ZpL: a p-adic precision package

Xavier Caruso, David Roe, **Tristan Vaccon**

Univ. Rennes 1 → Univ. Bordeaux; MIT; **Université de Limoges**

ISSAC 2018

What are p-adic numbers?

What are p-adic numbers?

p refers to a prime number

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \ldots a_i \ldots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \ldots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \ldots a_i \ldots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \ldots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \ldots a_i \ldots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \ldots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

A p-adic number with no digit after the comma is a p-adic integer.

What are p-adic numbers?

p refers to a prime number

p-adic numbers are numbers written in p-basis of the shape:

$$a = \dots a_i \dots a_2\ a_1\ a_0\ ,\ a_{-1}\ a_{-2} \dots\ a_{-n}$$

with $0 \leq a_i < p$ for all i.

Addition and multiplication on these numbers are defined by applying SchoolBook algorithms.

The valuation $v_p(a)$ of a is the smallest v such that $a_v \neq 0$.

The p-adic numbers form the field $\mathbb{Q}_p$.

A p-adic number with no digit after the comma is a p-adic integer.

The p-adic integers form a subring $\mathbb{Z}_p$ of $\mathbb{Q}_p$.

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N},\ \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N},\ \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.

Summary on p-adics

Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N},\ \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.
- We are **closer to arithmetic** : we can reduce modulo p.

Summary on p-adics

Proposition

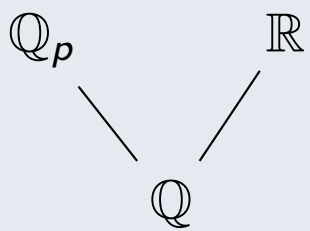
$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

$$\forall k \in \mathbb{N},\ \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

A first idea

- $\mathbb{Q}_p$ is an extension of $\mathbb{Q}$ where one can perform **calculus**, as simply as over $\mathbb{R}$.
- We are **closer to arithmetic** : we can reduce modulo p.

Remark



$$\begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \end{array}$$

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;
- *e.g.* Dixon's method (used in F4), polynomial factorization via Hensel's lemma.

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;
- *e.g.* Dixon's method (used in F4), polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation,

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;
- *e.g.* Dixon's method (used in F4), polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* solving differential equations over finite fields.

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;
- *e.g.* Dixon's method (used in F4), polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* solving differential equations over finite fields.
- Kedlaya's and Lauder's counting-point algorithms via p-adic cohomology.

Why should one work with p-adic numbers?

p-adic methods

- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth;
- *e.g.* Dixon's method (used in F4), polynomial factorization via Hensel's lemma.

p-adic algorithms

- Going from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$ and then back to $\mathbb{Z}/p\mathbb{Z}$ enables more computation, *e.g.* solving differential equations over finite fields.
- Kedlaya's and Lauder's counting-point algorithms via p-adic cohomology.

My personal (long-term) motivation

Computing (some) moduli spaces of p-adic Galois representations.

Motivations and goal

Today's goal

We present the ZpL package for Sage. It features:

Motivations and goal

Today's goal

We present the ZpL package for Sage. It features:

- Tracking of the optimal behaviour of p-adic precision.

Motivations and goal

Today's goal

We present the ZpL package for Sage. It features:

- Tracking of the optimal behaviour of p-adic precision.
- Portability: any existing p-adic code in Sage can use ZpL without any modification (outside of declaration of the fields).

Table of contents

Table of contents

Definition of the precision

Finite-precision p-adics: "interval arithmetc"

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics: "interval arithmetc"

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition of the precision

Finite-precision p-adics: "interval arithmetc"

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$ is d.

Definition of the precision

Finite-precision p-adics: "interval arithmetc"

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and p a prime number.
Working with a computer, we usually only can consider the beginning of this power series expansion: we only consider elements of the form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

Definition

The **order**, or the **absolute precision** of $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$ is d.

Example

The order of $\ldots 604, 3$ in $\mathbb{Q}_3$ is 3.

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{\min(k_0,k_1)})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{\min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) \times (x_1 + O(p^{k_1})) = x_0 x_1 + O(p^{\min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Precision formulae

Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{\min(k_0,k_1)})$$

Proposition (multiplication)

$$(x_0 + O(p^{k_0})) \times (x_1 + O(p^{k_1})) = x_0 x_1 + O(p^{\min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

Proposition (division)

$$\frac{xp^a + O(p^b)}{yp^c + O(p^d)} = \frac{x}{y} p^{a-c} + O(p^{\min(d+a-2c,b-c)})$$

In particular,

$$\frac{1}{p^c y + O(p^d)} = y^{-1} p^{-c} + O(p^{d-2c})$$

On "interval arithmetic"

Benefits

- Standard: available in most computer algebra softwares.

On "interval arithmetic"

Benefits

- Standard: available in most computer algebra softwares.
- Correctness: all digits are provably correct.

On "interval arithmetic"

Benefits

- Standard: available in most computer algebra softwares.
- Correctness: all digits are provably correct.

Drawbacks

- Precision: accumulation of loss in precision can happen (when used naively).

On "interval arithmetic"

Benefits

- Standard: available in most computer algebra softwares.
- Correctness: all digits are provably correct.

Drawbacks

- Precision: accumulation of loss in precision can happen (when used naively).
- Consequence: results can be far from optimal precision.

Optimality, intrinsicness

Step-by-step analysis is not optimal.

Let f : $\begin{array}{ccc} \mathbb{Q}_3^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

Optimality, intrinsicness

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_3^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (4 + \boxed{O(3^6)}, 2 + O(3^4))$.

Optimality, intrinsicness

Step-by-step analysis is not optimal.

Let f : $\begin{array}{ccc} \mathbb{Q}_3^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (4 + \boxed{O(3^6)}, 2 + O(3^4))$.

- If we apply f two times, we get :

$$f \circ f(x,y) = (8 + \boxed{O(3^4)}, 4 + O(3^4)).$$

Optimality, intrinsicness

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_3^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (4 + \boxed{O(3^6)}, 2 + O(3^4))$.

- If we apply f two times, we get :

$$f \circ f(x,y) = (8 + \boxed{O(3^4)}, 4 + O(3^4)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x,y) = (8 + \boxed{O(3^6)}, 4 + O(3^4)).$$

Optimality, intrinsicness

Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_3^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with $(x,y) = (4 + \boxed{O(3^6)}, 2 + O(3^4))$.

- If we apply f two times, we get :

$$f \circ f(x,y) = (8 + \boxed{O(3^4)}, 4 + O(3^4)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x,y) = (8 + \boxed{O(3^6)}, 4 + O(3^4)).$$

Table of contents

The Main lemma of p-adic differential precision

Lemma (CRV14)

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) **differentiable** mapping.*

The Main lemma of p-adic differential precision

Lemma (CRV14)

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*

The Main lemma of p-adic differential precision

Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective***.
Then for any ball $B = B(0, r)$ ***small enough***,

The Main lemma of p-adic differential precision

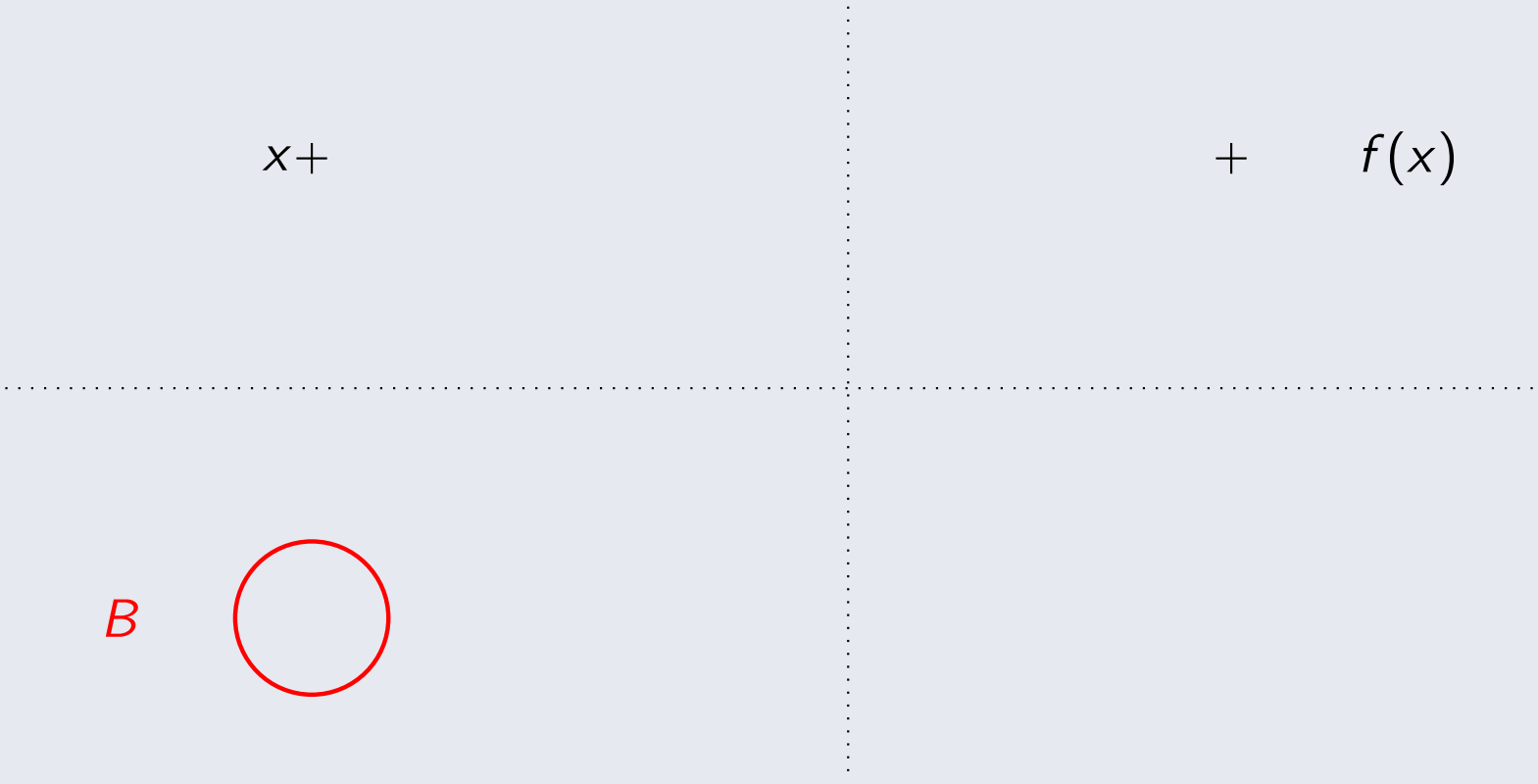
Lemma (CRV14)

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

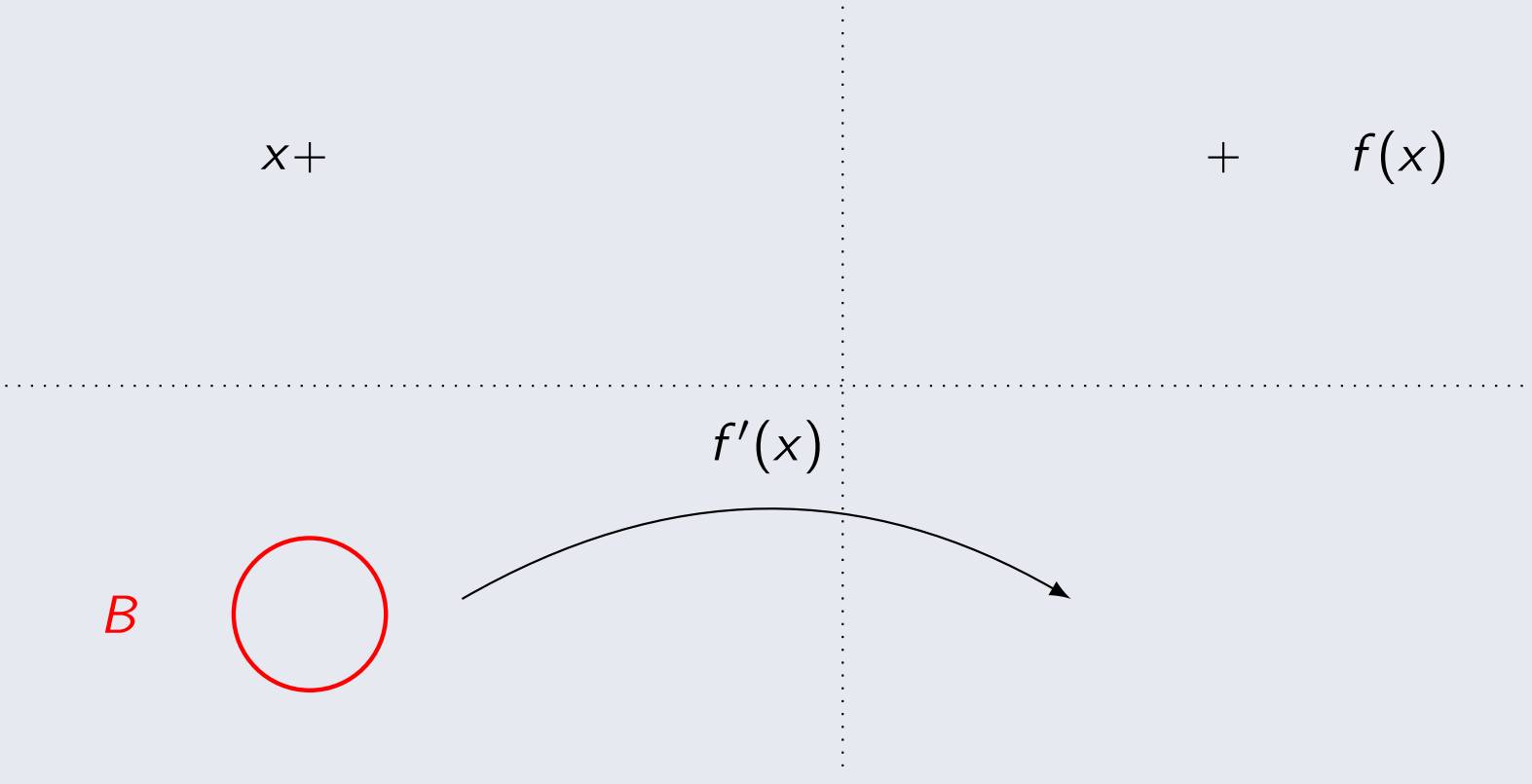
Geometrical meaning

Interpretation



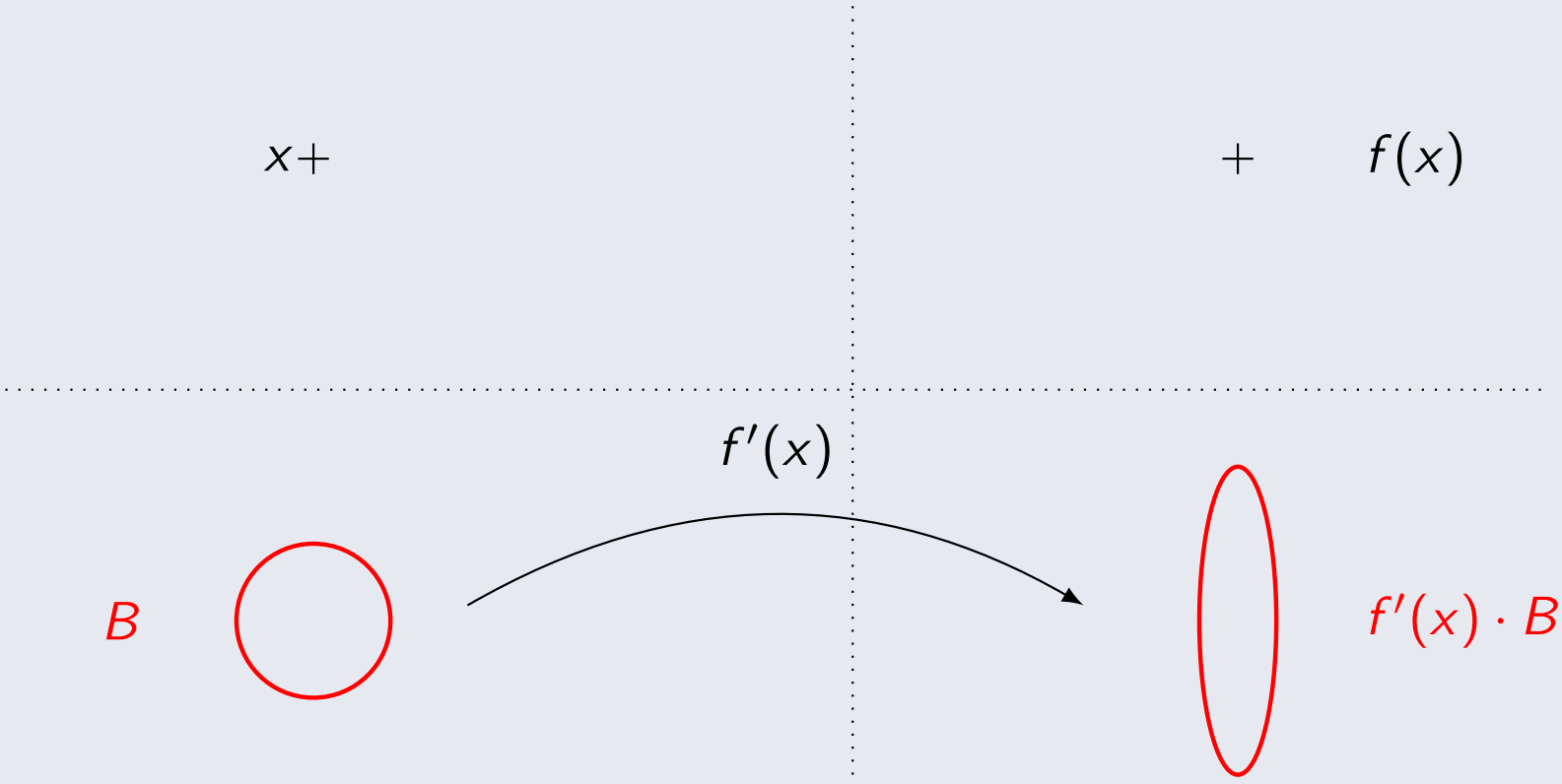
Geometrical meaning

Interpretation



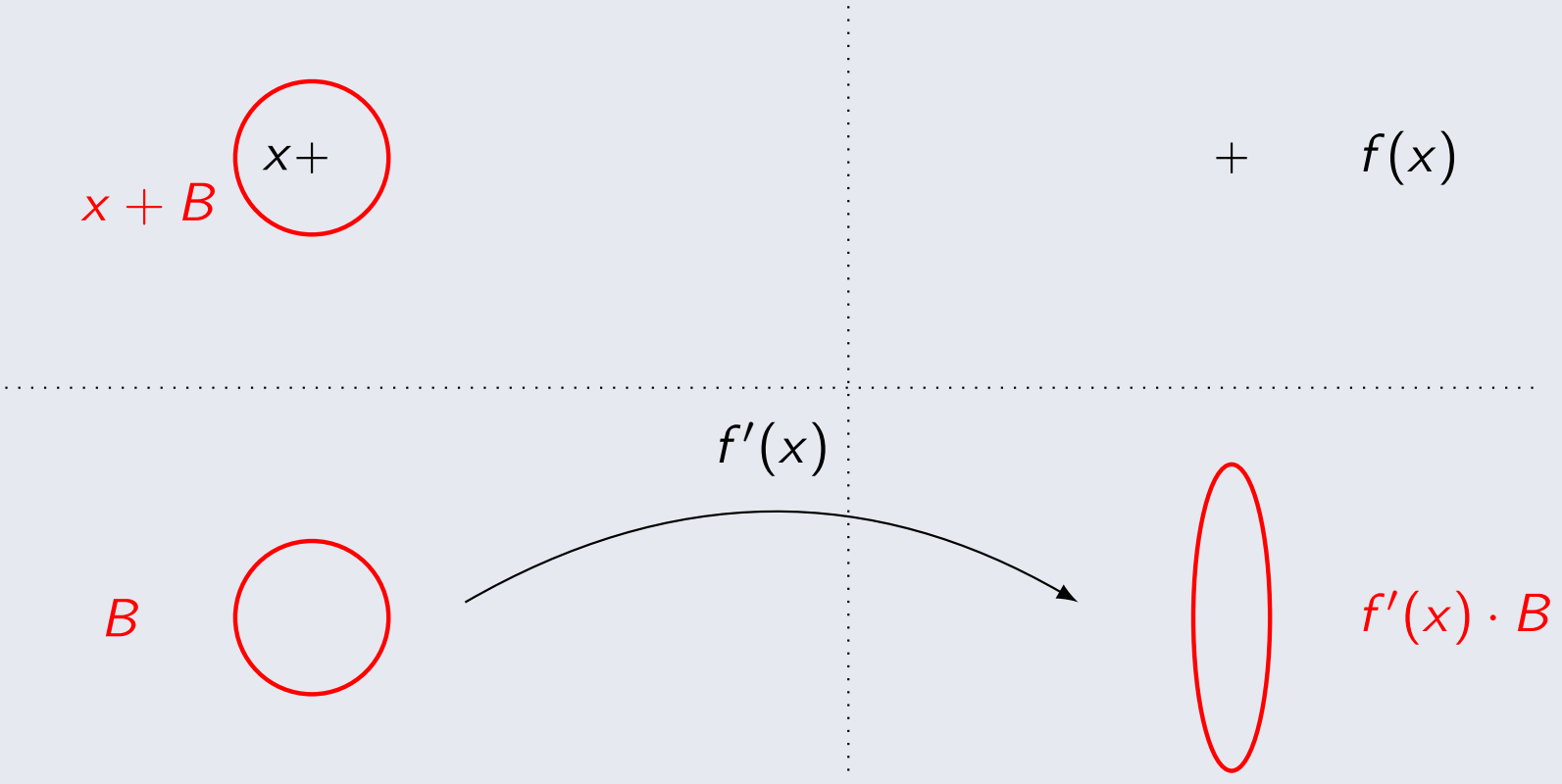
Geometrical meaning

Interpretation



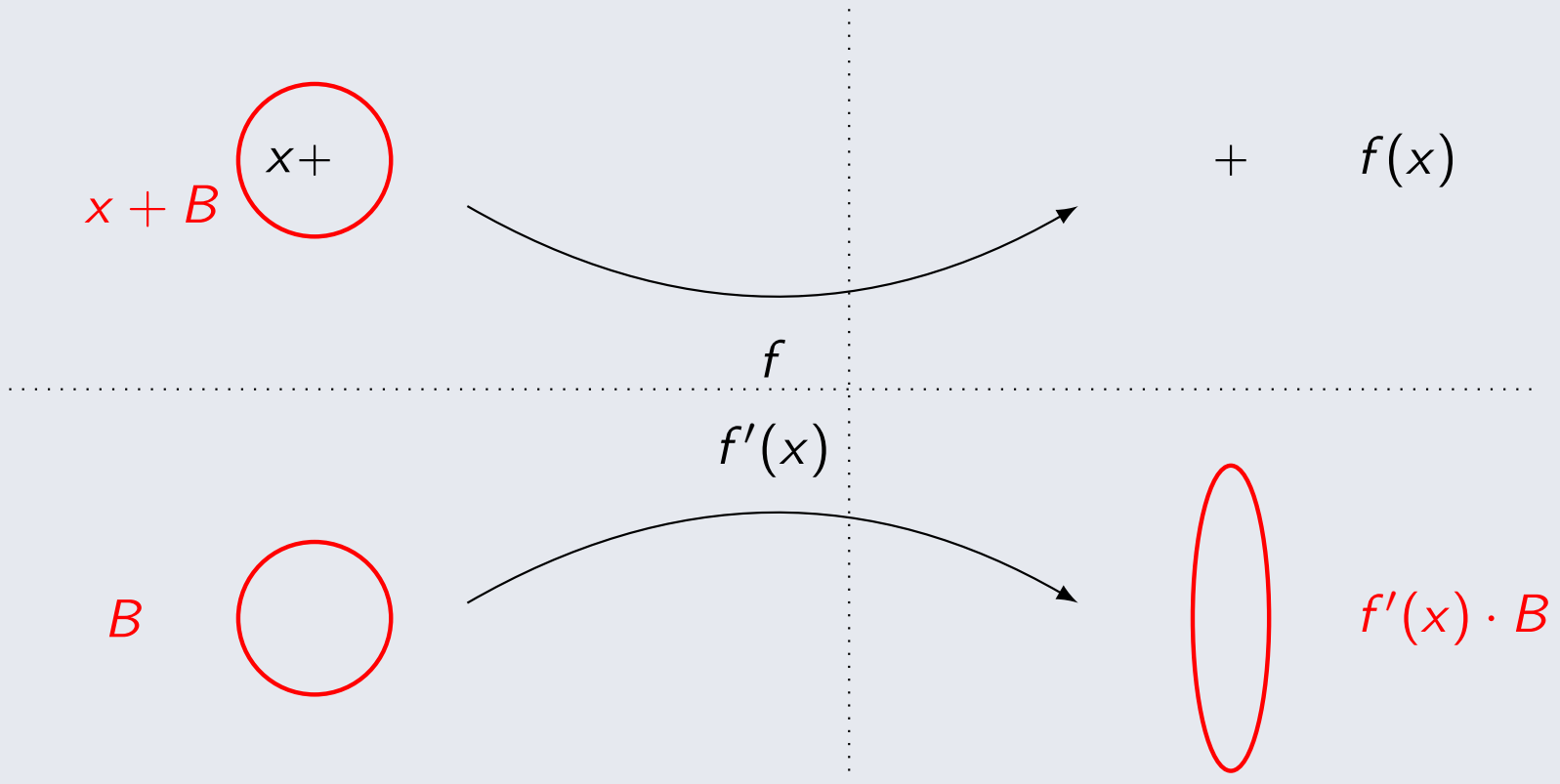
Geometrical meaning

Interpretation



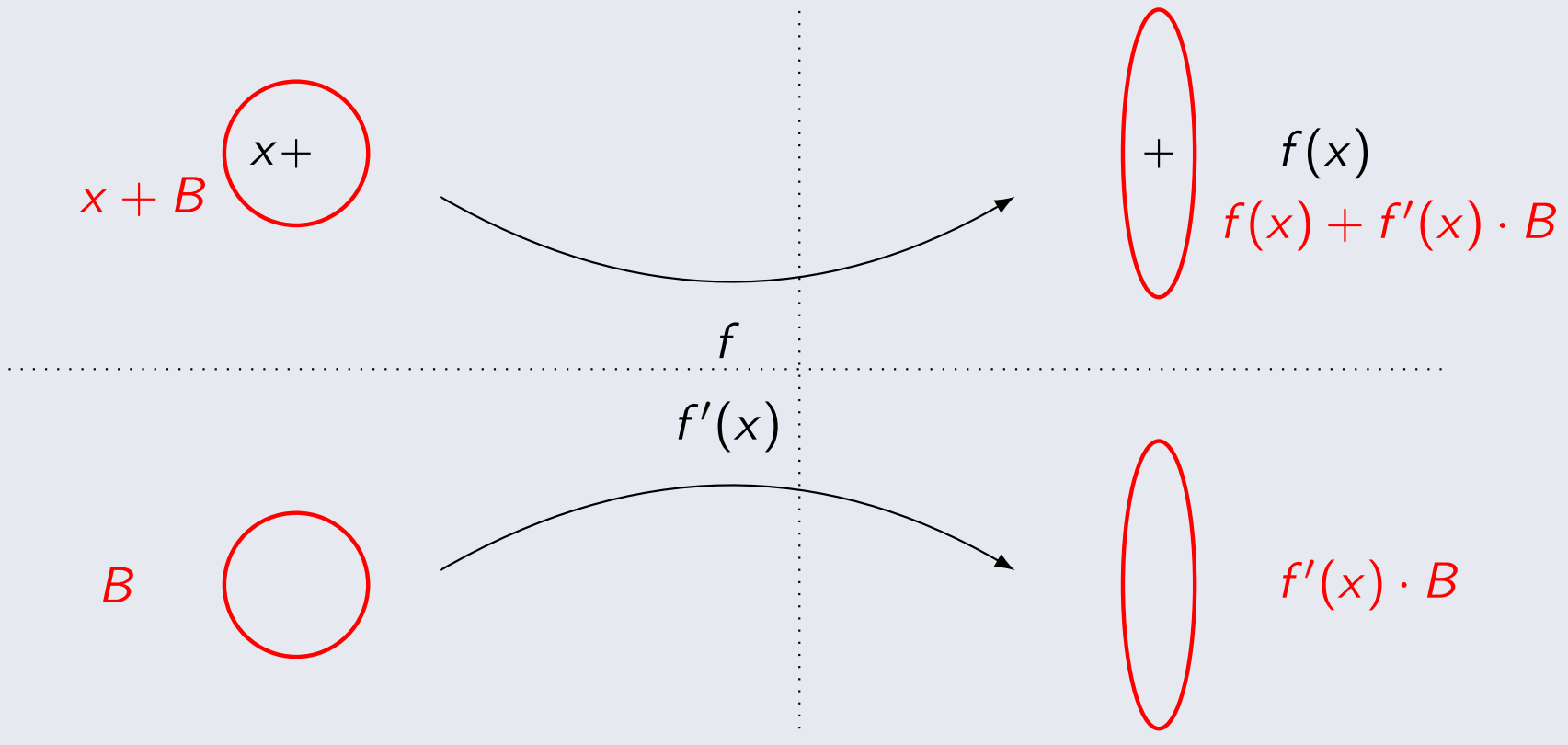
Geometrical meaning

Interpretation



Geometrical meaning

Interpretation



Lattices

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective***.
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective****.*
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

Lattices

Lemma

Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a (strictly) ***differentiable*** *mapping.*
Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is ***surjective***.
Then for any ball $B = B(0, r)$ ***small enough****, for any open $\mathbb{Z}_p$-**lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

Remark

This framework can be extended to **(complete) ultrametric K-vector spaces** (*e.g.* $\mathbb{F}_p((X))^n$, $\mathbb{Q}((X))^m$, ...).

Table of contents

Small demo

Go to Sage session.

Specific motivations

Our goal with ZpL

We would like to address the following:

Specific motivations

Our goal with ZpL

We would like to address the following:

- Be able to compute the optimal precision, even though there is no theoretical understanding of the computation.

Specific motivations

Our goal with ZpL

We would like to address the following:

- Be able to compute the optimal precision, even though there is no theoretical understanding of the computation.
- It should not require a specialized algorithm for every problem.

Specific motivations

Our goal with ZpL

We would like to address the following:

- Be able to compute the optimal precision, even though there is no theoretical understanding of the computation.
- It should not require a specialized algorithm for every problem.

Main idea

Carry on a lattice of precision. It represents the precision on all the quantities computed.

Representing lattices

Lattices in matrix representation

- We represent a precision lattice using an upper triangular matrix, whose rows give a basis for the lattice.

Representing lattices

Lattices in matrix representation

- We represent a precision lattice using an upper triangular matrix, whose rows give a basis for the lattice.
- We scale the diagonal entries to be powers of p.

Representing lattices

Lattices in matrix representation

- We represent a precision lattice using an upper triangular matrix, whose rows give a basis for the lattice.
- We scale the diagonal entries to be powers of p.

Remark

Note that lattices are exact, since we may use row operations to reduce each column modulo the power of p on the diagonal (**HNF**).

Operations and variables

Arithmetic operation

- When computing a new quantity:

$$w = f(v_1, \ldots, v_n),$$

we create a **new variable**.

Operations and variables

Arithmetic operation

- When computing a new quantity:

$$w = f(v_1, \ldots, v_n),$$

we create a **new variable**. We add a new column to the precision lattice with entries given by

$$\frac{\partial f}{\partial v_i}.$$

Operations and variables

Arithmetic operation

- When computing a new quantity:

$$w = f(v_1, \ldots, v_n),$$

we create a **new variable**. We add a new column to the precision lattice with entries given by

$$\frac{\partial f}{\partial v_i}.$$

- The resulting matrix is no longer square.

Operations and variables

Arithmetic operation

- When computing a new quantity:

$$w = f(v_1, \ldots, v_n),$$

we create a **new variable**. We add a new column to the precision lattice with entries given by

$$\frac{\partial f}{\partial v_i}.$$

- The resulting matrix is no longer square.
  - In one model (ZpLF) we allow such submodules (at the cost of working with inexact objects).

Operations and variables

Arithmetic operation

- When computing a new quantity:

$$w = f(v_1, \ldots, v_n),$$

we create a **new variable**. We add a new column to the precision lattice with entries given by

$$\frac{\partial f}{\partial v_i}.$$

- The resulting matrix is no longer square.
  - In one model (`ZpLF`) we allow such submodules (at the cost of working with inexact objects).
  - In the main model (`ZpLC`) we add a new row $(0, \ldots, 0, p^C)$ for some cap C.

Return to the original example

Computation

We compute successively:

$$x = 4 + O(3^6),\ y = 2 + O(3^4),$$

Return to the original example

Computation

We compute successively:

$$x = 4 + O(3^6),\ y = 2 + O(3^4),$$
$$u = x + y,\ v = x - y,$$

Return to the original example

Computation

We compute successively:

$$x = 4 + O(3^6),\ y = 2 + O(3^4),$$
$$u = x + y,\ v = x - y,$$
$$2x = u + v,\ 2y = u - v$$

Return to the original example

Computation

We compute successively:

$$x = 4 + O(3^6),\ y = 2 + O(3^4),$$
$$u = x + y,\ v = x - y,$$
$$2x = u + v,\ 2y = u - v$$

The corresponding lattice (for ZpLC)

$$\begin{pmatrix} 729 & 0 & 729 & 729 & 1458 & 0 \\ 0 & 81 & 81 & 3486784320 & 0 & 162 \\ 0 & 0 & 10460353203 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3486784401 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3486784401 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3486784401 \end{pmatrix}$$

Correctness and optimality

Proved digits?

Our current implementation does not check the smallness condition required to apply the precision lemma, so the results are not provably correct (yet).

Correctness and optimality

Proved digits?

Our current implementation does not check the smallness condition required to apply the precision lemma, so the results are not provably correct (yet).

The precision cap can reduce the precision of the result, but this is checkable a fortiori.

Correctness and optimality

Proved digits?

Our current implementation does not check the smallness condition required to apply the precision lemma, so the results are not provably correct (yet).

The precision cap can reduce the precision of the result, but this is checkable a fortiori.

Diffused digits

Can quantify the amount of precision lost by checking precision on individual variables.

Correctness and optimality

Proved digits?

Our current implementation does not check the smallness condition required to apply the precision lemma, so the results are not provably correct (yet).

The precision cap can reduce the precision of the result, but this is checkable a fortiori.

Diffused digits

Can quantify the amount of precision lost by checking precision on individual variables. More precisely, how far interval arithmetic is from lattice precision: the **number of diffused digits**.

Table of contents

Last demo

Back to Sage.

To sum up

On ZpL

To sum up

On ZpL

- Two variants available in Sage.

To sum up

On ZpL

- Two variants available in Sage.
- Obtain the theoretical optimal precision, except in very small precision (where the precision is too small for the Lemma to apply).

To sum up

On ZpL

- Two variants available in Sage.
- Obtain the theoretical optimal precision, except in very small precision (where the precision is too small for the Lemma to apply).
- There is obviously an overhead cost (rough estimation available in the article).

To sum up

On ZpL

- Two variants available in Sage.
- Obtain the theoretical optimal precision, except in very small precision (where the precision is too small for the Lemma to apply).
- There is obviously an overhead cost (rough estimation available in the article).
- Well suited for exploration and understanding the behaviour of the precision.

References

Initial article

- Xavier Caruso, David Roe and Tristan Vaccon Tracking p-adic precision, ANTS XI, 2014.

Linear Algebra

- Xavier Caruso, David Roe and Tristan Vaccon p-adic stability in linear algebra, ISSAC 2015.

Thank you for your attention

Thanks