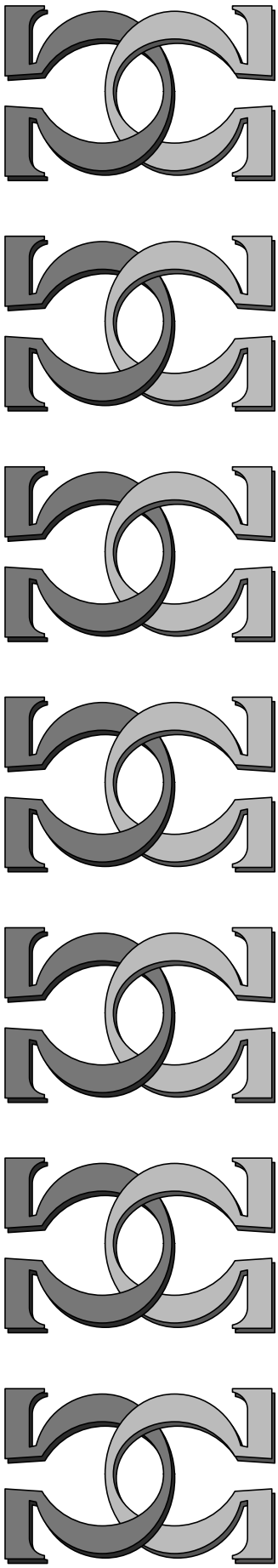

CDMTCS
Research
Report
Series

Computable p–adic Numbers

George Kapoulas
Athens Univ. of Economics and Bussiness, Greece

CDMTCS-115
November 1999

Centre for Discrete Mathematics and
Theoretical Computer Science

Computable p–adic Numbers

George Kapoulas
Dept. of Accounting and Finance,
Athens Univ. of Economics and Bussiness
Patission 76 St. Athens 10434, Greece
e–mal: gkapou@math.ntua.gr

Abstract: In the present work the notion of the computable (primitive recursive, polynomially time computable) p–adic number is introduced and studied. Basic properties of these numbers and the set of indices representing them are established and it is proved that the above defined fields are p–adically closed. Using the notion of a notation system introduced by Y. Moschovakis an abstract characterization of the indices representing the field of computable p–adic numbers is established.

Keywords: Computable numbers, computable (primitive recursive, polynomially time computable p–adic numbers, p–adically closed fields, notation systems.

1 Introduction

The present work brings together two ideas, namely type two computability, and p–adic fields. We start with a brief review of the notion a computable number and of a p–adic field as a background.

The basic idea for computable real numbers is contained in Turing's fundamental paper [20], where he introduced the notion of a computable (or recursive) real number, and initiated the study of the relevant concepts and notions. He described the recursive real numbers as a subset of the real numbers obtained by imposing restrictions on the definition of a real number. A real number can be given either as a digit expansion in some base $b \geq 2$, or as a limit of Cauchy sequence of rational numbers, or a Dedekind cut. In the above paper, Turing defined a computable real number to be a real number which admits an effective representation in base 2 expansion. The above definition (of effective representation) was enlarged by other researchers since the definition of a real number can be given also as a limit of a Cauchy sequence or as a Dedekind cut. A computable (or recursive) real number is currently defined in the literature in any of the above mentioned ways (limit of a Cauchy sequence, Dedekind cut, or digit expansion), subject to the requirement that the method that defines the number is effective (a partial list of related work is: [7, 8, 13, 14, 16, 17, 18]). In the literature the standard definition used is the one using Caychy sequences. The main reason for this developement is that there exist problems regarding the rational operations using the decimal (or some other base) expansion of a real number.

This idea of Turing can be viewed as the study of one of the topological completions of the field of the rational numbers, namely the one given by the usual absolute value, while imposing some restrictions on the way an element of the completion is defined. Namely either the sequence of digits is given by a total recursive function, or the Cauchy sequence and the modulus of convergence are given by a recursive function. This requirement can be seen as a restriction of the topology.

There are other topological completions of the field of the rational numbers, namely the p–adic fields, where a different absolute value is used. It is natural to consider the analogous effectiveness and complexity questions in these contexts. Regarding the possible topological completions of the fiels of the rational numbers, Ostrowski has shown that

the fields of the real and p–adic numbers are the only possible topological completions of the field of rational numbers [5].

We give a brief description of the p–adic fields and refer the reader to [4, 5, 9, 12], for detailed presentations. A p–adic field can be defined axiomatic definition or by a direcr construction of the p–adic numbers (or representatives of them) and defining the field operations. The definition through the representatives can be accomplished in various ways:

1) A p–adic field can be defined as a topological completion of the field of rational numbers. To achieve this first fix a prime number p. Define the valuation of a non zero integer number r with respect to p, denoted by $v_p(r)$, to be the highest exponent e such that $p^e|r$, and set $v_p(0) = \infty$. This valuation can be extended to the set of rational numbers. For a rational number $x = r/s$, with r, s integers, define $v_p(x) = v_p(r) - v_p(s)$. It can be easily shown that the above definition is independent of the representation of x. From this valuation it is possible to define an absolute value over the field of rational numbers as follows: $|r| = p^{-v_p(r)}$. This function absolute value function satisfies all the axioms for an absolute value function, and in addition to the usual triangle inequality, it satisfies the strong triangle inequality (referred to as *ultrametric inequality*) i.e.

$$|x + y| \leq \max\{|x|, |y|\}.$$

In addition, the above inequality reduces to equality if $|x| \neq |y|$, and also if $|x + y| < \max\{|x|, |y|\}$ then $|x| = |y|$. The ultrametric inequality shows that the field of p–adic numbers fails to satisfy the Archimedean axiom. From the definition of the absolute value over these fields (denoted by $\mathbf{Q}_p$) we have that for any "triangle" at least two of the three "sides" of the "triangle" have equal "length".

Having defined this absolute value, it is possible to define the notion of a Cauchy sequence with respect to it. After showing that the field of rational numbers is not (topologically) complete with respect to this absolute value, the field of p–adic numbers, is defined to be the completion of the field of rational numbers with respect to this absolute value. It can be shown that this field is unique up to isomorphism [5].

The notion of a valuation function over a field can be formulated in a more algebraic and abstract setting as follows: Given a field F, and an ordered Abelian group $\langle G, +, < \rangle$, a valuation is a map $v\colon F \setminus \{0\} \to G$ which satisfies:

$$v(xy) = v(x) + v(y),$$

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

The group G is called the value group of F with respect to this valuation. In the case of the p–adic numbers the absolute value group of the valuation is $\langle \mathbf{Z}, +, < \rangle$. For the notion of valuation related with p–adic fields, the necessary material can be found in [5].

An important subset of $\mathbf{Q}_p$ is the set of p–adic numbers x such that $v_p(x) \geq 0$ (or equivalently $|x| \leq 1$). They are called p–adic integers and this set is denoted by $\mathbf{Z}_p$. This set is the analogue of the set $[0, 1]$ (or $[-1, 1]$) in the case of real numbers, and it is a ring. Moreover it contains a unique maximal ideal namely the set $\{x \in \mathbf{Q}_p\colon |x| < 1\} = p\mathbf{Z}_p$ (such rings are known as local rings in Algebra).

An alternative way to view the field of p–adic numbers along with the absolute value function is the notion of a valued field. To do this the field of p–adic numbers is not considered as a field with an absolute value, but as a field with a distinguished subset. The

distinguished subset is the set $\mathbf{Z}_p$ or the set $\{x \in \mathbf{Q}_p : |x| \leq 1\}$. This set is algebraically a ring (called the valuation ring), and it has a unique maximal ideal, namely the set $p\mathbf{Z}_p$. The set $\mathbf{Z}_p$ can be defined in the language of fields as follows:

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid \exists y \quad y^2 - 1 = px^2\} \quad p \neq 2,$$

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid \exists y \quad y^3 - 1 = px^3\}, \quad p = 2.$$

The presentation of $\mathbf{Q}_p$ as a valued field with $\mathbf{Z}_p$ as a distinguished subset makes possible to express an algebraic property of the field of p–adic numbers, namely the notion of a Henselian field.

Definition 1 *(***Hensel's lemma, Newton's method***) Let $\langle F, \mathcal{O}, \mathcal{M}\rangle$ be a valued field, with $\mathcal{O} = \{x \in F \mid v(x) \geq 0\}$, $\mathcal{M} = \{x \in F \mid v(x) \geq 1\}$. Let $f \in \mathcal{O}[x]$, let $\bar{f}$ be the polynomial obtained from f by reducing the coefficients of $f \pmod{\mathcal{M}}$, let $\bar{f}'$ be the formal derivative of $\bar{f}$. The field $\langle F, \mathcal{O}, \mathcal{M}\rangle$ is* Henselian *if for $x \in F/\mathcal{M}$ such that $\bar{f}(x) \equiv 0 \pmod{\mathcal{M}}$, and $\bar{f}'(x) \not\equiv 0 \pmod{\mathcal{M}}$, there exists $\bar{z} \in F$ such that $f(z) = 0$, and $z \equiv x \pmod{\mathcal{M}}$.*

An alternative approach for defining the field of p–adic numbers is similar to the digit expansion of a real number i.e using a representation. A nonzero real number x can be represented as a digit expansion i.e.

$$x = (-1)^{\sigma} b^{e} \Sigma_{k=0}^{\infty} d_i b^{-i}, \quad e \in \mathbf{Z}, \quad d_i \in \{0, 1, \ldots, b-1\}, \quad d_0 \neq 0, \quad \sigma \in \{0, 1\}. \tag{1}$$

with $b \geq 2$.

For the p–adic case we have a similar representation, namely a nonzero p–adic number x can be represented as:

$$x = p^{e} \Sigma_{i=0}^{\infty} d_i p^{i} \quad \text{with} \quad e \in \mathbf{Z}, \quad d_i \in \{0, 1, \ldots, p-1\}, \quad d_0 \neq 0. \tag{2}$$

(in the case of a p–adic number the base p is fixed). The valuation of the element x is defined to be the number e. The above representation in the case of p–adic numbers is unique as opposed with the real numbers.

A variant of the base p representation is the Teichmüller representation. The representation of $\mathbf{Q}_p$ in base p (equation 2) consists of the formal expressions of the form

$$\Sigma_{n=i}^{\infty} a_n p^n \quad i \in \mathbf{Z}, \quad a_n \in \{0, 1, \ldots, p-1\}, \quad a_i \neq 0. \tag{3}$$

To obtain such an expression we choose a complete set of representatives to use as digits (coefficients) . A different complete set of representatives that can be used is the set of $(p-1)$st roots of unity and 0. This is a complete set of representatives since the equation $x^{p-1} - 1 = 0$ has at most one root x_i such that $x_i = i \pmod{p}$ for each $i \in \{1, \ldots, p-1\}$, and $\mathbf{Q}_p$ is Henselian. This representation is called the Teichmüller representation. We can endow the set $\{0, 1, \ldots, p-1\}$ with suitable operations such that $\mathbf{Q}_p$ in base p expansion becomes a field. Mapping the set $\{0, 1, \ldots, p-1\}$ to the set of $p-1$ roots of unity and 0 these operations induce operations on the set of $p-1$ roots of unity and 0 and then $\mathbf{Q}_p$ (in Teichmüller representation) becomes a field isomorphic to $\mathbf{Q}_p$ in base p expansion.

The field operations in the p–adic fields are defined as follows: In the definition via Cauchy sequences we have rational operations over rational numbers and we can extend

by continuity. In the case of the base p expansion, or the Teichmüller representation, the operations are carried out digit by digit (as in the case of the real numbers). In the base p expansion or the Teichmüller representation there is a carry digit also as in the case of real numbers, but this digit moves to the right. This last fact simplifies certain proofs and gives a difference contrasted with the real numbers. For example the $\epsilon/2$ arguments in the real number case are simplified to ϵ arguments in the case of p–adic numbers.

In the axiomatic definition, in the language of fields we describe a set of (second order) axioms and exhibit a model. It can be shown that any two models of the following set of axioms are isomorphic [5]. The axioms for the field of p–adic numbers F are the following:

1. The characteristic of the field F is 0.
2. The residue field $\mathbf{Z}_p/p\mathbf{Z}_p$ is isomorphic to $\mathbb{F}_p$, the finite field consisting of p elements.
3. The value group is $\langle \mathbf{Z}, +, < \rangle$.
4. The least element of the value group is equal to $v(p)$.
5. Every Cauchy sequence of elements of F converges to an element of F.

The definition of the p–adic fields as completions of the field of the rational numbers or the definition of a p–adic number as base p expansion gives a model for the axiomatic definition or alternatively the axiomatic definition can be used for a uniqueness characterization of the construction [5].

The approach taken here is the traditional approach of recursive analysis, i.e. a real or p–adic number is viewed as infinite object, and is understood as the limit of finite objects, namely rational numbers. This approach for the case of real numbers has been extensively developed by various authors. A partial list of related work follows: [1, 2, 7, 8, 6, 10, 13, 15, 16, 17, 18, 14, 20].

The main issue in the present work is to study the analogous problems in the case of p–adic numbers and verify which ones carry over and which ones fail and the reason for the failures.

The present approach to the nature of a real or a p–adic number should be contrasted with the superficially similar approach in in the work of Shub – Smale –Karp [3], where a (real or p–adic) number is taken as a completely known object and not taken as a limit of simpler objects. This difference on the nature of a real number as viewed by Shub – Smale – Karp also implies an understanding of the continuoum different than the one here. The nature of a computable (real or p–adic) number is the standard one in constructive mathematics where the notion of limit is employed to define these concepts. Also using the present setting it is possible to define and study naturally notions such as functions and functionals (representing the integral, the maximum value and the derivative of a function) over the basic objects of study. Such approach does not seem possible in the work of Shub – Smale –Karp [3].

Some natural questions to ask in the context of computability (and complexity) theory include the following: What are the properties (algebraic or analytic) of the set of numbers considered? There are several representations of the numbers introduced. One representation is using pairs of indices of recursive functions which functions code Cauchy sequences and moduli of convergence. An alternative representation is using indices of recursive functions which code the base p expansion of a p–adic number. Among these

representations is there a best representation, or are all of them of the same expressive power? Further work on functions and complexity considerations is under preparation.

Some of the results obtained are the following:

1. The definitions of the recursive p–adic numbers via Cauchy sequences and via base p expansion are recursively equivalent (Theorem 4, page 11).

2. The recursive, primitive recursive, and polynomially time computable p–adic numbers each form a p–adically closed field (Theorem 7, page 14, Theorem 8, page 16, Theorem 9, page 16).

3. The field of the recursive p–adic numbers is characterized up to recursive isomorphism (Theorem 14, page 20).

In the case of the real numbers there is a difference in the following case:

1. The set of numbers defined via base p expansion and via Cauchy sequences are the same, and we can effectively obtain an index of a Cauchy sequence for a p–adic number from an index of the base p expansion (as for the p–adic numbers). However we can effectively invert this translation. The effective inversion is not possible in the real number case.

This phenomenon (for the real number case) is well known and is related with the impossibility to determine correctly the digits of the binary (or decimal) expansion of a real number.

Notation: The set of natural numbers will be denoted by $\mathbf{N}$. The set of integers will be denoted by $\mathbf{Z}$. The set of rational numbers will be denoted by $\mathbf{Q}$. The set of p–adic numbers will be denoted by $\mathbf{Q}_p$. A standard enumeration of the general recursive functions is assumed. The notation ϕ_e will be used to denote the (general) recursive function with code number e. Lambda notation will be used occasionally to distinguish the variables of the functions from parameters. Kleene's primitive recursive predicate T will be used occasionally. The meaning of the predicate $T(x, y, z)$ will be that z is the complete computation history of the general recursive function with index x, on input y. We use $\{W_i \mid i \in \mathbf{N}\}$ to denote some standard enumeration of the r.e. subsets of the natural numbers, For coding pairs of integers $\langle x, y\rangle$ will denote the standard coding functions from pairs of natural numbers to the natural numbers, $\langle x, y, z\rangle$ will be used to denote the standard coding from triples of natural numbers to natural numbers etc. The functions for decoding codes for tuples of natural numbers will be denoted by $p_i(x)$, i.e. if x is a code for an n–tuple of natural numbers, then $p_i(x)$ is the ith component of this tuple. When a recursive function f is defined at the point x this will be denoted by $f(x)\downarrow$. The finite field consisting of p elements, with p a prime number will be denoted by $\mathbb{F}_p$. Equality between partial recursive function will be denoted by $\simeq$, that is for f, g partial recursive functions $f(x) \simeq g(x)$ denotes that for each x, both f and g are defined at x and have the same output value or both are undefined. The notation $f^{(m)}$ will be used to denote the mth derivative of a sufficiently differentiable function.

2 Recursive p–adic numbers

Definition 2 *A sequence of rational numbers* $\{a_n \mid n \in \mathbf{N}\}$ *is* recursive *if and only if there is a recursive function* f *s.t* $\forall n \in \mathbf{N}\ f(n) = a_n$. *An index* e *s.t.* $\phi_e(n) = f(n)$ *is called an* index *of the sequence* $\{a_n \mid n \in \mathbf{N}\}$.

Definition 3 *A recursive sequence of rational numbers* $\{a_n \mid n \in \mathbf{N}\}$ *is* Cauchy recursively or effectively (in the p–adic metric) *if and only if there is a recursive function* g *s.t.* $\forall n, m > g(l)$ *we have* $\mid a_n - a_m \mid < p^{-l}$. *The function* g *is called* a modulus of the Cauchy criterion *of the sequence* $\{a_n \mid n \in \mathbf{N}\}$. *An index of the function* g *is called an* index of the modulus of convergence.

Definition 4 *A* recursive p–adic number x *is the limit of recursive Cauchy sequence of rational numbers* $\{a_n \mid n \in \mathbf{N}\}$. *The sequence* $\{a_n \mid n \in \mathbf{N}\}$ *converges recursively (in the* p*–adic metric) to* x.

A *recursive p–adic number* x, given via as the limit of a Cauchy sequence, is a p–adic number represented by a natural number $\langle e, i\rangle$ in the following way: The number e is the code number (index) for a recursive function ϕ_e which generates a sequence of integers intepreted as codes for rational numbers. We have a recursive sequence of rational numbers via ϕ_e. The sequence $\{\phi_e(n) \mid n \in \mathbf{N}\}$ effectively converges to x. That is, $\phi_e(n)$ is the nth term of a Cauchy sequence of rational numbers converging to x with a (total) recursive function with index i as modulus of convergence (modulus for the Cauchy criterion). In other words we have:

$$\forall k \geq \phi_i(n) \Rightarrow |\phi_e(k) - x| < p^{-n}.$$

The definition given above does not directly refers to x but uses approximations to define the notion of a computable p–adic number.

Definition 5 *The index of pair* $\langle e, i\rangle$ *is called an* index *of the recursive p–adic number* x.

The set X of indices representing the computable p–adic numbers can be arithmetically defined as follows:

$$m \in X \iff m = \langle m_1, m_2\rangle \wedge \forall n \in \mathbf{N}\ \ \forall k, l \geq m_2(n) \Rightarrow\ p^n \mid \phi_{m_1}(k) - \phi_{m_1}(l).$$

One reason for starting from the rational numbers as fundamental objects of study, and not using some other set of numbers as basic objects, is their conceptual simplicity and the effectiveness of the basic operations. On the technical side we have that there is a primitive recursive function which enumerates a set of indices for the set of rational numbers. This is accomplished as follows: A rational number r/s can be coded as the pair $\langle r, s\rangle$. Any primitive recursive function which codes pairs of natural numbers (in lowest terms) to natural numbers can be used to give a primitive recursive enumeration of a set of indices for the rational numbers.

Since there are infinitely many indices representing the same recursive function f, we have that a recursive p–adic number is represented by an equivalence class of pairs of indices for recursive functions. The equivalence is defined as follows: Two indices for pairs $\langle f, m_1\rangle, \langle g, m_2\rangle$ representing recursive p–adic numbers are in the same equivalence class if and only if there exists a recursive function $m\colon \mathbf{N} \to \mathbf{N}$ such that:

$$\forall k, l \geq m(n) \Rightarrow\ \ |\phi_f(k) - \phi_g(l)| \leq p^{-n}.$$

The function m will be called *modulus of equivalence* of f and g. The equivalence relation between indices representing computable p–adic numbers can be defined arithmetically by the above relation (see [15]).

For x an index of a recursive p–adic number $[x]$ will denote the equivalence class that x belongs to. Given two indices $\langle e, m\rangle$ and $\langle e', m'\rangle$ which represent x we have that the function f defined by $f(n) = \max\{m(n), m'(n)\}$ is a modulus of equivalence for these two indices.

In general, there is going to be more than one natural number denoting the same object, so there is a nontrivial equivalence relation $\sim$ defined among the set of natural numbers used to denote the elements of the set under consideration (computable p–adic numbers). Two elements of the set X are equivalent if and only if they denote the same recursive p–adic number. In other words we associate each recursive p–adic number with an equivalence class of indices (pairs) for (total) recursive functions. Each index in an equivalence class codes a recursive Cauchy sequence of rational numbers, and the convergence rate is effective. In general the set X and the equivalence relation $\sim$ are not assumed to be recursive. Each equivalence class may contain infinitely many indices.

Definition 6 *(***Moschovakis [15]***) A* notation system *is a pair $\langle X, \sim\rangle$, with X a subset of the natural numbers, and $\sim$ an equivalence relation among elements of X.*

The above set of indices along with the equivalence relation is defined by Moschovakis [15] as a *notation system*. In the definition of a notation system in the present setting we use an arithmetically definable subset X of the natural numbers to denote the recursive p–adic numbers.

Notation: The set of recursive p–adic numbers will be denoted by $\mathbf{Q}_p^c$, the set of p–adic integers will be denoted by $\mathbf{Z}_p$. The set of codes of pairs of indices that represent recursive p–adic numbers will be denoted by Q_p^c. The set of equivalence classes of pairs of indices corresponding to a recursive p–adic number will be denoted by $\mathbb{Q}_p^c$. Otherwise $\mathbb{Q}_p^c = \langle Q_p^c, \sim\rangle$ is a notation system according to the definition 6, page 7.

3 Subsets of the computable p–adic numbers

By restricting the set of functions in the definition of a computable p–adic number, it is possible to obtain subclasses of $\mathbf{Q}_p^c$. Such nontrivial interesting subclasses are the polynomially time computable p–adic numbers and the primitive recursive p–adic numbers.

Definition 7 *A* polynomially time computable p–adic number *x is a p–adic number which is the limit of a recursive recursively convergent sequence of rational numbers. The number x is represented by a natural number $\langle e, m\rangle$. The sequence of values $\{\phi_e(n) \mid n \in \mathbf{N}\}$ is polynomially time computable, and is interpreted as a Cauchy sequence of rational numbers. The modulus of convergence of the sequence $\{\phi_e(n) \mid n \in \mathbf{N}\}$ (Cauchy criterion) m is a polynomially time computable function.*

Regarding the coding of the input n to the function ϕ_e we use unary notation. The reason for this is that using binary notation will give exponential complexity to simple functions as the identity function which should be computable as a function with linear modulus of continuity.

Notation: The set of polynomially time computable p–adic numbers will be denoted by $\mathbf{Q}_p^{\mathcal{P}}$. The set of indices that represent polynomially time computable p–adic numbers will be denoted by $\mathrm{Q}_p^{\mathcal{P}}$. The set of equivalence classes of indices that represent elements of $\mathbf{Q}_p^{\mathcal{P}}$ will be denoted by $\mathbb{Q}_p^{\mathcal{P}}$.

Equality among elements of $\mathrm{Q}_p^{\mathcal{P}}$ is defined as follows: Two indices i, j for elements of $\mathbf{Q}_p^{\mathcal{P}}$ represent the same element of $\mathbf{Q}_p^{\mathcal{P}}$ if and only if there exists a polynomially time computable function f such that:

$$\forall n, \forall m \quad m > f(n) \Rightarrow |\phi_i(m) - \phi_j(m)| < p^{-n}.$$

Definition 8 *A* primitive recursive p–adic number *is the limit of primitive recursive sequence of rational numbers with primitive recursive modulus of convergence. A primitive recursive p–adic number z is represented by a natural number $\langle e, m\rangle$, which is the Gödel number of a primitive recursive function $\phi_e: \mathbf{N} \to \mathbf{N}$ such that the sequence $\{\phi_e(n) | n \in \mathbf{N}\}$ codes a Cauchy sequence of rational numbers, with primitive recursive modulus of convergence m, which sequence converges to z.*

The set of primitive recursive p–adic numbers will be denoted by $\mathbf{Q}_p^{PR}$. The set of indices that represent polynomially time computable p–adic numbers will be denoted by Q_p^{PR}. The set of equivalence classes of notations for the primitive recursive p–adic numbers will be denoted by $\mathbb{Q}_p^{PR}$.

Equality among elements of Q_p^{PR} is defined as follows: Two indices i, j for elements of $\mathbf{Q}_p^{PR}$ represent the same element of $\mathbf{Q}_p^{PR}$ if and only if there exists a primitive recursive function f such that:

$$\forall n, \forall m \quad m > f(n) \Rightarrow |\phi_i(m) - \phi_j(m)| < p^{-n}.$$

Theorem 1 *There is no decision procedure to decide if two indices representing recursive p–adic numbers represent the same element of $\mathbf{Q}_p^c$.*

*Proof:*Suppose such a procedure exists, then taking the difference of the values of the recursive functions corresponding to these two indices we would have a decision procedure for the set of indices representing 0. That is there is a decision procedure for the following set:

$$\{\langle i, m\rangle \mid \text{ for all } k \geq m(n) \quad |\phi_i(k)| < p^{-n}\} =$$

$$\{\langle i, m\rangle \mid \text{ for all } k \geq m(n) \quad p^n | \phi_i(k)\}.$$

Consider the following reduction:

$$\phi_{f(x)}(z) = \begin{cases} 1, & \text{if } z = 0, \\ x + p^z, & \text{if } \phi_x(x) \text{ does not halt in } z \text{ steps}, \\ p^{z_0}, & \text{the least } z_0 \leq z \text{ such that } \phi_x(x) \text{ halts in } z_0 \text{ steps, and } z \text{ is even}, \\ 1 + p^{z_0}, & \text{the least } z_0 \leq z \text{ such that } \phi_x(x) \text{ halts in } z_0 \text{ steps, and } z \text{ is odd}. \end{cases}$$

We have that f is a recursive function and $x \in \bar{K} = \{x \mid x \notin W_x\}$ if and only if $\langle f(x), Id\rangle$ is an index for $x \in \mathbb{Q}_p^c$ with linear modulus of convergence. A decision procedure as in the statement of the theorem would give that set $K = \{x \mid x \in W_x\}$ is a recursive set, via $\langle f(x), Id\rangle$. Also the above reduction is an $1 - 1$ reduction.

Corollary 1 *Equality between equivalence classes of recursive p–adic numbers is not decidable.*

*Proof:*If equality between p–adic numbers were decidable then for $x, y \in \mathbf{Q}_p^c$, and i, j indices for x, y respectively we can decide if $[i] = [j]$ or not. This implies that an equivalence class of indices for a fixed recursive p–adic number is a recursive set. This contradicts the previous theorem. In particular it is not possible to decide equality with 0. However we can determine whether two recursive p–adic numbers are different (unequal).

The above corollary is a fundamental difference between the present approach to computability and the approach in [3] where a real or p–adic number is taken as a completely known object and hence equality between such objects can be decided.

Proposition 1 *For $x \in \mathbb{Q}_p^c$ and $n \in \mathbf{N}$, we can decide the following: $|x| < p^n$, $|x| = p^n$, $|x| > p^n$.*

Theorem 2 *The set of indices for recursive p–adic numbers is not a recursive set.*

*Proof:*Suppose it is a recursive set. Then we have that there is a decision procedure for the following set:

$$\{\langle i, m\rangle\text{: for all } k, l \geq m(n) \quad \phi_i(k)\downarrow, \phi_i(l)\downarrow \quad \wedge \quad |\phi_i(k) - \phi_i(l)| < p^{-n}\} =$$

$$\{\langle i, m\rangle\text{: for all } k, l \geq m(n) \quad \phi_i(k)\downarrow, \phi_{\ i}(l)\downarrow \quad \wedge \quad p^n|(\phi_i(k) - \phi_i(l))\}.$$

Consider the following reduction:

$$\phi_{f(x)}(z) = \begin{cases} 1, & \text{if } z = 0, \\ x + p^z, & \text{if } \phi_x(x) \text{ does not halt in } z \text{ steps}, \\ 1 + p^{z_0}, & \text{the least } z_0 \leq z \text{ such that } \phi_x(x)\downarrow \text{ in } z_0 \text{ steps, and} \\ & z \text{ is even}, \\ p^{z_0}, & \text{the least } z_0 \leq z \text{ such that } \phi_x(x)\downarrow \text{ in } z_0 \text{ steps, and} \\ & z \text{ is odd}. \end{cases}$$

We have that $f(x)$ is a recursive function, and $x \in \bar{K} = \{x \mid x \notin W_x\}$ if and only if $\langle f(x), Id\rangle$ is an index for a Cauchy sequence converging to x with linear modulus of convergence. A decision procedure for the set of indices for the recursive p–adic numbers then would give a decision procedure for the set $\bar{K}$ via the function f. As before the function f is $1-1$. The above theorem shows that the set of recursive p–adic numbers is a nontrivial subset of the set of p–adic numbers. A specific $x \in \mathbf{Q}_p \setminus \mathbf{Q}_p^c$ can be defined as in the case of the real numbers (the idea is essentially due to Specker). Let f be an $1-1$ enumeration of the halting problem. Then $x = \Sigma p^{f(n)}$ is a non computable p–adic number .

Also it shows that although Q_p^c is countable we cannot enumerate the above set by an effective procedure i.e. Q_p^c is effectively uncountable. It is not unknown to the author whether we can enumerate or not the set of polynomially time computable p–adic numbers by a polynomially time computable function. For the case of the primitive recursive p–adic numbers the corresponding question has negative answer by Theorem 6, page 13.

Theorem 3 *The set of indices representing recursive p–adic numbers is a Π_2 complete set.*

*Proof:*We have the following reduction. For $x \in Tot$ define

$$\phi_{f(x)}(z) = \begin{cases} x + p^{\Sigma_{i \leq z} i}, & \text{if } \phi_x(i) \downarrow \forall i \leq z, \\ \uparrow, & \text{otherwise.} \end{cases}$$

We have that $x \in Tot \Leftrightarrow \phi_{f(x)} \in Q_p^c$ and f is $1-1$. We also have that $x \in Q_p^c \Rightarrow x \in Tot$.

A similar proposition is mentioned in Beeson [1] (p. 67) for the real numbers.

4 Alternative definitions of computable p–adic numbers

Our standard approach is to define a recursive p–adic number as the limit of a recursive Cauchy sequence of rationals with recursive modulus of convergence. There are two alternative ways to define a p–adic number, one is via digit expansion and the other via the Teichmüller representation where the sequence of digits corresponding to a p–adic number is determined by a (total) recursive function. Comparing the constructive versions of these definitions, by Theorem 4, page 11 we have that these two definitions give rise to the same set of numbers.

The motivation for the recursive base p representation of a p–adic number is the following: According to the definition, the base p representation of a p–adic number is:

$$\frac{a_{-m}}{p^m} + \frac{a_{-(m+1)}}{p^{m-1}} + \ldots + \frac{a_{-1}}{p^{-1}} + \Sigma_{j=0}^{\infty} a_j p^j, \qquad a_m \neq 0, m \in \mathbf{Z}.$$

The part of the representation which consists of negative powers of p is finite and thus can be coded by a single number. The part of the representation consisting of positive powers of p is an infinite series, and the coefficients of the positive powers of p are the values of a total recursive function.

Definition 9 *A* recursive base p representation of a p–adic number*, is a natural number e, viewed as an index of a total recursive function ϕ_e such that $\phi_e(0)$ represents the part of x in $\mathbf{Q}_p \setminus \mathbf{Z}_p$ and for $n \geq 1$ $\phi_e(n) \in \{0, 1, \ldots, p-1\}$.*

The notation system consisting of the indices denoting a recursive base p representation of a p–adic number will be denoted by $\mathbb{Q}_p^{c,d}$ (the superscript d stands for digit and the superscript c stands for computable).

The set of indices representing a p–adic number in recursive base p representation can be characterized as follows:

$$x \in Q_p^{c,d} \Leftrightarrow \Big(\phi_x(0) = \langle m, p^n \rangle, \text{ length}(m) \leq n) \wedge (n \geq 1 \Rightarrow 0 \leq \phi_x(n) \leq p-1)\Big).$$

It is straightforward to translate the above definition to an arithmetical definition. Again as in the case of the Cauchy sequence definition of p–adic numbers we have that a p–adic number is an equivalence class defined in a similar manner as in the case of the Cauchy sequence definition.

Definition 10 *(***Moschovakis [15]***) Let N_1, N_2 be two notation systems, and let $F\colon N_1 \to N_2$ be a function or operator defined over equivalence classes of elements of N_1 and taking as values equivalence classes of elements of N_2. Let $[x]$ denote the equivalence class of an element x. A function (operator) F is* recursive *if and only if there*

exists a partial recursive function $f: N_1 \to N_2$ *such that whenever* i *is a member of an equivalence class of* N_1*, then* $f(i)\downarrow$*,* $f(i)$ *is an element of* N_2*,* $[i]_1 = [j]_1 \Rightarrow f(i) = f(j)$*, and* $F([i]_1) = [f(i)]_2$*.*

Definition 11 *(***Moschovakis [15]***) Let* N_1, N_2 *be two notation systems, and let* $F: N_1 \to N_2$ *be a partial function or operator defined over equivalence classes of elements of* N_1 *and taking as values equivalence classes of elements of elements of* N_2*. A function (operator)* F *is* partial recursive *if and only if there exists a partial recursive function* f *such that whenever* i *is a member of an equivalence class* $[i] \in N_1$*, then* $f(i)\downarrow \iff F(i)$ *is defined,* $f(i)$ *is an element of* N_2*,* $[i]_1 = [j]_1 \Rightarrow f(i) = f(j)$*, and* $F([i]_1) = [f(i)]_2$*.*

We note that the standard field operations (division by 0 is undefined) are recursive operators over $\mathbb{Q}_p^c$. We have the following proposition relating the different definitions of computable p–adic numbers:

Proposition 2 *There exists a recursive operator* $f^d: Q_p^{c,d} \to Q_p^c$*. Moreover* f^d *maps* $\mathbf{Q}_p^{c,d}$ *onto* $\mathbf{Q}_p^c$*.*

*Proof:*Let x be an index of a recursive base p expansion of a p–adic number. The sequence defined by:

$$a_n = \phi_x(0) + \Sigma_{i=1}^{n+1}\phi_x(i)p^{i-1},$$

is a Cauchy sequence converging to the p–adic number denoted by x, and has the identity function as modulus of the Cauchy criterion. An index i for this sequence is the value of $f(x)$.

For the onto we have the following. For $x \in \mathbf{Q}_p^c$, let $\{x_n \mid n \in \mathbf{N}\}$ be a Cauchy sequence representing x, with g as modulus of the Cauchy criterion. The sequence of digits of x can be obtained as follows: The part of x in $\mathbf{Q}_p^c \setminus \mathbf{Z}_p$, d is obtained by expanding $x_{g(0)}$ in base p and discarding the part of the result which contains the nonnegative powers of p. For the nontrivial part we have:

$$d(i+1) = \mu y[yp^{i+1} - (d + \Sigma_{j=0}^{i} d(j)p^j - x_{g(i+1)}) \equiv 0 \pmod{p^{i+2}}], \quad i \geq 0.$$

Theorem 4 *The sets of recursive* p*–adic numbers defined as limits of recursive Cauchy sequences with recursive moduli of convergence or as recursive base* p *expansions are the same.*

*Proof:*Follows from the last clause of the previous theorem.

The definition of a recursive p–adic number involves a Cauchy sequence of rational numbers converging to some p–adic number, and the modulus of convergence of this sequence. It is possible to define a notion of recursive p–adic number without the information about the modulus of convergence. The definition which contains the information about the modulus of convergence rate is better as we have from the following theorem that we cannot effectively invert the mapping that maps an index of the recursive base p expansion to an index of Cauchy sequence representation a recursive p–adic number.

Theorem 5 *Let* I_C *be the set of indices of total recursive functions that code a Cauchy sequence of rationals converging to a computable* p*–adic number (with a recursive function*

as modulus of convergence). Let f_d be the natural map, $f_d: Q_p^{c,d} \to I_C$ mapping an index of the recursive base p expansion of $x \in \mathbf{Q}_p^c$ to some index of an effective Cauchy sequence representing $x \in \mathbf{Q}_p^c$. Then there is no recursive function $f: I_C \to Q_p^{c,d}$ such that for i an index of a recursive base p expansion of a recursive p–adic number we have $[i] = [f_d(f(i))]$.

*Proof:*Suppose that such f exists, i.e. for x an index of a Cauchy sequence representing a recursive p–adic number, $f(x) \in Q_p^{c,d}$ and $[f_d(f(x))] = [x]$. Define $g : I_C \times \mathbf{N} \to I_C$ as follows:

$$g(m,t) = \begin{cases} 0, & \text{if } \forall u \leq t,\ f(m) \uparrow \text{ in } u \text{ steps, or } \phi_{f(m)}(1) \uparrow \text{ in } u \text{ steps,} \\ 1, & \text{if } \exists u \leq t,\ f(m) \downarrow \text{, and } \phi_{f(m)}(1) = 0, \text{ and the number of} \\ & \text{steps required for both computations is less than } u, \\ p & \text{if } \exists u \leq t,\ f(m) \downarrow \phi_{f(m)}(1) \neq 0, \text{ and the number of steps} \\ & \text{required for both computations is less than } u. \end{cases}$$

By the recursion theorem there exists a number $m \in \mathbf{N}$ such that for all $t \in \mathbf{N}$ $g(m,t) = \phi_m(t)$. We have that $f(m)$ is defined for all $m \in I_C$, $\phi_{f(m)} \in \{0, \ldots, p-1\}$, hence $g(m,t)$ is total so $\phi_m(t)$ is total. Thus for $m \in I_C$ eventually one of the last two clauses in the definition of g will be true. From this we have that for $m \in I_C$, ϕ_m represents a rational integer (viewed as an element of I_C). Hence we have $m \neq 0$, since eventually the computation will halt. In both cases we get the contradiction $[\phi_m] \neq [\phi_{f_d(f(m))}]$, since these two classes they differ at the first digit of their base p expansion.

One more reason for including the information about the convergence rate of a recursive sequence of rationals is that without this information it is not possible to determine effectively the digits of of the number (at base p expansion) that correspomnds to the limit of the sequence. Also such an approach would include as computable the number $\Sigma_{n=0}^{\infty} p^{f(n)}$, where $f(n)$ is a 1-1 recursive function enumerating K (or any other r.e. non recursive set).

5 Primitive recursive p–adic numbers

One of the basic subclasses of the class of recursive functions is the class of primitive recursive functions. This class of functions gives rise to a subclass of the recursive p–adic numbers: the p–adic numbers defined via primitive recursion.

It is well known in the theory of of recursive functions that the class of primitive recursive functions is less rich than the class of recursive functions. The reason for this is that the definitions by primitive recursion are simple definitions. As in the case of the recursive p–adic numbers we have that the set of indices denoting a primitive recursive p–adic number is not a recursive set and as a consequence this set has not primitive recursive characteristic function.

Lemma 1 *There exists a recursive function f such that: 1) For W_e an infinite recursively enumerable subset of $\mathbf{N}$, $f(e)$ is an index of a primitive recursive sequence of rational numbers that converges to a p–adic number with linear modulus of convergence. 2) For W_e a finite recursively enumerable subset of $\mathbf{N}$ $f(e)$ is an index for a finite sequence of rational numbers.*

*Proof:*Assume without loss of generality that $|W_e^{s+1} \setminus W_e^s| \leq 1$ Given W_e a recursively enumerable subset of $\mathbf{N}$ define a sequence $\{b_n \mid n \in \mathbf{N}\}$ as follows: Stage 0: Let $b_0 = 0$. Stage s+1: Let s_0 be the maximum of 0 and the last z+1 $< s$+1 such that $W_e^{z+1} \setminus W_e^z \neq \emptyset$. If $W_e^{s+1} \setminus W_e^s = \emptyset$, do nothing. If $W_e^{s+1} \setminus W_e^s \neq \emptyset$ then define $b_i = 0$ for $s_0 < i \leq s$ and $b_{s+1} = p^{s+1}$. The sequence $\{b_n \mid n \in \mathbf{N}\}$ is infinite for W_e infinite and $v(b_s) = s + 1$ for $b_s \neq 0$. Hence we have that $\{b_n \mid n \in \mathbf{N}\}$ converges to 0 with linear modulus of convergence. The above calculations are primitive recursive, hence the limit of the series is a primitive recursive p–adic number. The value of $f(e)$ is an index for this sequence. If W_e is finite then there exists an index i such that b_i is undefined for $n \geq i$. The value of $f(e)$ in this case is is an index for the above (finite) sequence.

Theorem 6 *The set of indices denoting a primitive recursive p–adic number is not a recursive set.*

*Proof:*Suppose it is. Then from the above lemma, for each e such that W_e is infinite we have that $f(e)$ is an index for a primitive recursive sequence of rational numbers that has a linear modulus of convergence. For e such that W_e is finite, $f(e)$ is an index for a finite sequence of rational numbers. Hence

$$e \in \{e \mid W_e \text{ is infinite } \} \iff \langle f(e), Id \rangle \in \mathbf{Q}_p^{PR},$$

which gives that the former set is decidable which is a contradiction. A somewhat similar theorem was proved by C. Jockush [11] (unpublished), under the assumption of decidable equality and that the carrier set is the set of natural numbers.

6 Algebraic properties of the recursive p–adic numbers

A standard question when dealing with some structure is determining whether it is closed with respect to certain operators. In the case of the p–adic fields the relevant closure is the notion of being p–adically closed, which implies that the field under consideration is elementarily equivalent with the field of p–adic numbers. As a consequence we have that a p–adically closed field satisfies the same first order axioms as the field of p–adic numbers.

Definition 12 *A valued field F, with $\mathcal{V}$ as the valuation ring is* p–adically closed *iff:*

1. *The residue field is $\mathbb{F}_p$ the finite field of p elements.*
2. *The value group of the field satisfies the axioms of $Th(\mathbf{Z}, +, <)$*
3. *The element $v_p(p)$ is the least positive element of the value group.*
4. *The characteristic of the field is* 0.
5. *The valued field $\langle F, \mathcal{V}, \mathcal{O} \rangle$ is Henselian.*

The important clause in the definition of p–adically closed is the clause for the field being Henselian. This clause gives conditions for the existence of roots of polynomial equations.

We have the following lemmata which are also a point of difference compared with the real number case.

Lemma 2 *The rational operators are continuous over $\mathbb{Q}_p^c$ (either in base p representation or as limits of Cauchy sequences).*

Lemma 3 *Let $f \in \mathbb{Q}_p^c[x](\mathbb{Z}_p^c[x])$ then $\forall n, f^{(n)} \in \mathbb{Q}_p^c[x](\mathbb{Z}_p^c[x]$ resp.).*

*Proof:*The formulae for the calculation of the derivatives are computable since they involve elementary algebra.

Theorem 7 *The recursive p–adic numbers $\mathbf{Q}_p^c$ form a p–adically closed field.*

The first four clauses in the definition of a p–adically closed field are trivially satisfied since $\mathbf{Q}_p^c \subseteq \mathbf{Q}_p$, so we need only to show that $\mathbf{Q}_p^c$ is Henselian. The proof of that is straightforward application of Newton's method. Let $f \in \mathbf{Z}_p^c[x]$, and let $\bar{f}(x) \in \mathbb{F}_p[x]$ be the polynomial obtained from f by reducing the coefficients of $f \pmod p$. Let f' be the formal derivative of f. Suppose that a is a number in $\mathbb{F}_p$ such that $\bar{f}(a) \equiv 0 \pmod p$, and $\bar{f}'(a) \not\equiv 0 \pmod p$, so $v_p(f(a)) > 0$ and $v_p(f'(a)) = 0$. Letting $n = deg(f)$, the Taylor expansion of f and f' gives that:

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \frac{f'''(x)}{3!}h^3 + \cdots + \frac{f^n(x)}{n!}h^n, \tag{4}$$

$$f'(x+h) = f'(x) + f''(x)h + \frac{f'''(x)}{2!}h^2 + \cdots + \frac{f^n(x)}{(n-1)!}h^{n-1}. \tag{5}$$

We have that the above expressions are computable since the coefficients of f are computable. Also we have that the factor $i!$ present in the ith summand does not affect the p–adic value of this summand since $i!$ divides the coefficients of the ith derivative of a polynomial. Let:

$$a_0 = a, \quad e_0 = -\frac{f(a_0)}{f'(a_0)}, \quad a_1 = a_0 + e_0.$$

Since $\bar{f}(a) \equiv 0 \pmod p$ and $\bar{f}'(a) \not\equiv 0 \pmod p$ we have that $v_p(h) \geq 1$. Substituting in equations (4) and (5) $x = a_0$ and $h = e_0$, and setting $a_1 = x + h = a_0 + e_0$ we have:

$$f(a_1) = \left(-\frac{f(a_0)}{f'(a_0)}\right)^2 \left[\frac{f''(a_0)}{2!} - \frac{f(a_0)}{f'(a_0)}\left(\frac{f'''(a_0)}{3!} + \cdots\right)\right], \tag{6}$$

and

$$f'(a_1) = f'(a_0) - \frac{f(a_0)}{f'(a_0)}\left[f''(a_0) + \cdots\right], \tag{7}$$

The terms in the square bracket in equation (6) have value ≥ 0, since the coefficients of the polynomial f and the derivatives are elements of $\mathbf{Z}_p$, and the factor $i!$ in the derivatives does not affect the valuation of the polynomials, hence we have:

$$v_p(f(a_1)) \geq 2v_p\left(-\frac{f(a_0)}{f'(a_0)}\right). \tag{8}$$

The term

$$-\frac{f(a_0)}{f'(a_0)}\left[f''(a_0) + \cdots\right], \tag{9}$$

in equation (7) has value ≥ 1, since $v\left(-\frac{f(a_0)}{f'(a_0)}\right) = 1$, and the value of the term in the square brackets in equation (9) is ≥ 0, so $f'(a_1)$ has value 0. Let $e_0 = h$. For $e_1 = -\frac{f(a_1)}{f'(a_1)}$ we have that $v_p(e_1) \geq 2$. Inductively, define for $n \geq 2$ the following sequences:

$$a_{n+1} = a_n + e_n, \quad e_n = -\frac{f(a_n)}{f'(a_n)}.$$

We have then the following by induction:

$$\begin{aligned} v_p\left(f\left(a_n\right)\right) &\geq 2^n, && (10)\\ v_p\left(f'\left(a_n\right)\right) &= 0, && (11)\\ v_p\left(e_n\right) &\geq 2^n, && (12)\\ a_n &\in \mathbf{Z}_p. && (13) \end{aligned}$$

The base steps have been established so the inductive steps remain to be proved.

1) Suppose $v_p(f(a_n)) \geq 2^n$. We have:

$$f(a_{n+1}) = \left(-\frac{f\left(a_n\right)}{f'\left(a_n\right)}\right)^2 \left[\frac{f''\left(a_n\right)}{2!} - \frac{f\left(a_n\right)}{f'\left(a_n\right)}\left(\frac{f'''\left(a_n\right)}{3!} + \cdots\right)\right],$$

The value of the term in the square brackets is ≥ 0, since $a_n \in \mathbf{Z}_p$, the derivatives $f^{(n)}$ are polynomials with coefficients in $\mathbf{Z}_p$, and $v_p(f'(a_n)) = 0$. Hence $v_p(f(a_{n+1})) \geq 2v_p(f(a_n)) \geq 2^{n+1}$.

2) Since

$$f'(a_{n+1}) = f'(a_n) - \frac{f(a_n)}{f'(a_n)}\left[f''(a_n) + \cdots\right],$$

we have that $v_p(f'(a_{n+1})) = 0$, because

$$v_p\left(\frac{f(a_n)}{f'(a_n)}\left[f''(a_n) + \cdots\right]\right) \geq 1, \quad \text{and} \quad v_p\left(f'\left(a_n\right)\right) = 0.$$

3) We have:

$$v_p(e_{n+1}) = v_p(-1) + v_p\left(f\left(a_{n+1}\right)\right) - v_p\left(f'\left(a_{n+1}\right)\right) \geq 2^{n+1}.$$

4) This follows since $a_n = a_{n-1} + e_{n-1}$ and $v_p(a_{n-1}) \geq 0\,, v_p(e_{n-1}) \geq 0$. Also:

$$\begin{gathered} v_p(a_n - a_{n+k}) = \\ = v_p(\Sigma_{i=n+1}^{k} e_i) \geq \\ \geq \min\left\{v_p(e_i) \mid n+1 \leq i \leq k\right\} \geq \\ \geq v_p(e_{n+1}) \geq 2^{n+1}. \end{gathered}$$

Let x be the root of the polynomial that the sequence $\{a_n \mid n \in \mathbf{N}\}$ determines. In order to show that x is a recursive p–adic number we have to exhibit a recursive sequence of rational numbers $\{b_n \mid n \in \mathbf{N}\}$ which converges to x with a recursive function as modulus of convergence. The modulus of convergence can be obtained from the above analysis and is $g(n) = \log(n)$. To obtain a rational number $b_{g(n)}$ such that $|b_{g(n)} - x| < p^{-n}$ we have to obtain a rational approximation $\bar{c}_i$ to each of the coefficients c_i of the

polynomials f and f' such that $|\bar{c}_i - c_i| < p^{-n}$, since the modulus of continuity of the rational operators is linear. This can be done uniformly since the coefficients are finitely many how do we extract the coefficients?? they are given by the statement f in qpc and are recursive p–adic numbers. Also the factor $i!$ present in the coefficients of f' is a constant and hence does not affect the computability of the coefficients of f'. Having the rational approximations of the coefficients then we have to iterate the above procedure for $\lceil \log(n) \rceil + 1$ steps to obtain (the rational number) b_n. We have that the sequence $\{b_n \mid n \in \mathbf{N}\}$ is a Cauchy sequence of rational numbers and the modulus of convergence which is $O(\log n)$, hence x is a computable p–adic number.

The importance of the above proposition lies in the fact that we have a uniform algorithm, and that the convergence rate of the algorithm is exponential. The convergence rate is well known for the real number case and is the same [19]. Also related with the present proof is a proof of a similar statement in Mazur [14] using Newton's method for the real numbers.

As we can see from the above proof, we have that for x a root of the polynomial f in order to obtain a p–adic number z such that $|z - x| \leq p^{-n}$ we have to iterate the algorithm which determines the sequence $\{a_n \mid n \in \mathbf{N}\}$ for $\lceil \log(n) \rceil - 1$ steps. From this observation we have also the following Theorems:

Theorem 8 *The polynomially time computable p–adic numbers are a p–adically closed field.*

*Proof:*For $f = \Sigma_{i=0}^{k} a_i x^i \in \mathbf{Z}_p^{\mathcal{P}}[x]$, $n \in \mathbf{N}$ and $x \in \mathbb{F}_p$ simple root of $\bar{f}$, in order to obtain $z \in \mathbf{Q}_p^{\mathcal{P}}$ such that $|z - x| \leq p^{-n}$ we have to iterate the above algorithm for $\lceil \log(n) \rceil - 1$ steps. For each coefficient a_i of f, we also need to determine a p–adic integer $\bar{a}_i$ such that $|\bar{a}_i - a_i| \leq p^{-n}$. This can be accomplished for all the coefficients of f in time bounded by a polynomial in n since the number of the coefficients is k. For the calculations of the derivative f', the ith term of f' can be calculated in time bounded by a polynomial. This is because each a_i is polynomially time computable, and $i!$ is constant. To determine now the approximation to the root we have to iterate the algorithm for $\lceil \log(n) \rceil - 1$ steps. From the above analysis we have a calculation bounded by a polynomial.

Theorem 9 *The primitive recursive p–adic numbers form a p–adically closed field.*

*Proof:*The above algorithm is a primitive recursive algorithm, since to obtain correctly n digits we have to calculate up to the $(\lceil \log(n) \rceil - 1)$th term of the sequence a_n and each coefficient of the polynomial is a primitive recursive p–adic number. Also the coefficients of the derivative f' can be calculated by a primitive recursive procedure.

A point of interest here is that the analogous closure property for the polynomially time computable real numbers (real closed) is proved in a different manner than the one for the p–adic case by H. Friedman and Ker – I Ko [6]. The statement for the polynomially time computable real numbers depends on the complexity of the roots of analytic functions. In the case of real numbers an upper bound for the complexity of roots of analytic polynomially time computable functions is proved. From this upper bound we have that roots of polynomials with polynomially time computable coefficients are polynomially time computable.

7 Notation systems for p–adic fields

In the present section we try to characterize abstractly the set of natural numbers that represent the recursive p–adic numbers and give an abstract characterization of the set of equivalence classes of such indices. The motivation is the analogous work for the computable real numbers by Moschovakis [15].

Definition 13 *A* recursive field *is a notation system with four recursive operators representing the rational operations over the field. For the case of the division (or multiplicative inverse) we postulate that the operation is undefined at* 0.

In the case of the p–adic fields there is more structure, namely the valuation. In the case of the recursive p–adic numbers there is an effective procedure to determine the valuation of a non zero element. It is impossible to determine effectively the valuation 0 because if not it would be possible to decide equality between indices for recursive p–adic numbers.

Definition 14 *A* recursive valued field F *is a recursive field with a recursive operator representing the valuation. The value group G is a group such that the group operations are represented by recursive functions. The valuation function $v\colon F \to G$ is a (partial) recursive operator undefined at* 0.

One of the fundamental properties of the field of the p–adic numbers is that it is maximal in the sense that it is the topological completion of the field of the rational numbers with respect to the p–adic valuation. From this maximal characterization we have that fields containing $\mathbf{Q}$ as a subfield and containing limits of Cauchy sequences can be embedded into $\mathbf{Q}_p$. The recursive valued field representing the recursive p–adic numbers has a similar maximal property.

Proposition 3 *Let F be a countable non-Archimedean recursive valued field satisfying:*

1. *The residue field of F is isomorphic to $\mathbb{F}_p$, the finite field of p elements,*
2. *The value group $v(F)$ is isomorphic to $\langle \mathbf{Z}, +, < \rangle$,*
3. *The element $v(p)$ is the least positive element of the value group of F,*
4. *The characteristic of the field F char(F) equals* 0.

Then there exists a unique recursive embedding of F in $\mathbb{Q}_p^c$ which preserves the valuation.

*Proof:*Let $\mathbb{Q}$ be the set of notations for the rational numbers in Q_p^c. Since char(F)=0 the field of rational numbers is a subfield of F. Let $+_F, -_F, *_F, /_F$ be indices for the partial recursive functions which represent the rational operations over F.

Let $\mathbf{0}_F, \mathbf{1}_F$ be indices for $0, 1$ considered as elements of F. From these indices using the indices for the rational operators we can define a recursively enumerable set of indices $\widehat{Q}$ which contains at least one index for each rational number. This set equipped with the natural operations and the valuation is a countable recursive valued field. The identity function is a natural field isomorphism $I\colon \widehat{Q} \to \mathbb{Q}$, which preserves the valuation function since $v(p)$ is the least element of the value group of both fields.

The field of rational numbers is topologically dense in F. To show this, for $x \in F$ and $n \in \mathbf{N}$ dovetail over the set of indices y for rational numbers, until a y is found such that $v(x-y) = n$ and let:

$$a_n = \mu y \left[y \in \widehat{Q} \wedge v(x-y) = n \right], \tag{14}$$

Such element y exists since $v(F) = v(F-x) \simeq \langle \mathbf{Z}, +, < \rangle$. The sequence $\{a_n \mid n \in \mathbf{N}\}$ gives a sequence of rational numbers which satisfies $v(a_n - x) = n$ for all $n \in \mathbf{N}$. Hence an element of F can be defined as a limit of (indices) of sequences of rational numbers. The sequence $\{a_n \mid n \in \mathbf{N}\}$ in equation 14, page 18 is a Cauchy sequence of rational numbers with the identity function as modulus of convergence. The sequence $\{I(a_n) \mid n \in \mathbf{N}\}$ is a recursive Cauchy sequence of indices for rational numbers in $\mathbb{Q}_p^c$ and has the identity function as modulus of convergence, hence converges to an element z of $\mathbb{Q}_p^c$. Extend I to F by continuity by defining: $\bar{I}(x) = z$.

By continuity of the rational operators we have that $\bar{I}: F \to \mathbb{Q}_p^c$ is a field isomorphism and also preserves the valuation function. The uniqueness of $\bar{I}$ follows from the uniqueness of the choice of the sequence of rational numbers in Eq. 14 which is used to approximate a p–adic number.

Proposition 3 now easily gives a uniqueness characterization of the fields of computable p–adic numbers.

Theorem 10 *A countable field of p–adic numbers is value isomorphic to a non Archimedean recursive valued field F satisfying 1) – 4) of Proposition 3, page 17 if and only if all elements of F are recursive p–adic numbers.*

*Proof:*Let F_1 be a countable subfield of the field of p–adic numbers, value isomorphic to a recursive valued field F as in the statement of the Theorem via $i: F_1 \to F$. If f is the recursive embedding of F into $\mathbb{Q}_p^c$ from the previous Proposition, then $i \circ f: F_1 \to \mathbb{Q}_p^c$ is a value isomorphism from F_1 to $\mathbb{Q}_p^c$. Since the only possible such isomorphism is the identity we have $F \subseteq \mathbb{Q}_p^c$.

From Proposition 3, page 17 we have a maximal characterization of the field of recursive p–adic numbers. However the field of recursive p–adic numbers is not maximal among countable models of the axioms of a p–adic field.

Theorem 11 *There exists a countable non–Archimedean valued field satisfying 1) – 4) of Proposition 3 properly extending $\mathbb{Q}_p^c$.*

*Proof:*Take $\mathbb{Q}_p^c$ and add an index for a non computable p–adic number then close with respect to the rational operations. Such an index exists by the discussion on page 4, and 3.

Having a class of structures (in the present case fields with valuation) gives rise to the isomorphism problem i.e. under what conditions are two members of the class isomorphic. For recursive structures we can refine the question to ask for a recursive isomorphism. One answer is having a classical isomorphism, and the other one is having an isomorphism which is a recursive operator. In the case of recursive structures the inverse operators should be recursive as well. In the particular case of fields with a valuation the isomorphism should preserve the valuation as well. The motivation for this group of question comes form Moschovakis [15] where a set of similar problems are discussed for the computable real numbers.

In the previous section it was shown that for every recursive valued field F satisfying some more conditions, there is a natural embedding $i: F \to \mathbb{Q}_p^c$ which preserves the valuation. The following questions arise as well:

1) Under what conditions is an embedding $i: F \to \mathbb{Q}_p^c$ onto? (so i is a classical isomorphism).

2)Under what conditions is $i: F \to \mathbb{Q}_p^c$ a recursive isomorphism?

The answer to the first question gives a characterization of the field of recursive p–adic numbers. The answer to the second question will characterize $\mathbb{Q}_p^c$ as a notation system.

The problem in 1 (classical case) is solved by requiring the field to be (Cauchy) complete. In 2 (recursive fields) the solution is obtained by constructivizing the notion of Cauchy completeness [15].

Definition 15 *Let F, G be two recursive fields. If there is a recursive operator $f: F \to G$ which is a field isomorphism and $f^{-1}: G \to F$ is a recursive operator as well then F and G are* recursively isomorphic. *In the case of recursive valued fields, we require that the isomorphism preserves the valuation as well.*

Definition 16 *A sequence $\{a_n \mid n \in \mathbf{N}\}$ of elements of $\mathbb{Q}_p^c$ is called* recursive *if and only if there is a total recursive function f such that $\forall n \in \mathbf{N}\ [f(n)] = a_n$. An index for the function f is called an index of $\{a_n \mid n \in \mathbf{N}\}$.*

Definition 17 *A sequence $\{a_n \mid n \in \mathbf{N}\}$ of elements of $\mathbb{Q}_p^c$ is called* recursively Cauchy *if and only if there is a (total) recursive function m such that $i, j \geq m(n) \Rightarrow | a_i - a_j | \leq p^{-n}$.*

Definition 18 *A field of computable p–adic numbers F is called* (weakly) recursively complete *if and only if every recursive, recursively Cauchy sequence of elements of F converges to an element $x \in F$.*

Definition 19 *A field of computable p–adic numbers F is called* strongly recursively complete *if there exists a (partial) recursive function c of two arguments, (called* a completeness function *for F) defined over $\mathbb{Q}_p^c \times \mathbf{N}$ and taking values in $\mathbb{Q}_p^c$ such that if $\{a_n \mid n \in \mathbf{N}\}$ is a recursive recursively Cauchy sequence of elements of F with index i, and m an index for the modulus of convergence, then $\lim_{n\to\infty} a_n = c(i, m)$.*

Theorem 12 *Let F be a recursive valued field satisfying 1)–4) of Proposition 3. If F is weakly recursively complete then the natural embedding $i: F \to \mathbb{Q}_p^c$ is onto, so F is isomorphic to $\mathbb{Q}_p^c$, and the isomorphism preserves the valuation. If F is strongly recursively complete then the above isomorphism is a recursive function.*

*Proof:*As in the proof of Proposition 3, page 17 $\mathbf{Q}$ is a subfield of F. Let Q be the set of equivalence classes of notations for the rational numbers in F. For $x \in \mathbb{Q}_p^c$, there is a recursive Cauchy sequence $\{x_n \mid n \in \mathbf{N}\}$ of rational numbers converging to x with a recursive function as modulus of convergence.

Taking the inverse image of this sequence via the identity function over the rationals, we have a recursive Cauchy sequence in F which sequence has the same modulus of convergence. This sequence must converge to some element of $z \in F$. By continuity we have $i(z) = x$. The valuation of a nonzero element x is obtained from the sequence of the rational numbers that define x.

For the second part, the following defines a recursive function from $\mathbb{Q}_p^c$ to F: Given $x \in \mathbb{Q}_p^c$, there exists a recursive recursively Cauchy sequence of rational numbers $\{x_n \mid n \in \mathbf{N}\}$, such that $\{x_n \mid n \in \mathbf{N}\}$ is recursive and converges recursively to x with modulus $\mathcal{M}$. We can take $i^{-1}(x_k)$ in F, and use the completeness function of F on an index of $\{i^{-1}(x_k) \mid n \in \mathbf{N}\}$ with modulus of continuity $\mathcal{M}$ to get $i^{-1}(x)$.

Definition 20 *Let F be a notation system with a recursive valuation. The valuation function* describes *F if and only if there exists a recursive function $\mathcal{D}: \mathbf{N} \to \mathbf{N}$ such that for any recursive function f with index i, for any $x_0 \in F$, and all $x \in F \setminus [x_0]$ we have:*

$$\Big(f(x) = n \Leftrightarrow v(x - x_0) = n\Big) \quad \Longrightarrow \quad \mathcal{D}(i) \in [x_0].$$

The motivation for the notion of the description function is that from information about the valuation of the numbers $x_0 - x$ (approximations to x_0) it is possible via $\mathcal{D}$ to obtain effectively an index of x_0. The notion of description function will make it possible to give a characterization of $\mathbb{Q}_p^c$ (Theorem 14, page 20). First we have a straightforward property of $\mathbb{Q}_p^c$.

Proposition 4 *$\mathbb{Q}_p^c$ is described by the valuation function.*

*Proof:*Let Q be the set of indices for the rational numbers in $\mathbb{Q}_p^c$ obtained from some indices of $0, 1 \in \mathbb{Q}_p^c$ via some indices for the rational operations. For $x_0 \in Q_p^c$ and $n \in \mathbf{N}$ we can determine $y \in Q$ by dovetailing over elements of Q until a y is found such that $v(x_0 - y) = n$. This procedure defines a recursive function f. Let i be an index for a recursive function f. Then the following sequence (defined by equation 15 below) is a recursive Cauchy sequence and converges to x_0 with the identity function as modulus of the Cauchy criterion. Let j be an index of the following function:

$$n \mapsto \mu z[z \text{ is a code for an element of } \mathrm{Q} \wedge f(z) = n]. \tag{15}$$

Then $\mathcal{D}(i) = j$.

Theorem 13 *Let F be a non–Archimedean recursive valued field satisfying 1)–4) of Proposition 3, and described by the valuation function. Suppose that the natural embedding $i: F \to \mathbb{Q}_p^c$ is onto. Then i^{-1} is recursive hence F and $\mathbb{Q}_p^c$ are recursively isomorphic.*

*Proof:*Let Q be defined as in the proof of Proposition 4. Let $i: F \to \mathbb{Q}_p^c$ be the natural embedding over an r.e. set of indices for the set of rational numbers. For $x \in \mathbb{Q}_p^c$, and $n \in \mathbf{N}$ we can determine a $y \in Q$ by dovetailing over elements of Q until a y is found such that $v(x - y) = n$. Let f be an index for the following sequence:

$$n \mapsto \mu y[v(i(y) - x) = n].$$

Then

$$i^{-1}(x) = \mathcal{D}(f).$$

The above statement can give a characterization of $\mathbb{Q}_p^c$ which can avoid some of the recursion theoretic assumptions.

Theorem 14 *Up to recursive isomorphism $\mathbb{Q}_p^c$ can be characterized as follows:*

1. *The residue field of F is isomorphic to $\mathbb{F}_p$,*

2. *The value group $v(F)$ is isomorphic to $\langle \mathbf{Z}, +, < \rangle$,*

3. *$v(p)$ is the least positive element of the value group of F,*

4. *$char(F) = 0$,*

5. *$\mathbb{Q}_p^c$ is described by the valuation function.*

*Proof:*Follows from Theorem 13.

Definition 21 *(***Moschovakis***) A predicate $P(a_1, \ldots, a_n)$ defined over a notation system N is* recursively enumerable *if there is a recursive function f of arity n such that for any tuple of indices $(i_1, \ldots, i_n)$ we have:*

$$P([i_1], \ldots, [i_n]) \iff f(i_1, \ldots, i_n) \downarrow .$$

A predicate $P(a_1, \ldots, a_n)$ over a notation system is recursive *if both P and its negation are recursively enumerable.*

The above definition enables us to give one more property of $\mathbb{Q}_p^c$.

Theorem 15 *No non–trivial predicates defined over $\mathbb{Q}_p^c$ are recursive.*

*Proof:*This follows from Rice's theorem, since the set of indices that correspond to recursive p–adic numbers is not $\mathbf{N}$ and not $\emptyset$.

Acknowledgments The present work is part of the author's Ph.D. thesis. The author would like to express his deep acknowledgement to my thesis advisor Prof. D. Marker and Prof. J. Baldwin, J. Berman, W. Howard, and R. Sloan for serving on my defense committee and for the valuable suggestions that they offered.

References

[1] M. Beeson. *Foundations of Constructive Mathematics*. Springer Verlag, 1980.

[2] E. Bishop. *Foundations of Constructive Analysis*. Mac Grow–Hill, 1967.

[3] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completenes, recursive functions and universal machines. *Bulletin of American Mathematical Society (New Series)*, 21:1–46, 1989.

[4] Z. I. Borevitch and I. R. Shafarevitch. *Number theory*. Academic Press, 1966.

[5] J. W. S. Cassels. *Local Fields*. Cambridge University Press, Cambridge, 1986.

[6] H. Friedman and K. Ko. Computational complexity of real functions. *Theoretical Computer Science*, 20:323–352, 1982.

[7] A. Gregorczyk. Computable functionals. *Fund. Math.*, 42:168–202, 1955.

[8] A. Gregorczyk. On the definitions of computable real continuous functions. *Fund. Math.*, 44:61–71, 1957.

[9] F. Q. Guvea. *p–adic numbers, an introduction*. Springer–Verlag, 1997.

[10] A. Heyting. *Intuitionism*, volume I, II. North Holland, third edition, 1971.

[11] C. Jockush. The primitive recursive reals do not form a recursive field. Unpublished, 1984.

[12] N. Koblitz. *p-adic numbers, p-adic analysis and zeta functions*. Springer–Verlag, 1984.

[13] B. A. Kushner. *Lectures on Constructive Mathematical Analysis*. Nauka, 1973.

[14] S. Mazur. Recursive analysis. *Rozprawy Matematiczne – (Dissertationes Math.)*, 33, 1963.

[15] Y. Moschovakis. Notation systems and recursive ordered fields. *Comp.Math.*, 17:40–71, 1965.

[16] A. Mostowski. On computable sequences. *Fund. Math.*, 44:37 – 55, 1957.

[17] M. B. Pour-El and J. Richards. *Computability in Mathematics and Physics*. Springer Verlag, 1988.

[18] H. G. Rice. Recursive real numbers. *Proc. Amer. Math. Soc.*, 5:784–791, 1954.

[19] J. Stoer and R. Bulirsh. *Introduction to Numerical Analysis*. Springer Verlag, 1980.

[20] A. M. Turing. On computable numbers, with an application to the entscheidungs problem. *Proc. London Math. Society*, 42:230–265, 1937.