p-Adic Numbers

K. Sutner

v0.5

1 Modular Arithmetic

add

rings
integral domains
integers
gcd, extended Euclidean algorithm
factorization
modular numbers

Lemma 1.1 (Chinese Remainder Theorem)

Let $a \perp b$. Then $\mathbb{Z}/(ab)$ is isomorphic to $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$.

2 Motivation

We can write non-negative integers in binary notation as sums

$$a = \sum_{i=0}^{k} a_i \cdot 2^i$$

where the digits a_i are in $\{0, 1\}$. Indeed, by adopting reasonable conventions about leading zeros, we obtain a unique representation. If we extend the summation "to the left," we can represent arbitrary non-negative reals:

$$a = \sum_{i=-\infty}^{k} a_i 2^i$$

All such series are automatically convergent with respect to the standard norm, but note that this representation is not unique:

$$1 \cdot 2^0 = \sum_{i<0} 1 \cdot 2^i$$

Arithmetic operations are defined in the usual manner. To deal with negative numbers we have admit signs as in

$$a = \pm \sum_{i=-\infty}^{k} a_i 2^i$$

Inquisitive minds might wonder what happens if we extend the summation to the right instead and consider "numbers" of the form, say,

$$a = \sum_{i=0}^{\infty} a_i 2^i$$

We will call these objects dyadic integers. It is convenient to abuse the standard decimal point and write these numbers in the format $a = \,.\, a_0 a_1 a_2 \ldots$ A priori, these expressions are just formal

Laurent series, there is no convergence unless all but finitely many of the digits are 0. Still, at the least we get back the non-negative integers. We can add two such numbers via the eminently reasonable rule $2^i + 2^i \mapsto 2^{i+1}$; note that we may have to apply this rule infinitely often in a single addition. Now consider

$$m = \sum_{i=0}^{\infty} 2^i = .1111\ldots$$

According to our rules for addition, $m + 1 = 0$. Hence $m = -1$. We can also define multiplication: to multiply by 2^i, shift by i places to the right and deal with sums by distributivity. For example, multiplying by $m = -1$ comes down to flipping all bits after the first 1. It turns out that our dyadic integers form a commutative ring. Moreover, we can represent all the integers in our new number system without use of a sign, and one can show that the representation is unique.
So far, so good. But unless the dyadic integers capture more numbers this would seem like so much wasted effort. What number would the expression

$$a = \mathbf{.}\,10101010\ldots$$

represent? Since $2a = \mathbf{.}\,0101010\ldots$ we have $3a = \mathbf{.}\,11111\ldots$ so that $a = -1/3$; likewise $1/3 = \mathbf{.}\,11010101\ldots$ This observation can be pushed further: suppose the bit-sequence associated with a dyadic number a is periodic. Then $a = r/q$ where the denominator q is odd. For suppose (a_i) has period $\pi \geq 1$. Then $2^\pi a = a - \sum_{i<\pi} a_i 2^i$ so that

$$a = -\frac{\sum_{i<\pi} a_i 2^i}{2^\pi - 1}$$

The numerator r here is constrained to $-2^\pi < r < 0$. But then a general rational r/q, q odd, corresponds to an ultimately periodic dyadic integer. This turns out to be an if-and-only-if situation. For example, $1/3 + 1/5 = 8/15$ translates into

$$\begin{array}{llllllllllllllllll}
\mathbf{.}1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \ldots \\
\mathbf{.}1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & \ldots \\
\hline
\mathbf{.}0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \ldots
\end{array}$$

Needless to say, instead of 2 we could also consider an arbitrary prime p and use digits $D = \{0, 1, \ldots, p-1\}$.

3 Completions of $\mathbb{Q}$

The reals $\mathbb{R}$ can be construed as the completion of $\mathbb{Q}$ with respect to the standard norm $|x|$ on $\mathbb{Q}$, the absolute value. Technically one considers all Cauchy sequences (a_n) over $\mathbb{Q}$:

$$\forall\, \varepsilon > 0\, \exists\, n\, \forall\, i, j > n\ (|a_i - a_j| < \varepsilon)$$

A null-sequence is a sequence (a_n) with

$$\forall\, \varepsilon > 0\, \exists\, n\, \forall\, i > n\ (|a_i| < \varepsilon)$$

We define an equivalence relation $\approx$ on these sequences: $(a_n) \approx (b_n) \iff (a_n - b_n)$ is a null-sequence.
Then the space of all Cauchy sequences over $\mathbb{Q}$ modulo $\approx$ is the completion of $\mathbb{Q}$ with respect to the standard norm. This space is isomorphic to the reals (assuming they were defined in some other way to begin with; say, via Dedekind cuts). In particular this space is complete: applying the same Cauchy completion a second time produces no new points. Note the role of the absolute value in the construction, it is worth while to take a closer look at this type of map.

3.1 Norms and Valuations

A norm (or absolute value, sometimes called the absolute value at infinity) on a field $\mathbb{F}$ is a map $|.| : \mathbb{F} \to \mathbb{R}_{\geq 0}$ subject to the following conditions:

- $|a| = 0 \iff a = 0$
- $|ab| = |a||b|$
- $|a + b| \leq |a| + |b|$ (triangle inequality)

Every field admits the trivial norm $|0| = 0$, $|x| = 1$ otherwise. The standard norm on $\mathbb{Q}$ or $\mathbb{R}$ is given by $|a| = a$ for $a \geq 0$, and $|a| = -a$ otherwise. For $\mathbb{C}$ we have the norm $|a| = \sqrt{a\overline{a}}$.

Proposition 3.1 *$a^n = 1$ implies $|a| = 1$. Also, $|a^n| = |a|^n$ for $n \in \mathbb{Z}$.*

It follows that a finite field admits only the trivial norm.
A norm is discrete if for some $\varepsilon > 0$ and all a

$$1 - \varepsilon < |a| < 1 + \varepsilon \quad \text{implies} \quad |a| = 1.$$

A discrete norm has a discrete range in $\mathbb{R}_{\geq 0}$.
A norm is non-archimedean if it satisfies a stronger version of the triangle inequality, the ultrametric inequality

$$|a + b| \leq \max(|a|, |b|).$$

It is easy to see that a norm is non-archimedean iff $|n| \leq 1$ for all $n \geq 0$. For a non-archimedean norm we have $|a| < |b|$ implies $|a + b| = |b|$.
Fields of positive characteristic admit only non-archimedean norms; finite fields in particular admit only the trivial norm.
Given a non-archimedean norm, it is interesting to consider the following subrings of $\mathbb{F}$

$$\mathfrak{o} = \{\, a \in \mathbb{F} \mid |a| \leq 1 \,\}$$
$$\mathfrak{m} = \{\, a \in \mathbb{F} \mid |a| < 1 \,\}$$

Note that $\mathfrak{o}$ is indeed a subring of $\mathbb{F}$, called the valuation ring (see below), and $\mathfrak{m}$ is the uniquely determined maximal ideal in $\mathfrak{o}$.

Lemma 3.1 *A non-archimedean norm is discrete if, and only if, $\mathfrak{m}$ is principal.*

Closely related to norms a valuations, intuitively obtained by taking the negative logarithm to a non-archimedean norm. A valuation on a field $\mathbb{F}$ is a group homomorphism $\nu : \mathbb{F}^\times \to (\mathbb{R}, +)$. It convenient to extend domain and codmain and we obtain

- $\nu(a) = \infty \iff a = 0$
- $\nu(ab) = \nu(a) + \nu(b)$
- $\nu(a + b) \geq \min(\nu(a), \nu(b))$ where equality holds for $\nu(a) \neq \nu(b)$.

The image of ν is the value group Γ; ν is discrete if Γ is isomorphic to $\mathbb{Z}_\infty$, the ordered, free Abelian group with a point at infinity. By rescaling, we may assume that Γ is equal to $\mathbb{Z}_\infty$.
Given a valuation ν we obtain a non-archimedean norm by setting

$$|a|_\nu = c^{\nu(a)}$$

for any constant $0 < c < 1$. For this norm we have the valuation ring

$$\mathfrak{o} = \{\, a \in \mathbb{F} \mid |a| \leq 1 \,\} = \{\, a \in \mathbb{F} \mid \nu(a) \geq 0 \,\}$$

One can verify that $\mathfrak{o}$ is indeed a commutative ring and even an integral domain; moreover, $\mathbb{F}$ is its field of fractions. In the discrete case, these rings are called discrete valuation rings (DVR). DVR carry a lot of interesting structure. The group of units of $\mathfrak{o}$ is

$$\{\, a \in \mathfrak{o} \mid |a| = 1 \,\} = \{\, a \in \mathfrak{o} \mid \nu(a) = 0 \,\}$$

Pick such a unit p and note that $a \in \mathbb{F}^\times$ can be written uniquely as $a = u\, p^n$ where $n = \nu(a)$. As a consequence, $\mathfrak{o}$ is a principal ideal domain and the non-trivial ideals of $\mathfrak{o}$ look like

$$I = (p^n) = \{\, a \in \mathfrak{o} \mid \nu(a) \geq n \,\}$$

But then $\mathfrak{m} = \{\, a \in \mathbb{F} \mid |a| < 1 \,\}$ is indeed the uniquely determined maximal ideal.

3.2 p-Adic norms on $\mathbb{Q}$

As an example, let us consider the norms on $\mathbb{Q}$. The standard norm clearly fails to be discrete or non-archimedean. Here is a more interesting alternative. Fix some prime p and define the p-adic valuation of an integer $n \neq 0$ to be the largest e such that p^e divides n, in symbols $\nu_p(n)$:

$$\nu_p(n) = \max(\, e \geq 0 \mid p^e \mid n \,)$$

Set $\nu_p(0) = \infty$. Lift to rational a/b in lowest common terms via $\nu_p(a/b) = \nu_p(a) - \nu_p(b)$. Clearly, on domain $\mathbb{Q}$, $\nu_p(.)$ has value group $\mathbb{Z}_\infty$. We obtain the associated p-adic norm by setting $c = 1/p$:

$$|a/b|_p = p^{-\nu_p(a/b)}$$

This produces a discrete non-archimedean norm, see section 5 for a discussion of the associated valuation ring.

Less formally, our valuation on $\mathbb{Z}$ is given by

$$\left|\pm \prod q^{e_q}\right|_p = e_p$$

where the product is supposed to extend over all primes, and each exponent e_q is a uniquely determined non-negative integer. To lift to the field of fractions, write a non-zero rational as $r = p^e a/b$ where $e \in \mathbb{Z}$ and p is coprime with ab. Then $|r|_p = p^{-e}$. Note that the p-adic norm produces a somewhat counterintuitive notion of size: for example, p^2 is smaller than p^{-2}.
By a theorem of Ostrowski, all the non-trivial norms on $\mathbb{Q}$ other than the standard norm are equivalent to p-adic norms (equivalent meaning $|x|_1 = |x|_2^c$ for some constant c.) In fact, we have for all $x \neq 0$:

$$\prod |x|_p = 1$$

The question arises what a completion of $\mathbb{Q}$ with respect to a p-adic norm might look like. One can follow the construction of the reals from $\mathbb{Q}$ using the p-adic norm instead of the standard, Archimedean norm. Here is a slightly more direct approach that focuses on reasonable representations of the objects under consideration.

4 Constructing p-Adic Integers

We now give a somewhat more constructive description of p-adic numbers, focusing on appropriate data structures and algorithms. First define the set of rationals without a factor p in the denominator:

$$\mathbb{Z}_{(p)} = \{\, r \in \mathbb{Q} \mid \nu_p(r) \geq 0 \,\} = \{\, r \in \mathbb{Q} \mid |r|_p \leq 1 \,\}$$

Then $\mathbb{Z}_{(p)}$ forms a ring, $p^{n+1}\mathbb{Z}_{(p)}$ is an ideal in this ring and thus defines a congruence. We write $s = t \pmod{p^{n+1}\mathbb{Z}_{(p)}}$ if $s - t \in p^{n+1}\mathbb{Z}_{(p)}$. Thus, writing $s - t = a/b$ in lowest common terms we have $\nu_p(a) \geq n + 1$.
A sequence (s_n) over $\mathbb{Z}_{(p)}$ is coherent if $s_n = s_{n+1} \pmod{p^{n+1}\mathbb{Z}_{(p)}}$. Thus, if the terms are integral, then $s_n - s_{n+1}$ must be divisible at least by p^{n+1}. Coherence allows one to think of such an integral sequence as defining an inverse limit in

$$Z/(p) \leftarrow Z/(p^2) \leftarrow Z/(p^3) \leftarrow \ldots$$

where the maps are the canonical epimorphisms; see also the standard sequences below.
Two sequences (s_n) and (t_n) are similar, in symbols $(s_n) \approx (t_n)$, if $s_n = t_n \pmod{p^{n+1}\mathbb{Z}_{(p)}}$.

Definition 4.1 *The p-adic integers are the quotient*

$$\mathbb{Z}_p = \mathbb{Z}_{(p)}^{\mathbb{N},\mathrm{coh}}/\approx$$

Addition and multiplication are defined point-wise.

Since p is prime we obtain an integral domain in this way (non-prime p still produce a commutative ring but one with zero-divisors). While the p-adic integers are defined in terms of sequences of fractions they can also be obtained from sequences of integers. This sequence is the standard sequence and can be seen as a canonical representation of the corresponding p-adic integer.

Lemma 4.1 *For each coherent sequence (s_n) over $\mathbb{Z}_{(p)}$ there exists a similar sequence (t_n) such that $t_n \in \mathbb{Z}$, $0 \leq t_n < p^{n+1}$.*

Proof. Let $s_n = a/b \in \mathbb{Z}_{(p)}$. Since b is a unit in the ring of modular numbers $\mathbb{Z}/(p^{n+1})$ we can choose an integer b' such that $bb' = 1 \pmod{p^{n+1}}$. Now set $t_n = ab' \bmod p^{n+1}$. □

It is often more convenient to write the elements of the standard sequence in radix p representation:

$$t_n = \sum_{i \leq n} \alpha_i p^i.$$

Note that this works since (t_n) is coherent. In the binary case, $\alpha_{n+1} = \alpha_n$ or $\alpha_{n+1} = \alpha_n + 2^n$. It is then natural to write

$$\alpha = \sum_{i < \infty} \alpha_i p^i$$

for a p-adic integer. Lastly, we can remover the powers of p as is standar practice in radix notation, yielding a sequence $.\alpha_0\alpha_1\alpha_2\ldots$ This is the p-adic digit representation of α. Note that this representation is unique (as opposed to the standard radix representation of reals).
The map $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$, $s \mapsto (s)$ is a ring monomorphism, so we can think of the integers as a subring of the p-adic integers. However, from the standard sequence representation it is easy to conclude that $\mathbb{Z}_p$ is uncountable, so this notion of integer is far from the standard one.

Example 4.1 For this example let $p = 2$, so we are dealing with dyadic integers.

r	standard sequence	digit form
-1	(1,3,7,15,...)	.11111 ...
5	(1,1,5,5,5,...)	.101
-5	(1,3,3,11,27,59,123,251,...)	.110111111 ...
1/5	(1,1,5,13,13,13,77,205,205,205,1229,...)	.10110011001100 ...

Computation of digit representation in Mathematica:

```
Reverse@IntegerDigits[ PowerMod[ 5, -1, 2^10 ], 2 ]
FromDigits[ {{1, {0, 1, 1, 0}}, 1}, 1/2 ]
```

Example 4.2 Consider the sequence $a_n = (1+p)^{p^n} - 1$. A simple computation shows that for $n > 0$ we have $|a_n|_p = p^{-(n+1)}$. Hence (a_n) is a null sequence.

Ultimately constant digit representations correspond to integers. For example, in the dyadic numbers, -5 corresponds to $.1101^\omega$. Ultimately periodic digit representations correspond to rational numbers. To see this, note that $\sum_{i\geq 0} p^i = 1/(1-p)$ in the p-adic norm (much like the case $|p| < 1$ in the standard norm). Consider $\alpha = .b_0 \dots b_r \overline{c_0 \dots c_{s-1}}$. Then

$$\alpha = \sum_{i \leq r} b_i p^i + \frac{\sum_{j<s} c_j p^j}{1 - p^s}$$

Lemma 4.2 *The p-adic digit representations of numbers in $\mathbb{Z}_{(p)}$ are ultimately periodic.*

Proof. Exercise. □

Here is a critical lemma that helps to determine solutions of polynomial equations over $\mathbb{Z}_p$.

Lemma 4.3 (Hensel) *Let $f \in \mathbb{Z}[x]$ be a polynomial with a root $f(r) = 0 \pmod{p^n}$ and $f'(r) \neq 0 \pmod{p}$. Then there exists an r' such that $f(r') = 0 \pmod{p^{n+1}}$ and $r = r' \pmod{p^n}$.*

Proof. As integers, the roots of f modulo p^n have the form $r + kp^n$ where $k \in \mathbb{Z}$. In order to determine appropriate values of k, let $f(x) = \sum_{i \leq d} a_i x^i$ so that

$$\begin{aligned} f(r + kp^n) &= \sum a_i (r + kp^n)^i \\ &= \sum a_i r^i + kp^n \sum_{i>0} i a_i r^{i-1} + A \\ &= f(r) + kp^n f'(r) + A \end{aligned}$$

where A is a multiple of p^{2n}. Hence

$$f(r + kp^n) = f(r) + kp^n f'(r) \pmod{p^{n+1}}$$

and it follows that

$$k\, f'(r) = f(r)/p^n \pmod{p}$$

Our claim follows. □

Note that polynomial equations over $\mathbb{Z}_p$ may have solutions even when the corresponding equation over $\mathbb{Q}$ does not. For example, consider $x^2 = 2$. There is a solution $x_n^2 = 2 \pmod{7^n}$ for all $n \geq 0$. In fact, we can obtain a coherent sequence of integers: $x = (3, 10, 108, 2166, 4567, 38181, \dots)$

defining a solution x in $\mathbb{Z}_7$. There is one other solution corresponding to $-x$ with sequence $(4, 39, 235, 235, 12240, 79468, \ldots)$. To prove the existence of these solutions we can use Hensel's lemma: let $f(x) = x^2 - 2$ so that $f'(x) = 2$. Then $r = 3$ satisfies the conditions of the lemma: $f(r) = 7 = 0 \pmod 7$ and $f'(r) = 2 \neq 0 \pmod 7$.
There are many versions of Hensel's lemma; here is one that deals more directly with the question of when a polynomial has a root over $\mathbb{Z}_p$.

Lemma 4.4 (Hensel, II) *Let $f \in \mathbb{Z}_p[x]$ be a polynomial. Suppose that for some $\alpha_0 \in \mathbb{Z}_p$ we have $f(\alpha_0) = 0 \pmod{p\mathbb{Z}_p}$ but $f'(\alpha_0) \neq 0 \pmod{p\mathbb{Z}_p}$. Then there is a unique p-adic integer α such that $f(\alpha) = 0$ and $\alpha = \alpha_0 \pmod{p\mathbb{Z}_p}$.*

5 p-Adic Rationals

We can extend the p-adic valuation to $\mathbb{Z}_p$ since, for all n, we must have $\nu_p(s_n) \geq n + 1$ or $\nu_p(s_n) = \nu_p(s_{n+1})$. So in the limit $\nu_p(s_n)$ is either infinite or $\nu_p(s_n) = \nu_p(s_m)$ for all $n \geq m$.
The units in $\mathbb{Z}_p$ are easy to characterize (note that there are uncountably many of them).

Lemma 5.1 *$\alpha \in \mathbb{Z}_p$ is a unit if, and only if, $|\alpha|_p = 1$.*

Proof. First suppose α is a unit and let (s_n) be the corresponding standard sequence. Then there is a standard sequence (t_n) such that $s_n t_n = 1 \pmod{p^{n+1}\mathbb{Z}_{(p)}}$. But then $\nu_p(s_n t_n) = 0$ and $\nu_p(s_n) = 0$. The claim follows.
For the opposite direction let m minimal such that $\nu_p(s_n) = 0$ for all $n \geq m$. If $m > 0$ we have by coherence $\nu_p(s_{m-1} - s_m) \geq m \geq 1$. But then $\nu_p(s_{m-1}) = 0$, a contradiction. Hence $m = 0$.
We need to show that the sequence (s_n^{-1}) is coherent. By coherence of s_n we have $s_n - s_{n+1} = r \cdot p^{n+1}$ where $r \in \mathbb{Z}_{(p)}$. Now

$$s_n^{-1} - s_{n+1}^{-1} = \frac{s_{n+1} - s_n}{s_n s_{n+1}} = \frac{-rp^{n+1}}{s_n s_{n+1}} \in \mathbb{Z}_{(p)}$$

Done. □

Thus, in the standard sequence representation, we need $s_0 \neq 0$ (same for digit representation). We can write any element $0 \neq \alpha \in \mathbb{Z}_p$ as

$$\alpha = \epsilon \cdot p^{\nu_p(\alpha)}$$

where ϵ is a unit: we simple shift the first non-zero term of α to the first position by multiplying by $|\alpha|_p$.
It is now easy to expand $\mathbb{Z}_p$ to a field by a modification of the standard quotient construction. To this end define an equivalence relation $\cong$ on $\mathbb{Z}_p \times \{\, p^i \mid i \geq 0 \,\}$ (rather than $\mathbb{Z}_p \times \mathbb{Z}_p^\times$ as in the standard construction) by

$$(\alpha, p^n) \cong (\beta, p^m) \iff \alpha p^m = \beta p^n$$

As usual, the equivalence classes are written in fractional notation: α/p^n. The operations are inherited from $\mathbb{Z}_p$:

$$\frac{\alpha}{p^n} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^n}{p^{n+m}}$$
$$\frac{\alpha}{p^n} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{n+m}}$$

Definition 5.1 *The p-adic numbers are defined to be*

$$\mathbb{Q}_p = \{\, \alpha/p^n \mid \alpha \in \mathbb{Z}_p, n \geq 0 \,\}$$

We can also think of $\mathbb{Q}_p$ as $\mathbb{Z}_p[1/p]$. It is natural to extend the p-adic norm to $\mathbb{Q}_p$ by

$$|\alpha/p^n|_p = |\alpha|_p - n$$

Then we have again that any non-zero p-adic number ζ can be written as

$$\zeta = \epsilon \cdot p^{\nu_p(\zeta)}$$

where ϵ is a unit in $\mathbb{Z}_p$. Hence we can compute reciprocals in $\mathbb{Q}_p$ essentially by finding the inverse of ϵ, a unit in $\mathbb{Z}_p$. The p-adic digit representation for $\mathbb{Q}_p$ is naturally written as

$$\alpha = \sum_{i \geq m} \alpha_i p^i$$

where m is an integer, possibly negative. Note that this is just a finite-tailed Laurent series if we consider p to be the unknown. The series is often written using a "p-adic point" in analogy to the standard decimal notation:

$$\alpha = \alpha_m \, \alpha_{m+1} \, \ldots \alpha_1 \, . \, \alpha_0 \, \alpha_1 \, \alpha_2 \, \ldots$$

Example 5.1 Let $p = 5$, $\alpha = 2/3$ so that $m = 0$. Then $\alpha = .4131313\ldots$ since

$$\begin{aligned}
\alpha_0 &= \quad 2 \cdot 3^{-1} \bmod p = 4 \qquad 2/3 - 4 = p \cdot (-2/3) \\
\alpha_1 &= -2 \cdot 3^{-1} \bmod p = 1 \qquad -2/3 - 1 = p \cdot (-1/3) \\
\alpha_2 &= -1 \cdot 3^{-1} \bmod p = 3 \qquad -1/3 - 3 = p \cdot (-2/3)
\end{aligned}$$

It follows that, say, $2/75 = 41.313131\ldots$ and $50/3 = 0.0041313131\ldots$

One can show that $\mathbb{Q}_p$ is complete: all Cauchy sequences over $\mathbb{Q}_p$ already converge to an element of $\mathbb{Q}_p$. We can think of $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$. For let $a/b \in \mathbb{Q}$ and set $n = |b|_p$. Then $a/b\, p^n \in \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$ and we can identify $a/b \in \mathbb{Q}$ with $(a/b\, p^n)/p^n \in \mathbb{Q}_p$. $\mathbb{Q}$ is then dense in $\mathbb{Q}_p$ and indeed $\mathbb{Q}_p$ could also have been constructed as the completion of $\mathbb{Q}$ with respect to the p-adic norm.
Using these identifications we have

$$\begin{aligned}
\mathbb{Z}_p &= \{\, x \in \mathbb{Q}_p \mid |x|_p \leq 1 \,\} \\
\mathbb{Z}_{(p)} &= \mathbb{Z}_p \cap \mathbb{Q} = \{\, a/b \in \mathbb{Q} \mid p \nmid b \,\} \\
\mathbb{Z}_p^{\times} \cap \mathbb{Q} &= \{\, a/b \in \mathbb{Q} \mid p \nmid ab \,\}
\end{aligned}$$

The first characterization relies on the fact that we are dealing with an ultrametric, so we get a compact subring of $\mathbb{Q}_p$ by restricting ourselves to norm at most 1. As a consequence, $\mathbb{Q}_p$ is totally disconnected.
There is a result, related to the Chinese Remainder Theorem, that shows that one can approximate rationals in several p-adic norms simultaneously.

Lemma 5.2 (Weak Approximation Theorem) *Let p_i, $i \leq n$, be distinct primes and r_i, $i \leq n$, rational numbers. For every $\varepsilon > 0$ there exists a rational r such that $|r_i - r|_{p_i} < \varepsilon$.*

This comes down to making sure that $r - r_i = 0 \pmod{p_i^k}$ for arbitrary k.

6 Axiomatic Approach

To give a more axiomatic description of the p-adic number, consider an integral domain $\mathfrak{o}$ with field of fractions $\mathbb{F}$, say, of characteristic 0. $\mathfrak{o}$ is a valuation ring if for any element $a \neq 0$ in $\mathbb{F}$, $a \in \mathfrak{o}$ or $a^{-1} \in \mathfrak{o}$. The ideals of a valuation ring are totally ordered by inclusion, so there is a unique maximal ideal $\mathfrak{m} \subseteq \mathfrak{o}$.
$\mathbb{F}$ is a p-adic field if the valuation ring $\mathfrak{o} \subseteq \mathbb{F}$ is a maximal subring of $\mathbb{F}$, subject to the following conditions. Letting $\mathfrak{m} \subseteq \mathfrak{o}$ be the maximal ideal, the canonical quotient map is an isomorphism $\mathfrak{o}/\mathfrak{m} \to \mathbb{F}_p$, for some prime p. The value group $\Gamma = \mathbb{F}^\times/\mathfrak{o}^\times$ is a $\mathbb{Z}$-group (there exists a unique minimal positive element, and $[\Gamma : n\Gamma] = n$ for all $n \geq 1$). Let ν be the canonical map $\mathbb{F}^\times \to \Gamma$; then $\nu(p)$ is the unique minimal positive element of Γ.
Lastly, Hensel's lemma holds in the following form: for any polynomial $f(x) \in \mathfrak{o}[x]$ and $a \in \mathfrak{o}$ such that $f(a) = 0$ but $f'(a) \neq 0$, there is a $a' \in \mathfrak{o}$ such that $f(a') = 0$ and $\nu(a' - a) > \nu(f'(a))$.

We can recover $\mathfrak{o}$ from a homomorphism $\nu : \mathbb{F}^\times \to \Gamma$ into a $\mathbb{Z}$-group by letting $\mathfrak{o} = \{\, x \in \mathbb{F}^\times \mid \nu(x) \geq 0 \,\} \cup \{0\}$.

The critical example is $\mathfrak{o} = \mathbb{Z}_p \subseteq \mathbb{Q}_p$. Here Γ is (isomorphic to) $\mathbb{Z}$, and $\mathfrak{m} = (p) \subseteq \mathbb{Z}_p$.

7 Dyadic Numbers and Circuits

The case $p = 2$ is particularly interesting, since we can naturally identify $\mathbb{Z}_2$ with the sequence space $\mathbf{2}^\omega$ or the Boolean space $\mathbb{B}^\omega$. As a consequence, there are natural operations on $\mathbb{Z}_2$ other than the algebraic ones considered so far.

Logical: We can think of $\mathbf{2}$ as $\mathbb{B}$ and apply logical operations pointwise; we obtain a Boolean algebra isomorphic to $\mathfrak{P}(\mathbb{N})$.

Combinatorial:

- up-shift $b = \mathbf{z}^-(a)$, $b_0 = 0$, $b_n = a_{n-1}$
- down-shift $b = \mathbf{z}(a)$, $b_n = a_{n+1}$
- up-power $b = \uparrow(a)$, $b_{2n} = a_n$, $b_{2n+1} = 0$
- down-sample, even $b = \mathsf{even}(a)$, $b_n = a_{2n}$
- down-sample, odd $b = \mathsf{odd}(a)$, $b_n = a_{2n+1}$
- shuffle $c = a \odot b$, $c_{2n} = a_n$, $c_{2n+1} = b_n$
- convolution $c = a \otimes b$, $c_n = \oplus_{i+j=n} a_i b_j$

The space of dyadic numbers together will all these operations is referred to as digital numbers $\mathbb{D}$ by Vuillemin. There are natural embeddings

$$\mathbb{B} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Z}_{(2)} \subseteq \mathbb{Z}_2 \simeq \mathbb{D}$$

from various important structures into the digital numbers. By selecting appropriate subsets of the operations get for example the Boolean algebra $\langle \mathbb{D}, \vee, \wedge, \neg \rangle$.
There are lots of equational relations between these operations. For example, we have

$$
\begin{aligned}
-a &= 1 + \neg a \\
\mathbf{z}\, a &= 2 \otimes a = 2 \times a \\
\uparrow a &= a \otimes a \\
\mathbf{z}\, \mathbf{z}^{-}\, a &= a \\
a &= (\mathsf{even}\, a) \odot (\mathsf{odd}\, a).
\end{aligned}
$$

Also, $\mathbb{D} \simeq \mathbb{D} \times \mathbb{D}$ since the shuffle operation is a pairing function $\odot : \mathbb{D} \times \mathbb{D} \to \mathbb{D}$. The corresponding unpairing functions are even and odd.
The additional operations can be useful in describing certain functions $f : \mathbb{D} \to \mathbb{D}$, in particular with a view towards their realization as a digital circuit. We will only consider circuits with discrete time, so the state of the circuit is defined only for $t = 0, 1, 2, \ldots$ It is convenient to consider a special ternary Boolean function, a so-called multiplexer: a type of controlled switch where the first input selects which of the other inputs is selected for output. Alternatively, we can think of a multiplexer as an if-then-else gate. In symbols:

$$\mathbf{?}(x, y, z) = (x \wedge y) \vee (\neg x \wedge z)$$

Note that $\mathbf{?}$ together with constants true and false forms a basis for all Boolean functions.

$$
\begin{aligned}
\neg x &= \mathbf{?}(x, \bot, \top) \\
x \wedge y &= \mathbf{?}(x, y, \bot) = \mathbf{?}(x, y, x) \\
x \vee y &= \mathbf{?}(x, \top, y) = \mathbf{?}(x, x, y) \\
x \oplus y &= \mathbf{?}(x, \mathbf{?}(y, \bot, y), y)
\end{aligned}
$$

Another important digital component is a register or unit delay: the output at time $t = 0$ is 0 and otherwise the input at time $t - 1$. A closely related gadget is a register that outputs a 1 at time 0. In order for a circuit built from multiplexers and registers to have well-defined behavior we require that there are no cycles in the corresponding diagram whose nodes are exclusively multiplexers (equivalently, there are no feedback loops in the purely Boolean part of the circuit).
Unless mentioned otherwise, we do not require circuits to be finite. However, all paths from input to output must be finite.

7.1 Types of Functions

Definition 7.1 *Let $f : \mathbb{D} \to \mathbb{D}$. f is continuous if it is continuous in the sense of the standard topology:*

$$\forall\, \varepsilon > 0, x\, \exists\, \delta > 0\, \forall\, y\, (|x - y| < \delta \to |f(x) - f(y)| < \varepsilon).$$

f is on-line or causal if

$$f(x) = \sum_{t \geq 0} f_t(x_0, \ldots, x_t)\, 2^t$$

where $x = \sum x_i 2^i$. f is 1-Lipschitz if

$$\forall\, x, y\, (|f(x) - f(y)| \leq |x - y|).$$

By the Heine-Cantor theorem, a continuous function on $\mathbb{D}$ is already uniformly continuous so that

$$\forall\, n\, \exists\, m\, \forall\, x, y\, (|x - y| < 2^{-m} \to |f(x) - f(y)| < 2^{-n}).$$

Thus, the first $m = m(n)$ input bits suffice to determine the first n output bits.

Theorem 7.1 *f can be computed by a combinational circuit iff f is continuous.*

In other words, we can write

$$f(x) = \sum_{t \geq 0} f_t(x_0, \ldots, x_{m(t)})\, 2^t$$

for some function $m : \mathbb{N} \to \mathbb{N}$. The component function f_t is a finite Boolean function can thus be computed by a combinational circuit. Note that we require paths from inputs to outputs to be finite (though the whole circuit might be infinite).

Lemma 7.1 *Let f be on-line. Then f is injective iff*

- $\exists\, g \forall\, x\ : g(f(x)) = x$.
- $\forall\, x, y\, (|f(x) - f(y)| = |x - y|)$.
- $\exists\, g, c \forall\, x\ : f(x) = x \oplus c \oplus 2 \times g(x)$.

Note that an injective on-line function is necessarily surjective.

The following theorem generalizes Boolean decision diagrams to synchronous decision diagrams, a type of (possibly infinite) digital circuit that describes on-line functions, much the way a BDD describes Boolean functions.

Theorem 7.2 *f can be computed by a synchronous digital circuit iff f is on-line iff f is 1-Lipschitz.*

Proof. The idea is to construct a circuit built from muxes and registers by exploiting the following analogue to Shannon expansion of Boolean functions:

$$f(x) = \mathbf{?}(x, b_1 + 2 \times f^1(x), b_0 + 2 \times f^0(x)).$$

To determine the right-hand side we compare coefficients:

f	f^1	f^0
$f_0(x_0)$	$b_1 = f_0(1)$	$b_0 = f_0(0)$
$f_0(x_0, x_1)$	$f_1(x_0, 1)$	$f_1(x_0, 0)$
$f_0(x_0, x_1, x_2)$	$f_2(x_0, x_1, 1)$	$f_2(x_0, x_1, 0)$

It is easy to build an infinite synchronous circuit with input x at the muxers, in the shape of a complete binary tree, that implements f. □

If $f = \underline{p}$ is given by a transducer we can construct the SDD as follows. First note that

$$f(x) = \sum_{za \sqsubset x} \partial_z f(a)\, 2^{|z|}$$

The functions f^u associated with f in the SDD construction then have the form

$$f^u(x) = \sum_{za \sqsubset x} \mathsf{lst}(\partial_z f(au))\, 2^{|z|}$$

Assuming that the transducer is accessible from state p, it follows that $f^u = f^v$ iff $\forall\, q, a\, (\mathsf{lst}(q * au) = \mathsf{lst}(q * av))$. Hence the SDD is finite whenever the transducer is finite.

References

[1] F. Q. Gouvêa. *p-Adic Numbers: An Introduction.* Springer Verlag, 2nd edition, 1997.

[2] J. Vuillemin. On circuits and numbers. *IEEE Transactions on Computers*, 43:868–879, 1994.