Lifting the j-Invariant and Computations with Witt Vectors

Luís Finotti

University of Tennessee

UCSB – Jan 11, 2013

p-Adic Integers

Let:

- p be a prime, $r \in \mathbb{Z}_{>0}$, and $q \stackrel{\text{def}}{=} p^r$
- $\mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_p$ of degree r;
- $\mathbb{Z}_q$ be the ring of integers of $\mathbb{Q}_q$.

Then $\mathbb{Z}_q$ is a p-adic ring (or strict p-ring) with residue field $\mathbb{F}_q$.

Question

Given a perfect field $\mathbb{k}$ of characteristic p, is there a p-adic ring $R_{\mathbb{k}}$ with residue field $\mathbb{k}$?

Yes! Witt gave an explicit construction of such ring!

Constructing $\boldsymbol{W}(\mathbb{F}_q)$

Let $\boldsymbol{\mu}_m$ denote the m-th roots of unity. We have:

- $\boldsymbol{\mu}_{q-1} \subseteq \mathbb{Z}_q$ (Hensel's Lemma).
- $\{0\} \cup \boldsymbol{\mu}_{q-1}$ is a complete set of representatives of $\mathbb{F}_q$ in $\mathbb{Z}_q$.
- $a \in \mathbb{Z}_q$ has a unique representation of the form $a = \sum_{i=0}^{\infty} a_i p^i$ with $a_i \in \{0\} \cup \boldsymbol{\mu}_{q-1}$.

We can then identify a with $(\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots)$. But how do we add and multiply these elements now? We have

$$(\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots) + (\bar{b}_0, \bar{b}_1, \bar{b}_2, \ldots) = (S_0(\bar{a}_0, \bar{b}_0), S_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \ldots),$$

where $S_n \in \mathbb{Z}[X_0, X_1^{1/p}, \ldots, X_n^{1/p^n}, Y_0, Y_1^{1/p}, \ldots, Y_n^{1/p^n}]$. The product is similar.

Constructing $\boldsymbol{W}(\mathbb{F}_q)$ (cont.)

Better idea: to identify $a = \sum a_i p^i$ with $(\bar{a}_0, \bar{a}_1^p, \bar{a}_2^{p^2}, \ldots)$. Then:

$$(\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots) + (\bar{b}_0, \bar{b}_1, \bar{b}_2, \ldots) = (S_0(\bar{a}_0, \bar{b}_0), S_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \ldots),$$
$$(\bar{a}_0, \bar{a}_1, \bar{a}_2, \ldots) \cdot (\bar{b}_0, \bar{b}_1, \bar{b}_2, \ldots) = (P_0(\bar{a}_0, \bar{b}_0), P_1(\bar{a}_0, \bar{a}_1, \bar{b}_0, \bar{b}_1), \ldots),$$

where $S_n, P_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n, Y_0, Y_1, \ldots, Y_n]$. ($S_n$ and P_n depend only on p.)

Hence, we have an isomorphism of ring $\mathbb{F}_q^\infty$ with sum and product defined by polynomial equations above and $\mathbb{Z}_q$.

The Ring $\boldsymbol{W}(\Bbbk)$

Given a perfect field $\Bbbk$ of characteristic p, this construction makes $\Bbbk^\infty$ a p-adic ring with residue field $\Bbbk$ (with $p = (0, 1, 0, \ldots)$), the ring of Witt vectors over $\Bbbk$, denoted by $\boldsymbol{W}(\Bbbk)$.

As we can see from the power series identification, we have that $\boldsymbol{W}_n(\Bbbk) \stackrel{\text{def}}{=} \boldsymbol{W}(\Bbbk)/(p^n)$ is the truncation of vectors to the n-th coordinate, and hence we call this quotient ring the ring of Witt vectors of length n.

The p-th power Frobenius σ of $\Bbbk$ lifts to $\boldsymbol{W}(\Bbbk)$ by $\sigma(a_0, a_1, \ldots) = (\sigma(a_0), \sigma(a_1), \ldots,) = (a_0^p, a_1^p, \ldots)$.

Computing in $\boldsymbol{W}(\Bbbk)$

To compute with $\boldsymbol{W}_n(\Bbbk)$, need S_i, P_i for $i \in \{0, \ldots, (n-1)\}$.

Problem: These polynomials are huge! E.g., for $p = 31$, S_2 has $152{,}994$ monomials!

Thus, if $\Bbbk = \mathbb{F}_q$, one should make computations in $\mathbb{Z}_q$.

But, depending on $\Bbbk$, we cannot see $\boldsymbol{W}(\Bbbk)$ as a known local ring, and so we might need to use S_n and P_n for sums and products.

The Polynomials S_n and P_n.

S_n and P_n are given recursively:

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}),$$

and

$$\begin{aligned} P_n = {} & (X_0^{p^n} Y_n + X_1^{p^{n-1}} Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ & + \frac{1}{p}(X_0^{p^n} Y_{n-1}^p + \cdots + X_{n-1}^p Y_0^{p^n}) \\ & \vdots \\ & + \frac{1}{p^n}(X_0^{p^n} Y_0^{p^n}) - \frac{1}{p^n} P_0^{p^n} - \cdots - \frac{1}{p} P_{n-1}^p \\ & + p(\cdots). \end{aligned}$$

We cannot plug in coordinates on these formulas! Have to expand and simplify!

Teichmüller Lift

Remember that we have a lift of the Frobenius from $\Bbbk$ to $\boldsymbol{W}(\Bbbk)$. We also the *Teichmüller lift* $\tau : a \mapsto (a, 0, 0, \dots)$, which yields the following diagram:

$$\begin{tikzcd} W^\times \arrow[r, "\boldsymbol{\sigma}"] \arrow[d, bend right, "\pi"'] & W^\times \arrow[d, bend left, "\pi"] \\ \Bbbk^\times \arrow[r, "\sigma"] \arrow[u, bend right, "\tau"'] & \Bbbk^\times \arrow[u, bend left, "\tau"] \end{tikzcd}$$

Question

Can we also lift the Frobenius for curves over $\Bbbk$?

Curves

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

$$\begin{tikzcd} \boldsymbol{C}(\boldsymbol{W}(\bar{\mathbb{k}})) \arrow[r, dotted, "\boldsymbol{\phi}"] \arrow[d, "\pi"'] & \boldsymbol{C}^{\sigma}(\boldsymbol{W}(\bar{\mathbb{k}})) \arrow[d, "\pi"] \\ C(\bar{\mathbb{k}}) \arrow[r, "\phi"] & C^{\sigma}(\bar{\mathbb{k}}) \end{tikzcd}$$

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 $E/\Bbbk : y_0^2 = x_0^3 + a_0x_0 + b_0$, then there exists $\boldsymbol{a} = (a_0, a_1, \dots), \boldsymbol{b} = (b_0, b_1, \dots) \in W$ such that $\boldsymbol{E}/W : \boldsymbol{y}^2 = \boldsymbol{x}^3 + \boldsymbol{a}\boldsymbol{x} + \boldsymbol{b}$ has a lifting of the Frobenius:

$$\begin{tikzcd} \boldsymbol{E}(\boldsymbol{W}(\bar{\Bbbk})) \arrow[r, dotted, "\boldsymbol{\phi}"] \arrow[d, "\pi"'] & \boldsymbol{E}^{\sigma}(\boldsymbol{W}(\bar{\Bbbk})) \arrow[d, "\pi"] \\ E(\bar{\Bbbk}) \arrow[r, "\phi"] & E^{\sigma}(\bar{\Bbbk}) \end{tikzcd}$$

Elliptic Teichmüller Lift

Moreover, the curve $\boldsymbol{E}$ above is unique up to isomorphism and it is called the *canonical lifting of E*. Canonical liftings are often used in point counting (e.g., Satoh's algorithm) and have applications in coding theory and computing torsion points of higher genus curves.
As with Witt vectors, we also have a section of the reduction modulo p, the so called *elliptic Teichmüller lift τ*:

$$\begin{tikzcd} \boldsymbol{E}(\boldsymbol{W}(\bar{\Bbbk})) \arrow[r, dotted, "\phi"] \arrow[d, bend right, "\pi"'] & \boldsymbol{E}^{\sigma}(\boldsymbol{W}(\bar{\Bbbk})) \arrow[d, bend right, "\pi"'] \\ E(\bar{\Bbbk}) \arrow[r, "\phi"] \arrow[u, bend right, "\tau"'] & E^{\sigma}(\bar{\Bbbk}) \arrow[u, bend right, "\tau^{\sigma}"'] \end{tikzcd}$$

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 $F_i, G_i \in \Bbbk[x_0]$.

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:

$$\begin{tikzcd} \tilde{\boldsymbol{E}}(\boldsymbol{W}_3(\bar{\mathbb{k}})) \arrow[r, dotted, "\tilde{\phi}"] \arrow[d, bend right, "\pi"'] & \tilde{\boldsymbol{E}}^{\sigma}(\boldsymbol{W}_3(\bar{\mathbb{k}})) \arrow[d, bend right, "\pi"'] \\ E(\bar{\mathbb{k}}) \arrow[r, "\phi"] \arrow[u, bend right, "\nu"'] & E^{\sigma}(\bar{\mathbb{k}}) \arrow[u, bend right, "\nu^{\sigma}"'] \end{tikzcd}$$

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 the theory of minimal degree liftings 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

Let, as before, $E/\Bbbk$ be an ordinary elliptic curve and $\boldsymbol{E}/\boldsymbol{W}(\Bbbk)$ be its canonical lifting.

Thus if $\Bbbk^{ord}$ denotes the set of ordinary j-invariants in $\Bbbk$, we have functions $J_i : \Bbbk^{ord} \to \Bbbk$ such that $(j_0, J_1(j_0), J_2(j_0), \dots)$ 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 $\boldsymbol{W}(\Bbbk)$ 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 $j_0 \notin \Bbbk^{\mathrm{ord}}$ 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 $y_0^2 = x_0^3 + a_0x_0 + b_0$, 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

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

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 $(x_0^3 + a_0x_0 + b_0)^{(p-1)/2}$), 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 $\boldsymbol{\lambda} = \tau(\lambda_0) = (\lambda_0, 0, 0, \dots)$.

Modular Polynomial

The classical modular polynomial is a polynomial $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ such that two elliptic curves with j-invariants j_1 and j_2 have a (roughly speaking) "p-to-one morphism" between them if and only if $\Phi_p(j_1, j_2) = 0$.

Then, the lifting of the Frobenius gives us:

$$\Phi_p((j_0, J_1(j_0), J_2(j_0), \ldots), (j_0^p, J_1(j_0)^p, J_2(j_0)^p, \ldots)) = 0.$$

So, to compute $J_i(X)$, we use

$$\Phi_p((X, J_1(X), J_2(X), \ldots), (X^p, J_1(X)^p, J_2(X)^p, \ldots)) = 0.$$

We just expand it as Witt vectors, and we can solve in the i-th coordinate for $J_{i-1}(X)$. (Difficult computation!)

Greenberg Transform

The Greenberg transform is a crucial step in the proof of the main theorems and in concrete computations.

Let $\boldsymbol{f} \in \boldsymbol{W}(\mathbb{k})[\boldsymbol{x}, \boldsymbol{y}]$. By letting $\boldsymbol{x}_0 = (x_0, x_1, \dots)$ and $\boldsymbol{y}_0 = (y_0, y_1, \dots)$, we have $\boldsymbol{f}(\boldsymbol{x}_0, \boldsymbol{y}_0) = (f_0, f_1, f_2, \dots) \in \boldsymbol{W}(\mathbb{k}[x_0, x_1, \dots, y_0, y_1, \dots])$. We call $\mathscr{G}(\boldsymbol{f}) \stackrel{\text{def}}{=} (f_0, f_1, \dots)$ the Greenberg transform of $\boldsymbol{f}$.

Examples

$$\mathscr{G}(\boldsymbol{x} + \boldsymbol{y}) = (\bar{S}_0, \bar{S}_1, \bar{S}_2, \dots)$$
$$\mathscr{G}(\boldsymbol{x} \cdot \boldsymbol{y}) = (\bar{P}_0, \bar{P}_1, \bar{P}_2, \dots).$$

Explicit Example of a Greenberg Transform

Let $\boldsymbol{E/W}(\mathbb{F}_5) : \boldsymbol{y^2 = x^3 + 1}$. Then, the first three equations of the Greenberg Transform are:

1. $y_0^2 = x_0^3 + 1$;
2. $2y_0^5 y_1 = 4x_0^{12} + 3x_0^{10}x_1 + 3x_0^9 + 3x_0^6 + 4x_0^3$;
3. $4y_0^{25}y_1^5 + 2y_0^{25}y_2 + y_1^{10} = 4x_0^{72} + 3x_0^{69} + 3x_0^{6}6 + 4x_0^{63} + 2x_0^{58}x_1 + 3x_0^{57} + 3x_0^{56}x_1^2 + x_0^{55}x_1 + x_0^{54}x_1^3 + 2x_0^{54} + 3x_0^{53}x_1^2 + x_0^{52}x_1^4 + 4x_0^{52}x_1 + 4x_0^{51}x_1^3 + 2x_0^{50}x_1^5 + 4x_0^{50}x_1^2 + 3x_0^{50}x_2 + 2x_0^{49}x_1^4 + 3x_0^{49}x_1 + 3x_0^{48}x_1^3 + x_0^{48} + 2x_0^{46}x_1^4 + 4x_0^{44}x_1^2 + x_0^{43}x_1^4 + 4x_0^{43}x_1 + 3x_0^{42}x_1^3 + 4x_0^{41}x_1^2 + 4x_0^{40}x_1 + 4x_0^{39}x_1^3 + 4x_0^{39} + 4x_0^{37}x_1 + x_0^{36}x_1^3 + 4x_0^{36} + 4x_0^{35}x_1^2 + 3x_0^{32}x_1^2 + 3x_0^{31}x_1 + 3x_0^{29}x_1^2 + 4x_0^{28}x_1 + x_0^{27} + 3x_0^{25}x_1^{10} + x_0^{25}x_1 + 2x_0^{22}x_1 + 2x_0^{21} + 3x_0^{18} + 4x_0^{12} + 3x_0^9 + 3x_0^6 + 4x_0^3$

Computing J_i

One way to compute $J_i(X)$ is to compute the Greenberg transform of $\Phi_p(\boldsymbol{x}, \boldsymbol{y})$, evaluate at $\boldsymbol{x} = (X, J_1(X), J_2(X), \ldots)$, $\boldsymbol{y} = (X^p, J_1(X)^p, J_2(X)^p, \ldots)$, set coordinates equal to zero and solve.

We deduced a (very long and highly recursive) formula for the Greenberg transform. From that one can get an immediate formula for the J_i's.

But, the necessary evaluation makes the computation simpler if one removes terms that vanish. In fact the simplification also helps in proving the main theorems.

A Word About the Proofs

The proof of the main theorems was done by:

1. Use the formula for the Greenberg transform applied to $\Phi_p(\boldsymbol{x}, \boldsymbol{y})$.
2. Simplify it by removing unnecessary terms.
3. Use results of Kaneko-Zagier on J_1.
4. Some results followed, others were rephrased as questions on coefficients of Φ_p.
5. Answered the questions above. (Thanks to A. Sutherland.)

Computing with Witt Vectors

Note that we cannot compute sums and products by plugging in the entries in the recursive formulas of S_n and P_n, as those have p in the denominator. Thus, in general, one has to expand those formulas.

Problem: These polynomials are huge! E.g., S_2 has $152{,}994$ monomials for $p = 31$.

I was not able to compute S_4 for $p = 11$ with 24 gigabytes of memory. So, in general one cannot expect to make computations with Witt vectors of length 5 (or more) over fields of characteristic 11.

In some particular cases, such as over finite fields, there are efficient methods (via canonical isomorphisms) which avoids that. But often times one has to resort to the defining polynomials. (E.g., over polynomial rings, as when we compute the Greenberg transform.)

Computing with Witt Vectors (cont.)

Ideas to improve computations:

- Avoid expanding unnecessary powers: to compute $(\alpha+\beta)^n$ is better to first add α and β and then take an n-th power than to expand and store the polynomial $(X+Y)^n$ and then evaluate it at $X=\alpha$ and $Y=\beta$.
- Perform (most) computations in characteristic p.
- Replace S_n and P_n with *simpler* polynomials that work for both!
- Perhaps evaluate the polynomials above "on the fly", without having to precompute and store them.

Computing with Witt Vectors (cont.)

To clarify the last item: instead of computing and storing the polynomial

$$\eta_1(X,Y) = \frac{X^p + Y^p - (X+Y)^p}{p} = -\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X^i Y^{p-i},$$

one can compute $\eta_1(a,b)$ with the routine

```
res=0
for i in {1...(p-1)} do
  res = res - (binom(p,i)/p) * a^(p-i) * b^i
end for
return res
```

Auxiliary Polynomials

Definition

Define $\eta_0(X_1, \ldots, X_r) = X_1 + \cdots + X_r$ and, recursively, for $k \geq 1$,

$$\eta_0(X_1, \ldots, X_r)^{p^k} + p\eta_1(X_1, \ldots, X_r)^{p^{k-1}} + \cdots + p^k \eta_k(X_1, \ldots, X_r) = X_1^{p^k} + \cdots + X_r^{p^k}$$

Proposition

We have that $\eta_k(X_0, Y_0) = S_k(X_0, 0, \ldots, 0, Y_0, 0, \ldots 0)$ and $\eta_k(X_1, \ldots, X_r)$ has integral coefficients.

Auxiliary Polynomials

The functions η_i "replace divisions by p" in the recursive formulas for S_n, P_n and the Greenberg transform. (Only two variables are needed!)

(Note that η_i is *much* simpler than S_i.)

The formula for the Greenberg transform heavily rely on these functions!

Moreover, their reduction modulo p can be computed mostly on characteristic p, they avoid expanding powers, and can be computed on the fly.

Witt Sum with η_i's (cont.)

We have that $\bar{S}_n = \sum_{t \in \mathcal{S}_n} t$, where:

$$\begin{aligned}
\mathcal{S}_0 &= (x_0, y_0) \\
\mathcal{S}_1 &= (x_1, y_1, \eta_1(\mathcal{S}_0)) \\
\mathcal{S}_2 &= (x_2, y_2, \eta_2(\mathcal{S}_0), \eta_1(\mathcal{S}_1)) \\
\mathcal{S}_3 &= (x_3, y_3, \eta_3(\mathcal{S}_0), \eta_2(\mathcal{S}_1), \eta_1(\mathcal{S}_2)) \\
&\vdots
\end{aligned}$$

Witt Products with η_i's

Similarly, we have that $\bar{P}_n = \sum_{t \in \mathcal{P}_n} t$, where:

$$\begin{aligned}
\mathcal{P}_0 &= (x_0 y_0) \\
\mathcal{P}_1 &= (x_1 y_0^p, x_0^p y_1) \\
\mathcal{P}_2 &= (x_2 y_0^{p^2}, x_1^p y_1^p, x_0^{p^2} y_2, \eta_1(\mathcal{P}_1)) \\
\mathcal{P}_3 &= (x_3 y_0^{p^3}, x_2^p y_1^{p^2}, x_1^{p^2} y_2^p, x_0^{p^3} y_3, \eta_2(\mathcal{P}_1), \eta_1(\mathcal{P}_2)) \\
&\vdots
\end{aligned}$$

Different Methods

There are two ways to compute $\eta_k(a_1, \ldots, a_n)$, for $a_i \in \mathbb{k}$ (in characteristic p).

- We compute and store the polynomials $\bar{\eta}_k(X, Y) \in \mathbb{F}_p[X, Y]$ (two variables only) and use a recursive algorithm to compute $\eta_k(a_1, \ldots, a_n)$.
- We compute and store some expansion of some binomials coefficients as Witt vectors (much smaller to store and quicker to compute) and use a highly recursive algorithm to compute $\eta_k(a_1, \ldots, a_n)$.

In either case we have great gains when performing computation with Witt vectors.

Example

For $p = 11$ we've computed S_3 using the usual recursive formula and using the formula for the GT. The former took 130.56 hours, while the latter took 7.20 hours. (The computation of $\bar{\eta}_i(X, Y)$ for $i = 1, 2, 3$ takes only 0.19 seconds in this case.)

Comparing the Methods

The 24 gigabytes of memory available were not enough to compute S_4 with either method. On the other hand, we do not need S_4 to add Witt vectors with our new methods.

Example

We can add two vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$ in about 1 second, after we spend approximately 3.61 hours to compute the $\bar{\eta}_i(X, Y)$ for $i \in \{1, 2, 3, 4, 5\}$. Using the other method, we need only 5.750 seconds to compute the Witt vectors of the binomial coefficients, but then it takes us about 26 seconds on average to add two Witt vectors in $\boldsymbol{W}_6(\mathbb{F}_{11^{10}})$.

Evaluating a Polynomial

The table below give times (in seconds) and memory usages (in MB) to evaluate a randomly chosen $\boldsymbol{f} \in \boldsymbol{W}_{n+1}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$, where $\deg_{\boldsymbol{x}} \boldsymbol{f}, \deg_{\boldsymbol{y}} \boldsymbol{f} \leq d$, at a randomly chosen $(\boldsymbol{x}_0, \boldsymbol{y}_0)$.

				Sum and Prod.		**GT form.**	
$\Bbbk$	n	d	$\bar{\eta}_i$ time	time	mem.	time	mem.
$\mathbb{F}_{3^{10}}$	9	20	108.78	433.31	12.22	130.28	16.40
$\mathbb{F}_{7^{10}}$	6	20	3554.78	2410.49	28.00	600.23	28.62
$\mathbb{F}_{11^{10}}$	5	20	5794.89	3564.62	37.44	839.37	30.88
$\mathbb{F}_{13^{10}}$	5	15	29854.75	4608.84	70.63	1045.08	49.00
$\mathbb{F}_{19^{10}}$	4	15	2760.36	2301.17	32.44	983.08	26.72

The sums and products were already the optimized ones!

Performance Differences for the GT

The following table shows the times and memory needed to compute the GT of

$$\boldsymbol{x}^3 + (a_0, a_1, a_2)\boldsymbol{x}^2 + (b_0, b_1, b_2)\boldsymbol{x} + (c_0, c_1, c_2),$$

with a_i's, b_i's and c_i's unknowns. ("orig." means evaluate the sums and products, "new" means use the GT formula.)
In Sage:

char.	$t_{\text{orig.}}$ (sec)	t_{new} (sec)	$m_{\text{orig.}}$ (MB)	m_{new} (MB)
5	0.50	0.29	5.82	4.82
7	27.48	1.30	65.82	33.82
11	10265.87	196.01	3566.32	1721.82
13	$--$	1368.54	$--$	8416.57

Note how demanding the computation of the GT is! E.g., the third coordinate for $p = 11$ is a polynomial in 12 variables with $31,216,093$ terms. For $p = 13$, it has $153,065,983$ terms!

Computing Times for J_3

The following table list times and memory usages to compute J_3 in the three different ways:

- **Method 1:** Use (standard, non-improved) sums and products of Witt vectors.
- **Method 2:** Use the formula for the Greenberg transform.
- **Method 3:** Use the formula of GT to make simplifications on J_3.

The Table

	Method 1		Method 2		Method 3	
p	time	mem.	time	mem.	time	mem.
5	407.089	376.78	0.480	21.28	0.990	36.91
7	−−	−−	7.300	40.97	5.089	33.22
11	−−	−−	421.090	1010.03	289.439	103.94
13	−−	−−	6542.590	4175.28	7496.840	356.16
17	−−	−−	−−	−−	45967.959	1982.28
19	−−	−−	−−	−−	267733.840	3650.62
23	−−	−−	−−	−−	1574171.979	13647.28

Table: Computations of J_3. (Time in sec., memory in MB.)

Recursive Definition

A general formula for the Greenberg transform was crucial to many of the results.
The starting point for the formula is the following theorem.

Theorem

Let $\boldsymbol{f}(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x},\boldsymbol{y}]$, and let $\boldsymbol{f}_n$ be defined recursively by $\boldsymbol{f}_0 \stackrel{\text{def}}{=} \boldsymbol{f}$ and

$$\begin{aligned} &\boldsymbol{f}_0^{p^n} + p\boldsymbol{f}_1^{p^{n-1}} + \cdots + p^n \boldsymbol{f}_n = \\ &\qquad \boldsymbol{f}^{\sigma^n}(\boldsymbol{x}_0^{p^n} + p\boldsymbol{x}_1^{p^{n-1}} + \cdots + p^n \boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + p\boldsymbol{y}_1^{p^{n-1}} + \cdots + p^n \boldsymbol{y}_n) \end{aligned}$$

Then, $\mathscr{G}(\boldsymbol{f}) = (f_0, f_1, \ldots)$ where f_i is the reduction modulo p of $\boldsymbol{f}_i$. (Remember that σ is the Frobenius of $\boldsymbol{W}(\Bbbk)$.)

Taylor Expansion

The idea is to use the Taylor expansion:

$$\boldsymbol{f}^{\sigma^n}(\boldsymbol{x}_0^{p^n} + p\boldsymbol{x}_1^{p^{n-1}} + \cdots + p^n\boldsymbol{x}_n, \boldsymbol{y}_0^{p^n} + p\boldsymbol{y}_1^{p^{n-1}} + \cdots + p^n\boldsymbol{y}_n) =$$
$$\sum_{r=0}^{\infty} p^r \sum_{i=0}^{r} (\boldsymbol{f}^{\sigma^n})^{(i,r-i)}(\boldsymbol{x}_0^{p^n}, \boldsymbol{y}_0^{p^n}) W_{n-1}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)^i W_{n-1}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n)^{r-i}$$

where,

$$(\boldsymbol{f}^{\sigma^n})^{(i,r-i)} \stackrel{\text{def}}{=} \frac{1}{i!(r-i)!} \frac{\partial^r \boldsymbol{f}^{\sigma^n}}{\partial^i \partial^{r-i}},$$

and

$$W_{n-1}(X_1, \ldots, X_n) = X_1^{p^{n-1}} + p\, X_2^{p^{n-2}} + \cdots + p^{n-1} X_n.$$

Notation

We need some notation. Let $\boldsymbol{g} \stackrel{\text{def}}{=} \sum_{i,j} \boldsymbol{a}_{i,j}\boldsymbol{x}^i\boldsymbol{y}^j \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x},\boldsymbol{y}]$.

1. Write $\boldsymbol{a}_{i,j} = \sum_{k=0}^{\infty} \boldsymbol{a}_{i,j,k}p^k$ (with the Teichmüller repres. $\boldsymbol{a}_{i,j,k}$).
2. Define $\xi_k(\boldsymbol{g}) \stackrel{\text{def}}{=} \sum_{i,j} \boldsymbol{a}_{i,j,k}\boldsymbol{x}^i\boldsymbol{y}^j$. (Hence, $\boldsymbol{g} = \sum_{k=0}^{\infty} \xi_k(\boldsymbol{g})p^k$.)
3. Define $\boldsymbol{g}^{(i,j)} \stackrel{\text{def}}{=} \frac{1}{i!j!}\frac{\partial^{i+j}}{\partial^i\partial^j}\boldsymbol{g}$, and $\boldsymbol{g}_{i,j,k} \stackrel{\text{def}}{=} \xi_k(\boldsymbol{g}^{(i,j)})$.
4. Define $D_{k,n}^{i,j}$ to be the coefficient of $\boldsymbol{t}^k$ in
$$(\boldsymbol{t}\boldsymbol{x}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{x}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{x}_n)^i(\boldsymbol{t}\boldsymbol{y}_1^{p^{n-1}} + \boldsymbol{t}^2\boldsymbol{y}_2^{p^{n-2}} + \cdots + \boldsymbol{t}^n\boldsymbol{y}_n)^j.$$
(E.g., $D_{4,n}^{1,2} = 2\boldsymbol{x}_1^{p^{n-1}}\boldsymbol{y}_1^{p^{n-1}}\boldsymbol{y}_2^{p^{n-2}} + \boldsymbol{x}_2^{p^{n-2}}\boldsymbol{y}_1^{2p^{n-1}}$.)
5. Finally, $D_{k,n,l}^{i,j} \stackrel{\text{def}}{=} \xi_l(D_{k,n}^{i,j})$.

The Formula

Let $\boldsymbol{f} \in \boldsymbol{W}(\Bbbk)[\boldsymbol{x}, \boldsymbol{y}]$.

1. For $l \geq 0$, let $\{\mathcal{G}_{l,1}, \ldots, \mathcal{G}_{l,N_l}\}$ be the monomials of $(\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i}$, for $0 \leq i \leq r \leq j, k \leq l$.
2. If $l > 1$, $\mathcal{G}_{l,N_l+i+1} \stackrel{\text{def}}{=} \eta_{l-i}(\mathcal{G}_{i,1}, \ldots, \mathcal{G}_{i,N_i+i})$, for $i \in \{0, \ldots, (l-1)\}$.
3. Let

$$\boldsymbol{f}_l \stackrel{\text{def}}{=} \sum_{i=1}^{N_l+l} \mathcal{G}_{l,i} = \sum_{r=0}^{l} \sum_{i=0}^{r} \sum_{j=r}^{l} \sum_{k=r}^{j} (\boldsymbol{f}^{\sigma^l})_{i,r-i,l-j}(\boldsymbol{x}_0^{p^l}, \boldsymbol{y}_0^{p^l}) D_{k,l,j-k}^{i,r-i} + \sum_{i=0}^{l-1} \eta_{l-i}(\mathcal{G}_{i,1}, \ldots, \mathcal{G}_{i,N_i+i})$$

Theorem

We have that $\mathscr{G}(\boldsymbol{f}) = (f_0, f_1, \ldots)$, where f_i is the reduction modulo p of $\boldsymbol{f}_i$.

The $\mathcal{G}_i$'s

With the notation above, let $\mathcal{G}_i = (\mathcal{G}_{i,1}, \dots \mathcal{G}_{i,N_i+i})$. Then:

- $(\mathcal{G}_{0,1}, \dots, \mathcal{G}_{0,N_0})$ is the vector of monomials of $\boldsymbol{f}$.

- $(\mathcal{G}_{1,1}, \dots, \mathcal{G}_{1,N_1})$ are the monomials from $(\boldsymbol{f}^{\sigma})_{i,r-i,1-j}(\boldsymbol{x}_0^p, \boldsymbol{y}_0^p)D^{i,r-i}_{k,1,j-k}$, for $0 \leq i \leq r \leq j, k \leq 1$, and $\mathcal{G}_{1,N_1+1} = \eta_1(\mathcal{G}_0)$. **Notation:** We write $\eta_k(\boldsymbol{f})$ for $\eta_k(\mathcal{G}_0)$, i.e., the evaluation of η_k at a vector made of the monomials of $\boldsymbol{f}$.

- $(\mathcal{G}_{2,1}, \dots, \mathcal{G}_{0,N_2})$ are the monomials from $(\boldsymbol{f}^{\sigma^2})_{i,r-i,2-j}(\boldsymbol{x}_0^{p^2}, \boldsymbol{y}_0^{p^2})D^{i,r-i}_{k,2,j-k}$, for $0 \leq i \leq r \leq j, k \leq 2$, $\mathcal{G}_{2,N_2+1} = \eta_2(\mathcal{G}_0)$, and $\mathcal{G}_{2,N_2+2} = \eta_1(\mathcal{G}_1)$.

Then, the $\boldsymbol{f}_n$ above is the sum of the entries of $\mathcal{G}_n$.

Thank you!