Tutorial for p-adics in SAGE

David Roe

March 11, 2007

1 Introduction

p-adics in SAGE are currently undergoing a transformation. Previously, SAGE has included a single class representing $\mathbb{Q}_p$, and a single class representing elements of $\mathbb{Q}_p$. Our goal is to create a rich structure of different options that will reflect the mathematical structures of the p-adics. This is very much a work in progress: some of the classes that we eventually intend to include have not yet been written, and some of the functionality for classes in existence has not yet been implemented. In addition, while we strive for perfect code, bugs (both subtle and not-so-subtle) continue to evade our clutches. As a user, you serve an important role. By writing non-trivial code that uses the p-adics, you both give us insight into what features are actually used and also expose problems in the code for us to fix.

Our design philosophy has been to get a robust, usable interface working first, with simpleminded implementations underneath. We want this interface to stabilize rapidly, so that users' code does not have to change. Once we get the framework in place, we can go back and work on the algorithms and implementations underneath. All of the current p-adic code is currently written in pure Python, which means that it does not have the speed advantage of compiled code. Thus our p-adics can be painfully slow at times when you're doing real computations. However, finding and fixing bugs in Python code is *far* easier than finding and fixing errors in the compiled alternative within SAGE (SageX), and Python code is also faster and easier to write. We thus have significantly more functionality implemented and working than we would have if we had chosen to focus initially on speed. And at some point in the future, we will go back and improve the speed. Any code you have written on top of our p-adics will then get an immediate performance enhancement.

If you do find bugs, have feature requests or general comments, please let me know at roed@math.harvard.edu.

This tutorial attempts to outline what you need to know in order to use the p-adics effectively. OUTLINE SECTIONS.

2 Terminology and types of p-adics

To write down a p-adic element completely would require an infinite amount of data. Since computers do not have infinite storage space, we must instead store finite approximations to elements. Thus, just as in the case of floating point numbers for representing reals, we have to store an element to a finite precision level. The different ways of doing this account for the different types of p-adics.

We can think of p-adics in two ways. First, as a projective limit of finite groups:

$$\mathbb{Z}_p = \lim_{\leftarrow n} \mathbb{Z}/p^n\mathbb{Z}.$$

Secondly, as Cauchy sequences of rationals (or integers, in the case of $\mathbb{Z}_p$, under the p-adic metric. Since we only need to consider these sequences up to equivalence, this second way of thinking of the p-adics is the same as considering power series in p with integral coefficients in the range 0 to $p-1$. If we only allow nonnegative powers of p then these power series converge to elements of $\mathbb{Z}_p$, and if we allow bounded negative powers of p then we get $\mathbb{Q}_p$.

Both of these representations give a natural way of thinking about finite approximations to a p-adic element. In the first representation, we can just stop at some point in the projective limit, giving an element of $\mathbb{Z}/p^n\mathbb{Z}$. As $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, this is is equivalent to specifying our element modulo $p^n\mathbb{Z}_p$.

Definition 2.1 *The* absolute precision *of a finite approximation $\bar{x} \in \mathbb{Z}/p^n\mathbb{Z}$ to $x \in \mathbb{Z}_p$ is the non-negative integer n.*

In the second representation, we can achieve the same thing by truncating a series

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

at p^n, yielding

$$a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} + O(p^n).$$

As above, we call this n the absolute precision of our element.

Given any $x \in \mathbb{Q}_p$ with $x \neq 0$, we can write $x = p^v u$ where $v \in \mathbb{Z}$ and $u \in Zpx$. We could thus also store an element of $\mathbb{Q}_p$ (or $\mathbb{Z}_p$) by storing v and a finite approximation of u. This motivates the following definition:

Definition 2.2 *The* relative precision *of an approximation to x is defined as the absolute precision of the approximation minus the valuation of x.*

For example, if $x = a_k p^k + a_{k+1} p^{k+1} + \cdots + a_{n-1} p^{n-1} + O(p^n)$ then the absolute precision of x is n, the valuation of x is k and the relative precision of x is $n-k$.

There are four different representations of $\mathbb{Z}_p$ in Sage and two representations of $\mathbb{Q}_p$: the fixed modulus ring, the capped absolute precision ring, the capped relative precision ring, the capped relative precision field, the lazy ring and the lazy field. In addition, unramified extensions are also currently supported.

One uses the function `Zp` to construct p-adic rings and `Qp` to construct p-adic fields. The only required parameter is the prime: the default type is capped relative.

2.1 Fixed Modulus Rings

The first, and simplest, type of $\mathbb{Z}_p$ is basically a wrapper around $\mathbb{Z}/p^n\mathbb{Z}$, providing a unified interface with the rest of the p-adics. You specify a precision, and all elements are stored to that absolute precision. If you perform an operation that would normally lose precision, the element does not track that it no longer has full precision.

The fixed modulus ring provide the lowest level of convenience, but it is also the one that has the lowest computational overhead. Once we have ironed out some bugs, the fixed modulus elements will be those most optimized for speed.

As with all of the implementations of $\mathbb{Z}_p$, one creates a new ring using the constructor `Zp`, and passing in `'fixed-mod'` for the `type` parameter. For example,

```
sage: R = Zp(5, prec = 10, type = 'fixed-mod', print_mode = 'series')
sage: R
5-adic Ring of fixed modulus 5^10
```

One can create elements as follows:

```
sage: a = R(375)
sage: a
3*5^3 + O(5^10)
sage: b = R(105)
sage: b
5 + 4*5^2 + O(5^10)
```

Now that we have some elements, we can do arithmetic in the ring.

```
sage: a + b
5 + 4*5^2 + 3*5^3 + O(5^10)
sage: a * b
3*5^4 + 2*5^5 + 2*5^6 + O(5^10)
sage: a // 5
3*5^2 + O(5^10)
```

Since elements don't actually store their actual precision, one can only divide by units:

```
sage: a / 2
4*5^3 + 2*5^4 + 2*5^5 + 2*5^6 + 2*5^7 + 2*5^8 + 2*5^9 + O(5^10)
sage: a / b
...
<type 'exceptions.ValueError'>: cannot invert non-unit
```

If you want to divide by a non-unit, do it using the `//` operator:

```
sage: a // b
3*5^2 + 3*5^3 + 2*5^5 + 5^6 + 4*5^7 + 2*5^8 + O(5^10)
```

2.2 Capped Absolute Rings

The second type of implementation of $\mathbb{Z}_p$ is similar to the fixed modulus implementation, except that individual elements track their known precision. The absolute precision of each element is limited to be less than the precision cap of the ring, even if mathematically the precision of the element would be known to greater precision (see Appendix A for the reasons for the existence of a precision cap).

Once again, use `Zp` to create a capped absolute p-adic ring.

```
sage: R = Zp(5, prec = 10, type = 'capped-abs', print_mode = 'series')
sage: R
5-adic Ring with capped absolute precision 10
```

We can do similar things as in the fixed modulus case:

```
sage: a = R(375)
sage: a
3*5^3 + O(5^10)
sage: b = R(105)
sage: b
5 + 4*5^2 + O(5^10)
sage: a + b
5 + 4*5^2 + 3*5^3 + O(5^10)
sage: a * b
3*5^4 + 2*5^5 + 2*5^6 + O(5^10)
sage: c = a // 5
sage: c
3*5^2 + O(5^9)
```

Note that when we divided by 5, the precision of `c` dropped. This lower precision is now reflected in arithmetic.

```
sage: c + b
5 + 2*5^2 + 5^3 + O(5^9)
```

Division is allowed: the element that results is a capped relative field element, which is discussed in the next section:

```
sage: 1 / (c + b)
5^-1 + 3 + 2*5 + 5^2 + 4*5^3 + 4*5^4 + 3*5^6 + O(5^7)
```

2.3 Capped Relative Rings and Fields

Instead of restricting the absolute precision of elements (which doesn't make much sense when elements have negative valuations), one can cap the relative precision of elements. This is analogous to floating point representations of real numbers. As in the reals, multiplication works very well: the valuations add and the relative precision

of the product is the minimum of the relative precisions of the inputs. Addition, however, faces similar issues as floating point addition: relative precision is lost when lower order terms cancel.

To create a capped relative precision ring, use `Zp` as before. To create capped relative precision fields, use `Qp`.

```
sage: R = Zp(5, prec = 10, type = 'capped-rel', print_mode = 'series')
sage: R
5-adic Ring with capped relative precision 10
sage: K = Qp(5, prec = 10, type = 'capped-rel', print_mode = 'series')
sage: K
5-adic Field with capped relative precision 10
```

We can do all of the same operations as in the other two cases, but precision works a bit differently: the maximum precision of an element is limited by the precision cap of the ring.

```
sage: a = R(375)
sage: a
3*5^3 + O(5^13)
sage: b = K(105)
sage: b
5 + 4*5^2 + O(5^11)
sage: a + b
5 + 4*5^2 + 3*5^3 + O(5^11)
sage: a * b
3*5^4 + 2*5^5 + 2*5^6 + O(5^14)
sage: c = a // 5
sage: c
3*5^2 + O(5^12)
sage: c + 1
1 + 3*5^2 + O(5^10)
```

As with the capped absolute precision rings, we can divide, yielding a capped relative precision field element.

```
sage: 1 / (c + b)
5^-1 + 3 + 2*5 + 5^2 + 4*5^3 + 4*5^4 + 3*5^6 + 2*5^7 + 5^8 + O(5^9)
```

2.4 Lazy Rings and Fields

The model for lazy elements is quite different from any of the other types of p-adics. In addition to storing a finite approximation, one also stores a method for increasing the precision. The interface supports two ways to do this: `set_precision_relative` and `set_precision_absolute`.

```
sage: R = Zp(5, prec = 10, type = 'lazy', print_mode = 'series', halt = 30)
sage: R
Lazy 5-adic Ring
sage: R.precision_cap()
10
sage: R.halting_parameter()
30
sage: K = Qp(5, type = 'lazy')
sage: K.precision_cap()
20
sage: K.halting_parameter()
40
```

There are two parameters that are set at the creation of a lazy ring or field. The first is `prec`, which controls the precision to which elements are initially computed. The second is `halt`: when computing with lazy rings, sometimes situations arise where the insolvability of the halting problem gives us problems. For example,

```
sage: a = R(16)
sage: b = a.log().exp() - a
sage: b
O(5^10)
sage: b.valuation()
...
<class 'sage.rings.padics.precision_error.HaltingError'>:
 Stopped computing sum: set halting paramter higher if you want computation to contin
```

Setting the halting parameter controls to what absolute precision one computes in such a situation.

The interesting feature of lazy elements is that one can perform computations with them, discover that the answer does not have the desired precision, and then ask for more precision. For example,

```
sage: a = R(6).log() * 15
sage: b = a.exp()
sage: c = b / R(15).exp()
sage: c
1 + 2*5 + 4*5^2 + 3*5^3 + 2*5^4 + 3*5^5 + 5^6 + 5^10 + O(5^11)
sage: c.set_precision_absolute(15)
sage: c
1 + 2*5 + 4*5^2 + 3*5^3 + 2*5^4 + 3*5^5 + 5^6 + 5^10 +
               4*5^11 + 2*5^12 + 4*5^13 + 3*5^14 + O(5^15)
```

There can be a performance penalty to using lazy p-adics in this way. When one does computations with them, the computer construct an expression tree. As you compute, values of these elements are cached, and the overhead is reasonably low

(though obviously higher than for a fixed modulus element for example). But when you set the precision, the computer has to reset precision throughout the expression tree for that element, and thus setting precision can take the same order of magnitude of time as doing the initial computation. However, lazy p-adics can be quite useful when experimenting.

2.5 Unramified Extensions

One can create unramified extensions of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ using the functions `Zq` and `Qq`. These extensions are still in a relatively primitive state, so I would suggest the following options when creating such extensions (more are available but may not currently work as well).

In addition to requiring a prime power as the first argument, `Zq` also requires a name for the generator of the residue field. One can specify this name as follows:

```
sage: R.<c> = Zq(125, prec = 20)
sage: R
Unramified Extension of 5-adic Ring with capped absolute precision 20 in x
 defined by (1 + O(5^20))*c^3 + O(5^20)*c^2 + (3 + O(5^20))*c + 3 + O(5^20)
```

3 New Versions of the p-adics

The code for p-adics is fairly rapidly changing. If there's a bug you want fixed, let me know and I'll try to fix it. Once I do, you'll need to get the latest version of p-adics with the bug fixed. If you don't want to wait for the next version of SAGE to come out, you can do the following to get the most recent version:

```
sage: hg_sage.pull(
 'http://sage.math.washington.edu/home/padicgroup/development-version.hg')
sage: hg_sage.apply(
 'http://sage.math.washington.edu/home/padicgroup/development-version.hg')
sage: quit
localhost:~$ sage
sage: run code that generated bug.
```

If you want a slightly more stable but older version, use `semistable-version.hg` instead.