The theory of canonical lifts for abelian varieties (draft version)

Chloe Martindale

February 10, 2016

These notes are from a talk at Leiden University, of which the aim was to understand Drinfeld's proof of the Serre-Tate theorem, following Katz' paper ([Kat]), and so the theory of canonical lifts of abelian varieties. That is, given an abelian variety defined over a finite field of characteristic $p > 0$, in what sense can one 'lift' said variety to be defined over a field of characteristic zero? The author thanks Bas Edixhoven for his explanation of the material, and Marco Streng, Giulio Orecchia, Erik Visse, Carlo Pagano, Peter Bruin, Martin Bright and Remy van Dobben de Bruyn for their helpful comments and questions. If there are any typos or mistakes the author welcomes further corrections.

1 Statement of the Serre-Tate theorem

Throughout this talk, k will be a field of characteristic $p > 0$, and R will be a nilpotent thickening of k, i.e. R is a ring with a nilpotent ideal I such that $R/I \cong k$. Let the nilpotency degree of I be $n+1$, i.e. $n+1$ is the smallest positive integer such that $I^{n+1} = 0$. Two examples of such an R would be

$$k[\mathcal{E}]/(\mathcal{E}^{n+1}) \quad \text{and} \quad W_{n+1}(k),$$

where $W_{n+1}(k)$ is the ring of Witt vectors for k of length $n+1$, the definition of which will be recalled in Definition 2.1. The Serre-Tate theorem will be an equivalence of categories, so we must first give these 2 categories.

Definition 1.1. We denote by $\mathscr{A}$ the category of abelian schemes over $\mathrm{Spec}(R)$, where R is as above.

Definition 1.2. [Tat, Definition 2.1]
Let p be prime, and let h be a non-negative integer. Let R' be a complete Noetherian local ring (in particular, as I is nilpotent the Artin local ring R is an example of a complete Noetherian local ring). Then a *p-divisible group G of height h* is an inductive system

$$G = (G_v, i_v)_{v \geq 0},$$

where
1. G_v is a finite group scheme over R' of order p^h,
2. for each $v \geq 0$,

$$0 \longrightarrow G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^h} G_{v+1}$$

is an exact sequence.

Definition 1.3. Let R, k and p be as above. We denote by $\mathscr{D}$ the category of triples

$$(A_k, G, \mathcal{E}),$$

where A_k is an abelian variety over $\mathrm{Spec}(k)$, G is a p-divisible group over $\mathrm{Spec}(R)$ and $\mathcal{E}$ is an isomorphism

$$\mathcal{E} : A_k[p^\infty] \xrightarrow{\sim} G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k).$$

Here, as usual, $A_k[p^\infty]$ denotes the p^∞ torsion subgroup of A_k. From now on we will drop 'Spec'.

We may now define a functor

$$\begin{array}{rccc} \Phi: & \mathscr{A} & \longrightarrow & \mathscr{D} \\ & A & \to & (A \times k, A[p^\infty], \text{natural } \mathcal{E}). \end{array}$$

Leading us to this amazing result!

Theorem (Serre-Tate)**.** *The functor Φ defined above is an equivalence of categories.*

Most of the rest of this talk will be dedicated to Drinfeld's proof of this theorem, but first we return to Witt vectors to give a nice application.

2 Application of the Serre-Tate Theorem

We will now show how me may use the Serre-Tate Theorem to *canonically* lift ordinary abelian varieties and their morphisms defined over a field of positive characteristic to a field of characteristic zero, for which Witt vectors will be a crucial tool, so we first recall the definition.

Definition 2.1. Let k be as above (that is, a field of characteristic $p > 0$). The ring $W_{n+1}(k)$ of Witt vectors is defined as follows.
• The elements of $W_{n+1}(k)$ are tuples $(\alpha_0, \ldots, \alpha_n) \in k^{n+1}$.
• The operations $+, \cdot$ of $W_{n+1}(k)$ are defined in the following way. For $i = 0, \ldots, n$ we will define polynomials $s_i, m_i \in \mathbb{Z}[x_0, \ldots, x_i, y_0, \ldots, y_i]$, and in turn we will define

$$(x_0, \ldots, x_n) + (y_0, \ldots, y_n) = (s_0, \ldots, s_n),$$
$$(x_0, \ldots, x_n) \cdot (y_0, \ldots, y_n) = (m_0, \ldots, m_n).$$

The polynomials $s_0, \ldots, s_n$ and $m_0, \ldots, m_n$ are defined iteratively by the following rules:
1. $s_0 = x_0 + y_0$, $m_0 = x_0 y_0$,
2. For $i = 1, \ldots, n$, define $\phi_i(z_0, \ldots, z_i) = z_0^{p^i} + pz_1^{p^{i-1}} + \cdots + p^i z_i$.
3. For $i = 1, \ldots, n$, define s_i and m_i by

$$\phi_i(s_0, ..., s_i) = \phi_i(x_0, ..., x_i) + \phi_i(y_0, ..., y_i),$$

$$\phi_i(m_0, ..., m_i) = \phi_i(x_0, ..., x_i) \cdot \phi_i(y_0, ..., y_i).$$

Just using the definition above, the two facts below are easy to check, so we leave them as an exercise for those who are interested.

Exercise.
1. The ideal $I := pW_{n+1}(k)$ of the ring $W_{n+1}(k)$ is nilpotent, with $I^{n+1} = 0$, and furthermore

$$W_{n+1}(k)/pW_{n+1}(k) \cong k.$$

2. If the field k is a finite extension of $\mathbb{Z}/p\mathbb{Z}$, then $W(k)$, which is defined by

$$W(k) = \lim_{n \to \infty} W_{n+1}(k),$$

is a finite extension of $\mathbb{Z}_p$.

By the first exercise, we see that for any field k of characteristic $p > 0$, and for any n, the ring $W_{n+1}(k)$ is a suitable candidate for our ring R (satisfying the hypotheses of the Serre-Tate Theorem), with nilpotent ideal $pW_{n+1}(k)$.
In particular, if we define abelian varieties A_k and A'_k over k, then for each $n \in \mathbb{Z}_{\geq 0}$, if there exist p-disivisble groups G and G' defined over $W_{n+1}(k)$, isomorphisms

$$\mathcal{E} : A_k[p^\infty] \tilde{\to} G \times k \quad \text{and} \quad \mathcal{E}' : A'_k[p^\infty] \tilde{\to} G' \times k,$$

and a morphism in $\mathscr{D}$ (see Definition 1.3)

$$\bar{f} : (A_k, G, \mathcal{E}) \longrightarrow (A'_k, G', \mathcal{E}'),$$

then using the Serre-Tate Theorem we may lift f via inverse of the functor Φ to a morphism in $\mathscr{A}$ (see Definition 1.1)

$$f : A_{W_{n+1}(k)} \longrightarrow A'_{W_{n+1}(k)}$$

of abelian varieties A and A' over $W_{n+1}(k)$, whose base changes to k are A_k and A'_k respectively.

Remark 2.2. In order for G, G', $\mathcal{E}$ and $\mathcal{E}'$ to exist (and for their choice to be canonical), it is sufficient to take A_k and A'_k to be ordinary abelian varieties, which we do not have time to prove rigorously here. The interested reader should see [LST], [Kat] or [Dos] for more details.

Now let k be a finite extension of $\mathbb{Z}/p\mathbb{Z}$, and A_k and A'_k be ordinary abelian varieties over k. Then by the above, for every $n \in \mathbb{Z}_{\geq 0}$, there exist canonical G, G', $\mathcal{E}$ and $\mathcal{E}'$ such that we have a morphism in $\mathscr{D}$,

$$\bar{f}_n : (A_k, G, \mathcal{E}) \longrightarrow (A'_k, G', \mathcal{E}'),$$

which upon restricting to the first coordinate yields a morphism $\tilde{f} : A_k \to A'_k$. We choose $\bar{f}_n$ in such a way that $\tilde{f}$ is the same for every n (this is possible by definition). The morphism $\bar{f}_n$ in turn may be lifted canonically to a morphism in $\mathscr{A}$,

$$f_n : A_{W_{n+1}(k)} \longrightarrow A'_{W_{n+1}(k)}$$

of abelian varieties over $W_{n+1}(k)$ such that the base changes to k are A_k and A'_k respectively. Recall now that $W(k)$ was defined in the second exercise to be $\lim_{n\to\infty} W_{n+1}(k)$, so that by the universal property of limits we get a unique morphism

$$f : A_{W(k)} \longrightarrow A'_{W(k)}$$

of abelian varieties over $W(k)$, such that the base change of f to k yields $\tilde{f}$ and the base changes of $A_{W(k)}$ and $A'_{W(k)}$ to k are A_k and A'_k respectively.

All of this shows us that we can canonically lift ordinary abelian varieties and their morphisms defined over a field k which is a finite extension of $\mathbb{Z}/p\mathbb{Z}$ to be defined over $W(k)$, which by the second exercise is a finite extension of $\mathbb{Z}_p$, which we can then embed into a finite extension of $\mathbb{Q}_p$, so we are done!

3 Proof of the Serre-Tate Theorem

We now turn to Drinfeld's proof of the Serre-Tate Theorem, which is far simpler than the original proof. Drinfeld first proves 4 'observations' about lifting morphisms which make the proof of the theorem relatively easy, so we first prove these observations.

Throughout this section, R, I, k and p remain as before (see the the first section), G and H will be either abelian schemes over R or p-divisible groups over R, and A will be an R-algebra. In order to gain a better understanding of lifting morphisms, we want to consider the map

$$\rho : \mathrm{Hom}(G, H) \longrightarrow \mathrm{Hom}(G \times k, H \times k).$$

We will write G_k and H_k for $G \times k$ and $H \times k$ respectively. ρ **versus** $\rho(A)$**???**

$$\rho(A) : \mathrm{Hom}(G(A), H(A)) \longrightarrow \mathrm{Hom}(G(A/IA), H(A/IA))$$

Observation 1. The kernel of $\rho(A)$ is given by

$$\mathrm{Hom}(G(A), \ker(\ H(A) \xrightarrow{\mathrm{res}} H(A/IA)\ ).$$

Proof. Let f be an element of $\mathrm{Hom}(G(A), H(A))$. Then

$$\begin{array}{ccc} G(A) & \xrightarrow{f} & H(A) \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ G(A/IA) & \xrightarrow{\rho(A)(f)} & H(A/IA) \end{array}$$

commutes, so that

$$\rho(A)(f) = 0 \Leftrightarrow \mathrm{im}(f)|_{H(A/IA)} = 0.$$

□

Observation 2.
a) G is p-divisible.
b) $\ker(\ H(A) \xrightarrow{\mathrm{res}} H(A/IA)\ )$ is p^{n+1}-torsion. (Here h is the height of H as a p-divisible group).

Proof. (Sketch)
b) Assume first that H is a formal Lie group, i.e. $H = \mathrm{Spf}R[[x_1, \ldots, x_k]]$ together with a formal group law

$$z_i = x_i + y_i + \text{ h.o.t.}$$

Therefore, coordinate-wise, multiplication by p gives

$$x_i^{(p)} = px_i + \text{ h.o.t.}$$

Furthermore, $p = 0$ in k so in fact $p \in I$, and for $(x_1, \ldots, x_k) \in \ker(H(A) \to H(A/IA))$, for all $i = 1 \ldots k$ we know that $x_i \in I$, so that

$$x_i^{(p)} \in I^2,$$

so by induction,

$$x_i^{(p^n)} \in I^{n+1}.$$

So if H were a formal Lie group, our assertion would hold. It remains to show that this is all we need. We state two lemmas without proof:

Lemma 3.1 (Grothendieck-Messing)**.** Let R be as above (so that in particular p is locally nilpotent on $\mathrm{Spec}(R)$), and let H be a p-divisible group. Then H is formally smooth and the formal completion of H along its unit section, denoted $\hat{H}$, is a formal Lie group.

Lemma 3.2 (Stack's project)**.** Let H be a commutative group scheme over R. Then by descent theory we may view H as an abelian f.p.p.f. sheaf and so

$$\hat{H} = \varinjlim \mathrm{Spec}(\mathcal{O}_H / I^{n+1})$$

is the formal completion of H along its unit section, and is a formal Lie group.

These two lemmas allow us to assume that in both of our cases (H a p-divisible group or H an abelian scheme), $\bar{H}$ is a formal Lie group, and so the above applies, so it remains to show that if (b) holds for $\bar{H}$, then it also holds for H.

assumption: H smooth

We assume without proof two more facts:

Fact 1. $\hat{H}(A) = \ker(\ H(A) \xrightarrow{\text{res}} H(A/\sqrt{0})\ )$.

Fact 2. If H is formally smooth, A is a R-algebra and J is an ideal of R, then the restriction map $H(A) \to H(A/JA)$ is surjective.

Now define

$$H_I(A) = \ker(\ H(A) \xrightarrow{\text{res}} H(A/IA)\ ),$$

and define α and β to be the induced maps making the diagram below commute:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \hat{H}_I(A) & \xrightarrow{\alpha} & H_I(A) & \longrightarrow & \operatorname{coker}(\alpha) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \hat{H}(A) & \longrightarrow & H(A) & \longrightarrow & H(A/\sqrt{0}A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \beta & & \\
0 & \longrightarrow & \hat{H}(A/IA) & \longrightarrow & H(A/IA) & \longrightarrow & H(A/\sqrt{I}A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0. & &
\end{array}$$

The horizontal (vertical) sequences are exact on the right (bottom) because H is formally smooth. Now as I is nilpotent, $\sqrt{I} = \sqrt{0}$ and so β is an isomorphism, and hence by the snake lemma, α is surjective, and so is also an isomorphism. $\square$

Observation 3. The cokernel of $\rho(A)$ is p^{n+1}-torsion.

Proof. Let f_k be a morphism

$$f_k : G \times k \to H \times k.$$

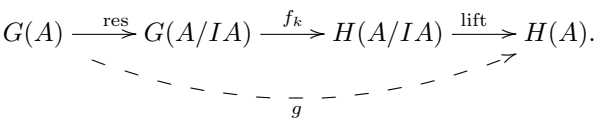
It is sufficient to prove that $p^{n+1} f_k$ lifts to a morphism $g : G \to H$. By Observation 2b and Fact 2 in the proof of Observation 2b, we have existence of the map 'lift', which satisfies the diagram

$$\begin{array}{ccccc}
 & & \overset{\text{res}}{\frown} & & \\
H(A) & \xrightarrow{p^{n+1}} & H(A) & \longrightarrow & H(A/IA)\ , \\
 & & \underset{\text{lift}}{\curvearrowleft} & &
\end{array}$$

from which we also see that

$$\text{lift} \circ \text{res} = p^{n+1}.$$

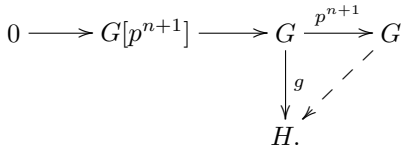
Then we may define our $g : G \to H$ by



G(A) versus G? □

Observation 4. The morphism $f_k : G \times k \to H \times k$ of Observation 3 lifts to some morphism $f : G \to H$ if and only if the morphism g of Observation 3 annihilates $G[p^{n+1}]$.

Proof. 'If' follows from the fact that lift $\circ$ res $= p^{n+1}$, so it remains to prove 'only if'. Now by definition of $G[p^{n+1}]$ and g, we have the following diagram:



That is, there exists a map $\tilde{f} : G \to H$ such that $g = \tilde{f} \circ p^{n+1}$, but by unicity (Observation 2), $\tilde{f}$ must life f_k. □

We are now ready for the proof of the Serre-Tate Theorem!

Proof of Theorem 1. **Proof that Φ is fully faithful.** We want to show that given
1. abelian schemes A and B over R and
2. a morphism of abelian varieties $f_k : A \times k \to B \times k$ and a morphism of p-divisible groups $f[p^\infty] : A[p^\infty] \to B[p^\infty]$ such that $\mathcal{E} : f_k[p^\infty] \tilde{\to} f[p^\infty] \times k$,
there exists a unique morphism $f : A \to B$ inducing both f_k and $f[p^\infty]$.

By unicity (Observation 2), it is sufficient to prove that f_k lifts, since is f lifts f_k, then $f[p^\infty] : A[p^\infty] \to B[p^\infty]$ lifts $f[p^\infty] \times k$, which by assumption is isomorphic to $f_k[p^\infty]$. Now by Observation 4, $f_k : A_k \to B_k$ lifts to some morphism $f : A \to B$ if and only if the morphism g of Observation 3 annihilates $A[p^{n+1}] = A[p^\infty][p^{n+1}]$, which by Observation 4 happens if and only if the morphism $f_k[p^\infty] : A_k[p^\infty] \to B_k[p^\infty]$ lifts to a morphism $f[p^\infty] : A[p^\infty] \to B[p^\infty]$.

Proof that Φ is essentially surjective.
We want now to show that given
1. an abelian variety A_k over k,
2. a p-divisible group G over R, and

3. an isomorphism $ep : A_k[p^\infty] \to G \times k$,
there exists an abelian scheme A over R lifting A_k with $A[p^\infty] = G$.

To prove this we must invoke the following theorem of Grothendieck:

Lemma 3.3 (Grothendieck)**.** Let $S = \mathrm{Spec}(R)$ and let $S_k = S \times k$. If A_k/S_k is an abelian scheme, then there exists an abelian scheme A/S whose base change to S_k is A_k.

By the above lemma, we may choose a lift A' over R of A_k. Then in particular

$$(A' \times k)[p^\infty] \cong A_k[p^\infty] \cong G \times k,$$

so by Observation 4, there exists a morphism

$$f : A'[p^\infty] \to G.$$

Claim 3.4. *The morphism f is an isogeny.*

Proof. Lift $\mathcal{E}^{-1}$ to $\phi : G \to A'[p^\infty]$. Then Observation 3 implies that

$$f \circ \phi = \phi \circ f = p^{n+1},$$

and so f is an isogeny, with $\ker(f)$ being a finite subgroup of $A'[p^{n+1}]$. □

If in addition to being finite, the kernel K of f is flat over R (implying that is a finite locally free subgroup of A'), the $A := A'/K$ is an abelian scheme over R (see SGA 3), and

$$A[p^\infty] = (A'/K)[p^\infty] = (A'[p^\infty])/K = G,$$

in which case we are done! Now as f is flat, by base change we may conclude that K is also flat over R, which is explained in detail in [Dos], but essentially follows from 'fibre-by-fire' criterion of flatness and Observation 3. □

References

[Ach] P. Achinger, *Drinfeld's proof of the Serre-Tate theorem* `https://math.berkeley.edu/~achinger/notes/old/p-div-10.pdf` (2011)

[Dos] G. Dospinescu, *Lifting abelian schemes: theorems of Serre-Tate and Grothendieck* `http://perso.ens-lyon.fr/gabriel.dospinescu/Serre-Tate.pdf`

[Kat] N. Katz, *Surfaces Algébriques: Séminaire de Géométrie Algébrique d'Orsay 1976–78*, pp. 138-202, Springer Berlin Heidelberg (1981)

[LST] Lubin, J-P. Serre and J. Tate, *Elliptic Curves and Formal Groups* `http://www.ma.utexas.edu/users/voloch/lst.html` (1964)

[Tat] J. Tate, *Proceedings of a Conference on Local Fields*, pp. 158-183, Springer Berlin Heidelberg (1967)