Geometry of p-jets, I

Alexandru Buium

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-53225 Bonn

Germany

MPI / 94-127

Geometry of $p-$jets, I

Alexandru Buium

Introduction. In a series of papers [B1-B4] the author developed a differential algebraic method which was used, among others, to prove diophantine results over function fields. In this paper we start developing an analogue of that method which is designed to work over number fields. The main point in our differential algebraic method was the geometric study of "jet spaces" along a fixed derivation of the ground field. Of course, there is no non zero derivation on a number field, so we cannot speak in the arithmetic context about usual jets. Instead of derivations we will use certain natural non additive maps on rings of integers, which we call $p-$derivations. The resulting "jet spaces" will be called *$p-$jet spaces*. The present paper is devoted mainly to applications of this technique to curves of genus $g \geq 2$ (and $g = 0$.) In a subsequent paper [B5] we shall investigate curves of genus $g = 1$, and more generally abelian varieties.

The present paper has two sections. In the first section we give a quick exposition of the theory in its simplest form: we shall only look at the geometry of "first order $p-$jets", and even this will be done in a special case. This case will be however enough to prove the following "quantitative version of the Manin-Mumford conjecture":

Theorem A. *Let $X \to J$ be the Abel map defined over a number field K of a smooth curve of genus $g \geq 2$ into its Jacobian. Let $\wp$ be a prime of K with $p = char\ \wp > 2g$. Assume that $K/\mathbf{Q}$ is unramified at $\wp$ and X/K had good reduction at $\wp$. Let K^a be the algebraic closure of K. Then*

$$\sharp(X(K^a) \cap J(K^a)_{tors}) \leq p^{4g} \cdot 3^g \cdot [p(2g-2) + 6g] \cdot g!$$

A few remarks are in order. The finiteness of $\sharp(X(K^a) \cap J(K^a)_{tors})$ was conjectured by Manin and Mumford and first proved by Raynaud [Ray1]. In [Co1] Coleman considered the special case when J has complex multiplication and, assuming in addition that X/K has ordinary reduction at $\wp$, he proved that $\sharp(X(K^a) \cap J(K^a)_{tors}) \leq p \cdot g$. (By the way, as shown by an example in [Co1] the bound $p \cdot g$ fails in general, in the non complex multiplication case.) Coleman's proof was based on his deep theory of $p-$adic Abelian integrals [Co1] and heavily relies on both the complex multiplication assumption and the ordinarity assumption (cf. the discussion in [Co1], p. 157).

Our strategy of proving Theorem A is the following. First we prove a "non ramified version" of Theorem A: more precisely we prove that Theorem A holds with K^a replaced by the maximal extension K^p of K contained in K^a which is unramified above p. Actually such a result will be proved to hold without the hypothesis $p > 2g$; cf. Theorem (1.11). The proof of this will be entirely elementary and self contained; here is where we shall use our first order p–jets by imitating our approach to the function field case [B4] [BV]. Note also that, although we shall be working with reduction p^2, our arguments will be quite different from (and simpler than) Raynaud's [Ray1] [Ray2]. In particular our arguments may be used to give an easy proof (which is in addition effective) of his "infinitesimal" results there.

Now Theorem A trivially follows from its "non ramified version" plus a result of Coleman's [Co2], p.615, which says that for $p > 2g$ we have $X(K^a) \cap J(K^a)_{tors} \subset J(K^p)$. (Note that this latter result of Coleman's depends again on his theory of p–adic Abelian integrals.)

The second section of the paper is devoted to developing a theory of "higher p–jets". Our main application here is a p–adic analogue of our "δ–polynomial affine embedding theorem for projective curves" in [B2]. In what follows we explain our main concepts and results.

Let R denote (throughout the paper) an absolutely unramified complete discrete valuation ring whith algebraically closed residue field k of characteristic p. Recall from [S] p.39 that R has a unique lifting $\phi : R \to R$ of the Frobenius of k. Define the map $\delta : R \to R$ by the formula $\delta x = (\phi(x) - x^p)/p$. Morally δ will play, in our approach, the role of a derivation. As for usual derivations, for any $x \in R$ we write $x', x'', ..., x^{(n)}$ in place of $\delta x, \delta^2 x, ..., \delta^n x$.

Now let X/R be a scheme of finite type. An R–valued function $\varphi : X(R) \to R$ will be called a *δ–formal function* on $X(R)$ if any point in $X(R)$ has an affine open neighbourhood $U \subset X$ where φ can be written as

$$\varphi(P) = \Phi(u(P), u(P)', u(P)'', ..., u(P)^{(n)}, ...), \quad P \in U(R)$$

where $u = (u_1, ..., u_N)$ is an N–uple of regular functions on U (so $u(P) \in R^N$) and Φ is an element in the p–adic completion of the ring of polynomials with coefficients in R in infinitely many indeterminates. (These are the analogues of δ–polynomial functions in [B1-B4].) Then we shall prove

Theorem B. *Let X/R be a smooth projective curve of genus $g \geq 2$. Then there exists finitely many δ–formal functions $\varphi_1, ..., \varphi_N$ on $X(R)$ such that the map $\varphi := (\varphi_1, ..., \varphi_N) : X(R) \to \mathbf{A}^N(R) = R^N$ is injective and any other δ–formal function ψ on $X(R)$ can be written as $\psi = \theta \circ \varphi$ for a suitable δ–formal function $\theta : \mathbf{A}^N(R) = R^N \to R$. In contrast, if X/R is a projective space then any δ–formal function $\psi : X(R) \to R$ is constant.*

Actually we shall be able to take the φ_i's above of "order one" (i.e. locally given by $\Phi(u(P), u(P)')$.

The second section of the paper will also contain a discussion of the relation between $p-$jets and the "Greenberg transform". Recall that to any scheme of finite type X/R one can associate a (proalgebraic) $k-$scheme $\tilde{X}$ called the Greenberg transform such that $X(R) \simeq \tilde{X}(k)$ functorially in X (this is a construction going back to Lang's thesis [L1], [L2] and to Greenberg's paper [Gr]). We will prove that for X/R smooth, the reduction modulo p of our "infinite $p-$jet space" of X coincides with the Greenberg transform $\tilde{X}$; cf. Theorem (2.10). This may be used to shed a new light on Greenberg transforms of curves. It will follow for instance that if X/R is a smooth projective curve of genus at least 2 then its Greenberg transform $\tilde{X}$ is an affine scheme, and if $\mathcal{O}^\infty(X)$ denotes the ring of $\delta-$formal functions on $X(R)$ then $\mathcal{O}(\tilde{X}) \simeq \mathcal{O}^\infty(X) \otimes k$. In contrast, if X is a projective space over R then its Greenberg transform $\tilde{X}$ has only constant global regular functions; i.e. $\mathcal{O}(\tilde{X}) = k$.

Acknowledgement. The present paper was written while the author was a member of the Institute for Advanced Study in 1993/94 (with support from the NSF Foundation, grant DMS 9304580) and while he was visiting the Max Planck Institute of Mathematics in Bonn in 1994/95. The author is grateful to E.Bombieri, R.Coleman and P. Deligne for their suggestions and comments as well as to F.Pop and F.Voloch for many useful "$p-$adic" discussions. The author would also like to thank the referee for his remarks on an earlier version of the paper.

1. First order $p-$jets and torsion points.

(1.1) Let $f : A \to B$ be a ring homomorphism. Let $W_2(B)$ be the ring of Witt vectors of length 2 with coordinates in B [S]. By a *$p-$derivation* (of f) we understand a map of sets $\delta : A \to B$ such that the induced map

$$(f, \delta) : A \to B \times B = W_2(B), \quad x \mapsto (f(x), \delta(x))$$

is a ring homomorphism. Using the explicit ring structure of $W_2(B)$, this condition means that for $x, y \in A$ we have:

$$\delta(x + y) = \delta x + \delta y + \Phi_p(f(x), f(y))$$

$$\delta(xy) = f(x)^p \delta y + f(y)^p \delta x + p \delta x \delta y$$

where $\Phi_p(X, Y)$ is the polynomial with integer coefficients $(X^p + Y^p - (X + Y)^p)/p$; so we see in particular that δ is non additive.

(1.2) **Remark.** If in the above definition we replace $W_2(B)$ by the ring of dual numbers $D_2(B) = B \oplus B\epsilon$, $\epsilon^2 = 0$ then we get the usual notion of *derivation*, which justifies our terminology.

The "main hope" beyond the present paper is that much of the theory done in [B1-B4] (as well as much of the "differential algebra" in [K], [R]) can be developped with

$p-$derivations in place of usual derivations; the applications one expects are $p-$adic analogues of the results in those papers. Our main results stated in the Introduction are samples of such analogues.

(1.3) Assume now R, k, ϕ, δ are as in the Introduction. Then $\delta : R \to R$ is trivially seen to be a $p-$derivation of the identity.

Note that $\delta p = 1 - p^{p-1}$ is invertible in R; more generally we have:

$$(p^n, \delta p^n, ..., \delta^i p^n)R = p^{n-i}R, \quad 0 \leq i \leq n$$

So if we assume that $B \neq 0$ is an $R-$algebra with a $p-$derivation extending the derivation on R, then the map $R \to B$ is injective (indeed p is not nilpotent in B, as shown by taking $i = n$ in the equality above).

(1.4) Now we pass to the construction of first order $p-$jet spaces. Let R, k, ϕ, δ be as above and assume we are given a finitely generated $R-$algebra $f : R \to B$. We shall construct a finitely generated $B-$algebra $f^1 : B \to B^1$ and a $p-$derivation (still denoted by) $\delta : B \to B^1$ of f^1 having the following universality property: for any ring homomorphism $g : B \to C$ and any $p-$derivation $\partial : B \to C$ such that $\partial \circ f = g \circ \delta : R \to C$, there exists a unique ring homomorphism $u : B^1 \to C$ such that $g = u \circ f^1$ and $\partial = u \circ \delta$. This B^1 will be called the *first order $p-$jet algebra* of B. The construction goes as follows. Write $B = R[T]/I$ where $T = (T_i)$ is a family of indeterminates and I is an ideal. Introduce a new family of indeterminates T', indexed by the same set as T, and prolong $\phi : R \to R$ to a ring homomorphism (also denoted by) $\phi : R[T] \to R[T, T']$ by requiring that

$$\phi(T_i) = T_i^p + pT_i'$$

Then define the map (still denoted by)

$$\delta : R[T] \to R[T, T']$$

by the formula

$$\delta F = (\phi(F) - F^p)/p, \quad F \in R[T]$$

This map is a $p-$derivation of the inclusion, prolonging our original $\delta : R \to R$. Finally set $B^1 = R[T, T']/(I, I')$ where I' is the image of I under δ. The map $\delta : R[T] \to R[T, T']$ induces a $p-$derivation $\delta : B \to B^1$. It is trivial to check that this construction satisfies the universality property mentioned above.

Note that the above construction does not behave well under localisation: if $f \in B$ then the natural map $(B^1)_f \to (B_f)^1$ need not be an isomorphism (take the case when $B = R[T]$ is a polynomial ring and $f = T$). However it is an easy exercise to check that if p is nilpotent in B then the map $(B^1)_f \to (B_f)^1$ is an isomorphism.

Consequently, if X/R is a scheme of finite type on which p is nilpotent we may define the *first order $p-$jet space* of X as the scheme X^1 obtained by gluing the schemes $Spec\ (\mathcal{O}(U)^1)$ for various affine open sets $U \subset X$. The construction $X \mapsto X^1$ is functorial

(X^1 represents the functor which associates to each scheme Z the set of all pairs (u, ∂) consisting of a morphism of schemes $u : Z \to X$ and a $p-$derivation $\delta : \mathcal{O}_X \to u_*\mathcal{O}_Z$; by the latter we understand a map of sheaves of sets inducing on each open set a $p-$derivation). Moreover if G/R is a group scheme then G^1/R is naturally a group scheme.

Finally, if X/R is a scheme of finite type on which p is not necessarily nilpotent, we set $R_1 = R/p^2R$ and $X_1 := X \otimes_R R_1$ and we may consider the first order $p-$jet space of X_1 which we denote by X_0^1 (in symbols $X_0^1 := (X_1)^1$). Note that p vanishes on X_0^1 (because $\delta(p^2)$ has valuation 1 in R). Hence we have a map $X_0^1 \to X_0$ where we set $X_0 = X \otimes k$. We have in this situation a "lifting map"

$$\nabla_0^1 : X(R) \to X_0^1(k)$$

defined as follows: for any point $P : Spec\ R \to X$ the $p-$derivation δ on R induces a $p-$derivation from the ring of regular functions in a neighbourhood of P in X_1 to k, hence by the universality property, we are provided with a $k-$point of X_0^1.

In what follows, for any $k-$scheme Y we denote by $F_Y : Y \to Y$ the absolute Frobenius endomorphism and by $FT(Y/k)$ the "Frobenius tangent scheme" $Spec\ S(F_Y^*\Omega_{Y/k}) \to Y$ (Frobenius tangent bundle, if Y is smooth).

Proposition (1.5). *Let X/R be a scheme of finite type, which is smooth along X_0. Then $X_0^1 \to X_0$ is a (Zariski locally trivial) principal homogenous space for the Frobenius tangent bundle $FT(X_0/k) \to X_0$. If in addition X/R is a group scheme then $Ker(X_0^1 \to X_0)$ is a vector group.*

Proof. The fact that X_0^1 is a principal homogenous space for the Frobenius tangent bundle (in the mere sense of functors to the category of sets) follows easily using the description of the functor that X_0^1 represents (1.4) plus the following trivial observation. Let $f : A \to B$ be a ring homomorphism where B has characteristic p. Then the set of $p-$derivations of f is either empty or a principal homogenous space for the group of all (usual) derivations of $f \circ F_B$ (F_B =Frobenius of B). To check that $X_0^1 \to X_0$ has local sections in the Zariski topology, we may assume X is affine. Then it is sufficient to prove Lemma (1.6) below. The assertion about the case when X is a group scheme may be checked via an argument similar to the one in [B1], pp1397-1398.

Lemma (1.6). *Assume we are given a finitely generated algebra $f : R \to B$ and its first order $p-$jet algebra $f^1 : B \to B^1$. Assume B is smooth over R at any prime of B containing p. Then for any integer $m \geq 1$ the natural projection $\pi : B \to B/p^mB$ factors through $f^1 : B \to B^1$.*

Proof. Consider the commutative diagram

$$\begin{array}{rcl} R & \xrightarrow{f} & B \\ (f,\delta)\downarrow & & \| \\ W_2(B) & \xrightarrow{p_1} & B \\ W_2(\pi)\downarrow & & \downarrow \pi \\ W_2(B/p^mB) & \xrightarrow{p_1} & B/p^mB \end{array}$$

Since the kernel of $W_2(B/p^mB) \xrightarrow{p_1} B/p^mB$ is nilpotent it follows, by smoothness of f in a neighbourhood of $Spec\ B/pB$ in $Spec\ B$, that there exists a ring homomorphism $\sigma : B \to W_2(B/p^mB)$ such that $\sigma \circ f = W_2(\pi) \circ (f,\delta)$ and $p_1 \circ \sigma = \pi$. So $p_2 \circ \sigma$ is a $p-$derivation of π prolonging δ. By the universality property (1.4), there exists a ring homomorphism $u : B^1 \to B/p^mB$ such that $u \circ f^1 = \pi$ (and $u \circ \delta = p_2 \circ \sigma$). This closes the proof of the Lemma and hence of Proposition (1.5).

In what follows it is convenient to use the following definition. A scheme X/R will be called *infinitesimally trivial* if the absolute Frobenius F_{X_0} of X_0 lifts to an endomorphism of the scheme X_1 compatibly with the unique lifting of the Frobenius of k to R_1. (Of course this notion depends only on X_1.) It will be called *infinitesimally non trivial* otherwise. Similar definitions can be given for group schemes, by requiring that the lifting of the Frobenius be compatible with multiplication, inverse and unit, in the obvious sense.

Proposition (1.7). *Assume we are in the situation of (1.5). Then the map $X_0^1 \to X_0$ has a section (equivalently X_0^1 is X_0-isomorphic to the "Frobenius tangent bundle" $FT(X_0/k)$) if and only if X/R is infinitesimally trivial. And the same statement holds in the category of group schemes.*

Proof. By the universlity property (1.4) there is a section of $X_0^1 \to X_0$ if and only if there is a $p-$derivation of $\mathcal{O}_{X_1} \to \mathcal{O}_{X_0}$ prolonging the $p-$derivation on R. Giving such a $p-$derivation ∂ is equivalent to giving a lifting $\phi : X_1 \to X_1$ of the Frobenius of X_0 compatible with the unique lifting of the Frobenius on R_1 (via the formula $\phi(x) = x^p + p\partial x$, well defined due to flatness) which closes the proof.

We will need the following important remark of Raynaud which is an easy consequence of basic properties of the Cartier operator:

Proposition (1.8). *(Raynaud [Ray2], I.5.4) Let X/R be a smooth projective curve of genus at least 2. Then X/R is infinitesimally non trivial.*

For the next Proposition we need the following easy consequence of known properties of vector bundles on curves.

Lemma (1.9). *Consider an exact sequence of vector bundles on a smooth projective curve X_0 of genus $g \geq 2$ over k:*

$$0 \to \mathcal{O}_{X_0} \to E \to L \to 0$$

where L is a line bundle of degree $> (2g-2)/p$. If the extension is non split then E is ample.

Proof. By [MD], Corollaire 3, p. 45 if E is not ample then the pull back by a suitable power of Frobenius of the sequence splits. But due to the condition on the degree of L the maps induced by Frobenius

$$Ext^1(L, \mathcal{O}_{X_0}) \to Ext^1(F^*L, \mathcal{O}_{X_0}) \to Ext^1(F^{*2}L, \mathcal{O}_{X_0}) \to \ldots$$

are injective by the criterion [T], Theorem 15, p. 73 (and definition 11, p.79). So if our sequence is non split, its pull back under a power of Frobenius cannot split, a contradiction. The Lemma is proved.

Proposition (1.10). *Let X/R be a smooth projective curve of genus at least 2. Then the scheme X_0^1 is affine.*

Proof. Recall by (1.5) that $X_0^1 \to X_0$ is a Zariski locally trivial principal homogenous space for the Frobenius tangent bundle $FT(X_0/k) = Spec(S(F^*\omega_{X_0}))$. So it is defined by some class

$$\eta \in H^1(X_0, F^*\omega_{X_0}^{-1})$$

This class is non zero by (1.7) and (1.8). But on the other hand the principal homogenous space corresponding to η has the following description. One considers the extension

$$0 \to \mathcal{O}_{X_0} \to E \to F^*\omega_{X_0} \to 0$$

corresponding to the image of η under the natural isomorphism

$$H^1(X_0, F^*\omega_{X_0}^{-1}) \simeq Ext(F^*\omega_{X_0}, \mathcal{O}_{X_0})$$

one considers the projective bundle $\mathbf{P}(E) \to X_0$ and one consider the divisor $D = \mathbf{P}(F^*\omega_{X_0}) \subset \mathbf{P}(E)$. Then the principal homogenous space corresponding to η identifies with the complement $\mathbf{P}(E) \backslash D$. Since the extension above is non split, we get by Lemma (1.9) that E is ample, i.e. that $\mathcal{O}_{\mathbf{P}(E)}(1)$ is ample. But D belongs to the linear system of $\mathcal{O}_{\mathbf{P}(E)}(1)$ hence D is ample, hence X_0^1 is affine and we are done.

Now, as explained in the Introduction, in order to prove Theorem A it is enough to prove the following "non ramified version" of it:

Theorem (1.11). *Let X/R be a smooth projective curve of genus $g \geq 2$ possessing an $R-$rational point and embedded via this point into its Jacobian J/R. If $p \geq 3$ then*

$$\sharp(X(R) \cap J(R)_{tors}) \leq p^{4g} \cdot 3^g \cdot [p(2g-2)+6g] \cdot g!$$

If $p = 2$ then the same estimate holds with p^{4g} replaced by 64^g.

Proof. The argument will be parallel to the one in [BV] or [B4] where we treated the function field case.

Set $\Gamma := J(R)_{tors}$ and consider the map

$$\nabla_0^1 : J(R) \to J_0^1(k)$$

The restriction of ∇_0^1 to Γ is injective if $p \geq 3$ and has kernel of order $\leq 4^g$ if $p = 2$; indeed the kernel of the reduction map $J(R) \to J_0(k)$ is torsion free for $p \geq 3$ and contains only points of order 2 if $p = 2$ (see [Sil], Chapter IV, Theorem (6.1) which extends with identical proof to abelian varieties of arbitrary dimension).

Note that by (1.5) J_0^1 is an extension of J_0 by a vector group so $B := pJ_0^1$ coincides with the maximal abelian subvariety of J_0^1 and the projection $B \to J_0$ is an isogeny through which the multiplication by p on J_0 factors; so the degree of $B \to J_0$ is at most p^{2g}.

Claim. The image of $\nabla_0^1(\Gamma)$ under the homomorphism $J_0^1(k) \to J_0^1(k)/B(k)$ has cardinality at most p^{2g}.

Indeed we will show that $\sharp(\Gamma/p\Gamma) \leq p^{2g}$. Write $\Gamma = \Gamma_p \oplus \Gamma_{p'}$ where Γ_p is the $p-$primary torsion of Γ and $\Gamma_{p'}$ is the prime to p torsion subgroup of Γ. Since $p\Gamma_{p'} = \Gamma_{p'}$ we only have to check that $\sharp(\Gamma_p/p\Gamma_p) \leq p^{2g}$. Let $\Gamma[p^n]$ be the subgroup of Γ consisting of all elements annihilated by p^n. If L is the algebraic closure of the quotient field of R then $\Gamma[p^n] \subset J(L)[p^n] \simeq (\mathbf{Z}/p^n\mathbf{Z})^{2g}$ hence the inverse image of $\Gamma[p^n]$ in $\mathbf{Z}^{2g}$ is a free abelian group of rank $\leq 2g$ hence $\Gamma[p^n]/\Gamma[p^n] \cap p\Gamma_p$ is an $\mathbf{F}_p-$linear space of dimension at most $2g$ which implies that the same holds for $\Gamma/p\Gamma = \bigcup_n (\Gamma[p^n]/\Gamma[p^n] \cap p\Gamma_p)$ and the Claim is proved.

By the Claim above we have

$$\nabla_0^1(X(R) \cap \Gamma) \subset X_0^1(k) \cap [\bigcup_{i=1}^{p^{2g}} (B(k) + b_i)]$$

for some $b_1, ..., b_{p^{2g}} \in J_0^1(k)$. which implies in particular that

$$\sharp(X(R) \cap \Gamma) \leq C \cdot \sum_{i=1}^{p^{2g}} \sharp[(B(k) + b_i) \cap X_0^1(k)]$$

where $C = 1$ if $p \geq 3$ and $C = 4^g$ if $p = 2$. On the other hand each $B_i := B + b_i$ is complete while X_0^1 is affine by (1.10). Since both are closed subvarieties in J_0^1 their intersection is both complete and affine so it is finite, i.e. the set $B_i(k) \cap X_0^1(k)$ is finite. Now we want to estimate the cardinality of this set. By (1.5) X_0^1 and J_0^1 are Zariski locally trivial principally homogenous spaces for the Frobenius tangent bundles of X_0 and J_0 respectively. Let $\eta_X \in H^1(X_0, F^*\omega_{X_0})$ and $\eta_J \in H^1(J_0, F^*\Omega^1_{J_0/k})$ be the corresponding cohomology classes defining these homogenous spaces and let

$$0 \to \mathcal{O}_{X_0} \to E_X \to F^*\omega_{X_0} \to 0$$

$$0 \to \mathcal{O}_{J_0} \to E_G \to F^*\Omega^1_{J_0/k} \to 0$$

be the extension corresponding to η_X, η_J respectively. Consider the divisors $D_X = \mathbf{P}(F^*\omega_{X_0}) \subset \mathbf{P}(E_X)$ and $D_J = \mathbf{P}(F^*\Omega^1_{J_0/k}) \subset \mathbf{P}(E_J)$. Since $\Omega^1_{J_0/k} \simeq \mathcal{O}^g_{J_0}$ we have $D_J \simeq J_0 \times \mathbf{P}^{g-1}$. Note that these divisors belong to the linear systems associated to $\mathcal{O}_{\mathbf{P}(E_X)}(1)$ and $\mathcal{O}_{\mathbf{P}(E_J)}(1)$ respectively and that we have identifications $X_0^1 \simeq \mathbf{P}(E_X)\backslash D_X$ and $J_0^1 \simeq \mathbf{P}(E_J)\backslash D_J$. Let $\alpha : X_0 \to J_0$ be the inclusion. An argument similar to the corresponding one in [B2] section 1 shows that there is a natural restriction homomorphism $\alpha^* E_J \to E_X$ prolonging the natural homomorphism $\alpha^*\Omega^1_{J_0/k} \to \omega_{X_0}$. The homomorphism $\alpha^* E_J \to E_X$ is clearly surjective so it induces a closed embedding $\mathbf{P}(E_X) \subset \mathbf{P}(E_J)$ prolonging the embedding $X_0^1 \subset J_0^1$. By abuse we shall still denote by π_X, π_J the projections $\mathbf{P}(E_X) \to X_0, \mathbf{P}(E_J) \to J_0$.

It is standard to prove that the line bundle $\mathcal{H} := \pi_J^*\mathcal{O}_{J_0}(3\Theta) \otimes \mathcal{O}_{\mathbf{P}(E_J)}(1)$ is very ample on $\mathbf{P}(E_J)$. Here Θ is the theta divisor on the Jacobian J_0. (Cf. [BV] for the argument.)

Next step is to compute the degree $deg_{\mathcal{H}}\mathbf{P}(E_X)$ of $\mathbf{P}(E_X)$ as a subvariety of $\mathbf{P}(E_J)$ with respect to the embedding defined by $\mathcal{H}$. Note that

$$\mathcal{H} \otimes \mathcal{O}_{\mathbf{P}(E_X)} = \pi_X^*\mathcal{O}_{X_{(0)}}(3\Theta) \otimes \mathcal{O}_{\mathbf{P}(E_X)}(1)$$

We may compute the selfintersection

$$(\mathcal{O}_{\mathbf{P}(E_X)}(1) \cdot \mathcal{O}_{\mathbf{P}(E_X)}(1))_{\mathbf{P}(E_X)} = deg\ F^*\omega_{X_0} = p(2g-2)$$

hence we get

$$deg_{\mathcal{H}}\mathbf{P}(E_X) = p(2g-2) + 6g$$

Finally we have

$$\mathcal{H} \otimes \mathcal{O}_{B_i} \simeq \pi_i^*\mathcal{O}_{J_0}(3\Theta) = T_{-b_i}^*\pi^*\mathcal{O}_{J_0}(3(\Theta - \pi(b_i)))$$

where $\pi_i : B_i \subset J_0^1 \to J_0$, $\pi : B \subset J_0^1 \to J_0$ are the projections which, as we have shown, have degree at most p^{2g} and $T_{-b_i} : B_i \to B$ is the translation by $-b_i$. So we get, using $(\Theta^g) = g!$, that

$$deg_{\mathcal{H}} B = p^{2g} \cdot 3^g \cdot g!$$

Now Bezout's theorem in Fulton's form [Fu] p.148, says that the number of irreducible components in the intersection of two projective varieties of degrees d_1, d_2 cannot exceed $d_1 d_2$. In particular

$$\sharp(X_0^1 \cap B_i) \leq deg_{\mathcal{H}} \mathbf{P}(E_X) \cdot deg_{\mathcal{H}} B_i \leq (p(2g-2)+6g) \cdot p^{2g} \cdot 3^g \cdot g!$$

which closes the proof of our Theorem (1.11), hence of Theorem A.

2. Higher p–jets, Greenberg transform, and δ–formal functions.

(2.1) The construction in (1.4) may be iterated, and this leads to "higher order p–jet spaces". Assume R, δ, ϕ and $f : R \to B$ are as in (1.4). We write B^{-1}, B^0 in place of R, B respectively and we write f^0 in place of f. One constructs a sequence of ring homomorphisms $f^n : B^{n-1} \to B^n$ $(n \geq 1)$ and a sequence of p–derivations $\delta : B^{n-1} \to B^n$ of f^n having the following universality property: for any ring homomorphism $g : B^{n-1} \to C$ and any p–derivation $\partial : B^{n-1} \to C$ such that $\partial \circ f^{n-1} = g \circ \delta : B^{n-2} \to C$, there exists a unique ring homomorphism $u : B^n \to C$ such that $g = u \circ f^n$ and $\partial = u \circ \delta$. This B^n will be called the *p–jet algebra of order n* of B. The construction is similar to the one in (1.4). If $B = R[T]/I$ we introduce families of indeterminates $T', T'', ..., T^{(n)}, ...$ and we prolong $\phi : R \to R$ to ring homomorphisms: $\phi : R[T, ..., T^{(n-1)}] \to R[T, ..., T^{(n)}]$ by requiring that

$$\phi(T_i^{(j)}) = (T_i^{(j)})^p + pT_i^{(j+1)}$$

We get as in (1.4) p–derivations

$$\delta : R[T, ..., T^{(n-1)}] \to R[T, ..., T^{(n)}]$$

of the inclusions and we set

$$B^n = R[T, T', ..., T^{(n)}]/(I, I', ..., I^{(n)})$$

$$B^\infty = R[T, T', ..., T^{(n)}, ...]/(I, I', ..., I^{(n)}, ...)$$

Here, as in the case of usual derivations, the upper $'$ and (n) stand for "image under δ and δ^n" respectively. As in (1.4) this construction does not commute with localisation. So if X/R is a scheme of finite type and U_i are affine open sets covering X then the schemes *Spec* $\mathcal{O}(U_i)^n$ will not glue together. But it is easy to see that their p–adic completion (i.e. the completions along the closed subset defined by p) do glue together to give a formal scheme X^n which we may call the *p–jet space of X of order n*. Similarly gluing the p–adic completions of *Spec* $\mathcal{O}(U_i)^\infty$ we get a formal scheme X^∞, the *infinite p–jet space of X*. (In the special case when p is nilpotent on X the X^n's are actually schemes, rather than merely formal schemes, and our X^1 here coincides with the X^1 defined in (1.4). Moreover the sheaf of rings $\mathcal{O}_{X^n}$ is generated in this case by $\mathcal{O}_{X^{n-1}}$ and $\delta\mathcal{O}_{X^{n-1}}$.) Coming back to the general case, when p is not necessarily nilpotent on X, note that our

construction is again functorial: X^n represents a functor analogue to the one in (1.4), but this time in the frame of formal schemes. Moreover we have a projective system of formal schemes

$$... \to X^n \to X^{n-1} \to ... \to X^0$$

where $X^0 = \hat{X}$ is the $p-$adic completion of X and X^∞ is the $p-$adic completion of the inverse limit of the X^n's. Reducing the above system modulo p we get a projective system of $k-$schemes:

$$... \to X_0^n \to X_0^{n-1} \to ... \to X_0^0$$

Note that $X_0^0 = X_0 = X \otimes k$; note also that all transition maps in the latter system are affine. The projective limit X_0^∞ of the latter system coincides of course with the reduction modulo p of X^∞.

Note also the following compatibility of the construction above with the construction done in (1.4). Set $R_m := R/p^{m+1}R$, $X_m := X \otimes R_m$ and $X_m^n := (X^n) \otimes R_m$; then the equality in (1.3) immediately implies that we have the identification $X_m^n \simeq (X_{m+n})^n$.

A similar (obvious) discussion holds if we start with a group scheme G/R instead of a scheme X/R.

Here is a basic smoothness property of $p-$jets:

Proposition (2.2). *Assume X/R is smooth along X_0. Then the morphisms $X^n \to X^{n-1}$ are smooth (by which we mean that they are locally obtained as $p-$adic completions of smooth morphisms of schemes).*

Proof. This is an easy exercise using Grothendieck's Jacobian criterion of smoothness, plus the explicit construction of $p-$jets given in (2.1). We leave this to the reader.

(2.3) **Remark.** A more precise statement can actually be proved, saying that $X^n \to X^{n-1}$ is locally a product with the $p-$adic completion of an affine space [B5]; we won't need this here.

Proposition (2.4). *Assume X/R is smooth along X_0. Then for $n \geq 1$, $X_0^n \to X_0^{n-1}$ is a (Zariski locally trivial) principal homogenous space for the "relative Frobenius tangent bundle"*

$$FT(X_0^{n-1}/X_0^{n-2}) := Spec\ S(F^*\Omega_{X_0^{n-1}/X_0^{n-2}}) \to X_0^{n-1}$$

If in addition X/R is a group scheme then $Ker(X_0^n \to X_0^{n-1})$ are vector groups.

Proof. Similar to the proof of (1.5) and (1.6). Note that in order to apply the arguments in (1.6) one needs a certain smoothness property; this is provided by Proposition (2.2).

(2.5) In what follows we prepare ourselves to prove that, at least in the smooth case, X_0^∞ coincides with the "Greenberg transform". In order to do this note that by the

universality property of p–jets there is, for any scheme of finite type X/R, a natural lifting map

$$\nabla : X(R) \to X^\infty(R)$$

In case X is the affine line X^∞ is the infinite affine space and ∇ is simply the map

$$\nabla : R \to R^{\mathbf{N}},\ a \mapsto \nabla a = (a, \delta a, \delta^2 a, \delta^3 a, ...)$$

Composing with the "reduction modulo p map" we get for any X a map

$$\nabla_0 : X(R) \to X_0^\infty(k)$$

In particular if X is the affine line we get the map

$$\nabla_0 : R \to k^{\mathbf{N}},\ a \mapsto \nabla_0 a = (\pi a, \pi\delta a, \pi\delta^2 a, \pi\delta^3 a, ...)$$

where $\pi : A \to k$ is the canonical projection. On the other hand recall from [S] p.35 that R has a unique multiplicative system of representatives $\psi : k \to R$ (i.e. a multiplicative map such that $\pi \circ \psi = Id_k$) and if $W(k)$ is the Witt ring of k then the map

$$\theta : W(k) = k^{\mathbf{N}} \to R,\quad \theta(\alpha_0, a_1, ...) = \sum_{i=0}^{\infty} \psi(\alpha_i^{p^{-i}}) p^i$$

is a ring isomorphism. The α_i's are called the *Witt coordinates* of a.

Lemma (2.6). *The composed map*

$$k^{\mathbf{N}} = W(k) \xrightarrow{\theta} R \xrightarrow{\nabla_0} k^{\mathbf{N}}$$

is bijective and its components, as well as the components of its inverse, are polynomials with integer coefficients. More precisely, there exist universal polynomials with integer coefficients $P_2, P_3, ..., P_n, ...$ such that

$$\nabla_0(\theta(\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, ...)) = (\alpha_0, \alpha_1, \alpha_2 + P_2(\alpha_0, \alpha_1), ..., \alpha_n + P_n(\alpha_0, \alpha_1, ..., \alpha_{n-1}), ...)$$

Example. $P_2(\alpha_0, \alpha_1) = \alpha_0^{p-1}\alpha_1$

Proof. We prove by induction on $n \geq 0$ that there exist universal polynomials P_{nk}, $k \geq 0$, with integer coefficients such that for any

$$a = \sum_{k \geq 0} x_k p^k \in R,\quad x_k = \psi(\alpha_k^{p^{-k}})$$

we have

$$\delta^n a = \sum_{k \geq 0} [x_{n+k}^{p^n} + P_{nk}(x_0, x_1, ..., x_k, x_{k+1}^p, ..., x_{n+k-1}^{p^{n-1}})] p^k$$

(Denote by Θ_k the coefficient of p^k in the above formula.) This will close the proof for we set $P_n := P_{n0}$ (one checks that $P_0 = P_1 = 0$). The case $n = 0$ is clear. Assume the above formula holds for n. We have

$$\phi(\delta^n a) = \sum_{k \geq 0} [x_{n+k}^{p^{n+1}} + P_{nk}(x_0^p, x_1^p, ..., x_k^p, x_{k+1}^{p^2}, ..., x_{n+k-1}^{p^n})]p^k$$

On the other hand we have

$$(\delta^n a)^p = \sum_{k \geq 0} \Omega_k p^k$$

where

$$\begin{aligned}
\Omega_0 &= \Theta_0^p \\
\Omega_1 &= p\Theta_0^{p-1}\Theta_1 \\
\Omega_k &= px_{n+k}^{p^n}\Theta_0^{p-1} + \\
&\quad + pP_{nk}(x_0, ..., x_k, x_{k+1}^p, ..., x_{n+k-1}^{p^{n-1}})\Theta_0^{p-1} + \\
&\quad + R_{nk}(x_0, ..., x_{k-1}, x_k^p, ..., x_{n+k-1}^{p^n}) \quad , k \geq 2
\end{aligned}$$

for some universal polynomials R_{nk}. Then a tedious but straightforward computation gives the desired type of formula for

$$\delta^{n+1} a = \frac{1}{p}(\phi(\delta^n a) - (\delta^n a)^p)$$

and we are done.

Lemma (2.7). *The map $\nabla_0 : X(R) \to X_0^\infty(k)$ is bijective for X any scheme of finite type over R.*

Proof. Of course it is enough to assume X is affine. If X is an affine space then the Corollary follows directly from Lemma (2.6). Assume now $X \subset \mathbf{A}^N$ is a closed subscheme so we may write

$$X = Spec\ R[T]/I$$

Consider the commutative diagram

$$\begin{array}{ccc}
X(R) & \stackrel{\nabla_{0,X}}{\to} & X_0^\infty(k) \\
\cap & & \cap \\
\mathbf{A}^N(R) & \stackrel{\nabla_0}{\to} & (\mathbf{A}^N)_0^\infty(k)
\end{array}$$

So injectivity of $\nabla_{0,X}$ is clear. To check surjectivity, take a point $\bar{P} \in X_0^\infty(k)$. Then we have $\bar{P} = \nabla^0(P)$ for some $P \in \mathbf{A}^N(R)$. Now the equations defining X_0^∞ in $(\mathbf{A}^N)_0^\infty$ have the form $(\delta^j F)_0$ where $j \geq 0$ and $F \in I$ (here the lower 0 means reduction mod p). So if we fix any $F \in I$ we have that

$$(0, 0, 0, ...) = ((\delta^j F)_0(\nabla_0 P))_{j \geq 0} = (((\delta^j F)(\nabla P))_0)_{j \geq 0} = ((\delta^j(F(\nabla P)))_0)_{j \geq 0} = \nabla_0(F(\nabla P))$$

By injectivity of ∇_0 we get $F(\nabla P) = 0$ hence $\nabla P \in X(R)$ and we are done.

(2.8) To make the following discussion easier, let's make a definition: by a *$p-$transform* we shall understand a functor $X \mapsto \tilde{X}$ from the category of $R-$schemes of finite type to the category of $k-$schemes, together with bijections $X(R) \simeq \tilde{X}(k)$ which are functorial in X, such that all these data commute (in the obvious sense) with open immersions, closed immersions and products. A construction due to Greenberg [Gr] (going back to Lang's thesis [L1], [L2]) provides a construction of a $p-$transform, called in the literature the *Greenberg transform*. All we need to know about the Greenberg transform is that, when restricted to smooth $R-$schemes, it gives reduced $k-$schemes, and, when applied to the affine line, it gives the infinite affine space, with coordinates given by the Witt coordinates. On the other hand Lemma (2.7) shows that the functor $X \mapsto X_0^\infty$ together with the bijections $\nabla_0 : X(R) \simeq X_0^\infty(k)$ also provide a $p-$transform. Now we have the following Lemma whose (trivial) proof will be left to the reader:

Lemma (2.9). *Assume we are given two $p-$transforms $X \mapsto \tilde{X}$ and $X \mapsto \bar{X}$. Assume the following conditon (which we call (*)) is satisfied: there is an isomorphism of $k-$schemes $u : \tilde{\mathbf{A}}^1 \to \bar{\mathbf{A}}^1$ such that the induced bijection $u(k) : \tilde{\mathbf{A}}^1(k) \to \bar{\mathbf{A}}^1(k)$ coincides with the bijection $\tilde{\mathbf{A}}^1(k) \simeq \mathbf{A}^1(R) \simeq \bar{\mathbf{A}}^1(k)$ Then the two $p-$transforms become isomorphic after composition with the functor $Z \mapsto Z_{red}$ (i.e. there exist isomorphisms $u_X : (\tilde{X})_{red} \to (\bar{X})_{red}$ (X any $R-$scheme of finite type) behaving functorially in X such that $u_X(k)$ coincides with the bijection $\tilde{X}(k) \simeq X(R) \simeq \bar{X}(k)$).*

Putting together the considerations above we get:

Theorem (2.10). *Let $X \mapsto \tilde{X}$ be the Greenberg transform. Then for any smooth X/R we have isomorphisms $\tilde{X} \simeq X_0^\infty$ behaving functorially in X.*

Proof. We apply Lemma (2.9) to the Greenberg transform and to $X \mapsto X_0^\infty$. Condition (*) follows from Lemma (2.6). Also, as noted before, the Greenberg transform of a smooth scheme X/R is reduced; but the same holds for X_0^∞ by (2.4) and we are done.

(2.11) In order to prove Theorem B in the Introduction we need more general discussion. Let X/R be a scheme of finite type and denote by $\mathcal{O}^\infty(X)$ the ring of $\delta-$formal functions on $X(R)$ (cf. the Introduction). Then there is a natural ring homomorphism $\mathcal{O}(X^\infty) \to \mathcal{O}^\infty(X)$, $f \mapsto \hat{f}$ defined as follows. For any $P \in X(R)$, consider its lifting $\nabla(P) \in X^\infty(R)$, $\nabla(P) : Spf\ R \to X^\infty$; the latter induces a ring homomorphism $\mathcal{O}(X^\infty) \to R$ and we let $\hat{f}(P) \in R$ be the image of f under the above ring homomorphism.

The following Lemma summarizes some basic properties of $\mathcal{O}(X^\infty)$ and $\mathcal{O}^\infty(X)$.

Lemma (2.12). *Let X/S be smooth. Then the following hold: 1) The map $\mathcal{O}(X^\infty) \to \mathcal{O}^\infty(X)$ is an isomorphism, in particular $\mathcal{O}(X^\infty)$ is reduced, flat over R, and $p-$adically complete, 2) The natural map $\mathcal{O}(X^\infty) \otimes k \to \mathcal{O}(X_0^\infty)$ is injective, 3) If $\mathcal{O}(X_0^\infty) = k$ then $\mathcal{O}(X^\infty) = R$, 4) If X_0^n is affine for some n then X^n and X^∞ are affine formal schemes. Moreover the maps $\mathcal{O}(X^n) \otimes k \to \mathcal{O}(X_0^n)$ and $\mathcal{O}(X^\infty) \otimes k \to \mathcal{O}(X_0^\infty)$ are isomorphisms. Finally $\mathcal{O}(X^n)$ is topologically finitely generated and $\mathcal{O}(X^\infty)$ is topologically $\delta-$finitely generated by elements of $\mathcal{O}(X^n)$ (i.e. topologically generated by finitely many elements of $\mathcal{O}(X^n)$ together with their $p-$derivatives of arbitrary order).*

Proof. To check 1) it is sufficient to check injectivity, for then surjectivity follows. So we may assume $X = Spec\ R[T]/I$, $T = (T_1, ..., T_N)$, hence

$$\mathcal{O}(X^\infty) = (R[T, T', ...]/(I, I', ...))\hat{} = R[T, T', ...]\hat{}/(I, I', ...)^{cl}$$

where the upper cl denotes the closure in the $p-$adic topology. Let $f \in \mathcal{O}(X^\infty)$ be represented by $\Phi \in R[T, T', ...]\hat{}$ and assume $\hat{f} = 0$. Let $u : X(R) \to R^N$ be the embedding defined by $T_1, ..., T_N$. We know that $\Phi(u(P), u(P)', ...) = 0$ for all $P \in X(R)$. Reducing modulo p we get $\Phi_0(\nabla_0(u(P))) = 0$ where $\Phi_0 \in k[T, T', ...]$ is the reduction of Φ. Now by (2.7) $\nabla_0(u(P))$ runns through all of $X_0^\infty(k)$. Since X_0^∞ is reduced (cf. (2.4)) we get by Hilbert's Nullstellensatz that $\Phi_0 \in (I, I', ...)_0$ =image of $(I, I', ...)$ in $k[T, T', ...]$. Hence $\Phi = \Psi^0 + p\Phi^1$ where $\Psi^0 \in (I, I', ...)$ and $\Phi^1 \in R[T, T', ...]\hat{}$. Repeating the above reasoning we may write $\Phi^1 = \Psi^1 + p\Phi^2, \Phi^2 = \Psi^2 + p\Phi^3, ...$ with $\Psi^i \in (I, I', ...)$ hence $\Phi = \Psi^0 + p\Psi^1 + p^2\Psi^2 + ... \in (I, I', ...)^{cl}$, hence $f = 0$ and 1) is checked.

2) follows immediately from the fact that p is a non zero divisor in $\mathcal{O}(X^\infty)$.

3) follows immediately from 2) and the completeness of R and $\mathcal{O}(X^\infty)$.

4) is an easy exercise with formal schemes; one has to use the remark in (2.1) about the generation of the structure sheaf of the schemes $(X_i)^j$, $i \geq j$.

We are now in the position to prove Theorem (2.13) below which proves in particular Theorem B from the Introduction.

Theorem (2.13). *If X/R is a smooth projective curve of genus at least 2 then, for $n \geq 1$, X^n are affine formal schemes, and the same holds for X^∞. Moreover $\mathcal{O}(X^n)$ are topologically finitely generated and $\mathcal{O}(X^\infty)$ is topologically $\delta-$finitely generated by elements in $\mathcal{O}(X^1)$. Finally $\mathcal{O}(X^\infty)$ separates points on $X(R)$. On the other hand if X is a projective space over R then $\mathcal{O}(X^\infty) = R$.*

Proof. Assume first X/R is a smooth projective curve of genus at least 2. We know from (1.10) that X_0^1 and hence the X_0^n's are affine varieties. So we simply apply assertion 4) in (2.12), plus the fact that $\mathcal{O}(X_0^\infty)$ separates points on the affine scheme X_0^∞.

Assume now X/R is a projective space. Since through any two points of $\mathbf{P}^N(R)$ passes a projective line we may restrict ourselves to the case of the projective line $X = \mathbf{P}_R^1$. By

assertion 3) in Lemma (2.12) all we have to prove is that $\mathcal{O}(X_0^\infty) = k$. Write $X = Spec\ R[y] \cup Spec\ R[z]$ with gluing defined by the isomorphism

$$R[y, y^{-1}] \to R[z, z^{-1}], \quad y \mapsto z^{-1}$$

Then we have

$$X^\infty = Spf\ R[y, y', y'', ...]\hat{} \cup Spf\ R[z, z', z'', ...]\hat{}$$

with gluing given by the unique isomorphism

$$R[y, y^{-1}, y', y'', ...]\hat{} \to R[z, z^{-1}, z', z'', ...]\hat{}$$

extending the above one and commuting with δ. One immediately checks by induction that under this isomorphism we have

$$y^{(n)} \mapsto -z^{-2p^n} z^{(n)} + F_{n-1} + pG_n$$

with

$$F_{n-1} \in R[z, z^{-1}, z', z'', ..., z^{(n-1)}]\hat{}, \quad G_n \in R[z, z^{-1}, z', z'', ..., z^{(n)}]\hat{}$$

Indeed, deriving $yz = 1$ we get

$$y' \mapsto -z^{-2p} z'[1 - (pz^{-p} z') + (pz^{-p} z')^2 - (pz^{-p} z')^3 + ...]$$

which proves our assertion for $n = 1$. Then using this formula, the induction step follows trivially.

Hence

$$X_0^\infty = Spec\ k[y, y', y'', ...] \cup Spec\ k[z, z', z'', ...]$$

with gluing given by

$$y^{(n)} \mapsto (z^{-1})^{(n)} = -z^{-2p^n} z^{(n)} + f_{n-1}$$

where $f_{n-1} \in k[z, z^{-1}, z', z'', ..., z^{(n-1)}]$. Assume now we have an element in $\mathcal{O}(X_0^\infty)$. This element is given by a polynomial

$$P(y) = \sum_{j=0}^{N} Q_j(y, y', ..., y^{(n-1)})(y^{(n)})^j \in k[y, y', y'', ..., y^{(n)}]$$

with the property that the rational fraction

$$P(z^{-1}) = \sum_{j=0}^{N} Q_j(z^{-1}, (z^{-1})', ..., (z^{-1})^{(n-1)})((z^{-1})^{(n)})^j$$

belongs to $k[z, z', z'', ..., z^{(n)}]$. We claim this forces P to belong to k. One proceeds by induction on n. Indeed the coefficient of $(z^{(n)})^N$ in $P(z^{-1})$ is

$$(-1)^N z^{-2p^n N} Q_N(z^{-1}, (z^{-1})', ..., (z^{-1})^{(n-1)})$$

By induction this forces $N = 0$ hence by induction again, $P \in k$.

References

[B1] A.Buium, Geometry of differential polynomial functions I: algebraic groups, Amer. J. Math. 115, 6 (1993), 1385-1444.

[B2] A.Buium, Geometry of differential polynomial functions II: algebraic curves, Amer. J. Math. 116, 4 (1994), 785-818.

[B3] A.Buium, Intersections in jet spaces and a conjecture of S.Lang, Annals of Math. 136 (1992) 557-567.

[B4] A.Buium, Effective bound for the geometric Lang conjecture, Duke Math. J. 71, 2 (1993), 475-499.

[B5] A.Buium, Geometry of $p-$jets, II, preprint.

[BV] A.Buium, F.Voloch, The Mordell conjecture in characteristic p: an explicit bound, preprint.

[Co1] R.Coleman, Torsion points on curves and $p-$adic abelian integrals, Ann.Math. 121 (1985), 111-168.

[Co2] R.Coleman, Ramified torsion points on curves, Duke Math. J. 54, 2, (1987), 615-640.

[Fu] W.Fulton, Intersection Theory, Springer 1984.

[Gr] M.Greenberg, Schemata over local rings, Ann. Math. 73 (1961), 624-648.

[EGA] A.Grothendieck, Elements de geometrie algebrique IV, Publ. Math. IHES.

[K] E.Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York 1973.

[L1] S.Lang, On quasi algebraic closure, Annals of Math. 55,2 (1952), 373-390.

[L2] S.Lang, Some applications of the local uniformization theorem, Amer. Math. J. 76, 2 (1954), 362-374.

[MD] M.Martin-Deschamps, Proprietes de descente des varietes a fibre cotangent ample, Ann.Inst.Fourier, 34,3(1984),39-64.

[Ray1] M.Raynaud, Courbes sur une variété abélienne et points de torsion, Invent.Math. 71 (1983), 207-235.

[Ray2] M.Raynaud, Around the Mordell conjecture for function fields and a conjecture of S.Lang, LNM 1016 (1983), 1-20.

[R] J.F.Ritt, Differential Algebra, Amer.Math.Soc.1950.

[S] J.P.Serre, Local Fields, Springer 1979.

[Sil] J.H.Silverman, The Arithmetic of Elliptic Curves, Springer.

[T] H.Tango, On the behaviour of extensions of vector bundles under the Frobenius map, Nagoya Math. J. 48 (1972), 73-89.

Institute for Advanced Study, Princeton and
Max Planck Institut fur Mathematik, Bonn.