Math. Struct. in Comp. Science (2015), *vol.* 25, *pp.* 1147–1171. © Cambridge University Press 2015
doi:10.1017/S0960129514000541 First published online 13 February 2015

A univalent formalization of the *p*-adic numbers

ÁLVARO PELAYO[¶,‖,†], VLADIMIR VOEVODSKY[‖,‡]
and MICHAEL A. WARREN[§,††]

[¶]*Department of Mathematics, University of California, San Diego, 9500 Gilman Dr #0112, La Jolla, California 92093-0112, U.S.A.*
Email: alpelayo@math.ucsd.edu
[‖]*School of Mathematics, Institute for Advanced Study, Einstein Drive, Princeton, New Jersey 08540, U.S.A.*
Email: vladimir@ias.edu
[††]*Los Angeles, California, U.S.A.*
Email: maw@mawarren.net

Received 6 February 2013; revised 31 January 2014

The goal of this paper is to report on a formalization of the *p*-adic numbers in the setting of the second author's univalent foundations program. This formalization, which has been verified in the Coq proof assistant, provides an approach to the *p*-adic numbers in constructive algebra and analysis.

1. Introduction

In this paper, we present a formalization of the construction of the *p*-adic numbers in the Coq proof assistant. The formalization is carried out in the *univalent setting* introduced by the second author Voevodsky (2010 Extended version of NSF proposal at www.math.ias.edu/vladimir) and described in more detail in Voevodsky (2014 Experimental library of univalent formalization of mathematics. To appear). This setting, which is based on insights from homotopy theory and higher-dimensional category theory, serves as an overall organizational and methodological framework which informs our construction. At the same time, our construction has several ingredients which are familiar in constructive mathematics. The formalization described in this paper will be hosted on the associated journal website and presents a fixed picture of the development at this time. However, because work on formalization in this direction is ongoing, we expect that the Coq code associated with this paper may be updated accordingly in the future by the authors and others. As such, the structure and content of the Coq code described here, and hosted on the journal website, may not match exactly the code which is ultimately included in the univalent foundations libraries found on the authors' websites. Readers interested in making use of the code should accordingly consult the latest version available.

[†] Partly supported by NSF Grant DMS-0635607, an NSF CAREER Award DMS-1055897, Spain Ministry of Science Grant MTM 2010-21186-C02-01, and Spain Ministry of Science Sev-2011-0087.
[‡] Supported by NSF Grant DMS-1100938.
[§] Supported by the Oswald Veblen fund. Support also received from NSF Grant DMS-0635607 during the preparation of this paper.

1.1. *Motivation*

Our motivation in this project is twofold. Firstly, we chose to formalize the p-adic numbers as an initial step in the development and formalization of the p-adic theory of integrable systems. We hope that in the future, this will prove to be a promising approach to this theory which should facilitate progress in the field, in particular with regard to the construction of algorithms and their numerical analysis. Ultimately, we hope that insights from this project could be useful in the setting of real integrable systems. Secondly, the formalization of the p-adic numbers served as an appealing test case for formalization in the univalent setting of the kinds of structures required by working mathematicians in areas outside of homotopy theory and logic.

1.2. *Choice of setting*

The idea of the univalent perspective is, roughly, to develop mathematics within the world of homotopy types. By virtue of taking this approach we are able to make use of type theory as a calculus for formal reasoning about homotopy types. We hope that in the future, because this development of mathematics can be carried out in a proof assistant such as Coq so that the proofs carry some algorithmic content, it will be possible to extract good algorithms from the proofs. One of our motivations is that the construction of such algorithms would in turn help with some problems concerning integrable systems which are of particular interest in applications. For instance, one outstanding problem is: given numerical spectral data about a quantum system (coming from an experiment), extract an algorithm to reconstruct the classical integrable system, see Section 7.

Although, we have chosen to work in the univalent setting, it should be possible to adapt the construction of the p-adic numbers given here to any sensible constructive setting. That being said, we believe that a number of features of the univalent setting have resulted in a much more natural and efficient formalization than would have otherwise been possible (not to mention that this setting is semantically well-understood). E.g. using the second author's *set quotients* we are able to make direct use of the usual universal property of quotients in our constructions. Similarly, by situating our constructions within the filtration of homotopy types by *h-levels* we avoid complications involving identity types which might otherwise arise.

We will only briefly touch upon the technical details of homotopy type theory and the univalence axiom, and we refer the reader to Awodey (2010) for a basic introduction to homotopy type theory. For univalent foundations and the second author's Coq library (Voevodsky 2011, 2014) we refer readers to Pelayo and Warren (2014), where a description of the research program, its motivations, and its implementation in Coq, are given. Because it is assumed that the reader is already familiar with Coq and with the second author's program, this paper has been written in a style which we foresee future papers in formalization taking: it is a summary of the Coq code written in ordinary mathematical English. The details are of course in the Coq code, but the overall structure of the formalization (as well as the key steps of the proofs) should be apparent from the sketch given here. The actual Coq code associated to this paper can be found on the websites of

the authors, as supplementary files to the arXiv posting of this paper, and on the journal website associated to this issue.

1.3. *Structure of paper*

Hensel (1900) invented the p-adic numbers $\mathbb{Q}_p$ about one hundred years ago. The p-adic numbers and the reals are the canonical metric completions of the rationals. Classically, there are a number of ways to construct the p-adic numbers, and we refer the reader to Gouvêa (1993), Koblitz (1984) and Schikhof (1984) for further details regarding the classical theory. The construction of the p-adic numbers given in this paper is constructive and uses algebraic, rather than analytic, techniques. Namely, we first construct the integral domain of p-adic integers $\mathbb{Z}_p$ as a quotient of the ring $\mathbb{Z}[[X]]$ of formal power series over $\mathbb{Z}$. We were unable to find the specific construction of $\mathbb{Z}_p$ we employ in the literature, but we believe that it is known. We then take the p-adic numbers $\mathbb{Q}_p$ to be the field of fractions of $\mathbb{Z}_p$. Because we are working constructively, and because $\mathbb{Z}[[X]]$ does not have decidable equality, it is necessary to work with an apartness relation and with the corresponding notions of integral domains and fields. We will refer to the apartness versions of fields as *Heyting fields* following the standard usage in constructive mathematics.

In detail, this paper is organized as follows. In Section 2, we give a brief overview of the univalent setting. In Section 3, we review some basic constructive algebra. Section 4 contains our construction of formal power series and the proofs of several results on formal power series. The proof that it is possible to form the Heyting field of fractions for an integral domain is given in Section 5. The construction of the p-adic numbers appears in Section 6. Section 7 is a brief epilogue containing a sketch of some future plans concerning p-adic integrable systems. Finally, a more detailed summary of the Coq code, and a sample of the Coq code of one of the proofs, can be found in the Appendix A.

We should note that the p-adic numbers are also relevant in the physics literature, see Brekke and Freund (1993) and the references therein. In fact, one of our main motivations in wanting to develop a p-adic theory of integrable systems is to study inverse spectral problems concerning p-adic analogues of real quantum integrable systems. We refer to Section 7.2 for a list of short term plans concerning the p-adic numbers.

2. Univalent basics

The second author's Coq library spans a large portion of mathematics and we make free use of this library. However, for the sake of clarity we will mention here those specific parts of the library which we use in the construction of the p-adic numbers. A survey of the development of univalent mathematics in Coq can be found in Pelayo and Warren (2014).

2.1. *Notation and conventions*

In this paper, and in the Coq files, all rings are assumed to be commutative and with 1.

$\mathbb{N}$ denotes the type of natural numbers which is defined as an inductive type in the standard way. In the Coq code $\mathbb{N}$ is denoted by `nat`. Similarly, $\mathbb{Z}$ denotes the type of integers which is constructed as the group completion of the abelian monoid of natural numbers. In the Coq code $\mathbb{Z}$ is denoted by `hz`. This type is constructed as the completion of the commutative rig of natural numbers to a commutative ring. It therefore automatically possesses the appropriate algebra structure and universal property.†

$\mathcal{U}$ denotes a fixed universe of types. In the Coq code this is denoted by `UU`. The identity type $\mathtt{Id}_A(a,b)$ is denoted by $a \rightsquigarrow b$. In the Coq files this is denoted by either `paths a b` or by $a \sim> b$.

We write $\prod_{x:A} .B(x)$ for dependent products and $\sum_{x:A} .B(x)$ for dependent sums (defined here as the record type `total2`).

We will generally use the same naming conventions as used in the Coq files, but in some cases we will introduce abbreviations, such as $\sum_{i=0}^{n} f(i)$ for summation, when it will improve the readability.

Because the current implementation of the underlying type system of Coq does not handle universes (and several related matters) in a way which is completely suited for the univalent development of mathematics, it is necessary to apply several patches to the Coq system in order to compile the second author's Coq library as well as the files described in this paper. Instructions on how to compile a patched version of Coq can be found in the second author's library.

2.2. *Basic homotopy theoretic notions in Coq*

We think of $\mathcal{U}$ as the universe of small homotopy types (or fibrant and cofibrant spaces). For $B : \mathcal{U}$, we represent a dependent type over B as a term $E : B \to \mathcal{U}$. From the perspective of homotopy theory this corresponds to a fibration over B and, for $b : B$, $E(b)$ corresponds to the fiber over b. The dependent product $\prod_{x:B} E(x)$ is regarded as the space of sections of the fibration represented by E. Similarly, the dependent sum, $\sum_{x:B} E(x)$ corresponds to the total space of the fibration. We think of the identity type $a \rightsquigarrow b$ as denoting the fiber of the path space over (a,b). We will use the phrases 'path space' and 'type of paths' interchangeably for this type. I.e. a term $f : a \rightsquigarrow b$ corresponds to a path from a to b.

Given a path $f : b \rightsquigarrow b'$ in B and a point $e : E(b)$ in the fiber over b we obtain a corresponding point $f_!(e) : E(b')$ in the fiber over b'. In the Coq code $f_!$ is denoted by `transportf E f e`. In order to construct a path $x \rightsquigarrow y$ in the total space $\sum_{x:B} E(x)$ it suffices to construct a path $f : \pi_1(x) \rightsquigarrow \pi_1(y)$ and a path $g : f_!(\pi_2(x)) \rightsquigarrow \pi_2(y)$.

Given a term $g : B \to A$ and a path $f : b \rightsquigarrow b'$ in B, we obtain a path $g(f) : g(b) \rightsquigarrow g(b')$. In the Coq code $g(f)$ is denoted by `maponpaths g f`. This corresponds, regarding a homotopy type as an ∞-groupoid, to the weakly functorial action of g on the path f.

† This is one of the reasons we use this implementation of the integers instead of the built-in Coq integers.

Definition 2.1 (`hfiber`). Given types A and B, $g : B \to A$ and $a : A$, the **homotopy fiber of** g **over** a is the type

$$\mathbf{hfiber}\ g\ a := \sum_{x:B} \big(g(x) \rightsquigarrow a\big).$$

Definition 2.2 (`iscontr`). We define the type $\mathbf{iscontr}(A)$ of proofs that A is contractible as

$$\mathbf{iscontr}(A) := \sum_{c:A} \prod_{x:A} \big(x \rightsquigarrow c\big).$$

We say that A is **contractible** if $\mathbf{iscontr}(A)$ is inhabited.

We will see below that contractibility in this setting plays the same role as canonical existence in the classical development of mathematics.

Definition 2.3 (`isweq` and `weq`). Given $g : B \to A$ we define the type $\mathbf{isweq}(g)$ of proofs that g is a weak equivalence as

$$\mathbf{isweq}(g) := \prod_{x:A} \mathbf{iscontr}(\mathbf{hfiber}\ g\ x).$$

If $\mathbf{isweq}(g)$ is inhabited, then we say that g is a **weak equivalence**.

There is a filtration of types into different 'h-levels'. Homotopy theoretically this is a slight extension of the usual filtration by homotopy n-types. We will only require the first few h-levels in this paper.

Definition 2.4 (`isofhlevel`, `isaprop`, `hprop`, `isaset` and `hset`). A type A is of **h-level**:[†]

— 0 if A is contractible;
— $(n+1)$ if, for all $a, b : A$, the type $(a \rightsquigarrow b)$ is of h-level n.

We denote by $\iota_n(A)$ the type of proofs that A is of h-level n. We abbreviate $\iota_1(A)$ by $\mathbf{isaProp}(A)$ and $\iota_2(A)$ by $\mathbf{isaSet}(A)$. We write **hProp** for the type of (small) types of h-level 1 and **hSet** for the type of (small) types of h-level 2.

Intuitively, **hProp** consists of those spaces which are homotopy equivalent to either the empty space 0 or to the one element space 1. Accordingly, **hProp** plays the role played by the Booleans in classical logic or by the subobject classifier in topos logic. Types in **hProp** satisfy proof-irrelevance (`proofirrelevance`) and, indeed (`invproofirrelevance`), being an h-prop is equivalent to being proof-irrelevant. For a type A, $\mathbf{hRel}(A)$ is the type of relations on A. I.e., it is the type $A \to A \to \mathbf{hProp}$.

Intuitively, **hSet** consists of those spaces which are homotopy equivalent to discrete spaces. I.e., these are the sets. Most of the types which we will be dealing with are either h-props or h-sets. We will sometimes refer to h-sets simply as 'sets' when no confusion will result.

We make use of a number of basic properties of h-levels. E.g.

[†] Note that in order to define `isofhlevel` as a type which has values in $\mathcal{U}$, as is done in the file `uu0.v` from the second author's Coq library, it is necessary to compile Coq with a patch.

1. `impred`: for $n : \mathbb{N}$, $B : \mathcal{U}$ and $E : B \to \mathcal{U}$, the type

$$\prod_{x:B} \mathbf{isofhlevel}_n(E(x)) \to \mathbf{isofhlevel}_n \left(\prod_{x:B} E(x) \right)$$

   is inhabited.
2. `impredfun`: for $n : \mathbb{N}$, $A, B : \mathcal{U}$, if A is of h-level n, then so is $(B \to A)$.
3. `isofhleveldirprod`: If A is of h-level n and B is of h-level n, then so is $A \times B$.

2.3. *Function extensionality*

We make extensive use of the principle of function extensionality (`funextfun`), which follows from the second author's *Univalence Axiom.*

Definition 2.5 (`funextfun`). The principle of **function extensionality** states that, for any two functions $f, g : A \to B$, the type

$$\left(\prod_{x:A} f(x) \rightsquigarrow g(x) \right) \to (f \rightsquigarrow g)$$

is inhabited.

2.4. *Properties of* **hProp**

Given a type $A : \mathcal{U}$, there is a universal way to turn A into a h-prop. This is the 'inhabited' construction:

Definition 2.6 (`ishinh_UU`). We say that $A : \mathcal{U}$ is **h-inhabited** if the type

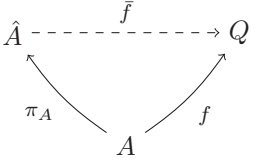
$$\hat{A} := \prod_{P : \mathbf{hProp}} ((A \to P) \to P)$$

is inhabited.

It is immediate, using the facts about h-levels sketched above to see that $\hat{A}$ is an h-prop. Moreover, there is a projection $\pi_A : A \to \hat{A}$ given by

$$\pi_A := \lambda_{x:A}.\lambda_{P:\mathbf{hProp}}.\lambda_{f:A\to P}.f(x).$$

The map π_A is the universal map from A into a h-prop. To see this, observe that if Q is any h-prop and $f : A \to Q$, then we have a commutative (up to definitional equality) diagram



where

$$\bar{f} := \lambda_{t:\hat{A}}.t(Q)(f).$$

Moreover, since Q is a h-prop it follows (using function extensionality) that the space of such extensions $\bar{f}$ is contractible.

Using the h-inhabited construction it is possible to endow **hProp** with the structure of a Heyting algebra. This structure is summarized below:

Definition 2.7 (`htrue`,`hfalse`,`hconj`,`hdisj`,`hneg`,`himpl`). For $P, Q : \mathbf{hProp}$ and $X, Y : \mathcal{U}$ we define logical operations on **hProp** as follows:

— 1 and 0 are h-props.
— $P \wedge Q := P \times Q$.
— $X \vee Y := \widehat{X + Y}$.
— $\neg X := X \to 0$.
— $X \implies P := X \to P$.

In addition to the Heyting algebra operations, there is an existential quantifier (`hexists`) which is defined by

$$\exists_{x:X} P(x) := \widehat{\sum_{x:X} P(x)}$$

for any $P : X \to \mathcal{U}$ and $X : \mathcal{U}$. This quantifier satisfies the usual properties of the existential quantifier in intuitionistic logic. Note that our $\exists$ does *not* correspond to the built-in existential quantifier '`exists`' in Coq.

The proof that, with the operations above, **hProp** is a Heyting algebra makes use of the *Propositional Univalence Axiom* (`uahp`) which says that every logical equivalence between h-props induces a path between them. I.e. it says that the type

$$\prod_{P,Q:\mathbf{hProp}} (P \to Q) \to \big((Q \to P) \to (P \rightsquigarrow Q)\big).$$

is inhabited.

2.5. *Set quotients of types*

The second author has given several constructions of quotients of types. A **hsubtype** of a type A is given by a map $S : A \to \mathbf{hProp}$. Denote by $\mathcal{P}(A)$ the type of hsubtypes of A. Given a relation R on A (that is, $R : A \to A \to \mathbf{hProp}$), an **equivalence class** consists of a subtype S of A together with the following data:

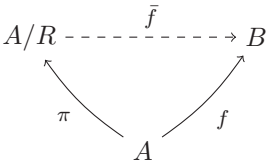
1. a term of type $\widehat{\sum_{x:A} S(x)}$.
2. a term of type $\prod_{x,y:A}(xRy \to S(x) \to S(y))$.
3. a term of type $\prod_{x,y:A}(S(x) \to S(y) \to xRy)$.

Given a subtype S, we denote by $\mathbf{iseqclass}_R(S)$ the type consisting of such data. The **set quotient** A/R (`setquot`) of a type A by a relation R is then defined by

$$A/R := \sum_{S:\mathcal{P}(A)} \mathbf{iseqclass}_R(S).$$

It is shown (`isasetsetquot`) in the second author's library that A/R is a set and that, when R is an equivalence relation, this set has the usual universal property. In particular,

there is a function $\pi : A \to A/R$ (`setquotpr`) which is compatible with the equivalence relation and, for any set B and function $f : A \to B$ which is compatible with R, there exists an extension $\bar{f}$ making the diagram



commute. We will make free use throughout of the results on set quotients from the second author's library.

3. Basics on constructive algebra

We will here briefly recall some basics of constructive algebra. For a more detailed treatment we refer to Bridges and Richman (1987) and Mines *et al.* (1988).

The usual definitions of fields and integral domains are not entirely satisfactory from the perspective of constructive algebra since they deal with negative properties (the property of being a non-zero element of the field). From the constructive perspective, it is more appropriate to replace the notion of an element x being non-zero ($x \neq 0$) with x being **apart from zero**, written $x \# 0$.

We will now recall the basics regarding apartness relations.

Definition 3.1. (`isapart`) A relation $R : \mathbf{hRel}(X)$ is an **apartness relation** provided that it satisfies the following conditions:

Irreflexive for all $x : X$, $\neg(xRx)$.
Symmetric for all $x, y : X$, xRy implies yRx.
Cotransitive for all $x, y : X$, if xRy, then either xRz or zRy, for any $z : X$.

Classically, the negation of the equality $x \neq y$ relation is an apartness relation. However, negation of equality is not the only classical apartness relation. For example, if X is a topological space, then the relation R given by xRy if and only if x and y are in different connected components is an apartness relation. (This example can be generalized to give a limitless number of classical examples of apartness relations.)

For $X : \mathbf{hSet}$, we denote by $\mathbf{Apart}(X)$ the type of apartness relations on X. We generally denote apartness relations by $x \# y$. When a type has decidable equality the negation of equality is an apartness relation:

Lemma 3.2 (`deceqtoneqapart`). If $X : \mathbf{hSet}$ has decidable equality, then negation of equality

$$\neg(x \rightsquigarrow y)$$

is an apartness relation on X.

Definition 3.3 (`isapartdec`). Given X : **hSet** and R : **Apart**(X), we say that R is a **decidable apartness relation on** X if the type

$$(aRb) + (a \rightsquigarrow b)$$

is inhabited.

It is immediate (`isapartdectodeceq`) that if R is a decidable apartness relation on X, then X has decidable equality.

When we are considering algebraic structures equipped with apartness relations we will require that the relation is compatible with the operations under consideration. In particular, for rings we have the following.

Definition 3.4 (`acommrng`). The type **aCRng** consists of commutative rings A together with an apartness relation $x \# y$ on A which is compatible with the ring structure of A in the sense that[†]

— For all $a, b, c : A$, if $(c + a) \# (c + b)$, then $a \# b$.
— For all $a, b, c : A$, if $(c \cdot a) \# (c \cdot b)$, then $a \# b$.

When a commutative ring A has decidable equality it is straightforward to verify that negation of equality is compatible with the ring operations in the sense of Definition 3.4.

Definition 3.5 (`aintdom`). The type **aDom** consists of A : **aCRng** such that

— $1 \# 0$.
— For all $a, b : A$, if $a \# 0$ and $b \# 0$, then $(a \cdot b) \# 0$.

We refer to the terms of type **aDom** as **apartness domains**.

Heyting fields are the appropriate generalization of fields to the constructive setting when one considers algebraic structures with apartness relations.

Definition 3.6 (`afld`). The type **aFld** of **Heyting fields** consists of A : **aCRng** such that

— $1 \# 0$.
— For all $a : A$, if $a \# 0$, then a has a multiplicative inverse (the type of multiplicative inverses of a is inhabited).

We have the following immediate observation:

Lemma 3.7 (`afldtoaintdom`). If A is a Heyting field, then A is an apartness domain.

Proof. It is immediate to prove that, in a Heyting field, if a has a multiplicative inverse, then it is apart from 0 (`afldinvertibletoazero`). It follows that $1 \# 0$. One can show that if a and b both possess multiplicative inverses, then so does their product $a \cdot b$ (`multinvmultstable`). It is then immediate that $(a \cdot b) \# 0$ when $a \# 0$ and $b \# 0$. □

[†] Note that in the Coq files we actually require the corresponding cancellation properties also on the right. This is redundant for commutative rings, but for general rings one requires also these further properties.

4. Formal power series

Our treatment of formal power series makes use of function extensionality, since formal power series $R[[X]]$ over a commutative ring R are here defined as terms of type $\mathbb{N} \to R$ with the operations of addition and multiplication given in the usual way. The main result of this section is that, with these operations, formal power series is a commutative ring. Moreover, there is a natural apartness relation on formal power series and, furthermore, when the ring R has decidable equality the ring of formal power series over R forms an apartness domain. We will now fill in the details of this sketch.

4.1. *Summation in a ring*

We define both a restrictive summation operation (`natsummation0`), which allows us to form the sum $\sum_{i=0}^{n} a_i$ of a sequence $a : \mathbb{N} \to R$, and a more general operation (`summation`), which allows us to form the sum $\sum_{i=m}^{n} a_i$ of a sequence $a : \mathbb{Z} \to R$. However, we will only really require the former of these two constructions and so we will omit details related to the more general summation. In order to avoid confusion with our notation for dependent sums, we write $\bigoplus_{i=0}^{n} a_i$ for the sum $\sum_{i=0}^{n} a_i$. Summation is, of course, defined inductively by setting

$$\bigoplus_{i=0}^{0} a_i := a_0 \quad \text{and} \quad \bigoplus_{i=0}^{n+1} a_i := \left(\bigoplus_{i=0}^{n} a_i\right) + a_{n+1}.$$

4.1.1. *Manipulation of sums.* It is important to note that when we manipulate sums, to obtain new sums, what is relevant is that there is a path between them, and not whether they are equal in the strict sense. This is justified because the structures we are considering are themselves sets. The following lemma includes several basic facts regarding the behaviour of summation of which we will make frequent use:

Lemma 4.1. Given a natural number n and sequences $a, b : \mathbb{N} \to R$, we have the following:

1. (`natsummationpathsupperfixed`) Given $p : \prod_{x:\mathbb{N}}(x \leqslant n) \to (a_x \rightsquigarrow b_x)$, the type
$$\bigoplus_{i=0}^{n} a_i \rightsquigarrow \bigoplus_{i=0}^{n} b_i$$
is inhabited.
2. (`natsummationshift0`) The type
$$\bigoplus_{i=0}^{n+1} a_i \rightsquigarrow \left(\bigoplus_{i=0}^{n} a_{i+1}\right) + a_0$$
is inhabited.

In order to more easily handle reindexing of sums we introduce, for $f : \mathbb{N} \to \mathbb{N}$, the type $\mathbf{Aut}_n(f)$ (`isnattruncauto`) of proofs that f is an automorphism of the interval $[0, n]$ of

natural numbers. Explicitly, $\mathbf{Aut}_n(f)$ is defined to be the following type:[†]

$$\left(\prod_{x\leqslant n}\sum_{y\leqslant n}\left((f(y)\rightsquigarrow x)\times\prod_{z\leqslant n}(f(z)\rightsquigarrow x)\to(y\rightsquigarrow z)\right)\right)\times\left(\prod_{x\leqslant n}(f(x)\leqslant n)\right),$$

where we have abbreviated $\prod_{x:\mathbb{N}}(x\leqslant n)\to\cdots$ as $\prod_{x\leqslant n}\cdots$ and $\sum_{x:\mathbb{N}}(x\leqslant n)\times\cdots$ as $\sum_{x\leqslant n}\cdots$. It is possible to reindex sums along such automorphisms, as shown by the following lemma:

Lemma 4.2. (`natsummationreindexing`) Given a natural number n and a map $f:\mathbb{N}\to\mathbb{N}$ such that $\mathbf{Aut}_n(f)$ is inhabited, the type

$$\bigoplus_{i=0}^{n}a_i\rightsquigarrow\bigoplus_{i=0}^{n}a_{f(i)}$$

for any sequence $a:\mathbb{N}\to R$, is inhabited.

The final fact regarding summation which we require is the following:

Lemma 4.3. (`natsummationswap`) Given $f:\mathbb{N}\to\mathbb{N}\to R$ and a natural number n, the type

$$\bigoplus_{k=0}^{n}\bigoplus_{l=0}^{k}f(l,k-l)\rightsquigarrow\bigoplus_{k=0}^{n}\bigoplus_{l=0}^{n-k}f(k,l)$$

is inhabited.

4.2. *The ring of formal power series*

We define, for a type A, the type of sequences of elements of A (`seqson`) as the function space $\mathbb{N}\to A$. When A is a set so is $\mathbb{N}\to A$ and for A a commutative ring we take $\mathbb{N}\to A$ as the underlying set (`fps`) of the ring of formal power series over A. If a is a sequence on A, then we write $a_n:A$ for the result of evaluating the sequence at the natural number n. Such a sequence $a:\mathbb{N}\to R$ represents the formal power series

$$\sum_{i=0}^{\infty}a_iX^i$$

in a single indeterminate X. In this notation, the indeterminate X on its own denotes the sequence $X:\mathbb{N}\to R$ with $X_i=1$ when $i=1$ and $X_i=0$ otherwise.

[†] Note that we could, alternatively, have used the type $(\prod_{x\leqslant n}\sum_{y\leqslant n}(f(y)\rightsquigarrow x))\times(\prod_{x\leqslant n}(f(x)\leqslant n))$. However, the more verbose type we give here is convenient, for purposes of formalization, as it allows for more direct proofs of subsequent lemmas.

4.2.1. *Ring operations on formal power series.* For a given commutative ring R, addition and multiplication of formal power series are defined as usual by the formulae:

$$(a+b)_n := a_n + b_n$$
$$(a \cdot b)_n := \bigoplus_{k=0}^{n} a_k b_{n-k}.$$

The zero sequence 0 is given by $0_n := 0$ for all natural numbers n and the sequence 1 is given by $1_0 := 1$ and $1_{n+1} := 0$ for all natural numbers n.

Proposition 4.4 (`fpscommrng`). Let $(R, +, \cdot)$ be a commutative ring. Then the set of sequences on R with the operations given above is a commutative ring.

Proof. The proof follows from the facts about summation described above. For example, to prove associativity of multiplication, we must show that, for all natural numbers n,

$$\bigoplus_{i=0}^{n} \left(\bigoplus_{k=0}^{i} a_k \cdot b_{i-k} \right) \cdot c_{n-i} \rightsquigarrow \bigoplus_{j=0}^{n} a_j \cdot \left(\bigoplus_{l=0}^{n-j} b_l \cdot c_{(n-j)-l} \right).$$

For this, we reason as follows

$$\bigoplus_{j=0}^{n} \bigoplus_{l=0}^{n-j} a_j \cdot (b_l \cdot c_{(n-j)-l}) \rightsquigarrow \bigoplus_{l=0}^{n} \bigoplus_{j=0}^{l} (a_l \cdot b_{k-l}) \cdot c_{n-l-(k-l)} \rightsquigarrow \bigoplus_{l=0}^{n} \bigoplus_{j=0}^{l} a_l \cdot (b_{k-l} \cdot c_{n-k}),$$

where the first path is given by Lemma 4.3 and associativity of multiplication in R. In the Coq proof this line of reasoning is put together with generous use of Lemma 4.1, (`funextfun`), several minor lemmas such as (`natsummationtimesdistl`), and associativity of R itself. □

4.3. *The apartness relation on formal power series*

Although it is not used in the construction of the p-adic numbers, we mention here some results contained in the Coq files regarding apartness relations on formal power series.

Assume that R is a commutative ring with an apartness relation. Then there is an induced apartness relation on formal power series given by setting (`fpsapart`)

$$a \# b \quad \text{if and only if} \quad \exists_{n:\mathbb{N}}. a_n \# b_n \tag{1}$$

for $a, b : R[[X]]$. This apartness relation is compatible with the ring operations and so we see that $R[[X]] : \mathbf{aCRng}$ (`acommrngfps`).

For R an apartness domain, provided that the apartness relation on R is decidable in the sense of Definition 3.3, it is possible to show that $R[[X]]$ is an apartness domain.

Proposition 4.5 (`apartdectoisaintdomfps`). For $R : \mathbf{aDom}$ with decidable apartness, the commutative ring $R[[X]]$ of formal power series is an apartness domain when equipped with the apartness relation (1).

The proof of Proposition 4.5 is a consequence of the following lemma:

Lemma 4.6 (`leadingcoefficientapartdec`**).** For R : **aDom** and $a : R[[X]]$, if $a_0 \# 0$, then for any $n : \mathbb{N}$ and $b : R[[X]]$, if $b_n \# 0$, then $(a \cdot b) \# 0$.

Proof. The proof is by induction on n and is obvious in the base case. The induction case splits into two subcases depending on whether $b_0 \# 0$ or $b_0 \rightsquigarrow 0$. In the former case, $(a \cdot b)_0 \# 0$, whereas in the latter case the claim follows by applying the induction hypothesis to the sequence $b' : R[[X]]$ given by $b'_n := b_{n+1}$. □

5. The Heyting field of fractions

The construction of the Heyting field of fractions from an apartness domain is a classical result in constructive algebra due to Heyting and we therefore give only a brief sketch of the details here.

Definition 5.1 (`aintdomazerosubmonoid`**).** Given A : **aDom**, we denote by $\tilde{A}$ the submonoid of A (with respect to the multiplicative structure of A) consisting of those $a : A$ such that $a \# 0$.

It follows (`commrngfrac`) that there exists a commutative ring $A[\tilde{A}^{-1}]$ obtained by localizing with respect to $\tilde{A}$. It remains to show that there exists an apartness relation on $A[\tilde{A}^{-1}]$ which makes it into a Heyting field.

Definition 5.2 (`afldfracapartrel0`**).** For elements $a, c : A \times \tilde{A}$ we define

$$a \# c \quad \text{if and only if} \quad \big((\pi_1 a) \cdot (\pi_2 c)\big) \# \big((\pi_1 c) \cdot (\pi_2 a)\big).$$

This relation extends to a relation (`afldfracapartrel`) on $A[\tilde{A}^{-1}]$ and it is straightforward to show that it is an apartness relation (`afldfracapart`) which is compatible with the ring structure of $A[\tilde{A}^{-1}]$ (`afldfrac0`). For instance (`iscotransafldfracapartrelpre`), to see that it is cotransitive suppose given $(a, a') \# (c, c')$ and some (b, b'). Then, by the fact that A is an apartness domain, we see that $a \cdot c' \cdot b' \# c \cdot a' \cdot b'$. Therefore, by cotransitivity of the apartness relation of A, we have that either $a \cdot c' \cdot b' \# b \cdot a' \cdot c'$ or $b \cdot a' \cdot c' \# c \cdot a' \cdot b'$. In the former case it follows that $a \cdot b' \# b \cdot a'$. I.e. $(a, a') \# (b, b')$. In the latter case it similarly follows that $(b, b') \# (c, c')$.

Given $a \in A \times \tilde{A}$ such that $a \# 0$, we have $\pi_1(a) \# 0$ and therefore, we take a^{-1} to be given by the pair $(\pi_2(a), \pi_1(a))$. This definition extends to a definition of the inverse of an element apart from 0 in $A[\tilde{A}^{-1}]$ and it is straightforward to show that this makes $A[\tilde{A}^{-1}]$ a Heyting field.

Theorema 5.3 (`afldfracisafld`**).** For A : **aDom**, with the definitions given above, $A[\tilde{A}^{-1}]$ forms a Heyting field.

We refer to the Heyting field from Theorem 5.3 as the **Heyting field of fractions of** A and we write **Frac**(A) for it.

6. The p-adic numbers

The p-adic numbers were invented about one hundred years ago by German mathematician K. Hensel.

6.1. *Basic number theory*

The following definition is the relation of integer divisibility, and is given as a two part definition in the Coq file. The first part says that, given three integers n, m, k, if the product of n and k is m, then n divides m. The general definition starts only with n and m, and appeals to the existence of k.

Definition 6.1 (`hzdiv0` and `hzdiv`). Let n and m be integers. We write $n|m$ for the type

$$n|m := \exists_{k:\mathbb{Z}}.(m \rightsquigarrow n \cdot k)$$

and we say that n **divides** m when $n|m$ is inhabited.

The division algorithm is then shown to hold via a series of steps. First, we prove the division algorithm for natural numbers. Recall that `pr1` and `pr2` are defined as projections (π_1 and π_2) onto the base and 'specialization' to a fiber:

Lemma 6.2 (`divalgorithmnonneg`). For n and m of type `nat`, with m non-zero, there exists a term $qr : (\mathbb{Z} \times \mathbb{Z})$ such that there is a term of type

$$n \rightsquigarrow \big(m \cdot \pi_1(qr)\big) + \pi_2(qr)$$

and there are proofs that $0 \leqslant \pi_2(qr) < m$.

The proof of Lemma 6.2 is by induction on n with, in the successor step, a case analysis on whether $(r' + 1) < m$ or $r' \rightsquigarrow m$ (that such a case analysis is possible follows from decidability of equality using `hzlehchoice` from the second author's library). The proof of the general division algorithm is then done by a detailed case analysis (on whether n and m are negative, non-negative or propositionally equal to 0):

Theorema 6.3 (`divalgorithmexists`). For n and m of type $\mathbb{Z}$ with m non-zero, the space of terms $qr : \mathbb{Z} \times \mathbb{Z}$ such that the types $n \rightsquigarrow (m \cdot \pi_1(qr)) + \pi_2(qr)$ and $0 \leqslant \pi_2(qr) < |m|$ are inhabited is contractible.

Here, as throughout, *contractibility* corresponds to *unique existence* in the traditional setting. One consequence of the division algorithm is that we obtain the operations of taking the quotient and remainder of an integer modulo a non-zero integer (`hzquotientmod` and `hzremaindermod`). These two operations will play a role in a number of calculations in the sequel.

In addition to the division algorithm we also obtain the familiar Euclidean algorithm (again stated in terms of contractibility of an appropriate space):

Theorema 6.4 (`euclideanalgorithm`). Let n and m be integers with n non-zero. Then the space $\mathtt{hzgcd}(n, m)$ of greatest common divisors of n and m is contractible.

We also obtain a form of the Bézout lemma:

Lemma 6.5 (`bezoutstrong`). For all $m, n : \mathbb{Z}$ such that n is non-zero, the type of $ab : \mathbb{Z} \times \mathbb{Z}$ for which there exists a term of type $\gcd(n, m) \rightsquigarrow \pi_1(ab) \cdot n + \pi_2(ab) \cdot m$ is inhabited.

Given $p : \mathbb{Z}$, the type of proofs that p is a prime is defined by setting

$$\texttt{isaprime}(p) :\equiv (1 < p) \times \big((m|p) \to (m \rightsquigarrow 1) \vee (m \rightsquigarrow p)\big).$$

As a consequence of Lemma 6.5 we obtain:

Theorema 6.6 (`acommrng_hzmod` and `ahzmod`). For non-zero p of type $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with compatible apartness relation. When p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a Heyting field.

Note that the apartness relation on $\mathbb{Z}/p\mathbb{Z}$ is the one induced by the fact that equality of $\mathbb{Z}/p\mathbb{Z}$ is decidable (`isdeceqhzmodp`).

6.2. *The construction of* $\mathbb{Q}_p$

Throughout this section we assume given a prime p. Explicitly, we require the proof witnessing the fact that p is a prime. We note though that for some of the results stated here it is only necessary that p be non-zero. We also introduce some notation for quotients and remainders modulo p. We denote by $\{a\}$ the quotient of a modulo p (`hzquotientmod`) and by $[a]$ the remainder of a modulo p.

We will now summarize our construction of the apartness domain $\mathbb{Z}_p$ of p-adic integers.

Definition 6.7 (`precarry`). Given a formal power series a over $\mathbb{Z}$, we define a new formal power series $\mathbf{p}(a)$ over $\mathbb{Z}$ inductively by

$$\begin{aligned} \mathbf{p}(a)_0 &:\equiv a_0 \\ \mathbf{p}(a)_{n+1} &:\equiv a_{n+1} + \{\mathbf{p}(a)_n\}. \end{aligned}$$

Definition 6.8 (`carry`). Given a formal power series a over $\mathbb{Z}$, we define a new formal power series $a^\natural$ over $\mathbb{Z}$ by

$$(a^\natural)_n :\equiv \big[\mathbf{p}(a)_n\big].$$

We call $a^\natural$ the **carried power series of** a.

Example 6.9. For $p = 3$, the formal power series $a = (4, 1, 8, 0, \ldots)$ is sent to $\mathbf{p}(a) = (4, 2, 8, 2, 0, \ldots)$ and to $a^\natural = (1, 2, 2, 2, 0, \ldots)$.

The operation of carrying (mod p) for power series induces an equivalence relation $\sim$ (`carryequiv`) on $\mathbb{Z}[[X]]$ by setting

$$a \sim b \quad \text{if and only if} \quad a^\natural \rightsquigarrow b^\natural.$$

Observe that $X - p \sim 0$. Furthermore, for any $a \in \mathbb{Z}[[X]]$, if $a \sim 0$, then there exist integers λ_i such that $a_0 = -\lambda_0 p$ and $a_{n+1} = -\lambda_{n+1} p + \lambda_n$. Using these facts it follows that $\sim$ is the equivalence relation corresponding to the ideal $(X - p)$ in $\mathbb{Z}[[X]]$. Ultimately,

once the theory of ideals has been developed in the univalent foundations library, $\mathbb{Z}_p$ will be constructed as the quotient of $\mathbb{Z}[[X]]$ by this ideal. However, because quotients of rings are given in the second author's library in terms of congruences, we here describe $\mathbb{Z}_p$ using the corresponding congruence $\sim$.

We will now describe the proof that this relation is a congruence with respect to the ring operations on $\mathbb{Z}[[X]]$.

Lemma 6.10 (`quotientprecarryplus`**).** For formal power series a and b over $\mathbb{Z}$,

$$\{\mathbf{p}(a+b)_n\} \rightsquigarrow \{\mathbf{p}(a)_n\} + \{\mathbf{p}(b)_n\} + \{\mathbf{p}(a^\natural + b^\natural)_n\}$$

for $n : \mathbb{N}$.

Proof. The proof is by induction on n. In the base case it is trivial and in the induction case it is by the following calculation:

$$\begin{aligned}\{\mathbf{p}(a+b)_{n+1}\} &\rightsquigarrow \{\mathbf{p}(a)_{n+1} + \mathbf{p}(b)_{n+1} + \{\mathbf{p}(a^\natural + b^\natural)_n\}\}\\ &\rightsquigarrow \{\mathbf{p}(a)_{n+1}\} + \{\mathbf{p}(b)_{n+1}\} + \{\mathbf{p}(a^\natural + b^\natural)_n\} + \{a^\natural_{n+1} + b^\natural_{n+1} + [\mathbf{p}(a^\natural + b^\natural)_n]\}\\ &\rightsquigarrow \{\mathbf{p}(a)_{n+1}\} + \{\mathbf{p}(b)_{n+1}\} + \{\mathbf{p}(a^\natural + b^\natural)_{n+1}\}\end{aligned}$$

where the first path is by definition of precarry and the induction hypothesis, the second path is by the familiar decomposition of the quotient of a sum, and the final path is by definition and the fact that the quotient of a remainder is zero. □

The following observation is a consequence of Lemma 6.10.

Lemma 6.11 (`carryandplus`**).** For a and b formal power series over $\mathbb{Z}$, $(a+b)^\natural \rightsquigarrow (a^\natural + b^\natural)^\natural$.

Similarly, a straightforward induction gives us the following lemma:

Lemma 6.12 (`precarryandtimesl`**).** Given formal power series a and b over $\mathbb{Z}$,

$$\{\mathbf{p}(a \cdot b)_n\} \rightsquigarrow (\{\mathbf{p}(a)\} \cdot b)_n + \{\mathbf{p}(a^\natural \cdot b)_n\}$$

for $n : \mathbb{N}$.

The proof that carrying is compatible with multiplication of power series is then an immediate consequence of Lemma 6.12.

Lemma 6.13 (`carryandtimes`**).** Given formal power series a and b over $\mathbb{Z}$, $(a \cdot b)^\natural \rightsquigarrow (a^\natural \cdot b^\natural)^\natural$.

It follows from Lemmas 6.11 and 6.13 that the quotient of $\mathbb{Z}[[X]]$ by the equivalence relation $\sim$ is itself a commutative ring (`commrngofpadicints`). Indeed, it is the commutative ring $\mathbb{Z}_p$ of **p-adic integers**. Moreover, there is an apartness relation (`padicapart`) on p-adic integers obtained as the extension of the relation (`padicapart0`)

$$a \# b \quad \text{if and only if} \quad \exists_{n:\mathbb{N}}.\neg(a^\natural_n \rightsquigarrow b^\natural_n), \tag{2}$$

for $a, b : \mathbb{Z}[[X]]$, to the p-adic integers. This apartness relation is straightforwardly seen to be compatible with the ring structure of $\mathbb{Z}_p$ (`acommrngofpadicints`).

Theorema 6.14 (`padicintsareintdom`,`padicintegers`)**.** The commutative ring $\mathbb{Z}_p$ with the apartness relation described above forms an apartness domain.

Proof. It suffices to prove that for $a, b : \mathbb{Z}[[X]]$ such that $a \# 0$ and $b \# 0$ it follows that $a \cdot b \# 0$, where we are considering only the apartness relation (2). Since $\mathbb{Z}$ has decidable equality, it follows (`leastelementprinciple`) that there are natural numbers k and m which are the least natural numbers such that $\neg(a_k^\natural \rightsquigarrow 0)$ and $\neg(b_m^\natural \rightsquigarrow 0)$, respectively. It then follows that $\neg((a \cdot b)_{k+m}^\natural \rightsquigarrow 0)$.

To see this, assume for a contradiction that there is a path $(a \cdot b)_{k+m}^\natural \rightsquigarrow 0$ and consider first the case where $k + m = 0$. Then we have that $a_0 \cdot b_0$ is congruent to 0 modulo p and therefore, since p is prime, either a_0 is congruent to 0 modulo p or b_0 is congruent to 0 modulo p. In either case we have obtained a contradiction.

On the other hand, when $k + m$ is a successor $k + m = n + 1$, we have that

$$(a \cdot b)_{k+m}^\natural \rightsquigarrow \left[(a^\natural \cdot b^\natural)_{k+m} + \{\mathbf{p}(a^\natural \cdot b^\natural)_n^\natural\}\right]. \tag{3}$$

By the choice of k and m it follows that there is a further term (`precarryandzeromult`) of type $\mathbf{p}(a^\natural \cdot b^\natural)_n^\natural \rightsquigarrow 0$. Therefore, we obtain a term of type

$$0 \rightsquigarrow [(a^\natural \cdot b^\natural)_{k+m}].$$

However, it is easy (`hzfpstimeswhenzero`) to see that $(a^\natural \cdot b^\natural)_{k+m} \rightsquigarrow a_k^\natural \cdot b_m^\natural$. So, since p is prime, either $a_k^\natural \rightsquigarrow 0$ or $b_m^\natural \rightsquigarrow 0$ is inhabited. In either case we obtain a contradiction. □

Using Theorem 6.14, we now arrive at our definition of the p-adic numbers.

Definition 6.15 (`padics`)**.** The Heyting field $\mathbb{Q}_p$ of p-adic numbers is defined as the Heyting field of fractions of $\mathbb{Z}_p$:

$$\mathbb{Q}_p := \mathbf{Frac}(\mathbb{Z}_p).$$

As the field of fractions of the p-adic integers, possessing the appropriate universal property, it is clear that what we have described are indeed the p-adic numbers.

7. Future directions: towards p-adic integrable systems

Next we present an outline of the work on p-adic integrable systems that we plan to carry out following this paper. The long term goal is to develop an analogue of the symplectic theory of finite-dimensional real integrable systems in Pelayo and Vũ Ngọc (2009, 2011) for p-adic integrable systems in the univalent setting, and implement it in Coq.

We are beginning to explore this, and what we give next is a brief and informal glimpse of our plans. At this point, this section is a discussion without rigorous descriptions as we are not yet convinced of the optimal definition of p-adic integrable system. We hope to convey the fact that the p-adic and real theories are expected to be different, and draw attention to the topic; in fact, we are not aware of a uniform treatment of p-adic integrable systems in the symplectic setting.

7.1. *Definition of p-adic integrable systems*

7.1.1. *A word on the contrast between p-adic and real notions.* We refer to (Gouvêa 1993, Section 3) for basic algebraic and topological aspects concerning the p-adic numbers. Many aspects do not match the intuition we have for the real numbers. For instance, there are no nontrivial connected sets and there are non-empty sets which are both compact and open. Other aspects are more familiar: on $\mathbb{Q}_p$ there is an absolute value $|\cdot|$ and $\mathbb{Q}_p$ is complete with respect to it, and there is an inclusion $\mathbb{Q} \to \mathbb{Q}_p$ with dense image. Continuity and differentiability of functions is defined in the usual way (Gouvêa 1993, Definitions 4.2.1 and 4.2.2). Continuous functions are uniformly continuous on compact sets, as in the real case.

The notions of continuity and differentiability extend to functions $f : U \subset (\mathbb{Q}_p)^n \to \mathbb{Q}_p$ of several variables $(x_1, \ldots, x_n)$ on open sets U of the Cartesian product $(\mathbb{Q}_p)^n$, in direct analogy with the real case, and in particular we have analogous definitions for partial derivatives $\frac{\partial f}{\partial x_i}$, for all $i = 1, \ldots, n$. But although the definitions are the same, differentiability behaves differently in the p-adic case than in the real case. For instance, there are functions $f : \mathbb{Q}_p \to \mathbb{Q}_p$ which have zero derivative everywhere but are *not* locally constant. Also, the natural extension of the real mean value theorem to the p-adic case is false in general (although a version holds for sufficiently close points), as seen for instance by considering $f(x) = x^p - x$ between the extreme points $a = 0$ and $b = 1$. In this case, (Gouvêa 1993, Proposition 4.2.3) $f'(x) = px^{p-1} - 1$ and $f(a) = f(b) = 0$ and it is easy to check that any element 'in between' a and b, that is, of the form $at + b(1-t) = 1 - t$ for some t with $|t| \leqslant 1$, gives rise to a unit $f'(1-t)$ in $\mathbb{Z}_p$.

These differences are an indication that the theory of p-adic integrable systems is not expected to be a direct extension of the theory of real integrable systems, even if the basic definitions are analogous. One can explore such theory classically only, but we hope to do it in the univalent setting, building on the constructions of $\mathbb{Q}_p$ which we have given in the previous sections.

7.1.2. *Integrable systems.* We are here going to propose a notion of p-adic integrable systems in parallel with the commonly accepted notion of real integrable systems, at least in symplectic geometry.

Because in the univalent foundations, and in Coq, it is nontrivial to define manifolds, for now we are going to work with the p-adic Cartesian product

$$M := (\mathbb{Q}_p)^{2n} = \mathbb{Q}_p \times \cdots (2n \text{ times}) \cdots \times \mathbb{Q}_p$$

with coordinates $(x_1, y_1, \ldots, x_n, y_n)$. In this way, we also avoid a discussion of differential or symplectic forms. Fix a p-adic measure on $\mathbb{Q}_p$, and endow M with the induced product measure.

On M we may consider differentiable functions in the p-adic sense[†]. The following is the formal extension of the definition of real integrable system in finite dimensions. There

[†] For now we are thinking only of polynomials on $2n$-variables, which are easy to deal with in Coq.

is, however, a critical point which is not clear to us at the moment, and that's why we restrict our definition to analytic maps, see Remark 7.2.

Definition 7.1. We will say that a (p-adic) analytic map $F := (f_1, \ldots, f_n) : M \to (\mathbb{Q}_p)^n$ is a **p-adic integrable system** if two conditions hold:

1. The collection $f_1, \ldots, f_n$ satisfies Hamilton's equations:
$$\sum_{k=1}^{n} \frac{\partial f_i}{\partial x_k} \frac{\partial f_j}{\partial y_k} - \frac{\partial f_i}{\partial y_k} \frac{\partial f_j}{\partial x_k} = 0, \quad \forall\ 1 \leqslant i \leqslant j \leqslant n. \tag{4}$$
2. The set where the n formal differentials
$$\mathrm{d}p_i := \left(\frac{\partial f_i}{\partial x_1}, \ldots, \frac{\partial f_i}{\partial x_n}, \frac{\partial f_i}{\partial y_1}, \ldots, \frac{\partial f_i}{\partial y_n} \right), \quad \forall\ 1 \leqslant i \leqslant n$$
are linearly dependent has p-adic measure 0.
That is, there exists a p-adic measure 0 set A such that $\mathrm{d}f_1, \ldots, \mathrm{d}f_n$ are linearly independent on $M \setminus A$. The points where $\mathrm{d}f_1, \ldots, \mathrm{d}f_n$ are linearly dependent are called *singularities*.

Remark 7.2. This remark explains why we have to restrict to analytic functions in Definition 7.1, when in the real theory one likes to include all smooth functions in the definition of integrable system. There are many interesting, nontrivial p-adic functions that are smooth and have zero derivative everywhere. *However this is not possible if one restricts to analytic functions.* Therefore, if f is a smooth solution to a linear differential equation, we could add to f any of these nontrivial functions with zero derivative and obtain a new solution. It follows that all collections of n smooth functions $f_1, \ldots, f_n$ which are smooth and have zero derivative everywhere would also form a kind of integrable system, but a very 'degenerate' one (in the sense that the differentials $\mathrm{d}f_1, \ldots, \mathrm{d}f_n$ would not be linearly independent almost everywhere as it is normally required for real integrable systems). So this undesirable case does not occur. However, adding functions with zero derivative to an existing system would be unavoidable, giving rise to a new, seemingly very different, p-adic integrable system. We currently understand neither what this means geometrically, nor what it implies for the development of the theory.

7.2. *Future plans*

The following is a rough outline of what we would like to do next.

7.2.1. *Towards p-adic symplectic geometry.*

- ▷ *p-adic manifolds*: formalize the notion of p-adic manifold in the univalent foundations with Coq. Formalize Serre's theorem (Serre 1965) classifying compact p-adic manifolds.
- ▷ *p-adic symplectic forms*: a p-adic symplectic form ω may be defined as in the real case. The closedness condition $\mathrm{d}\omega = 0$ makes sense in the p-adic setting, and so does the non-degeneracy condition (in fact, over any field). In the real setting, a theorem of Darboux says that all symplectic forms are locally equivalent, so real symplectic manifolds have no local invariants. It is natural to wonder whether this result holds

in the p-adic setting 'as is'. Because of our previous discussion (see Remark 7.2) one should probably restrict to the analytic setting since $d\omega = 0$ is in fact a system of partial differential equations. Darboux's theorem plays a leading role in the theory of real integrable systems.

7.2.2. *Towards p-adic integrable systems: basic theory.*

- ▷ *construction of p-adic integrable systems*: define p-adic integrable systems on p-adic manifolds, not just $(\mathbb{Q}_p)^n$, and implement this in the univalent foundations using Coq.
- ▷ *p-adic local and semiglobal theory*: develop the local and semilocal theory of p-adic integrable systems in Coq. The local theory basically refers to local models, and the semilocal theory refers to local models in neighborhoods of fibers. One is interested in both the topological and symplectic classification of such models. We are not aware of results describing the topological, or symplectic, structure of regular or singular fibers in the p-adic setting.
  In the real case, the regular fibers and their neighborhoods are understood (this is the famous action-angle theorem due to Mineur and Arnold.) The singular fibers may be complicated and are not yet well understood in the real setting either (if one restrict to the real analytic setting, then the theory is better understood).

7.2.3. *Towards p-adic toric and semitoric systems.*

- ▷ *p-adic toric systems*: a particular class of real integrable systems which has been thoroughly studied and is well understood, is that of toric integrable systems $F = (f_1, \ldots, f_n)$ on $2n$-dimensional compact symplectic manifolds (M, ω). These are systems in which each component f_i generates a flow which is periodic of a fixed period. In this case, F is called a *momentum map*. Atiyah (1982), Guillemin and Sternberg (1982) and Delzant (1988) proved a series of striking theorems concerning these systems in the 1980s, which in particular led to complete combinatorial classification in terms of convex polytopes by Delzant (these convex polytopes are nothing but the images of M under F). A theorem of Serre (1965) classifies compact p-adic analytic varieties. If on these varieties we would consider actions of the p-adic n-torus, we do not know to what extent the above results could be extended. If in Definition 7.1 one allows smooth non-analytic functions, these results would not hold (see Remark 7.2).
- ▷ *p-adic semitoric systems*: give a classification of p-adic integrable systems under some periodicity condition in analogy with Pelayo and Vũ Ngọc (2009, 2011).

7.2.4. *Spectral questions for p-adic integrable systems.* Here we restrict to the systems in the previous section, for which we know that in the real case a full classification may be given.

- ▷ *Inverse spectral problems*: construct algorithms to solve inverse spectral problems about quantum integrable systems. The leading question in the real case is: given the spectrum, can one recover the system from it?
- ▷ *Numerical implementation of inverse spectral problems*: constructing numerically accurate algorithms to solve inverse spectral problems.

The first subsection above should be within reach. We expect the second and third subsections to be substantial. The fourth one depends on the third and it is difficult to predict how complicated it will be.

Acknowledgements

We thank Mark Goresky, Helmut Hofer, Gopal Prasad and Bas Spitters for discussions. We also thank the referees for their useful comments and suggestions.

Appendix A. Getting and Reading the Coq Code

The Coq code can be found on the website associated to this issue of the journal. In order to compile the code we have used Coq 8.3pl2 together with the patches included in the second author's Coq library (Fall 2011 version). All of the files associated with this paper require the second author's Coq library. For more on this library we refer the reader to the library itself and to the tutorial (Pelayo and Warren 2014). Figures A1 and A2 give the dependences of the second author's library and the library associated with this paper, respectively.

Of the new files, the file `lemmas.v` contains a number of small lemmas which, such as basic facts about apartness relations, some lemmas on rings, *et cetera*, which are required by the other files. The file `fps.v` contains all of the material on formal power series. The construction of the Heyting field of fractions can be found in `frac.v`. The basic number theoretic results which we require are in `zmodp.v`. Finally, the construction of the *p*-adic numbers is given in `padics.v`.

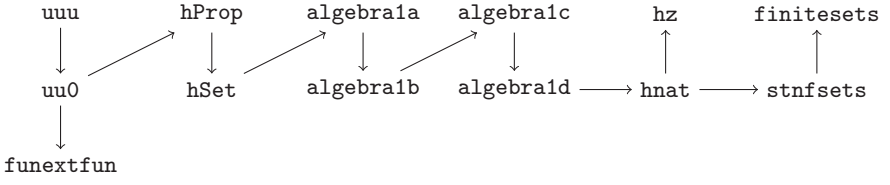


Fig. A1. Dependence diagram of the second author's Coq library.

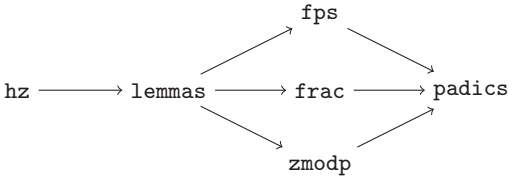


Fig. A2. Dependence diagram of the additional Coq files for the *p*-adics.

A.1. *A sample Coq proof*

We include below a sample of the Coq code as an illustration for the interested reader. The particular example we give is the statement of the lemma `quotientprecarryplus` which is Lemma 6.10 above. The proof in the Coq code is as described in the text above and the reader can see that the proof consists almost entirely of rewriting. This is typical of many of the proofs given in the Coq files, although others rely on a careful analysis into smaller lemmas and several proofs related to the apartness relation on the field of fractions were simplified using a custom built tactic (`permute`).

```
Lemma quotientprecarryplus
 ( m : hz ) ( is : hzneq 0 m ) ( a b : fpscommrng hz ) ( n : nat ) :
   hzquotientmod m is ( precarry m is ( a + b ) n ) ~>
   ( hzquotientmod m is ( precarry m is a n ) +
     hzquotientmod m is ( precarry m is b n ) +
     hzquotientmod m is (
       precarry m is ( carry m is a + carry m is b ) n
     )
   ).
Proof.

intros. induction n.

simpl.
change ( hzquotientmod m is ( a 0%nat + b 0%nat ) ~>
  (hzquotientmod m is (a 0%nat) + hzquotientmod m is (b 0%nat) +
   hzquotientmod m is ( hzremaindermod m is ( a 0%nat ) +
   hzremaindermod m is ( b 0%nat ) )
  ) ).
rewrite hzquotientmodandplus.  apply idpath.

change ( hzquotientmod m is ( a ( S n ) + b ( S n ) +
  hzquotientmod m is ( precarry m is (a + b) n ) ) ~>
  (hzquotientmod m is (precarry m is a (S n)) +
   hzquotientmod m is (precarry m is b (S n)) +
   hzquotientmod m is (
     carry m is a ( S n ) +
     carry m is b ( S n ) + hzquotientmod m is (
       precarry m is (carry m is a + carry m is b) n)
  )
  ) ).
rewrite IHn.
rewrite ( rngassoc1 hz ( a ( S n ) ) ( b ( S n ) ) _ ).
rewrite <- ( rngassoc1 hz ( b ( S n ) ) ).
rewrite ( rngcomm1 hz ( b ( S n ) ) _ ).
```

```
rewrite <- 3! ( rngassoc1 hz ( a ( S n ) ) _ _ ).
change ( a ( S n ) + hzquotientmod m is ( precarry m is a n ) )
  with ( precarry m is a ( S n ) ).
set ( pa := precarry m is a ( S n ) ).
rewrite ( rngassoc1 hz pa _ ( b ( S n ) ) ).
rewrite ( rngcomm1 hz _ ( b ( S n ) ) ).
change ( b ( S n ) + hzquotientmod m is ( precarry m is b n ) )
  with ( precarry m is b ( S n ) ).
set ( pb := precarry m is b ( S n ) ).
set ( ab := precarry m is ( carry m is a + carry m is b ) ).
rewrite ( rngassoc1 hz ( carry m is a ( S n ) )
  ( carry m is b ( S n ) ) ( hzquotientmod m is ( ab n ) ) ).
rewrite ( hzquotientmodandplus m is ( carry m is a ( S n ) ) _ ).
unfold carry at 1.
rewrite <- hzqrandremainderq. rewrite hzplusl0.
rewrite ( hzquotientmodandplus m is ( carry m is b ( S n ) ) _ ).
unfold carry at 1.
rewrite <- hzqrandremainderq. rewrite hzplusl0.
rewrite ( rngassoc1 hz pa pb _ ).
rewrite ( hzquotientmodandplus m is pa _ ).
change (pb + hzquotientmod m is (ab n))
  with (pb + hzquotientmod m is (ab n))%hz.
rewrite ( hzquotientmodandplus m is pb ( hzquotientmod m is ( ab n ) ) ).
rewrite <- 2! ( rngassoc1 hz ( hzquotientmod m is pa ) _ _ ).
rewrite <- 2! ( rngassoc1 hz
  ( hzquotientmod m is pa + hzquotientmod m is pb ) _ ).
rewrite 2! ( rngassoc1 hz ( hzquotientmod m is pa +
  hzquotientmod m is pb +
  hzquotientmod m is (hzquotientmod m is (ab n)) ) _ _ ).
apply ( maponpaths
  ( fun x : hz => ( hzquotientmod m is pa +
    hzquotientmod m is pb +
    hzquotientmod m is (hzquotientmod m is (ab n)) ) +
    x
  ) ).
unfold carry at 1 2. rewrite 2! hzremaindermoditerated.
change ( precarry m is b ( S n ) ) with pb.
change ( precarry m is a ( S n ) ) with pa.
apply ( maponpaths
  ( fun x : hz => ( hzquotientmod m is ( hzremaindermod m is pb +
    hzremaindermod m is (hzquotientmod m is (ab n)))%hz ) + x
  ) ).
apply maponpaths.
```

```
apply ( maponpaths
  ( fun x : hz => hzremaindermod m is pa + x ) ).
rewrite ( hzremaindermodandplus m is ( carry m is b ( S n ) ) _ ).
unfold carry. rewrite hzremaindermoditerated.
rewrite <- ( hzremaindermodandplus m is ( precarry m is b ( S n ) ) _ ).
apply idpath.

Defined.
```

References

Atiyah, M. (1982) Convexity and commuting Hamiltonians. *Bulletin of the London Mathematical Society* **14** 1–15.

Awodey, S. (2012) Type theory and homotopy. In: Dybjer, P., Lindström, S., Palmgren, E. and Sundholm, B. G. (eds.) *Epistemology versus Ontology: Essays on the Philosophy and Foundations of Mathematics in Honour of Per Martin-Löf* Logic, Epistemology, and the Unity of Science volume 27, Springer, Dordrecht 183–201.

Awodey, S., Pelayo, Á. and Warren, M. A. (2013) Voevodsky's univalence axiom in homotopy type theory, *Notices of the American Mathematical Society* 60 (08) 1164–1167.

Bertot, Y. and Castéran, P. (2004) *Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions,* Texts Theoretical Computer Science An EATCS Series, Springer-Verlag.

Brekke, L. and Freund, P. G. O. (1993) *p*-adic numbers in physics. *Physics Reports* **233** (1) 1–66.

Bridges, D. and Richman, F. (1987) *Varieties of Constructive Mathematics*, London Mathematical Society Lecture Note Series, Cambridge University Press.

Delzant, T. (1988) Hamiltoniens périodiques et image convexe de l'application moment. *Bulletin de la Société Mathématique de France* **116** 315–339.

Gouvêa, F. (1993) *p-adic Numbers. An Introduction,* Universitext, Springer-Verlag.

Guillemin, V. and Sternberg, S. (1982) Convexity properties of the moment mapping. *Inventiones Mathematicae* **67** 491–513.

Hensel, K. (1900) Über eine Theorie der algebraischen Functionen zweier Variablen. *Acta Mathematica* **23** (1) 339–416.

Koblitz, N. (1984) *p-adic Numbers, p-adic Analysis and Zeta-Functions*, 2nd ed. Graduate Texts in Mathematics volume 58, Springer-Verlag.

Mines, R., Richman, F. and Ruitenburg, W. (1988) *A Course in Constructive Algebra*, Springer-Verlag.

Pelayo, Á. and Vũ Ngọc, S. (2009) Semitoric integrable systems on symplectic 4-manifolds, *Inventiones Mathematicae* **177** 571–597.

Pelayo, Á. and Vũ Ngọc, S. (2011) Constructing integrable systems of semitoric type. *Acta Mathematica* **206** 93–125.

Pelayo, Á. and Warren, M. A. (2014) Homotopy type theory and Voevodsky's Univalent Foundations *Bulletin of the American Mathematical Society* **51** (4), 597–648.

Schikhof, W. H. (1984) *Ultrametric Calculus. An Introduction to p-adic Analysis,* Cambridge Studies in Advanced Mathematics volume 4, Cambridge University Press.

Serre, J. P. (1965) Classification des variétés analytiques *p*-adiques compactes. *Topology* **3** 409–412.

Voevodsky, V. (2010) Extended version of NSF proposal at: `www.math.ias.edu/~vladimir`.

Voevodsky, V. (2011) Coq library at: `www.math.ias.edu/~vladimir`, Fall 2011 version.

Voevodsky, V. (2014) Experimental library of univalent formalization of mathematics. *Mathematical Structures Computer Science*, to appear. (Preprint on the arxiv as `arXiv:1401.0053`.)