Math. Res. Lett.
Volume 21, Number 04, 677–689, 2014

The first p-jet space of an elliptic curve: global functions and lifts of Frobenius

Alexandru Buium and Arnab Saha

We prove that there are no non-constant global functions and no lifts of Frobenius on the first p-jet space on an elliptic curve unless the elliptic curve itself has a lift of Frobenius.

1. Introduction and main results

The aim of this paper is to settle two basic issues in the theory of arithmetic differential equations that were (implicitly) left open in the papers on the subject, in particular in [2, 4, 6]. Our main result is Theorem 1.1 below. To explain our result, let us recall some basic concepts from loc. cit. Let p be an odd prime and let R be the p-adic completion of the maximum unramified extension of the ring $\mathbb{Z}_p$ of p-adic integers. By a p-formal scheme (over R) we understand a formal scheme over R with ideal of definition generated by p. A p-formal scheme over R is said to have a lift of Frobenius if it possesses an endomorphism over $\mathbb{Z}_p$ whose reduction mod p is the absolute p-power Frobenius. For any R-scheme of finite type X the paper [2] introduced a projective system of p-formal schemes $J^n(X)$, $n \geq 0$, called the p-jet spaces of X; morally their rings of global functions $\mathcal{O}(J^n(X))$ should be viewed as rings of *arithmetic differential equations* on X [4]. If X is a group scheme then $J^n(X)$ are groups in the category of p-formal schemes. See Section 2 below for a review of these spaces. Here is our main result; in its statement, by an elliptic curve over R we understand a smooth projective curve of genus 1 with an R-point.

Theorem 1.1. *Let E be an elliptic curve over R that does not have a lift of Frobenius. The following hold:*

(1) *$J^1(E)$ has no global functions except the elements of R, i.e., $\mathcal{O}(J^1(E)) = R$;*

(2) *$J^1(E)$ has no lift of Frobenius.*

Remark 1.2. The space $J^1(E)$ played a key role in the theory of arithmetic differential equations [2, 4, 6]; to give just one recent example, this space was used in [6] as the natural phase space for the arithmetic Painevé VI equation in Hamiltonian description. Somehow the above-mentioned theory could be developed by finding ways around proving a result such as Theorem 1.1; this theorem, however, further clarifies the situation.

Remark 1.3. To place the above theorem in context, let us mention that if X is a smooth projective curve of genus g over R then the following results were previously known:

(1) If $g = 0$ then $\mathcal{O}(J^n(X)) = R$ for $n \geq 0$;[3].

(2) If $g \geq 2$ then $J^n(X)$ is affine for $n \geq 1$ [3]; in particular $\mathcal{O}(J^1(X)) \neq R$ and $J^1(X)$ has a lift of Frobenius.

(3) If $g = 1$ (so $X = E$, an elliptic curve) the situation is as follows:

If E *does* have a lift of Frobenius then, trivially, $J^1(E) = \widehat{E} \times \widehat{\mathbb{G}_a}$ as groups (where $\mathbb{G}_a$ is the additive group) and hence $\mathcal{O}(J^1(E)) = \mathcal{O}(\widehat{\mathbb{G}_a}) \neq R$; also $J^1(E)$ possesses lifts of Frobenius (because both E and $\mathbb{G}_a$ do).

If E does *not* have a lift of Frobenius there is no non-zero homomorphism $J^1(E) \to \widehat{\mathbb{G}_a}$ (no *δ-character of order* 1); [4], p. 194, Proposition 7.15. On the other hand, there exists a non-zero homomorphism $\psi = \psi_{2,\mathrm{can}} : J^2(E) \to \widehat{\mathbb{G}_a}$ with the property that any other such homomorphism is an R-multiple of ψ. See [2] and [4] (p. 201, Definition 7.24 and p. 205, Theorem 7.34). This ψ can be called a *canonical δ-character of order* 2 *of* E and should be viewed as an arithmetic analogue of the "Manin map" of elliptic curves defined over a differential field [1, 8]. (This ψ is then unique up to multiplication by an element in $R^\times$; given an invertible 1-form on E, ψ can be further normalized and is unique with this normalization; we will not need this normalized version here but this is sometimes important, e.g., in [6].) Although Theorem 1.1 does not refer to $J^2(E)$ its proof will use $J^2(E)$ and the map ψ.

(4) If E is an elliptic curve over R, we have an extension

$$0 \to \widehat{\mathbb{G}_a} \to J^1(E) \to \widehat{E} \to 0$$

of groups in the category of p-formal schemes; [2]. Note that $J^1(E)$ is not, in general, the universal vectorial extension of E in the sense of [9], i.e., the map $\mathrm{Hom}(\widehat{\mathbb{G}_a}, \widehat{\mathbb{G}_a}) \to H^1(E, \mathcal{O})$ is not generally an

isomorphism. However, for E "sufficiently generic over R" the latter map *is* an isomorphism. The genericity required for that is that the value on E of the differential modular form f^1 in [4], pp. 193–194, be invertible in R. In this latter case, our Theorem 1.1 becomes, therefore, a theorem about the universal vectorial extension of E.

Remark 1.4. Assertion (1) in Theorem 1.1 is analogous to the situation in differential algebra where the differential algebraic first jet space (still denoted in this remark by) $J^1(E)$ of an elliptic curve E defined over a differential field F (and not defined over the constants of that field) has no other global functions except the elements of F; this follows from the fact that $J^1(E)$ is isomorphic, in this case, to the universal vectorial extension of E. See [1], p. 125. On the other hand, assertion (2) in Theorem 1.1 is in deep contrast with the situation in differential algebra where $J^1(E)$ always possesses a derivation on its structure sheaf that lifts the derivation on F; this is because, in this case, $J^2(E) \to J^1(E)$, has a section; the latter, in its turn, follows again trivially from the fact that $J^1(E)$ is the universal vectorial extension of E.

2. Review of p-jets and complements

We start by recalling some concepts from [2–4]. If A is a ring and B is an A-algebra then a *p-derivation* from A to B is a map of sets $\delta : A \to B$ such that the map $A \to W_2(B)$, $a \mapsto (a, \delta a)$ is a ring homomorphism, where $W_2(B)$ is the ring of Witt vectors on B of length 2. For any such δ the map $\phi : A \to B$, $\phi(a) = a^p \cdot 1 + p\delta a$ is a ring homomorphism. For any ring A we denote by $\widehat{A}$ the p-adic completion of A; a ring is called complete if it is its own completion. For any scheme X we denote by $\widehat{X}$ the p-adic completion of X. If $R = \widehat{\mathbb{Z}_p^{ur}}$ is as in the introduction then R has a unique p-derivation δ. We set $k = R/pR$; it is an algebraic closure of the prime field with p elements. For A an R-algebra and X a scheme or a p-formal scheme over R, we write $\overline{A} = A/pA = A \otimes_R k$ and $\overline{X} = X \otimes_R k$, respectively. All p-derivations on R-algebras are assumed compatible with that of R. A *prolongation sequence* of rings (over R) is an inductive system of R-algebras $(A^n)_{n \geq 0}$ together with p-derivations $\delta_n : A^n \to A^{n+1}$ such that δ_n restricted to A^{n-1} is δ_{n-1}. We usually write $\delta_n = \delta$ for all n. Recall the definition of p-formal scheme from the introduction. A prolongation sequence of p-formal schemes is a projective system of p-formal schemes $(X^n)_{n \geq 0}$ such that for any open set $U \subset X^0$ the inductive system $(\mathcal{O}(U^n))$ (where U^n is the pre-image of U in X^n) has a structure of prolongation sequence of rings,

and these structure are compatible when U varies. Prolongation sequences form a category in the obvious way. For any scheme of finite type X (or any p-formal scheme locally isomorphic to the p-adic completion of such a scheme) there exists a (necessarily unique up to isomorphism) prolongation sequence $(J^n(X))_{n\geq 0}$ with $J^0(X) = \widehat{X}$ and with the property that for any prolongation sequence (Y^n) and any morphism $Y^0 \to J^0(X)$ there exists a unique morphism of prolongation sequences from (Y^n) to $(J^n(X))$ extending $Y^0 \to J^0(X)$. The p-formal schemes $J^n(X)$ are called the p-jet spaces of X. If X is smooth over R so are $J^n(X)$; here, for p-formal schemes, smoothness means "locally isomorphic to the p-adic completion of a smooth scheme over R". Actually more is true: if X is affine and has an étale map $T : X \to \mathbb{A}^N$ then, viewing T as an N-tuple of elements in $\mathcal{O}(X)$, we have that $\mathcal{O}(J^n(X)) \simeq \mathcal{O}(X)[T', \dots, T^{(n)}]\hat{}$, where $T', \dots, T^{(n)}$ are N-tuples of variables that are mapped to $\delta T, \dots, \delta^n T$, respectively. For all of the above the references are [2–4]. In what follows, we add some complements to the above.

Let X be a smooth scheme or p-formal scheme over R. We may consider the prolongation sequence

$$\cdots \to J^n(X) \to J^{n-1}(X) \to \cdots \to J^2(X) \to J^1(X) \tag{2.1}$$

and also the prolongation sequence

$$\cdots \to J^n(J^1(X)) \to J^{n-1}(J^1(X)) \to \cdots \to J^1(J^1(X)) \to J^1(X). \tag{2.2}$$

By the universality property of the latter there is a morphism of prolongation sequences from 2.1 to 2.2; in particular there is a canonical morphism

$$c : J^2(X) \to J^1(J^1(X)). \tag{2.3}$$

See [6] where this played a key role by analogy with classical mechanics. We also denote by $\pi^i_X : J^i(X) \to J^{i-1}(X)$ the canonical projections. Note that π^1_X induces, by functoriality, a morphism $J^1(\pi^1_X) : J^1(J^1(X)) \to J^1(X)$. On the other hand, we have a morphism $\pi^1_{J^1(X)} : J^1(J^1(X)) \to J^1(X)$. We get an induced morphism

$$\pi^{11}_X := \pi^1_{J^1(X)} \times J^1(\pi^1_X) : J^1(J^1(X)) \to J^1(X) \times_{J^0(X)} J^1(X). \tag{2.4}$$

Assume in the following Lemma that X is smooth over R. Also Δ below denotes the diagonal embedding.

Lemma 2.1. *The following diagram is commutative and Cartesian:*

$$\begin{array}{ccc} J^1(J^1(X)) & \xrightarrow{\pi_X^{11}} & J^1(X) \times_{J^0(X)} J^1(X) \\ c \uparrow & & \uparrow \Delta \\ J^2(X) & \xrightarrow{\pi_X^2} & J^1(X). \end{array}$$

Proof. It is enough to prove the above in case X possesses an étale map $T : X \to \mathbb{A}^N$ to an affine space. View T as an N-tuple of elements in $\mathcal{O}(X)$. Denote by

$$\delta : \mathcal{O}(X)\hat{} \to \mathcal{O}(J^1(X)) = \mathcal{O}(X)[\delta T]\hat{},$$
$$\delta_1 : \mathcal{O}(J^1(X)) = \mathcal{O}(X)[\delta T]\hat{} \to \mathcal{O}(J^1(J^1(X))) = \mathcal{O}(X)[\delta T, \delta_1 T, \delta_1 \delta T]\hat{}$$

the universal p-derivations; and recall also that

$$\mathcal{O}(J^2(X)) = \mathcal{O}(X)[\delta T, \delta^2 T]\hat{};$$

[4], p. 75, Proposition 3.13. Then the diagram in the statement of the lemma is deduced from the following diagram of $\mathcal{O}(X)\hat{}$-algebras:

$$\begin{array}{ccc} \mathcal{O}(X)[\delta T, \delta_1 T, \delta_1 \delta T]\hat{} & \leftarrow & \mathcal{O}(X)[\delta T]\widehat{\otimes}_{\mathcal{O}(X)}\mathcal{O}(X)[\delta T], \\ \downarrow & & \downarrow \\ \mathcal{O}(X)[\delta T, \delta^2 T]\hat{} & \leftarrow & \mathcal{O}(X)[\delta T]\hat{} \end{array} \tag{2.5}$$

where the top horizontal arrow sends $\delta T \otimes 1 \mapsto \delta T$, $1 \otimes \delta T \mapsto \delta_1 T$, the bottom horizontal arrow is the inclusion, the left vertical arrow sends $\delta_1 T \mapsto \delta T$, $\delta_1 \delta T \mapsto \delta^2 T$, and the right vertical arrow sends $\delta T \otimes 1 \mapsto \delta T$, $1 \otimes \delta T \mapsto \delta T$. Diagram 2.5 is clearly commutative and Cartesian; this ends the proof. □

Assume in addition that $X = G$ is a smooth group scheme. Define

$$L_\delta(G) = Ker(J^1(G) \to J^0(G)). \tag{2.6}$$

This plays the role, in our theory, of arithmetic analogue of the Lie algebra of G. See [5]. However, if G is non-commutative, $L_\delta(G)$ is also non-commutative so we denote by 1 its identity element; if G is commutative so is $L_\delta(G)$ and

its identity element will be denoted by 0. The quotient map

$$J^1(G) \times J^1(G) \to J^1(G), \quad (a, b) \mapsto ba^{-1}$$

induces a morphism

$$q : J^1(G) \times_{J^0(G)} J^1(G) \to L_\delta(G).$$

Composing the latter with the morphism

$$\pi_G^{11} : J^1(J^1(G)) \to J^1(G) \times_{J^0(G)} J^1(G)$$

defined in 2.4, we get a morphism

$$l^1\delta^1 : J^1(J^1(G)) \to L_\delta(G). \tag{2.7}$$

The notation $l^1\delta^1$ is motivated by the analogy with Kolchin's logarithmic derivative in differential algebra [7]. Clearly π_G^{11} is a group homomorphism. If in addition G is commutative then q is also a group homomorphism so $l^1\delta^1$ is a group homomorphism. Assume again G not necessarily commutative. Then note that the restriction of $l^1\delta^1$ to $L_\delta(J^1(G))$ is the map $L_\delta(\pi_G^1) : L_\delta(J^1(G)) \to L_\delta(G)$ (induced by $J^1(\pi_G^1)$) composed with the antipode $L_\delta(G) \to L_\delta(G)$. Moreover, by Lemma 2.1, we have:

Corollary 2.2. $(l^1\delta^1)^{-1}(1) = J^2(G)$.

Remark 2.3. In our proof of Theorem 1.1, we will repeatedly use the following facts which are easily checked by passing to affine open covers. Let Z be a smooth p-formal scheme; in particular Z can be $J^n(X)$ where X is a smooth R-scheme. Then,

(1) $\mathcal{O}(Z)$ are flat over R and p-adically complete,

(2) The natural map $\overline{\mathcal{O}(Z)} \to \mathcal{O}(\overline{Z})$ is injective,

(3) $\mathcal{O}(Z \times \widehat{\mathbb{A}^1}) = \mathcal{O}(Z)[x]\hat{}$ where $\mathbb{A}^1 = Spec\ R[x]$.

We will also need the following lemmas.

Lemma 2.4. *Let $A \to B$ be a homomorphism between p-adically complete rings in which p is a non-zero divisor. If the induced map $\overline{A} \to \overline{B}$ is injective (respectively, finite) then the map $A \to B$ is injective (respectively, finite).*

Proof. A trivial exercise. □

Lemma 2.5. *Let $A \subset B$ be an integral extension of integral domains of characteristic zero with A integrally closed. Assume that there exists a derivation $\theta : B \to B$ such that*

(1) *$\theta A \subset A$ and*

(2) *A and B have the same constants with respect to θ, i.e., if $c \in B$ and $\theta c = 0$ then $c \in A$.*

Then for any $b \in B$ with $\theta b \in A$ we have $b \in A$.

Proof. Let $K \subset L$ be the extension of the corresponding fields of fractions and let $\theta : L \to L$ be the unique derivation extending $\theta : B \to B$; clearly $\theta K \subset K$. Let $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in K[t]$ be the minimal polynomial of b over K. Then $\theta(f(b)) = 0$ hence

$$(n\theta b + \theta a_1)b^{n-1} + ((n-1)a_1\theta b + \theta a_2)b^{n-2} + \cdots = 0.$$

By minimality of f we get $n\theta b + \theta a_1 = 0$ hence $\theta(nb + a_1) = 0$. By condition 2) we have $nb + a_1 \in K$ hence (since K has characteristic zero) $b \in K$. Since A is integrally closed, $b \in A$. □

3. Proof of Theorem 1.1

Proof of assertion 1. Step 1. Let $\mathbb{G}_a$ be the line $\mathbb{A}^1 = Spec\ R[x]$ with group structure defined by $x \mapsto x \otimes 1 + 1 \otimes x$. Then recall from [4], p. 127, that

$$L_\delta(E) \simeq \widehat{\mathbb{G}_a} = Spf\ R[x]\hat{} \tag{3.1}$$

we view the above isomorphism as an identification, so we have a closed immersion $\iota : \widehat{\mathbb{G}_a} \subset J^1(E)$. Let $A = \mathcal{O}(J^1(E))$. We then have a restriction map

$$\rho : A \to R[x]\hat{} \tag{3.2}$$

induced by the inclusion ι. Let $\overline{G}$ be the image of the multiplication by p map $[p] : \overline{J^1(E)} \to \overline{J^1(E)}$. Then the intersection $\overline{G} \cap \overline{\mathbb{G}_a}$ in $\overline{J^1(E)}$ is finite over k. So the addition map $\beta : \overline{G} \times \overline{\mathbb{G}_a} \to \overline{J^1(E)}$ is an isogeny and $\overline{G} \to \overline{E}$

is an isogeny. In particular $\overline{G}$ is an elliptic curve. Using Künneth's formula we get a map

$$\beta^* : \mathcal{O}(\overline{J^1(E)}) \to \mathcal{O}(\overline{G} \times \overline{\mathbb{G}_a}) = \mathcal{O}(\overline{G}) \otimes \mathcal{O}(\overline{\mathbb{G}_a}) = k[x]. \tag{3.3}$$

One trivially checks that the map 3.3 coincides with the restriction map

$$\bar{\iota}^* : \mathcal{O}(\overline{J^1(E)}) \to \mathcal{O}(\overline{\mathbb{G}_a}) = k[x] \tag{3.4}$$

induced by the inclusion $\bar{\iota} : \overline{\mathbb{G}_a} \subset \overline{J^1(E)}$. We conclude that the restriction map $\bar{\iota}^*$ is injective. By Remark 2.3, (2), the natural map $\overline{A} \to \mathcal{O}(\overline{J^1(E)})$ is injective. So the composition of the latter with $\bar{\iota}^*$ in 3.4 is an injective map

$$\overline{\rho} : \overline{A} \to \mathcal{O}(\overline{\mathbb{G}_a}) = k[x]. \tag{3.5}$$

Since, by Remark 2.3, (1), A is p-adically complete and flat over R it follows that ρ in 3.2 is injective, with torsion free cokernel.

Step 2. If $\overline{A} = k$ then, since A is flat over R, we get by induction that the map $R/p^nR \to A/p^nA$ is an isomorphism for all n. Since A is p-adically complete we get $A = R$ and assertion 1) in Theorem 1.1 follows. So we may (and will) assume, in what follows, that $\overline{A} \neq k$ and we seek a contradiction. Now since $\overline{A} \neq k$ it follows that $k[x]$ is finite over $\overline{A}$. In particular, $\overline{A}$ is finitely generated over k. Let $\overline{X} = Spec\ \overline{A}$ and let $\overline{\eta} : \overline{\mathbb{G}_a} \to \overline{X}$ be the map induced by the map $\overline{\rho}$ in 3.5. So $\overline{\eta}$ is a finite dominant map, hence it is surjective. Similarly consider the affine (a priori not necessarily Noetherian) p-formal scheme $X = Spf\ A$ and the map

$$\eta : \widehat{\mathbb{G}_a} \to X \tag{3.6}$$

induced by the map ρ in 3.2.

Step 3. Consider the action by translation

$$\widehat{\mathbb{G}_a} \times J^1(E) \to J^1(E). \tag{3.7}$$

Using Remark 2.3, (3), we get an induced map

$$A = \mathcal{O}(J^1(E)) \to \mathcal{O}(\widehat{\mathbb{G}_a} \times J^1(E)) = A[x]\hat{}. \tag{3.8}$$

One immediately checks that 3.8 induces an action

$$\mu : \widehat{\mathbb{G}_a} \times X \to X; \tag{3.9}$$

to prove coassociativity one uses, again, Remark 2.3, (3). Also clearly $\widehat{\mathbb{G}_a}$ acts on itself by translation and the map $\eta : \widehat{\mathbb{G}_a} \to X$ is equivariant because the action of $\widehat{\mathbb{G}_a}$ on itself is compatible with the action of $\widehat{\mathbb{G}_a}$ on $J^1(E)$ and hence with the action μ of $\widehat{\mathbb{G}_a}$ on X.

Step 4. By Step 3, $\overline{\mathbb{G}_a}$ acts on $\overline{X}$ and $\overline{\eta} : \overline{\mathbb{G}_a} \to \overline{X}$ is equivariant. Since $\overline{\eta}$ is surjective the action of $\widehat{\mathbb{G}_a}$ on $\overline{X}$ is transitive so $\overline{X}$ is a smooth affine curve. Since the group $\mathcal{O}(\overline{X})^\times$ of invertible global functions on $\overline{X}$ injects into $\mathcal{O}(\overline{\mathbb{G}_a})^\times = k^\times$ it follows that $\mathcal{O}(\overline{X})^\times = k^\times$ so $\overline{X} \simeq \overline{\mathbb{A}^1}$. So $\overline{A}$ identifies via $\overline{\rho}$ with a subring $k[\overline{s}]$ of $k[x]$ where $\overline{s} = \overline{s}(x) \in k[x]$ is some polynomial. We may assume that $\overline{s}(0) = 0$. Let $s \in A$ be any lift of $\overline{s}$ which, viewed as an element of $R[x]\hat{}$ satisfies $s(0) = 0$. Since A is flat over R we get, by induction, that the natural maps $R[s]/p^n R[s] \to A/p^n A$ are isomorphisms for all n. Since A is p-adically complete we get an isomorphism $R[s]\hat{} \simeq A$ which we view from now on as an equality; hence $A = R[s]\hat{} \subset R[x]\hat{}$, so $s = s(x)$ is a restricted power series. Note that by Lemma 2.4 the extension $A \subset R[x]\hat{}$ is integral. Also A is integrally closed because it is a regular ring.

Step 5. The action of $\widehat{\mathbb{G}_a}$ on X is given by a map $\mu^* : A \to A[x]\hat{}$,

$$\mu^*(a) = a + (Da)x + \cdots,$$

where $D : A \to A$ is an R-derivation. By the equivariance of η we have a commutative diagram

$$\begin{array}{rcl} A & \xrightarrow{\mu^*} & A[x]\hat{} \\ \rho \downarrow & & \downarrow \rho \otimes 1 \\ R[x]\hat{} & \longrightarrow & R[x]\hat{}\widehat{\otimes}R[x]\hat{} \end{array}$$

where ρ is the inclusion and the bottom arrow sends $x \mapsto x \otimes 1 + 1 \otimes x$, hence sends any $g \in R[x]\hat{}$ into $g \otimes 1 + \frac{dg}{dx} \otimes x + \cdots$. In particular, we get

$$a \otimes 1 + (Da) \otimes x + \cdots = a \otimes 1 + \frac{da}{dx} \otimes x + \cdots$$

for $a \in A$; so $Da = \frac{da}{dx}$, $a \in A$. So $\frac{d}{dx}$ defines an R-derivation $R[x]\hat{} \to R[x]\hat{}$ which sends $R[s]\hat{}$ into itself. Furthermore $R[s]\hat{}$ and $R[x]\hat{}$ have the same constants with respect to this derivation (the constant ring is R in both cases). Since $R[s]\hat{}$ is integrally closed and $R[s]\hat{} \subset R[x]\hat{}$ is integral, and since

$\frac{dx}{dx} = 1 \in R[s]\hat{}$ it follows, by Lemma 2.5 that $x \in R[s]\hat{}$, hence $A = R[x]\hat{}$, in other words the restriction homomorphism $\rho : \mathcal{O}(J^1(E)) \to \mathcal{O}(\widehat{\mathbb{G}_a})$ is an isomorphism.

Step 6. Exactly as in Step 1 we get that the restriction map

$$\mathcal{O}(J^1(E) \times J^1(E)) \to \mathcal{O}(\widehat{\mathbb{G}_a} \times \widehat{\mathbb{G}_a}) = \mathcal{O}(\widehat{\mathbb{G}_a}) \hat{\otimes} \mathcal{O}(\widehat{\mathbb{G}_a}) \tag{3.10}$$

is injective. Since, by Step 5, the restriction homomorphism $\rho : \mathcal{O}(J^1(E)) \to \mathcal{O}(\widehat{\mathbb{G}_a})$ is an isomorphism we conclude that 3.10 is an isomorphism. Let $\psi_1 \in \mathcal{O}(J^1(E))$ be the unique function whose restriction to $\widehat{\mathbb{G}_a}$ is x. Then ψ_1 defines a homomorphism $J^1(E) \to \widehat{\mathbb{G}_a}$ (hence a non-zero δ-character of order 1 in the sense of [4], p. 190). By [4], p. 194, Proposition 7.15, E has a lift of Frobenius, a contradiction. This ends the proof of assertion 1 in our Theorem. □

Proof of assertion 2. Step 1. We start by assuming that $J^1(E)$ has a lift of Frobenius and we shall derive a contradiction. By the universality property of p-jets the lift of Frobenius on $J^1(E)$ induces a section $s : J^1(E) \to J^1(J^1(E))$, in the category of p-formal schemes, of the canonical projection $\pi^1_{J^1(E)} : J^1(J^1(E)) \to J^1(E)$. We may (and will) assume $s(0) = 0$. Consider the homomorhism

$$l^1\delta^1 : J^1(J^1(E)) \to L_\delta(E) = \widehat{\mathbb{G}_a}$$

defined in 2.7. By Corollary 2.2 we have that $Ker(l^1\delta^1) = J^2(E)$. Now the composition

$$(l^1\delta^1) \circ s : J^1(E) \to \widehat{\mathbb{G}_a}$$

defines a function in $\mathcal{O}(J^1(E))$ sending 0 into 0. By the first assertion of Theorem 1.1, $(l^1\delta^1) \circ s$ is a constant function, hence $s = 0$, hence s factors through $Ker(l^1\delta^1) = J^2(E)$; in other words s induces a section $\sigma : J^1(E) \to J^2(E)$ of the canonical projection $\pi^2_E : J^2(E) \to J^1(E)$; this is a section in the category of p-formal schemes (not a priori a group homomorphism). Also $\sigma(0) = 0$.

Step 2. Recall from [2], Proposition 2.2 and Lemma 2.3, that $Ker(\pi^2_E)$ is isomorphic to $\widehat{\mathbb{G}_a}$. Fix a point $P \in J^1(E)(R)$. The morphism of formal schemes $f_P : J^1(E) \to J^2(E)$ defined by

$$f_P(Q) = \sigma(P + Q) - \sigma(P) - \sigma(Q)$$

factors through $Ker(\pi_E^2)$ hence gives rise to a morphism (still denoted by)

$$f_P : J^1(E) \to \widehat{\mathbb{G}_a} = \widehat{\mathbb{A}^1}.$$

Since, by assertion 1) of the Theorem, $\mathcal{O}(J^1(E)) = R$ we must have $f_P \in R$. Since $f_P(0) = 0$ we get $f_P = 0$. Since P was arbitrary it follows that σ is a group homomorphism. Then the morphism $\chi : J^2(E) \to J^2(E)$ defined by

$$\chi(P) = P - \sigma(\pi_E^2(P))$$

is a homomorphism. Clearly χ factors through a homomorphism (still denoted by) $\chi : J^2(E) \to Ker(\pi_E^2) = \widehat{\mathbb{G}_a}$ and $Ker(\chi) = Im(\sigma)$ as formal schemes. In particular, χ gives rise to a δ-character of order 2 of E. So $\chi = c \cdot \psi$ for some $c \in R$, where $\psi = \psi_{2,\mathrm{can}}$ is a canonical δ-character of order 2 of E; [4], p. 201, Definition 7.24, and p. 205, Theorem 7.34.

Step 3. Let Z be the subscheme of $J^2(Y)$ defined by the ideal generated by $\chi \in \mathcal{O}(J^2(E))$. Then

$$\overline{Z} \to \overline{J^1(E)} \tag{3.11}$$

is an isomorphism. Let Y be an affine open subset of E such that $\mathcal{O}(Y)$ has an étale coordinate $T \in \mathcal{O}(Y)$. Now by [4], Theorem 7.22 plus equation (7.73), we have identifications

$$\mathcal{O}(J^1(Y)) = \mathcal{O}(Y)[T']\hat{}, \quad \mathcal{O}(J^2(Y)) = \mathcal{O}(Y)[T', T'']\hat{},$$

where T', T'' are new variables, $T' = \delta T$, $T'' = \delta^2 T$, and

$$\psi \in \mathcal{O}(Y)[T']\hat{} + p\mathcal{O}(Y)[T', T'']\hat{}.$$

Hence the reduction mod p, $\overline{\chi}$, of $\chi = c\psi$ belongs to $\mathcal{O}(\overline{Y})[T']$ and so the map

$$\mathcal{O}(\overline{Y})[T'] \to \frac{\mathcal{O}(\overline{Y})[T', T'']}{(\overline{\chi})} \simeq \frac{\mathcal{O}(\overline{Y})[T']}{(\overline{\chi})}[T'']$$

induced by 3.11 is not an isomorphism. This is a contradiction, which concludes the proof. □

Acknowledgment

The work on this paper was partially done while the first author was visiting the Australian National University in Canberra; special thanks go to James Borger for his hospitality and for inspiring conversations. Also the first author would like to acknowledge partial support from the NSF through grant DMS 0852591.

References

[1] A. Buium, *Differential algebra and diophantine geometry*, Hermann, Paris, 1994.

[2] A. Buium, *Differential characters of Abelian varieties over p-adic fields*, Invent. Math., **122** (1995), 309–340.

[3] A. Buium, *Geometry of p-jets*, Duke J. Math. **82**(2) (1996), 349–367.

[4] A. Buium, *Arithmetic differential equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.

[5] A. Buium and T. Dupuy, *Arithmetic differential equations on GL_n, II: arithmetic Lie theory*, preprint.

[6] A. Buium and Yu. I. Manin, *Arithmetic differential equations of Painlevé VI type*, `arXiv`.

[7] E.R. Kolchin, *Differential algebra and algebraic groups*. Pure and Applied Mathematics, Vol. 54. Academic Press, New York–London, 1973. xviii+446 pp.

[8] Yu.I. Manin, *Algebraic curves over fields with differentiation*, Izv. Akad. Nauk SSSR, Ser. Mat. **22** (1958), 737–756 = AMS Translations Series 2, **37** (1964), 59–78.

[9] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, LNM 370, Springer 1974.

Department of Mathematics and Statistics
University of New Mexico
Albuquerque, NM 87131
USA
E-mail address: `buium@math.unm.edu`

Mathematical Sciences Institute
Australian National University, ACT 2601
Australia
E-mail address: arnab.saha@anu.edu.au

Received August 3, 2013