(x(z)^2 + 1) > 0\}.$$

where val_{w_i} is the valuation on K_{w_i}. The non-trivial rational points of X of small height X are given by the $\mathrm{Aut}(X)$-orbit of $\left(\frac{\sqrt{2883589+3072\sqrt{11}}}{2}, \frac{1476400640\sqrt{11}+20185085}{8}\right)$, and hence all of the (known) rational points z satisfy $\pi_{w_i}(z) = 1/2$. To determine (a finite superset of) $X(K_{\mathfrak{p}})_2$ in this case, one would presumably have to find some other way of constructing (and computing localisations of) non-trivial cohomology classes in $H^1(G_{K,T}, \mathrm{Sym}^2 V_E)$, or dually of $H^1(G_{K,T}, \mathrm{ad}^0 V_E)$.

A Appendix: Universal enveloping algebras in unipotent Tannakian categories

In this appendix we recall certain notions regarding universal pointed objects in unipotent Tannakian categories. None of the material is original. These objects are studied in [29, §2], [3, §3] and [11, §6.2] in the context of specific unipotent Tannakian categories, but as we explain below, the constructions can be made in much greater generality. A lot of the results are also implicit in [22], but formulated slightly differently.

A.1 Universal pointed objects in neutral Tannakian categories

Before we proceed to the properties of unipotent Tannakian categories, we record a tautological relationship between changing fibre functors and twisting by path torsors. Let $\mathcal{C}$ be a neutral Tannakian category over a field K, with fibre functors ω_1, ω_2. Via Tannaka duality, we view ω_i as an equivalence of strict tensor categories from $\mathcal{C}$ to the category of representations of $\pi_1(\mathcal{C}, \omega_i)$. The torsor of isomorphisms of functors $\pi_1(\mathcal{C}; \omega_1, \omega_2)$ is a $(\pi_1(\mathcal{C}, \omega_1), \pi_1(\mathcal{C}, \omega_2))$-bitorsor, giving an equivalence of categories

$$\begin{aligned} \mathrm{tw}_{\omega_1,\omega_2} : (\pi_1(\mathcal{C}, \omega_1) - \mathrm{rep}) &\to (\pi_1(\mathcal{C}, \omega_2) - \mathrm{rep}) \\ V &\mapsto \pi_1(\mathcal{C}; \omega_1, \omega_2) \times_{\pi_1(\mathcal{C},\omega_1)} V. \end{aligned}$$

We deduce the following result.

Lemma A.1. We have an isomorphism of functors

$$\mathrm{tw}_{\omega_1,\omega_2} \circ \omega_1 \xrightarrow{\simeq} \omega_2,$$

given by $\pi_1(\mathcal{C}; \omega_1, \omega_2) \times_{\pi_1(\mathcal{C},\omega_1)} \omega_1(\mathcal{V}) \to \omega_2(\mathcal{V})$ being the map sending (σ, v) to $\sigma(v)$, (for $\mathcal{V}$ in $\mathcal{V}$, $\sigma \in \pi_1(\mathcal{C}; \omega_1, \omega_2)(K), v \in \omega_1(\mathcal{V})$). □

When $U = \varprojlim U_n$ is a pro-unipotent group over a field K, a representation of U will always mean a continuous representation, i.e. one which factors through U_n for some n. The completed universal enveloping algebra R of U is the completion of the universal enveloping algebra of $\mathrm{Lie}(U)$ with respect to its augmentation ideal. An R module will always mean a continuous R-module.

Definition A.2. Let $(\mathcal{C}, \omega)$ be a neutral Tannakian category over a field K. We say that $(\mathcal{C}, \omega)$ is *unipotent* if $\pi_1(\mathcal{C}, \omega)$ is pro-unipotent and for all V, W in $\mathcal{C}$, the K-dimension of $\mathrm{Ext}^1_{\mathcal{C}}(V, W)$ is finite. □

By Tannaka duality, the statement that $\pi_1(\mathcal{C}, \omega)$ is pro-unipotent is equivalent to the condition that every non-zero object W of $\mathcal{C}$ admits a non-trivial morphism $\mathbf{1} \to W$.

Definition A.3. Let $\mathcal{C}$ be a unipotent Tannakian category with fibre functor ω. We say $X \in \mathcal{C}$ is n-unipotent if it admits a filtration $X = X_0 \supset X_1 \supset \ldots \supset X_{n+1} = 0$ such that, for all i, X_i/X_{i+1} is isomorphic to a direct sum of copies of the unit object $\mathbf{1}$ (this includes the possibility that $X_i/X_{i+1} = 0$). Let $\mathcal{C}_n$ denote the full sub-category of $\mathcal{C}$ consisting of n-unipotent objects (note that this is not a tensor sub-category in general). We denote by ω_n the restriction of ω to $\mathcal{C}_n$. □

Lemma A.4. Let U be a pro-unipotent group over a field K. Let R be its completed universal enveloping algebra. Let I be the augmentation ideal of R. Under the equivalence between representations of U and R-modules, n-unipotent representations of U correspond to R-modules for which the action of R factors through R/I^{n+1}. □

Proof. Let X be a representation of U for which the action of R factors through R/I^{n+1}. Then X is n-unipotent, with filtration $X_i := I^i X$. Conversely, if X is n-unipotent with filtration (X_i), then I annihilates X_i/X_{i+1}, hence I^{n+1} annihilates X. ■

Define $A_n(\mathcal{C}, \omega)$ to be the K-vector space

$$A_n(\mathcal{C}, \omega) := \mathrm{Hom}(\omega_n, \omega_n).$$

More generally, for fibre functors ω, ν on $\mathcal{C}$, we define

$$A_n(\mathcal{C}; \omega, \nu) := \mathrm{Hom}(\omega_n, \nu_n).$$

We also have an interpretation of $A_n(\mathcal{C}; \omega, \nu)^*$ in terms of $\mathcal{O}(\pi_1(\mathcal{C}; \omega, \nu))$. The pro-finite dimensional vector space $\mathrm{Hom}(\omega^*, \nu^*)$ has a co-commutative co-product structure given by

$$\begin{aligned} \varprojlim A_n(\mathcal{C}; \omega, \nu) &\to \varprojlim A_n(\mathcal{C}; \omega, \nu)^{\otimes 2} \\ f &\mapsto \big(v \otimes w \mapsto f(v \otimes w)\big) \end{aligned}$$

where $V, W \in \mathcal{C}$, $v \in \omega(V), w \in \omega(W)$, and we identify $f(v \otimes w) \in \nu(V \otimes W)$ with an element of $\nu(V) \otimes \nu(W)$ by tensor compatibility of ν.

Lemma A.5. We have functorial isomorphisms of K-algebras

$$\mathcal{O}(\pi_1(\mathcal{C}; \omega, \nu))^* \simeq \varinjlim A_n(\mathcal{C}; \omega, \nu)^*.$$

□

Proof. Surjective homomorphisms

$$\varinjlim A_n(\mathcal{C}; \omega, \nu)^* \to K$$

which are compatible with the algebra structure correspond to non-zero tensor compatible morphisms of functors from ω to ν, which are necessarily isomorphisms by [22, Proposition 1.13]. Applying a similar argument over a general K-algebra S, we deduce that $\mathrm{Spec}(\varinjlim A_n(\mathcal{C}; \omega, \nu)^*)$ satisfies the defining property of $\pi_1(\mathcal{C}; \omega, \nu)$. ■

In the case when $\omega = \nu$, we obtain a Hopf algebra structure on $\varprojlim A_n(\mathcal{C}, \omega)$ from this isomorphism. The product structure obtained is exactly the product structure on $\mathrm{End}(\omega)$.

Definition A.6. We define the category $\mathcal{C}^\omega$ of *pointed objects* as follows. An object of $\mathcal{C}^\omega$ is a pair $(\mathcal{V}, v)$, with $v \in \omega(\mathcal{V})$. A morphism of pointed objects $f : (\mathcal{V}_1, v_1) \to (\mathcal{V}_2, v_2)$ is a morphism $f : \mathcal{V}_1 \to \mathcal{V}_2$ in $\mathcal{C}$ such that $\omega(f)(v_1) = v_2$. We say that (V_n, v_n) is a universal n-unipotent pointed object if V_n is n-unipotent, and for every n-unipotent pointed object (W, w), there exists a unique morphism $(V_n, v_n) \to (W, w)$ in $\mathcal{C}^\omega$. We say a pro-object $((V_n, v_n))_{n>0})$ in $\mathcal{C}^\omega$ is a universal pointed pro-object if for all (W, w) in $\mathcal{C}^\omega$, there exists a unique morphism $(V_n, v_n) \to (W, w)$ for all $n \gg 0$. □

If, for all n, (V_n, v_n) is a universal n-unipotent pointed object, then (by definition) there is a unique way to give $((V_n, v_n))_{n>0}$ the structure of a pro-object in $\mathcal{C}^\omega$, and this pro-object is a universal pointed pro-object, since every W in $\mathcal{C}$ is n-unipotent for $n \gg 0$.

Lemma A.4 implies that universal pointed pro-objects in unipotent Tannakian categories exist, and are isomorphic to the completed universal enveloping algebra of U. An equivalent form of this Lemma can be found in [11, Proposition 6.2.1 and Proposition 6.2.2].

Lemma A.7. Let $(\mathcal{C}, \omega)$ be a unipotent Tannakian category.

1. For all n, a universal n-unipotent pointed object $(\mathcal{A}_n(\mathcal{C}, \omega), e_n)$ exists (and hence is unique up to unique isomorphism). The pro-object $((\mathcal{A}_n(\mathcal{C}, \omega))_n, (e_n)_n)$ is a universal pointed pro-object in $(\mathcal{C}, \omega)$. Furthermore, under Tannaka equivalence the universal pointed pro-object in $\mathcal{C}$ is canonically isomorphic, as a pointed pro-$\pi_1(\mathcal{C}, \omega)$-representation, to the completed universal enveloping algebra of $\mathrm{Lie}(\pi_1(\mathcal{C}, \omega))$.
2. Let $(\mathcal{V}_n, e_n)$ be a universal n-pointed object in $\mathcal{C}^\omega$. Then, for any fibre functor ν, we have an isomorphism

$$\nu(\mathcal{A}_n(\mathcal{C}, \omega)) \simeq A_n(\mathcal{C}; \omega, \nu).$$

□

Proof. 1. This theorem is proved in [29, Theorem 2.1] in the case that $\mathrm{Ext}^2(\mathbf{1},\mathbf{1})=0$. The general case is proved in [3, Proposition 3.4]. In both cases, the proof is given in the context of specific unipotent Tannakian categories of interest (e.g. unipotent $\mathbb{Q}_p$-local systems on $X_{\overline{K},\acute{e}t}$, unipotent flat connections on X/K, etc.) but the proofs work in a more general context. An alternative proof of these results is to use Tannaka duality to reduce to the case where $\mathcal{C}$ is the category of representations of a pro-unipotent group with finite-dimensional abelianisation, and ω is the forgetful functor.
Take R to be the completed universal enveloping algebra of its Lie algebra. The Hopf algebra R has an augmentation ideal I, and we define $R_n := R/I^{n+1}$. By Lemma A.4, an object is n-unipotent if and only if it is annihilated by I^{n+1}. It follows that $(R_n, \omega(1))$ is the universal pointed n-unipotent object: for a pointed n-unipotent object $(V,\omega(v))$, the unique morphism $R_n \to V$ is just given by $r \mapsto r\cdot v$.

2. If $(\mathcal{A}_n(\mathcal{C},\omega), e_n)$ is a universal pointed object, then by definition $\mathcal{A}_n(\mathcal{C},\omega)$ represents the functor ω_n, with isomorphism
$$\mathrm{Hom}(\mathcal{A}_n(\mathcal{C},\omega),.) \simeq \omega$$
given by
$$(\mathcal{A}_n(\mathcal{C},\omega) \xrightarrow{f} V) \mapsto \omega(f)(e_n).$$

■

We denote the universal n-unipotent pointed object of $\mathcal{C}^\omega$ by $\mathcal{A}_n(\mathcal{C},\omega)$, as in the lemma. By the universal property, for all $n>1$ we have unique morphisms of pointed objects
$$(\mathcal{A}_n(\mathcal{C},\omega), e_n) \mapsto (\mathcal{A}_{n-1}(\mathcal{C},\omega), e_{n-1})$$
and as explained above, the inverse limit is the Tannaka dual of the completed universal enveloping algebra of $\mathrm{Lie}(\pi_1(\mathcal{C},\omega))$, with (e_n) corresponding to the unit element 1. We denote by $I_{\mathcal{C}}$ the kernel of the morphism
$$\varprojlim A_n(\mathcal{C},\omega) \to K$$
associated to the unique (pro-)morphism
$$\varprojlim \mathcal{A}_n(\mathcal{C},\omega) \to \mathbf{1}$$
defined by sending e_n to 1. Then under the identification of $\varprojlim A_n(\mathcal{C},\omega)$ with the completed universal enveloping algebra of $\mathrm{Lie}(\pi_1(\mathcal{C},\omega))$, $I_{\mathcal{C}}$ corresponds to the augmentation ideal.

A.2 Computing the graded pieces of $A_n(\mathcal{C},\omega)$

The vector space $A_n(\mathcal{C},\omega)$ has a filtration with graded pieces $\mathbf{1}, \mathrm{Ker}(A_k(\mathcal{C},\omega) \to A_{k-1}(\mathcal{C},\omega))$, $(1\le k\le n)$. Under the identification of $A_n(\mathcal{C},\omega)$ with a quotient R_n of the universal enveloping algebra of $\mathrm{Lie}(\pi_1(\mathcal{C},\omega))$ given by Lemma A.7, this filtration is the I-adic filtration, where $I\subset R$ is the image of augmentation ideal in R_n.

In [3], a cohomological construction of $A_n(\mathcal{C},\omega)$ is given, which gives an inductive description of the graded pieces $I_{\mathcal{C}}^i/I_{\mathcal{C}}^{i+1}$ of $A_n(\mathcal{C},\omega)$ in terms of ext groups in $\mathcal{C}$. As we will only need this when $n=2$, we only state this case (the general case is somewhat more elaborate, and can be found in [3, §3.6]).

Lemma A.8. 1. We have a functorial isomorphism
$$\mathrm{Ext}^1_{\mathcal{C}}(\mathbf{1},\mathbf{1}) \simeq (I_{\mathcal{C}}/I_{\mathcal{C}}^2)^*.$$

2. We have a functorial isomorphism
$$(I_{\mathcal{C}}^2/I_{\mathcal{C}}^3) \simeq \mathrm{Ker}(\mathrm{Ext}^1_{\mathcal{C}}(\mathbf{1},\mathbf{1})^{\otimes 2} \xrightarrow{\cup} \mathrm{Ext}^2_{\mathcal{C}}(\mathbf{1},\mathbf{1}))^*$$
where the cup product is the Yoneda cup product. Moreover the diagram
$$\begin{array}{ccc} (I_{\mathcal{C}}/I_{\mathcal{C}})^{\otimes 2} & \xrightarrow{\simeq} & (\mathrm{Ext}^1(\mathbf{1},\mathbf{1})^*)^{\otimes 2} \\ \downarrow & & \downarrow \\ (I_{\mathcal{C}}^2/I_{\mathcal{C}}^3) & \xrightarrow{\simeq} & \mathrm{Ker}(\mathrm{Ext}^1_{\mathcal{C}}(\mathbf{1},\mathbf{1})^{\otimes 2} \xrightarrow{\cup} \mathrm{Ext}^2_{\mathcal{C}}(\mathbf{1},\mathbf{1}))^* \end{array}$$
commutes.

□

Proof. This is a special case of [3, Proposition 3.4]. ■

This gives a cohomological description of the graded pieces of the central series filtration on $\pi_1(\mathcal{C},\omega)$. To explain this, we first explain how $A_n(\mathcal{C},\omega)$, which by the above is a quotient of the universal enveloping algebra of $\pi_1(\mathcal{C},\omega)$, can also be thought of as a quotient of the universal enveloping algebra of the maximal n-unipotent quotient of $\pi_1(\mathcal{C},\omega)$. Recall that the universal enveloping algebra of a Lie algebra L is isomorphic to the tensor algebra of L modulo the two sided ideal generated by $x\otimes y - y\otimes x - [x,y]$ for $x,y\in L$. A more general statement which implies the lemma below can be found in [11, Proposition 1.0.9].

Lemma A.9. Let L be a nilpotent Lie algebra, and let R be its completed universal enveloping algebra. Let $\overline{R}$ be the universal enveloping algebra of L_n, and $\overline{R}_n := \overline{R}/\overline{I}^{n+1}$, where $\overline{I}\subset\overline{R}$ is the augmentation ideal. Then the natural map $R\to\overline{R}$ induces an isomorphism $R_n\simeq\overline{R}_n$. □

Proof. This can be seen from the characterisation of R_n and $\overline{R}_n$ in terms of universal properties. Alternatively, it can be computed directly: the map $R\to\overline{R}_n$ is surjective and factors through R_n, hence it is enough to show that this map is injective. By the description of R given above, we see that the ith term of the central series filtration of L is contained I^iR. Hence the induced map $L\to R_n$ factors through $L\to L_n$, and hence the surjection $R\to R_n$ factors uniquely through $R\to\overline{R}$ by the universal property of $\overline{R}$, and hence through $\overline{R}_n$. ■

Let U_2 denote the maximal 2-unipotent quotient of $\pi_1(\mathcal{C},\omega)$, and let L_2 denote its Lie algebra. Let R_2 denote the quotient of the universal enveloping algebra of $\mathrm{Lie}(\pi_1(\mathcal{C},\omega))$ by the third power of its augmentation ideal. From Lemma A.9 we obtain an isomorphism $I_{\mathcal{C}}^2/I_{\mathcal{C}}^3\simeq[L_2,L_2]\oplus\mathrm{Sym}^2 L_2^{\mathrm{ab}}$. Taking exponentials yields a short exact sequence

$$1\to[U_2,U_2]\to I_{\mathcal{C}}^2/I_{\mathcal{C}}^3\to\mathrm{Sym}^2 U_1\to 1.$$

Hence we obtain the following corollary of Lemma A.8.

Lemma A.10. We have a functorial exact sequence

$$1\to\mathrm{Ker}(\wedge^2\mathrm{Ext}^1_{\mathcal{C}}(\mathbf{1},\mathbf{1})\to\mathrm{Ext}^2_{\mathcal{C}}(\mathbf{1},\mathbf{1}))^*\to U_2\to\mathrm{Ext}^1_{\mathcal{C}}(\mathbf{1},\mathbf{1})^*\to 1.$$

□

Acknowledgements

We are indebted to Minhyong Kim and Jan Vonk for helpful discussions, encouragement, and suggestions on the material in this paper. We thank the anonymous referees for several valuable comments on an earlier version of this manuscript. Part of this paper builds on the thesis of the second author, who is very grateful to his examiners Victor Flynn and Guido Kings for several suggestions which have improved the present work. The first author was supported by NSF grant DMS-1702196 and the Clare Boothe Luce Professorship (Henry Luce Foundation). The second author was supported by the EPSRC during his thesis and by NWO/DIAMANT grant number 613.009.031.

References

[1] Allen, P. B. "Deformations of polarized automorphic Galois representations and adjoint Selmer groups." *Duke Math. J.* 13, (2016): 2407–2460.

[2] André, Y. and Baldassarri, F. "De Rham cohomology of differential modules on algebraic varieties" *Progress in Mathematics*, 189, Birkhäuser Verlag, (2001).

[3] Andreatta, F. and Iovita, A. and Kim, M. "A p-adic nonabelian criterion for good reduction of curves" *Duke Math. J.*, 164 (2015): 2597–2642.

[4] Balakrishnan, J. S. "Coleman integration for even-degree models of hyperelliptic curves" *LMS J. Comput. Math.*, 18 (2015): 258–265.

[5] Balakrishnan, J.S. and Besser, A. and Müller, J.S. "Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves" *J. Reine und Angew. Math.*, 720 (2016): 51–79.

[6] Balakrishnan, J.S. and Dogra, N. "Quadratic Chabauty and rational points I: p-adic heights" *Duke Math. J.*, 167 (2018): 1981–2038.

[7] Balakrishnan, J.S. and Dogra, N. *SageMath code*, https://github.com/jbalakrishnan/QCII.

[8] Balakrishnan, J.S. and Kedlaya, K.S. and Kim, M., "Appendix and erratum to 'Massey products for elliptic curves of rank 1'" *J. Amer. Math. Soc.*, 24 (2011) 281–291.

[9] Beacom, J. "The unipotent Albanese map on elliptic and hyperelliptic curves." *ArXiv preprint 1711.03932*, (2017).

[10] Besser, A. "Coleman integration using the Tannakian formalism." *Math. Ann.*, 322 (2002): 19–48.

[11] Betts, L.A. "The motivic anabelian of local heights on abelian varieties" *ArXiv preprint* , (2018).

[12] Betts, L.A. and Dogra, N. "Ramification of unipotent path torsors and harmonic analysis on graphs" *Preprint*, (2019).

[13] Bosma, W. and Cannon, J. and Playoust, C. "The Magma algebra system. I. The user language" *J. Symbolic Comput.*, 24 (1997) 235-265.

[14] Bloch, S. and Kato, K. "L-functions and Tamagawa numbers of motives" *The Grothendieck Festschrift, Vol. I, Birkhäuser Boston*, (1990): 333-400.

[15] Chabauty, C. "Sur les points rationnels des courbes algébriques de genre supérieur à l'unité" *C. R. Math. Acad. Sci. Paris*, 212 (1941): 882-885.

[16] Coates, J. and Kim, M. "Selmer varieties for curves with CM Jacobians" *Kyoto J. Math.*, 50 (2010): 827–852.

[17] Coleman, R.F. "Effective Chabauty" *Duke Math. J.*, 52 (1985): 765–770.

[18] Coleman, R.F. and Gross, B.H. "p-adic heights on curves" *Algebraic Number Theory – in honor of K. Iwasawa*, (Berkeley, CA, 1987), edited by J. Coates et al., 73–81. Adv. Stud. Pure Math. 17, Tokyo: Math. Soc. 1989.

[19] Darmon, H. and Rotger, V. and Sols, I. "Iterated integrals, diagonal cycles and rational points on elliptic curves" *Publ. Math. Besançon.* Algèbre Théorie (2012): 19–46.

[20] Deligne, P. "Le groupe fondamental de la droite projective moins trois points" *Galois groups over* $\mathbb{Q}$ *(Berkeley, CA, 1987)*, 79–297, Math. Sci. Res. Inst. Publ. 16. New York: Springer, 1989.

[21] Deligne, P. *Équations différentielles à points singuliers réguliers*, Lecture Notes in Math. 163, Berlin–New York: Springer, 1970.

[22] Deligne, P. and Milne, J.S. "Tannakian categories" *Hodge cycles, motives, and Shimura varieties*, 101–228, Springer, Berlin, Heidelberg, 1982.

[23] Ellenberg, J. S. and Hast, D. R. "Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty." *ArXiv preprint 1706.00525*, (2017).

[24] Flach, M. "A finiteness theorem for the symmetric square of an elliptic curve" *Invent. Math.*, 109 (1992): 307-327.

[25] Flynn, E. V. "A flexible method for applying Chabauty's theorem" *Compositio Math.*, 105 (1997): 79–94.

[26] Fontaine, J.-M. and Perrin-Riou, B. "Autour des Conjectures de Bloch et Kato: Cohomologie Galoisienne et valeurs de fonctions L" *Motives (Seattle, WA, 1991)*, edited by Jannsen U., Kleiman S. and Serre J.P. 599–706. Proc. Sympos. Pure Math., Vol. 55. Providence, RI: American Mathematical Society, 1994.

[27] Freitas, N. and Le Hung, B. V. and Siksek, S. "Elliptic curves over real quadratic fields are modular" *Invent. Math.* 201, (2015): 159–206.

[28] Grothendieck, A. *Groupes de monodromie en géométrie algébrique. I, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I)* Lecture Notes in Math. 288, Berlin–New York: Springer, 1972.

[29] Hadian, M. "Motivic fundamental groups and integral points" *Duke Math. J.*, 160 (2011): 503–565.

[30] Hain, R.M. "The Geometry of the Mixed Hodge Structure on the Fundamental Group", In *Algebraic Geometry: Bowdoin 1985*, 247–282, Proc. Sympos. Pure Math., Vol. 46. Providence, RI :American Mathematical Society, 1987.

[31] Hain, R. M. "Relative weight filtrations on completions of mapping class groups", In *Groups of diffeomorphisms*, 309–368, Adv. Stud. Pure Math., Vol. 52. Math. Soc. Japan, Tokyo, 2008.

[32] Hain, R. M. and Matsumoto, M. "Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ *Compositio Math.*, 139 (2003), 119–167.

[33] Hain, R. M. and Matsumoto, M. "Galois actions on fundamental groups of curves and the cycle $C - C^-$ *J. Inst. Math. Jussieu*, 4 (2005), 363–403.

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

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

[36] Kim, M. and Tamagawa, A. "The l-component of the unipotent Albanese map" *Math. Ann.*, 340 (2008): 223-235.

[37] Kim, M. "Massey products for elliptic curves of rank 1" *J. Amer. Math. Soc.*, 23 (2010): 725–747.

[38] Kulesz, L. and Matera, G. and Schost, É. "Uniform bounds on the number of rational points of a family of curves of genus 2" *J. Number Theory*, 108 (2004) 141–267.

[39] Lang, S. *Algebra* , Grad. Texts in Math., 3rd ed. (2002), Berlin: Springer-Verlag.

[40] Liu, Q. *Algebraic geometry and arithmetic curves*, Oxf. Grad. Texts Math., London: Oxford University Press (2002).

[41] Manin, J.I. "The p-torsion of elliptic curves is uniformly bounded" *Izv. Math.*, 3 (1969):433–438.

[42] McCallum, W. and Poonen, B. "The method of Chabauty and Coleman", Explicit methods in number theory, Panor. Synthèses 36 (2012): 99–117.

[43] Nekovář, J. "On p-adic height pairings" *Séminaire de Théorie des Nombres, Paris, 1990–91*, Birkhäuser (1993): 127–202.

[44] Neukirch, J. and Schmidt, A. and Wingberg, K. *Cohomology of Number Fields, volume 323 of Grundlehren der Mathematischen Wissenschaften*, Berlin: Springer-Verlag, (2000).

[45] Oda, T. "A note on ramification of the Galois representation on the fundamental group of an algebraic curve, II" *J. Number Theory*, 53 (1995): 342-355.

[46] Olsson, M. C. "Towards non-abelian p-adic Hodge theory in the good reduction case" *Mem. Amer. Math. Soc.*, 210, Providence, RI: Amer. Math. Soc., 2011.

[47] Paulhus, J. "Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups", *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*,487–505, Open Book Ser., Berkeley CA: Math. Sci. Publ., 2013.

[48] Scharaschkin, V. "Local-global problems and the Brauer-Manin obstruction". *Thesis (Ph.D.)–University of Michigan*, 1999.

[49] Serre, J.P. "Galois cohomology, corrected reprint of the 1997 English edition. Translated from the French by Patrick Ion and revised by the author." *Springer Monogr. Math.*, Berlin: Springer-Verlag, 1997.

[50] Serre, J.P. *Lectures on the Mordell-Weil Theorem, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt*, Braunschweig: Friedrich Vieweg & Sohn, 1997.

[51] Shaska, T. "Some special families of hyperelliptic curves" *J. Algebra Appl.*, 74–89, 2004.

[52] Stein, W.A. and others, *Sage Mathematics Software (Version 7.6)*, 2017.

[53] Washington, L. C. "Galois cohomology" *Modular forms and Fermat's last theorem*, Berlin: Springer, 1997.

[54] Wojtkowiak, Z. "Cosimplicial objects in algebraic geometry" *Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991)*, NATO Sciences Series C: Mathematical and Physical Sciences 407. Dordrecht: Kluwer Acad. Publ., 1993.