Faster Computation of Witt Vectors Ring Laws

Rubén Muñoz--Bertrand

CNRS / Université Marie & Louis Pasteur

29/04/2025

Constructing $\mathbb{R}$

In the beginning, we created $\mathbb{N}$:
$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\ldots$

Constructing $\mathbb{R}$

In the beginning, we created $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10...

And $\mathbb{Z}$:
-1, -2...

Constructing $\mathbb{R}$

In the beginning, we created $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10...

And $\mathbb{Z}$:
-1, -2...

From which we made $\mathbb{Q}$:
$\frac{3}{2} = 1.5$
$\frac{1}{7} = 0.142857142857\ldots$

Constructing $\mathbb{R}$

In the beginning, we created $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10...

And $\mathbb{Z}$:
-1, -2...

From which we made $\mathbb{Q}$:
$\frac{3}{2} = 1.5$
$\frac{1}{7} = 0.142857142857\ldots$

And its completion $\mathbb{R}$:
$\sqrt{2} = 1.4142135623\ldots$
$\pi = 3.1415926535897\ldots$

Constructing $\mathbb{R}$ in base-7

In the beginning, we created $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 10, 11, 12, 13...

And $\mathbb{Z}$:
-1, -2...

From which we made $\mathbb{Q}$:
$\frac{3}{2} = 1.3333333333333\dots$
$\frac{1}{10} = 0.1$

And its completion $\mathbb{R}$:
$\sqrt{2} = 1.26203454521\dots$
$\pi = 3.0663651432\dots$

p-adic numbers

Ostrowski's theorem tells us that completing « after the point » is not the only option : one can also complete « before the point ».

p-adic numbers

Ostrowski's theorem tells us that completing « after the point » is not the only option : one can also complete « before the point ».

One then gets $\mathbb{Q}_7$, a ring containing $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 10, 11, 12, 13. . .

p-adic numbers

Ostrowski's theorem tells us that completing « after the point » is not the only option : one can also complete « before the point ».

One then gets $\mathbb{Q}_7$, a ring containing $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 10, 11, 12, 13...

In that ring, one has:
$\ldots 6666666 + 1 = 0$.

p-adic numbers

Ostrowski's theorem tells us that completing « after the point » is not the only option : one can also complete « before the point ».

One then gets $\mathbb{Q}_7$, a ring containing $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 10, 11, 12, 13...

In that ring, one has:
$\ldots 6666666 + 1 = 0$.
So we can write the elements of $\mathbb{Z}$ in the following manner:
$\ldots 6666666 = -1, \ldots 6666665 = -2 \ldots$

p-adic numbers

Ostrowski's theorem tells us that completing « after the point » is not the only option : one can also complete « before the point ».

One then gets $\mathbb{Q}_7$, a ring containing $\mathbb{N}$:
0, 1, 2, 3, 4, 5, 6, 10, 11, 12, 13...

In that ring, one has:
$\dots 6666666 + 1 = 0$.
So we can write the elements of $\mathbb{Z}$ in the following manner:
$\dots 6666666 = -1$, $\dots 6666665 = -2 \dots$

Similarly, for $\mathbb{Q}$:
$\frac{3}{2} = \dots 33333335$
$\frac{1}{10} = 0.1$

p-adic integers

We now fix a prime number p. The ring $\mathbb{Z}_p$ of p-adic integers is the set of every number in $\mathbb{Q}_p$ « without digits afters the point ».

p-adic integers

We now fix a prime number p. The ring $\mathbb{Z}_p$ of p-adic integers is the set of every number in $\mathbb{Q}_p$ « without digits afters the point ».

There is a surjective morphism $\pi\colon \mathbb{Z}_p \to \mathbb{F}_p$ of rings, which to a p-adic integer associates its rightmost digit.

$$\ldots 12345612345600123 \mapsto 3$$

$$12 \mapsto 2$$

Hensel's lemma

Hensel's lemma (1904)

Let $P \in \mathbb{Z}_p[X]$. If there is $\alpha \in \mathbb{F}_p$ such that $P(\alpha) = 0$ and $P'(\alpha) \neq 0$, then there is $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and that $\pi(x) = \alpha$.

Hensel's lemma

Hensel's lemma (1904)

Let $P \in \mathbb{Z}_p[X]$. If there is $\alpha \in \mathbb{F}_p$ such that $P(\alpha) = 0$ and $P'(\alpha) \neq 0$, then there is $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and that $\pi(x) = \alpha$.

For instance, if $\ell \in \mathbb{N}^*$ is coprime with p, then $P = \ell X - 1$ satisfies the conditions of Hensel's lemma: we find that $\frac{1}{\ell} \in \mathbb{Z}_p$.

Hensel's lemma (1904)

Let $P \in \mathbb{Z}_p[X]$. If there is $\alpha \in \mathbb{F}_p$ such that $P(\alpha) = 0$ and $P'(\alpha) \neq 0$, then there is $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and that $\pi(x) = \alpha$.

For instance, if $\ell \in \mathbb{N}^*$ is coprime with p, then $P = \ell X - 1$ satisfies the conditions of Hensel's lemma: we find that $\frac{1}{\ell} \in \mathbb{Z}_p$.

More generally, one can show that $x \in \mathbb{Z}_p$ is invertible if and only if $\pi(x) \neq 0$.

Hensel's lemma

Hensel's lemma (1904)

Let $P \in \mathbb{Z}_p[X]$. If there is $\alpha \in \mathbb{F}_p$ such that $P(\alpha) = 0$ and $P'(\alpha) \neq 0$, then there is $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and that $\pi(x) = \alpha$.

For instance, if $\ell \in \mathbb{N}^*$ is coprime with p, then $P = \ell X - 1$ satisfies the conditions of Hensel's lemma: we find that $\frac{1}{\ell} \in \mathbb{Z}_p$.

More generally, one can show that $x \in \mathbb{Z}_p$ is invertible if and only if $\pi(x) \neq 0$.

In $\mathbb{Z}_7$, the polynomial $P = X^2 - 2$ satisfies the conditions of Hensel's lemma.

Hensel's lemma

Hensel's lemma (1904)

Let $P \in \mathbb{Z}_p[X]$. If there is $\alpha \in \mathbb{F}_p$ such that $P(\alpha) = 0$ and $P'(\alpha) \neq 0$, then there is $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and that $\pi(x) = \alpha$.

For instance, if $\ell \in \mathbb{N}^*$ is coprime with p, then $P = \ell X - 1$ satisfies the conditions of Hensel's lemma: we find that $\frac{1}{\ell} \in \mathbb{Z}_p$.

More generally, one can show that $x \in \mathbb{Z}_p$ is invertible if and only if $\pi(x) \neq 0$.

In $\mathbb{Z}_7$, the polynomial $P = X^2 - 2$ satisfies the conditions of Hensel's lemma.

So there are two square roots of 2 in $\mathbb{Z}_7$:
$\ldots 421216213$
$\ldots 245450454$

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

In what follows, fix a precision `n`.

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

In what follows, fix a precision `n`.

One can implement elements in $\mathbb{Z}_p$ simply by only looking at the `n` rightmost digits.

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

In what follows, fix a precision `n`.

One can implement elements in $\mathbb{Z}_p$ simply by only looking at the `n` rightmost digits.

$\ldots 1303 + \ldots 2311 = \ldots 3614$
$\ldots 1111 - \ldots 0002 = \ldots 1106$
$\ldots 1111 \times \ldots 2222 = \ldots 1642$
$\ldots 4422 \div \ldots 1111 = \ldots 0202$

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

In what follows, fix a precision `n`.

One can implement elements in $\mathbb{Z}_p$ simply by only looking at the `n` rightmost digits.

$\dots 1303 + \dots 2311 = \dots 3614$
$\dots 1111 - \dots 0002 = \dots 1106$
$\dots 1111 \times \dots 2222 = \dots 1642$
$\dots 4422 \div \dots 1111 = \dots 0202$

Beware: $\dots 1110 \div \dots 0010 = \dots 111$ (we lose precision).

The simplest implementation: absolute capping

Like real numbers, p-adic numbers are infinite, and one can only implement them up to some precision.

In what follows, fix a precision $\mathtt{n}$.

One can implement elements in $\mathbb{Z}_p$ simply by only looking at the $\mathtt{n}$ rightmost digits.

$\ldots 1303 + \ldots 2311 = \ldots 3614$
$\ldots 1111 - \ldots 0002 = \ldots 1106$
$\ldots 1111 \times \ldots 2222 = \ldots 1642$
$\ldots 4422 \div \ldots 1111 = \ldots 0202$

Beware: $\ldots 1110 \div \ldots 0010 = \ldots 111$ (we lose precision).

Notice that $\mathbb{Z}_p / p^{\mathtt{n}} \mathbb{Z}_p \cong \mathbb{Z} / p^{\mathtt{n}} \mathbb{Z}$.

Extending the implementation: relative capping

In order to extend the implementation to $\mathbb{Q}_p$, one can still implement p-adic numbers by storing `n` digits without non-zero digits at their right, and the position of the rightmost of these digits.

Extending the implementation: relative capping

In order to extend the implementation to $\mathbb{Q}_p$, one can still implement p-adic numbers by storing `n` digits without non-zero digits at their right, and the position of the rightmost of these digits.

$$\ldots 1342 = \ldots 1342 \times p^0$$
$$\ldots 235500 = \ldots 2355 \times p^2$$
$$\ldots 6.555 = \ldots 6555 \times p^{-3}$$

Extending the implementation: relative capping

In order to extend the implementation to $\mathbb{Q}_p$, one can still implement p-adic numbers by storing `n` digits without non-zero digits at their right, and the position of the rightmost of these digits.

$\dots 1342 = \dots 1342 \times p^0$
$\dots 235500 = \dots 2355 \times p^2$
$\dots 6.555 = \dots 6555 \times p^{-3}$

$\dots 1342 \times p^0 + \dots 2355 \times p^2 = \dots 0142 \times p^0$

Extending the implementation: relative capping

In order to extend the implementation to $\mathbb{Q}_p$, one can still implement p-adic numbers by storing `n` digits without non-zero digits at their right, and the position of the rightmost of these digits.

$$\ldots 1342 = \ldots 1342 \times p^0$$
$$\ldots 235500 = \ldots 2355 \times p^2$$
$$\ldots 6.555 = \ldots 6555 \times p^{-3}$$

$$\ldots 1342 \times p^0 + \ldots 2355 \times p^2 = \ldots 0142 \times p^0$$
$$\ldots 2355 \times p^2 \times \ldots 6555 \times p^{-3} = \ldots 6244 \times p^{-1}$$

Extending the implementation: relative capping

In order to extend the implementation to $\mathbb{Q}_p$, one can still implement p-adic numbers by storing `n` digits without non-zero digits at their right, and the position of the rightmost of these digits.

$$\ldots 1342 = \ldots 1342 \times p^0$$
$$\ldots 235500 = \ldots 2355 \times p^2$$
$$\ldots 6.555 = \ldots 6555 \times p^{-3}$$

$$\ldots 1342 \times p^0 + \ldots 2355 \times p^2 = \ldots 0142 \times p^0$$
$$\ldots 2355 \times p^2 \times \ldots 6555 \times p^{-3} = \ldots 6244 \times p^{-1}$$

We still lose precision when dividing by $\ldots 0010 \times p^0$.

Another implementation: floating point arithmetic

Similarly as with real numbers, there is a floating point implementation for p-adic numbers.

Another implementation: floating point arithmetic

Similarly as with real numbers, there is a floating point implementation for p-adic numbers.

Write a p-adic number as $p^e s$, where $e_{\min} \leqslant e \leqslant e_{\max}$ is an integer, and $-\frac{p^{\mathtt{n}}-1}{2} < s \leqslant \frac{p^{\mathtt{n}}-1}{2}$ is an integer coprime with p.

Another implementation: floating point arithmetic

Similarly as with real numbers, there is a floating point implementation for p-adic numbers.

Write a p-adic number as $p^e s$, where $e_{\min} \leqslant e \leqslant e_{\max}$ is an integer, and $-\frac{p^{n}-1}{2} < s \leqslant \frac{p^{n}-1}{2}$ is an integer coprime with p.

The main difference here is asking s to be coprime with p. Whereas we were allowed to use ...0010 $\times p^0$ with relative capping, now we have to write it as ...0001 $\times p^1$

Another implementation: floating point arithmetic

Similarly as with real numbers, there is a floating point implementation for p-adic numbers.

Write a p-adic number as $p^e s$, where $e_{\min} \leqslant e \leqslant e_{\max}$ is an integer, and $-\frac{p^{\mathrm{n}}-1}{2} < s \leqslant \frac{p^{\mathrm{n}}-1}{2}$ is an integer coprime with p.

The main difference here is asking s to be coprime with p. Whereas we were allowed to use $\ldots 0010 \times p^0$ with relative capping, now we have to write it as $\ldots 0001 \times p^1$

We do not lose precision any longer after dividing by this number! But now, there is overflow and underflow with e.

Unramified extensions

We have discovered a new field $\mathbb{Q}_p$ of characteristic zero.

Unramified extensions

We have discovered a new field $\mathbb{Q}_p$ of characteristic zero.
It has a subring $\mathbb{Z}_p$ with a surjection to $\mathbb{F}_p$.

Unramified extensions

We have discovered a new field $\mathbb{Q}_p$ of characteristic zero.
It has a subring $\mathbb{Z}_p$ with a surjection to $\mathbb{F}_p$.

If one takes a polynomial $P(X) \in \mathbb{Z}_p[X]$ reducing to an irreducible polynomial in $\mathbb{F}_p$, it defines an extension of finite fields $\mathbb{F}_p \to \mathbb{F}_q \cong \mathbb{F}_p[X]/\langle P(X) \rangle$.

Unramified extensions

We have discovered a new field $\mathbb{Q}_p$ of characteristic zero.
It has a subring $\mathbb{Z}_p$ with a surjection to $\mathbb{F}_p$.

If one takes a polynomial $P(X) \in \mathbb{Z}_p[X]$ reducing to an irreducible polynomial in $\mathbb{F}_p$, it defines an extension of finite fields $\mathbb{F}_p \to \mathbb{F}_q \cong \mathbb{F}_p[X]/\langle P(X) \rangle$.

We call the extension $\mathbb{Q}_p \to \mathbb{Q}_q \cong \mathbb{Q}_p[X]/\langle P(X) \rangle$ an unramified extension.

Unramified extensions

We have discovered a new field $\mathbb{Q}_p$ of characteristic zero.
It has a subring $\mathbb{Z}_p$ with a surjection to $\mathbb{F}_p$.

If one takes a polynomial $P(X) \in \mathbb{Z}_p[X]$ reducing to an irreducible polynomial in $\mathbb{F}_p$, it defines an extension of finite fields $\mathbb{F}_p \to \mathbb{F}_q \cong \mathbb{F}_p[X]/\langle P(X) \rangle$.

We call the extension $\mathbb{Q}_p \to \mathbb{Q}_q \cong \mathbb{Q}_p[X]/\langle P(X) \rangle$ an unramified extension.

Philosophically, we have allowed division by p in finite fields!

Some strange ring laws

There is a bijection between $\mathbb{Z}_p$ and ${\mathbb{F}_p}^{\mathbb{N}}$ given by looking at the sequence of the digits of a p-adic integer.

$$\begin{aligned} \ldots 421216213 &\longleftrightarrow (3, 1, 2, 6, 1, 2, 1, 2, 4, \ldots) \\ 54 &\longleftrightarrow (4, 5, 0, 0, 0, 0, 0, 0, 0, \ldots) \end{aligned}$$

Some strange ring laws

There is a bijection between $\mathbb{Z}_p$ and ${\mathbb{F}_p}^{\mathbb{N}}$ given by looking at the sequence of the digits of a p-adic integer.

$$\begin{aligned} \ldots 421216213 &\longleftrightarrow (3, 1, 2, 6, 1, 2, 1, 2, 4, \ldots) \\ 54 &\longleftrightarrow (4, 5, 0, 0, 0, 0, 0, 0, 0, \ldots) \end{aligned}$$

This yields new ring laws on the set of sequences with values in $\mathbb{F}_p$.

Some strange ring laws

There is a bijection between $\mathbb{Z}_p$ and ${\mathbb{F}_p}^{\mathbb{N}}$ given by looking at the sequence of the digits of a p-adic integer.

$$\begin{aligned} \dots 421216213 &\longleftrightarrow (3, 1, 2, 6, 1, 2, 1, 2, 4, \dots) \\ 54 &\longleftrightarrow (4, 5, 0, 0, 0, 0, 0, 0, 0, \dots) \end{aligned}$$

This yields new ring laws on the set of sequences with values in $\mathbb{F}_p$.

This is something a mathematician has to generalise!

Witt vectors

Let A be (any) commutative ring. The ring $W_p(A)$ of Witt vectors with coefficients in A is, as a set, $A^{\mathbb{N}}$ (the sequences with coefficients in A).

Witt vectors

Let A be (any) commutative ring. The ring $W_p(A)$ of Witt vectors with coefficients in A is, as a set, $A^{\mathbb{N}}$ (the sequences with coefficients in A). Think of this set as digits.

Let A be (any) commutative ring. The ring $W_p(A)$ of Witt vectors with coefficients in A is, as a set, $A^{\mathbb{N}}$ (the sequences with coefficients in A). Think of this set as digits.

For $n \in \mathbb{N}$, we introduce the polynomial $W_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$.

Witt vectors

Let A be (any) commutative ring. The ring $W_p(A)$ of Witt vectors with coefficients in A is, as a set, $A^{\mathbb{N}}$ (the sequences with coefficients in A). Think of this set as digits.

For $n \in \mathbb{N}$, we introduce the polynomial $W_n = \sum_{i=0}^{n} p^i {X_i}^{p^{n-i}}$.

$$
\begin{aligned}
W_0 &= X_0 \\
W_1 &= {X_0}^p + pX_1 \\
W_2 &= {X_0}^{p^2} + p{X_1}^p + p^2 X_2 \\
&\dots
\end{aligned}
$$

Witt vectors

Let A be (any) commutative ring. The ring $W_p(A)$ of Witt vectors with coefficients in A is, as a set, $A^{\mathbb{N}}$ (the sequences with coefficients in A). Think of this set as digits.

For $n \in \mathbb{N}$, we introduce the polynomial $W_n = \sum_{i=0}^{n} p^i {X_i}^{p^{n-i}}$.

$$\begin{aligned} W_0 &= X_0 \\ W_1 &= {X_0}^p + pX_1 \\ W_2 &= {X_0}^{p^2} + p{X_1}^p + p^2 X_2 \\ &\dots \end{aligned}$$

Think of them as truncations of p-adic expansions (for instance $201 = 1^{p^2} + p \times 0^p + p^2 \times 2$ in $\mathbb{Z}_p$).

Witt vectors polynomials

By induction on $n \in \mathbb{N}$, we can construct polynomials S_n such that:

$$W_n(S_0, \ldots, S_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n).$$

Witt vectors polynomials

By induction on $n \in \mathbb{N}$, we can construct polynomials S_n such that:

$$W_n(S_0, \ldots, S_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n).$$

We must have $S_0 = X_0 + Y_0$.

Witt vectors polynomials

By induction on $n \in \mathbb{N}$, we can construct polynomials S_n such that:

$$W_n(S_0, \ldots, S_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n).$$

We must have $S_0 = X_0 + Y_0$.

Then we look for S_1 satisfying:

$${S_0}^p + pS_1 = {X_0}^p + pX_1 + {Y_0}^p + pY_1.$$

Witt vectors polynomials

By induction on $n \in \mathbb{N}$, we can construct polynomials S_n such that:

$$W_n(S_0, \dots, S_n) = W_n(X_0, \dots, X_n) + W_n(Y_0, \dots, Y_n).$$

We must have $S_0 = X_0 + Y_0$.

Then we look for S_1 satisfying:

$${S_0}^p + pS_1 = {X_0}^p + pX_1 + {Y_0}^p + pY_1.$$

That is: $pS_1 = {X_0}^p + pX_1 + {Y_0}^p + pY_1 - (X_0 + Y_0)^p$.

Witt vectors polynomials

By induction on $n \in \mathbb{N}$, we can construct polynomials S_n such that:

$$W_n(S_0, \ldots, S_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n).$$

We must have $S_0 = X_0 + Y_0$.

Then we look for S_1 satisfying:

$$S_0{}^p + pS_1 = X_0{}^p + pX_1 + Y_0{}^p + pY_1.$$

That is: $pS_1 = X_0{}^p + pX_1 + Y_0{}^p + pY_1 - (X_0 + Y_0)^p$.

We find:

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{\binom{i}{p}}{p} X_0{}^i Y_0{}^{p-i}.$$

Witt vectors ring laws

This method is actually an algorithm to compute every S_n.

This method is actually an algorithm to compute every S_n.

Similarly, for every $n \in \mathbb{N}$, we get polynomials P_n such that:

$$W_n(P_0, \ldots, P_n) = W_n(X_0, \ldots, X_n) \times W_n(Y_0, \ldots, Y_n).$$

Witt vectors ring laws

This method is actually an algorithm to compute every S_n.

Similarly, for every $n \in \mathbb{N}$, we get polynomials P_n such that:

$$W_n(P_0, \ldots, P_n) = W_n(X_0, \ldots, X_n) \times W_n(Y_0, \ldots, Y_n).$$

Let $(x_0, x_1, x_2, \ldots)$ and $(y_0, y_1, y_2, \ldots)$ be two Witt vectors.

Witt vectors ring laws

This method is actually an algorithm to compute every S_n.

Similarly, for every $n \in \mathbb{N}$, we get polynomials P_n such that:

$$W_n(P_0, \dots, P_n) = W_n(X_0, \dots, X_n) \times W_n(Y_0, \dots, Y_n).$$

Let $(x_0, x_1, x_2, \dots)$ and $(y_0, y_1, y_2, \dots)$ be two Witt vectors.

We define:
$(x_0, x_1, x_2, \dots) + (y_0, y_1, y_2, \dots) := (S_0(x_0, y_0), S_1(x_0, x_1, y_0, y_1), S_2(\dots), \dots)$.

Witt vectors ring laws

This method is actually an algorithm to compute every S_n.

Similarly, for every $n \in \mathbb{N}$, we get polynomials P_n such that:

$$W_n(P_0, \dots, P_n) = W_n(X_0, \dots, X_n) \times W_n(Y_0, \dots, Y_n).$$

Let $(x_0, x_1, x_2, \dots)$ and $(y_0, y_1, y_2, \dots)$ be two Witt vectors.

We define:
$(x_0, x_1, x_2, \dots) + (y_0, y_1, y_2, \dots) \coloneqq (S_0(x_0, y_0), S_1(x_0, x_1, y_0, y_1), S_2(\dots), \dots).$
$(x_0, x_1, x_2, \dots) \times (y_0, y_1, y_2, \dots) \coloneqq (P_0(x_0, y_0), P_1(x_0, x_1, y_0, y_1), P_2(\dots), \dots).$

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

The ring $W_p(\mathbb{F}_q)$ embeds naturally into $\mathbb{Q}_q$. It is the ring of integers of $\mathbb{Q}_q$: that is, the ring of elements with positive p-adic valuation.

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

The ring $W_p(\mathbb{F}_q)$ embeds naturally into $\mathbb{Q}_q$. It is the ring of integers of $\mathbb{Q}_q$: that is, the ring of elements with positive p-adic valuation.

Witt vectors are a standard tool in number theory. They can be used to:

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

The ring $W_p(\mathbb{F}_q)$ embeds naturally into $\mathbb{Q}_q$. It is the ring of integers of $\mathbb{Q}_q$: that is, the ring of elements with positive p-adic valuation.

Witt vectors are a standard tool in number theory. They can be used to:

1. to compute cyclic Galois extensions of function fields (Witt, 1936);

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

The ring $W_p(\mathbb{F}_q)$ embeds naturally into $\mathbb{Q}_q$. It is the ring of integers of $\mathbb{Q}_q$: that is, the ring of elements with positive p-adic valuation.

Witt vectors are a standard tool in number theory. They can be used to:

1. to compute cyclic Galois extensions of function fields (Witt, 1936);
2. to compute p-adic cohomology (Davis–Langer–Zink, 2011);

Examples

We have $W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$.

The ring $W_p(\mathbb{F}_q)$ embeds naturally into $\mathbb{Q}_q$. It is the ring of integers of $\mathbb{Q}_q$: that is, the ring of elements with positive p-adic valuation.

Witt vectors are a standard tool in number theory. They can be used to:

1. to compute cyclic Galois extensions of function fields (Witt, 1936);
2. to compute p-adic cohomology (Davis–Langer–Zink, 2011);
3. to try to break NTRU (Silverman–Smart–Vercauteren, 2005)...

Computing Witt vectors

Similarly as with absolute capping, one only compute with the first `n` coefficients of Witt vectors in practice.

Computing Witt vectors

Similarly as with absolute capping, one only compute with the first `n` coefficients of Witt vectors in practice.

It is expensive to compute with Witt vectors using the naive algorithm: when $p = 31$ the polynomial S_2 has 152994 coefficients!

Computing Witt vectors

Similarly as with absolute capping, one only compute with the first `n` coefficients of Witt vectors in practice.

It is expensive to compute with Witt vectors using the naive algorithm: when $p = 31$ the polynomial S_2 has 152994 coefficients!

Only Finotti's algorithm (2014) used another approach when the coefficient ring has characteristic p. It is much faster.

Similarly as with absolute capping, one only compute with the first `n` coefficients of Witt vectors in practice.

It is expensive to compute with Witt vectors using the naive algorithm: when $p = 31$ the polynomial S_2 has 152994 coefficients!

Only Finotti's algorithm (2014) used another approach when the coefficient ring has characteristic p. It is much faster.

I have implemented in SageMath a new algorithm when the coefficient ring is a polynomial ring over $\mathbb{F}_q$.

Similarly as with absolute capping, one only compute with the first `n` coefficients of Witt vectors in practice.

It is expensive to compute with Witt vectors using the naive algorithm: when $p = 31$ the polynomial S_2 has 152994 coefficients!

Only Finotti's algorithm (2014) used another approach when the coefficient ring has characteristic p. It is much faster.

I have implemented in SageMath a new algorithm when the coefficient ring is a polynomial ring over $\mathbb{F}_q$. It is fast[1], especially for $W_p(\mathbb{F}_p[X])$.

[1] Vite.

From characteristic p to characteristic 0

When A is a commutative ring of characteristic p, $W_p(A)$ has characteristic 0.

From characteristic p to characteristic 0

When A is a commutative ring of characteristic p, $W_p(A)$ has characteristic 0.

The map $a \mapsto [a] := (a, 0, 0, 0, \ldots)$ is a multiplicative map from A to $W_p(A)$.

From characteristic p to characteristic 0

When A is a commutative ring of characteristic p, $W_p(A)$ has characteristic 0.

The map $a \mapsto [a] := (a, 0, 0, 0, \dots)$ is a multiplicative map from A to $W_p(A)$.

The map $V\colon (x_0, x_1, x_2, \dots) \mapsto (0, x_0, x_1, x_2, \dots)$ is additive.

From characteristic p to characteristic 0

When A is a commutative ring of characteristic p, $W_p(A)$ has characteristic 0.

The map $a \mapsto [a] \coloneqq (a, 0, 0, 0, \ldots)$ is a multiplicative map from A to $W_p(A)$.

The map $V \colon (x_0, x_1, x_2, \ldots) \mapsto (0, x_0, x_1, x_2, \ldots)$ is additive.

There is a morphism of rings $F \colon W_p(A) \to W_p(A)$ such that for $a \in A$ in characteristic p:

$$p[a] = F \circ V([a]) = V \circ F([a]),$$
$$[a]^p = [a^p] = F([a]).$$

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

Proof:

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

Proof: by induction on $\mathtt{n}$.

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

Proof: by induction on $\mathtt{n}$.

Assume that $[\overline{Q}]^{p^{\mathtt{n}-1}} = Q^{p^{\mathtt{n}-1}}([X]) + V^{\mathtt{n}}(\epsilon)$ for some $\epsilon \in W_p(A)$.

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

Proof: by induction on $\mathtt{n}$.

Assume that $[\overline{Q}]^{p^{\mathtt{n}-1}} = Q^{p^{\mathtt{n}-1}}([X]) + V^{\mathtt{n}}(\epsilon)$ for some $\epsilon \in W_p(A)$.
Then $[\overline{Q}]^{p^{\mathtt{n}}} = Q^{p^{\mathtt{n}}}([X]) + V^{\mathtt{n}}(\epsilon)^p + \sum_{i=0}^{p} \binom{p}{i} Q^{ip^{\mathtt{n}-1}}([X]) V^{\mathtt{n}}(\epsilon)^{p-i}$.

The main lemma

Lemma (M--B)

Let $Q \in \mathbb{Z}_q[X]$, with projection $\overline{Q} \in \mathbb{F}_q[X]$. The $\mathtt{n}$ first coefficients of $[\overline{Q}]^{p^{\mathtt{n}-1}}$ equal the ones of $Q^{p^{\mathtt{n}-1}}([X])$ in $W_p(\mathbb{F}_q[X])$.

Example: put $\mathtt{n} = 10$, $p = 5$ and $Q = 1 + 5X + X^2$.

Then $Q^{5^9}([X]) = ((1 + X^2)^{5^9}, 0, 0, 0, 0, 0, 0, 0, 0, 0, ?, ?, \ldots)$.

Proof: by induction on $\mathtt{n}$.

Assume that $[\overline{Q}]^{p^{\mathtt{n}-1}} = Q^{p^{\mathtt{n}-1}}([X]) + V^{\mathtt{n}}(\epsilon)$ for some $\epsilon \in W_p(A)$.
Then $[\overline{Q}]^{p^{\mathtt{n}}} = Q^{p^{\mathtt{n}}}([X]) + V^{\mathtt{n}}(\epsilon)^p + \sum_{i=0}^{p} \binom{p}{i} Q^{ip^{\mathtt{n}-1}}([X]) V^{\mathtt{n}}(\epsilon)^{p-i}$.

We conclude because $p = V \circ F$ and
$V^n(W(A))V^m(W(A)) \subset V^{n+m}(W(A))$. $\square$

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \ldots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \ldots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i Q_i{}^{p^{\mathtt{n}-i}}([X]).$$

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \ldots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i Q_i{}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \ldots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i {Q_i}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \dots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i {Q_i}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

Algorithm (M--B)

0. $\mathtt{Input:}$ two truncated Witt vectors $\mathcal{Q}$ and $\mathcal{Q}'$.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \dots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i {Q_i}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

Algorithm (M--B)

0. `Input`: two truncated Witt vectors $\mathcal{Q}$ and $\mathcal{Q}'$.
1. Compute the image $F^{\mathtt{n}}(\mathcal{Q})$ as a polynomial in $\mathbb{Z}_q[T]$.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \ldots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i Q_i^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

Algorithm (M--B)

0. `Input`: two truncated Witt vectors $\mathcal{Q}$ and $\mathcal{Q}'$.
1. Compute the image $F^{\mathtt{n}}(\mathcal{Q})$ as a polynomial in $\mathbb{Z}_q[T]$. Do the same thing with $\mathcal{Q}'$.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \dots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i Q_i{}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

Algorithm (M--B)

0. `Input`: two truncated Witt vectors $\mathcal{Q}$ and $\mathcal{Q}'$.
1. Compute the image $F^{\mathtt{n}}(\mathcal{Q})$ as a polynomial in $\mathbb{Z}_q[T]$. Do the same thing with $\mathcal{Q}'$.
2. Compute the sum (or the product) of the above results.

The algorithm

Given a (truncated) Witt vector $\mathcal{Q} = (\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \dots, \overline{Q}_{\mathtt{n}})$ in $W_p(\mathbb{F}_q[X])$, we have $\mathcal{Q} = \sum_{i=0}^{\mathtt{n}} V^i([\overline{Q}_i])$.

So, by our lemma:

$$F^{\mathtt{n}}(\mathcal{Q}) = \sum_{i=0}^{\mathtt{n}} p^i {Q_i}^{p^{\mathtt{n}-i}}([X]).$$

This is a polynomial in $\mathbb{Z}_q[T]$ with $T := [X]$. So this method gives an effective way to compute Illusie's isomorphism (1979).

Algorithm (M--B)

0. `Input`: two truncated Witt vectors $\mathcal{Q}$ and $\mathcal{Q}'$.
1. Compute the image $F^{\mathtt{n}}(\mathcal{Q})$ as a polynomial in $\mathbb{Z}_q[T]$. Do the same thing with $\mathcal{Q}'$.
2. Compute the sum (or the product) of the above results.
3. `Return`: the preimage of the above result.

Computing the preimage

The result will be of the form $F^{\mathtt{n}}(\mathcal{R}) = \sum_{i=0}^{\mathtt{n}} p^i {R_i}^{p^{\mathtt{n}-i}}(T)$ and we want to return the $\overline{R}_i$.

Computing the preimage

The result will be of the form $F^{n}(\mathcal{R}) = \sum_{i=0}^{n} p^i {R_i}^{p^{n-i}}(T)$ and we want to return the $\overline{R}_i$.

By reducing modulo p, we get ${\overline{R}_0}^{p^{n}}(T)$.

Computing the preimage

The result will be of the form $F^{\mathtt{n}}(\mathcal{R}) = \sum_{i=0}^{\mathtt{n}} p^i {R_i}^{p^{\mathtt{n}-i}}(T)$ and we want to return the $\overline{R}_i$.

By reducing modulo p, we get ${\overline{R}_0}^{p^{\mathtt{n}}}(T)$.

From this, we compute $\overline{R}_0$, and by our lemma this yields ${R_0}^{p^{\mathtt{n}}}(T)$ up to our precision.

Computing the preimage

The result will be of the form $F^{\mathtt{n}}(\mathcal{R}) = \sum_{i=0}^{\mathtt{n}} p^i {R_i}^{p^{\mathtt{n}-i}}(T)$ and we want to return the $\overline{R}_i$.

By reducing modulo p, we get ${\overline{R}_0}^{p^{\mathtt{n}}}(T)$.

From this, we compute $\overline{R}_0$, and by our lemma this yields ${R_0}^{p^{\mathtt{n}}}(T)$ up to our precision.

So get $p \sum_{i=0}^{\mathtt{n}-1} p^i {R_{i+1}}^{p^{\mathtt{n}-1-i}}(T)$.

Computing the preimage

The result will be of the form $F^{\mathtt{n}}(\mathcal{R}) = \sum_{i=0}^{\mathtt{n}} p^i {R_i}^{p^{\mathtt{n}-i}}(T)$ and we want to return the $\overline{R}_i$.

By reducing modulo p, we get ${\overline{R}_0}^{p^{\mathtt{n}}}(T)$.

From this, we compute $\overline{R}_0$, and by our lemma this yields ${R_0}^{p^{\mathtt{n}}}(T)$ up to our precision.

So get $p\sum_{i=0}^{\mathtt{n}-1} p^i {R_{i+1}}^{p^{\mathtt{n}-1-i}}(T)$.

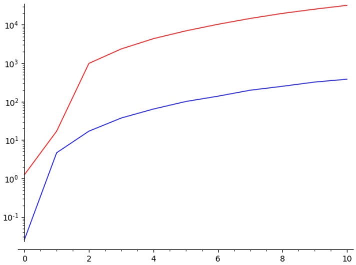
Repeat!

Speed

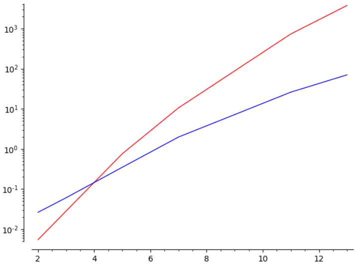
The most expensive operation is the exponentiation of polynomials by a power of p.

Speed

The most expensive operation is the exponentiation of polynomials by a power of p.



$\mathtt{n} = 5$, $p = 7$



$d = 5$, $\mathtt{n} = 4$

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$.

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$. Lift it to a curve over $W_{\mathtt{n}}(\mathbb{F}_q)$.

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$. Lift it to a curve over $W_{\mathtt{n}}(\mathbb{F}_q)$. Consider an AG-code C constructed with the lift.

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$. Lift it to a curve over $W_{\mathrm{n}}(\mathbb{F}_q)$. Consider an AG-code C constructed with the lift. Looking at C coordinates-by-coordinates, this yields a non-linear code.

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$. Lift it to a curve over $W_n(\mathbb{F}_q)$. Consider an AG-code C constructed with the lift. Looking at C coordinates-by-coordinates, this yields a non-linear code.

In 2006, using hyperelliptic curves Finotti constructed non-linear binary codes. One example had length 26, 2^{14} codewords and minimum weight 6. (the best one has 2^{15} codewords)

The future: error correcting codes?

In 2000 Voloch and Walker introduced a construction using Witt vectors for error correcting codes.

Rough idea: start with your favourite curve over $\mathbb{F}_q$. Lift it to a curve over $W_n(\mathbb{F}_q)$. Consider an AG-code C constructed with the lift. Looking at C coordinates-by-coordinates, this yields a non-linear code.

In 2006, using hyperelliptic curves Finotti constructed non-linear binary codes. One example had length 26, 2^{14} codewords and minimum weight 6. (the best one has 2^{15} codewords)

Using Finotti's algorithm, Groves gave in 2023 some examples for $p > 2$. He noticed that singular curves gave the best results: one example over $\mathbb{F}_3$ had length 18, 3^6 codewords and minimum weight 8. (the best one has weight 9)

Thank you for listening!