Liftings of Elliptic and Hyperelliptic Curves

Luís Finotti

University of Tennessee

AMS Joint Meeting
Jan 10, 2013

Witt Vectors

Let $\mathbb{k}$ be a *perfect* field of characteristic $p > 0$ and $W = \boldsymbol{W}(\mathbb{k})$ be the ring of Witt vectors over $\mathbb{k}$.
Remember also that we have a Frobenius map, which we denote by $\boldsymbol{\sigma}$ on W, defined by

$$\boldsymbol{\sigma}(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots).$$

So, if σ denotes the Frobenius in characteristic p (i.e., $\sigma(a) = a^p$), we have a *lifting of the Frobenius*. More precisely, if $\pi : W \to \mathbb{k}$ is the reduction modulo p, we have the following diagram on multiplicative groups:

$$\begin{array}{ccc} W^\times & \overset{\boldsymbol{\sigma}}{\dashrightarrow} & W^\times \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{k}^\times & \xrightarrow{\sigma} & \mathbb{k}^\times \end{array}$$

Witt Vectors (cont.)

Moreover, the *Teichmüller lift* $\tau : a \mapsto (a, 0, 0, \ldots)$ (a *group homomorphism*) yields the following diagram:

$$\begin{array}{ccc} W^{\times} & \xrightarrow{\boldsymbol{\sigma}} & W^{\times} \\ \pi \downarrow \uparrow \tau & & \tau \uparrow \downarrow \pi \\ \mathbb{k}^{\times} & \xrightarrow{\sigma} & \mathbb{k}^{\times} \end{array}$$

Question

Can we also lift the Frobenius for curves over $\mathbb{k}$?

Curves

More precisely, given a curve $C/\mathbb{k}$ and if $\phi : C \to C^\sigma$ is the Frobenius map, is there a lifting $\boldsymbol{C}/\boldsymbol{W}$ for which we can lift the Frobenius:

$$\begin{array}{ccc} \boldsymbol{C}(\boldsymbol{W}(\bar{\mathbb{k}})) & \overset{\boldsymbol{\phi}}{\dashrightarrow} & \boldsymbol{C}^\sigma(\boldsymbol{W}(\bar{\mathbb{k}})) \\ \downarrow \pi & & \downarrow \pi \\ C(\bar{\mathbb{k}}) & \xrightarrow{\phi} & C^\sigma(\bar{\mathbb{k}}) \end{array}$$

Answer: Yes, for *ordinary* elliptic curves and Abelian varieties (Deuring and Serre-Tate), but no for higher genus curves (Raynaud). In the case of elliptic curves we also have a *Teichmüller lift*.

Also, Mochizuki showed that one can lift the Frobenius for some curves of genus $g \geq 2$ if we allow singularities (at $(p-1)(g-1)$ points).

Ordinary Elliptic Curve

An elliptic curve (given by $y^2 = x^3 + ax + b$) over a field $\Bbbk$ of characteristic $p > 3$ is *ordinary* if $E[p] \cong \mathbb{Z}/p$. (Or, equivalently, if the coefficient of x^{p-1} in $(x^3 + ax + b)^{(p-1)/2}$ is non-zero.) Otherwise, the elliptic curve is said to be *supersingular*.

Note: Only finitely many elliptic curves (up to isomorphism) are supersingular.

We can lift the Frobenius for ordinary elliptic curves, i.e., if $\Bbbk$ is a perfect field with $\mathrm{char}(\Bbbk) = p$ and $E/\Bbbk : y_0^2 = x_0^3 + a_0 x_0 + b_0$, then there exists $\boldsymbol{a} = (a_0, a_1, \ldots), \boldsymbol{b} = (b_0, b_1, \ldots) \in W$ such that $\boldsymbol{E}/W : \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}$ has a lifting of the Frobenius:

$$
\begin{array}{ccc}
\boldsymbol{E}(\boldsymbol{W}(\bar{\Bbbk})) & \overset{\boldsymbol{\phi}}{\dashrightarrow} & \boldsymbol{E}^{\sigma}(\boldsymbol{W}(\bar{\Bbbk})) \\
\downarrow \pi & & \downarrow \pi \\
E(\bar{\Bbbk}) & \xrightarrow{\phi} & E^{\sigma}(\bar{\Bbbk})
\end{array}
$$

Elliptic Teichmüller Lift

Moreover, the curve $\boldsymbol{E}$ above is unique up to isomorphism and it is called the *canonical lifting of E*.
As with Witt vectors, we also have a section of the reduction modulo p, the so called *elliptic Teichmüller lift τ*:

$$\begin{array}{ccc} \boldsymbol{E}(\boldsymbol{W}(\bar{\mathbb{k}})) & \overset{\phi}{\dashrightarrow} & \boldsymbol{E}^{\sigma}(\boldsymbol{W}(\bar{\mathbb{k}})) \\ \pi \downarrow \uparrow \tau & & \pi \downarrow \uparrow \tau^{\sigma} \\ E(\bar{\mathbb{k}}) & \xrightarrow{\phi} & E^{\sigma}(\bar{\mathbb{k}}) \end{array}$$

Also, τ is a *group homomorphism*, and one can show that:

$$\tau(x_0, y_0) = ((F_0, F_1, F_2, \ldots), (y_0, y_0 G_1, y_0 G_2, \ldots)),$$

where $F_i, G_i \in \mathbb{k}[x_0]$.

Error Correcting Codes

Voloch and Walker used canonical liftings and the elliptic Teichmüller lift to create error-correcting codes. The bounds for the parameters (which measure "how good" the resulting codes are likely to be) depend on the degrees of F_i's and G_i's, with lower degrees giving better bounds. They showed that F_1 and G_1 had minimal degrees, making the canonical lifting the natural choice.

On the other hand, F_i and G_i for $i \geq 2$ are *not* minimal.

One should note that, one can construct codes with more general liftings of curves in a very similar way.

Error Correcting Codes (cont.)

With elliptic curves, we have:

Theorem

Let $E/\mathbb{k}$ *as above and* $\tilde{\boldsymbol{E}}/\boldsymbol{W}_3(\mathbb{k})$ *be a lifting for which we have a lifting of points* $\nu : E(\bar{\mathbb{k}}) \to \tilde{\boldsymbol{E}}/\boldsymbol{W}_3(\bar{\mathbb{k}})$ *having "minimal degrees". Then* $\tilde{\boldsymbol{E}}$ *is the canonical lifting of* E *(modulo* p^3*) and we have a lifting of the Frobenius on the affine part of* E *so that the following diagram commutes:*

$$\begin{array}{ccc}
\tilde{\boldsymbol{E}}(\boldsymbol{W}_3(\bar{\mathbb{k}})) & \overset{\tilde{\phi}}{\dashrightarrow} & \tilde{\boldsymbol{E}}^{\sigma}(\boldsymbol{W}_3(\bar{\mathbb{k}})) \\
\pi \downarrow \uparrow \nu & & \pi \downarrow \uparrow \nu^{\sigma} \\
E(\bar{\mathbb{k}}) & \xrightarrow{\phi} & E^{\sigma}(\bar{\mathbb{k}})
\end{array}$$

Moreover, any supersingular elliptic curve will yield larger degrees.

Minimal Degree Liftings

Therefore, the notions of *ordinary elliptic curve* and its *canonical lifting* (at least modulo p^3) can be defined strictly from the point of view of minimal degree liftings:

- E is ordinary if there is a lifting satisfying the lower bound on the degrees of the lifting map;
- $\boldsymbol{E}$ is the canonical lifting of E if there is a lifting map satisfying the lower bound.

On the other hand, in this way, these notions can be generalized to higher genus curves, and in a very similar way, one can obtain very similar results for *hyperelliptic* curves!

Mochizuki Liftings

For genus 2 curves (and so hyperelliptic) in characteristic 3, one can have a Mochizuki lifting of the Frobenius if one removes (some) 2 points from the curve. These two points are invariant by the hyperelliptic involution and thus can be put at "infinity".

We then have:

Theorem (F.-Mochizuki)

The notions of "ordinary" and "canonical lifting" (modulo p^2) from minimal degree liftings theory coincide with the ones coming from Mochizuki's theory.

Thus, we were able to give a concrete example of a family of Mochizuki liftings.

The J_n Functions

We now return to ordinary elliptic curves and their canonical liftings.

If $\Bbbk^{ord}$ denotes the set of ordinary j-invariants in $\Bbbk$, we have functions $J_i : \Bbbk^{ord} \to \Bbbk$ such that $(j_0, J_1(j_0), J_2(j_0), \ldots)$ is the j-invariant of the canonical lifting of the curve with j-invariant $j_0 \in \Bbbk^{ord}$.

Mazur's Question (to John Tate)

What kind of functions are these J_n? Can one say anything about them?

First Computations

Examples:

$p = 5$

- $J_1 = 3j_0^3 + j_0^4$;
- $J_2 = 3j_0^5+2j_0^{10}+2j_0^{13}+4j_0^{14}+4j_0^{15}+4j_0^{16}+j_0^{17}+4j_0^{18}+j_0^{19}+j_0^{20}+3j_0^{23}+j_0^{24}$.

Question: Can these functions all be polynomials?

$p = 7$

- $J_1 = 3j_0^5 + 5j_0^6$;
- $J_2 = (3j_0^{21}+6j_0^{28}+3j_0^{33}+5j_0^{34}+4j_0^{35}+2j_0^{36}+3j_0^{37}+6j_0^{38}+3j_0^{39}+5j_0^{40}+5j_0^{41}+5j_0^{42}+2j_0^{43}+3j_0^{44}+6j_0^{45}+3j_0^{46}+5j_0^{47}+5j_0^{48}+3j_0^{49}+3j_0^{54}+5j_0^{55})/(1+j_0^7)$.

Note: If $j_0 = -1$, then E is supersingular, i.e., no canonical lifting.

Pseudo-Canonical Liftings

(Superficial) Answer to Mazur's Question

For any p, we have that $J_n \in \mathbb{F}_p(X)$.

Tate's Question

Is there a supersingular value of j_0 (for some fixed characteristic p) for which all functions J_n are regular at j_0. (E.g., $j_0 = 0$ for $p = 5$ for J_1 and J_2?)

This lead us to define:

Definition

The elliptic curve over $\boldsymbol{W}(\mathbb{k})$ given by $\boldsymbol{j} \stackrel{\text{def}}{=} (j_0, J_1(j_0), J_2(j_0), \ldots)$ for such a supersingular j_0 is a pseudo-canonical lifting of the elliptic curve given by j_0.**Tate's question:** do they exist at all?

Answer to Tate's Question

Theorem

Let $j_0 \notin \mathbb{k}^{ord}$ and $p \geq 5$. Then:

1. J_1 *is regular at* j_0 *if, and only if,* j_0 *is either* 0 *or* 1728.
2. J_2 *is regular at* j_0 *if, and only if,* j_0 *is* 0.
3. *For* $n \geq 3$, *we have that* J_n *is never regular at* j_0.

For $p = 2, 3$ *(in which case only* $j_0 = 0$ *is supersingular), we have that* J_i *is regular at* 0 *if, and only if,* $i \leq 11$ *for* $p = 2$ *or* $i \leq 5$ *for* $p = 3$.

So, (unrestricted) pseudo-canonical liftings don't exits.

Answer to Mazur's Question

We need some notation: let

$$\mathrm{ss}_p(X) \stackrel{\text{def}}{=} \prod_{j \text{ supers.}} (X - j)$$

(the *supersingular polynomial*) and

$$S_p(X) \stackrel{\text{def}}{=} \prod_{\substack{j \text{ supers.} \\ j \neq 0, 1728}} (X - j).$$

One then has that $\mathrm{ss}_p(X), S_p(X) \in \mathbb{F}_p[X]$, and $S_p(0), S_p(1728) \neq 0$. Also, let

$$\iota = \begin{cases} 8, & \text{if } p = 2; \\ 3, & \text{if } p = 3; \\ 2, & \text{if } p = 31; \\ 1, & \text{otherwise.} \end{cases}$$

Answer to Mazur's Question

Then, we have:

Theorem

Let $J_i = F_i/G_i$, *with* $F_i, G_i \in \mathbb{F}_p[X]$, $(F_i, G_i) = 1$, *and* G_i *monic. Also, let* $r_i = (i-1)p^{i-1}$, $s_i = ((i-3)p^i + ip^{i-1})/3$ *and* $s_i' = \max\{0, s_i\}$. *Then, for all* $i \in \mathbb{Z}_{>0}$ *we have:*

1. $\deg F_i - \deg G_i = p^i - \iota$;
2. *if* $p \geq 5$, *then* $G_i = S_p(X)^{ip^{i-1}+(i-1)p^{i-2}} \cdot H_i$, *where* $H_i \mid X^{s_i'} \cdot (X - 1728)^{r_i}$;
3. *if* $p = 2, 3$, *then* $G_i = X^{t_i}$, *where* $t_i \leq p^i$.

Also, there is a formula for $J_i(X)$ (which can be simplified if $p \geq 3$) obtained from the *classical modular polynomial*.

Modular Functions

Assume from now $p \geq 5$. Another perspective: if $E/\Bbbk$, ordinary, is given by $y_0^2 = x_0^3 + a_0 x_0 + b_0$, and $\boldsymbol{E}/W$ is its canonical lifting and (after some "choice") is given by $\boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}$, then

$$\boldsymbol{a} = (A_0, A_1, A_2, \ldots),$$
$$\boldsymbol{b} = (B_0, B_1, B_2, \ldots),$$

where $A_i, B_i \in \Bbbk(a_0, b_0)$. In fact, if $\mathcal{H}$ is the *Hasse invariant* of E (i.e., the coefficient of x_0^{p-1} is $(x_0^3 + a_0 x_0 + b_0)^{(p-1)/2}$), then A_i, B_i possibly have poles only at the zeros of $\mathcal{H}$ (or $\Delta = 4a_0^3 + 27b_0^2$).

Question

What are the weights of the A_i's and B_i's? What are the order of the poles?

Modular Functions (cont.)

Conjecture

1. A_i has weight $4p^i$.
2. B_i has weight $6p^i$.
3. A_i and B_i have poles of order at most $(i-1)p+1$ at the zeros of $\mathcal{H}$. (At least for $i \leq 2$. Not enough data yet.)
4. A_i and B_i have no zeros at zeros of Δ.

So, if true, the isomorphism $(a_0, b_0) \leftrightarrow (\lambda_0^4 a_0, \lambda_0^6 b_0)$ corresponds, via canonical liftings, to the isomorphism $(\boldsymbol{a}, \boldsymbol{b}) \leftrightarrow (\boldsymbol{\lambda}^4 \boldsymbol{a}, \boldsymbol{\lambda}^6 \boldsymbol{b})$, where $\boldsymbol{\lambda} = \tau(\lambda_0) = (\lambda_0, 0, 0, \dots)$.

Thank you!