p-adic precision

Xavier Caruso

September 5, 2013

Current philosophy

Currently, in Sage (any many other softwares), a precision data is attached to each element in $\mathbb{Q}_p$ and it is tracked operation by operation.

Nevertheless, using this philosophy, it might be difficult is many situations to produce *stable* and efficient algorithms.
Here are some basic examples:

- computing inverse using Newton iteration
- computing efficiently products of polynomials
- computing efficiently products of matrices

Other examples — a stupid example

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

We want to compute

$$f \circ f(x, y) \text{ with } x = 1 + O(p^{10}),\ y = 1 + O(p).$$

- if we apply f two times, we get:

$$f \circ f(x, y) = (2 + O(p), 2 + O(p))$$

- if we note that $f \circ f(x, y) = (2x, 2y)$, we get:

$$f \circ f(x, y) = (2 + O(p^{10}), 2 + O(p))$$

Other examples – LU factorization

Gauss elimination is very unstable.

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known with precision $O(p^N)$.

Write $M = LU$ for its LU factorization where all diagonal entries of L are equal to 1 (it exists almost surely). Then:

- Using Gauss elimination to compute L, the average precision we will get on L is $O(p^{N - \frac{2d}{p-1}})$
- One can show that the theorical precision of L is at least $O(p^{N - 2\log_p d})$.

Other examples – Differential equations

Let $f(t) = \sum_{i=0}^{\infty} a_i t^i$
with $a_i \in \mathbb{Z}_p$ known with precision $O(p^N)$.

Consider the p-adic differential equation $y'(t) = f(t) \cdot y(t)$
and assume if $y(t) = \sum_{i=0}^{\infty} b_i t^i$, all b_i's lie in $\mathbb{Z}_p$.

Then:

- one can compute the b_i's using a recursive formula;
  however, doing this, we find b_i with precision $O(p^{N-\frac{i}{p-1}})$
- one can prove theoretically that b_i is known with precision
  at least $O(p^{N-c\log_p i})$ where c is some constant

A possible solution

Two ideas:

- separate precision and approximation, *i.e.* do all computations as follows:
  - precompute the precision of the result
  - perform the computation with taking care of precision
  - put together precision and approximation to get the desired result
- work with more precision data, *i.e.* if X is a p-adic object, allow us to write:

$$X + O(\text{something})$$

where *something* can be different from p^N.

Example: if $X = (x, y)$, *something* may be a lattice in $\mathbb{Q}_p^2$.

What is a p-adic object

Here are some examples:

- a p-adic number
- an element of a finite dimensional $\mathbb{Q}_p$-vector space:

  a p-adic polynomial

  a p-adic matrix
- an element of a infinite dimensional $\mathbb{Q}_p$-vector space:

  a p-adic series
- an element of a p-adic variety:

  a point on an elliptic curve,

  a subspace of $\mathbb{Q}_p^n$ (which is an element of a grassmannian)

And... what is *something*?

Let X be a p-adic object which lives in a variety $\mathcal{V}$. We shall write:

$$X + O(H)$$

where H is any lattice in the tangent space of $\mathcal{V}$ at X.

Important note: if H is small enough, $X + O(H)$ defines an actual subset of $\mathcal{V}$.

Theorem

Let $f : \mathcal{V}_1 \to \mathcal{V}_2$ be a function of class $\mathcal{C}^1$. Let $X \in \mathcal{V}_1$. Assume that df_X is surjective. Then, for all lattice H in the tangent space of $\mathcal{V}$ at X, there exists an integer n_0 such that, for $n \geq n_0$:

$$f(X + O(p^n H)) = f(X) + O(p^n df_X(H))$$