AN INTRODUCTION TO p-ADIC SYSTEMS: A NEW KIND OF NUMBER SYSTEMS INSPIRED BY THE COLLATZ $3n+1$ CONJECTURE

MARIO WEITZER

ABSTRACT. This article introduces a new kind of number systems on p-adic integers which is inspired by the well-known $3n+1$ conjecture of Lothar Collatz. A p-adic system is a piecewise function on $\mathbb{Z}_p$ which has branches for all residue classes modulo p and whose dynamics can be used to define digit expansions of p-adic integers which respect congruency modulo powers of p and admit a distinctive "block structure". p-adic systems generalize several notions related to p-adic integers such as permutation polynomials and put them under a common framework, allowing for results and techniques formulated in one setting to be transferred to another. The general framework established by p-adic systems also provides more natural versions of the original Collatz conjecture and first results could be achieved in the context. A detailed formal introduction to p-adic systems and their different interpretations is given. Several classes of p-adic systems defined by different types of functions such as polynomial functions or rational functions are characterized and a group structure on the set of all p-adic systems is established, which altogether provides a variety of concrete examples of p-adic systems. Furthermore, p-adic systems are used to generalize Hensel's Lemma on polynomials to general functions on $\mathbb{Z}_p$, analyze the original Collatz conjecture in the context of other "linear-polynomial p-adic systems", and to study the relation between "polynomial p-adic systems" and permutation polynomials with the aid of "trees of cycles" which encode the cycle structure of certain permutations of $\mathbb{Z}_p$. To outline a potential roadmap for future investigations of p-adic systems in many different directions, several open questions and problems in relation to p-adic systems are listed.

CONTENTS

2010 *Mathematics Subject Classification.* Primary: 11S82, Secondary: 11A63, 11C08.
Key words and phrases. p-adic systems, number systems, permutation polynomials, Collatz conjecture.

1. Introduction and motivation

The aim of this paper is to introduce a new kind of number systems on the p-adic integers denoted by *p-adic systems* and to derive first non-trivial results. It is the author's hope that p-adic systems will provide a useful framework to describe several deeply mysterious phenomena (a central one being the famous Collatz conjecture or $3n+1$-problem) which will allow to express related results thus far contained in conceptionally and notationally isolated papers in terms of a common language, but also to gain entirely new results and insights. While problems such as the Collatz conjecture may remain a distant goal at the horizon, embedding them into a set of related yet more accessible questions will, hopefully, indicate a path in the right direction.

In order to motivate the definition of p-adic systems, we will start by repeating the statement of the $3n+1$-problem formulated by the German mathematician Lothar Collatz in 1937. For that we define the transformation

$$\mathrm{F}_C : \mathbb{N} \to \mathbb{N}. \tag{1.1}$$
$$n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{3n+1}{2} & \text{if } n \equiv 1 \mod 2 \end{cases}$$

Applying F_C repeatedly, one finds that the orbit of any natural number up to 2^{60} [46, 51] eventually reaches 1 where it enters the 2-cycle $(1, 2)$. Remarkably, despite the extremely simple formulation and high popularity of the problem (for an extensive overview of related work see [33, 34, 35, 58] which can all be found in the book [36], and [58]), it has remained unproven for more than 80 years and it appears that we are no closer to a solution than Lothar Collatz was when he first found it. To continue we consider the slightly modified transformation

$$\mathrm{F}_2 : \mathbb{N}_0 \to \mathbb{N}_0. \tag{1.2}$$
$$n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{n-1}{2} & \text{if } n \equiv 1 \mod 2 \end{cases}$$

It is of course the transformation which can be used to compute the standard binary expansion of a natural number by taking its orbit modulo 2. Obviously, the orbit of any natural number under F_2 eventually enters the 1-cycle (0). By simply replacing the linear polynomial $3x+1$ by another linear polynomial $(x-1)$ the question for the ultimate behavior of the corresponding transformation changes from extremely hard to trivial. Yet, there is one decisive property which the orbits produced by both transformations have in common, i.e. that they can be used to define a "number system" on the p-adic integers that satisfies a rather natural condition. It is this property which will be central to the definition of p-adic systems. Clearly, the definitions of both F_C and F_2 naturally extend to the 2-adic integers (for an introduction to p-adic integers see e.g. [40, 20, 25]) with the only parts to change being the domains and codomains:

$$\mathrm{F}_C : \mathbb{Z}_2 \to \mathbb{Z}_2, \qquad \mathrm{F}_2 : \mathbb{Z}_2 \to \mathbb{Z}_2. \tag{1.3}$$
$$n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{3n+1}{2} & \text{if } n \equiv 1 \mod 2 \end{cases} \qquad n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \equiv 0 \mod 2 \\ \frac{n-1}{2} & \text{if } n \equiv 1 \mod 2 \end{cases}$$

The term "number system" above is put in quotation marks, as there is no strict definition of what a number system "of" or "on" some set X actually is. To the author's mind it is something that can be used to give unique "names" (in our case infinite strings over a finite alphabet) to all elements of said set X which, ideally, are not chosen at random but follow certain rules and encode some information on the represented elements. Examples would be the usual binary or decimal representations of natural numbers which come with easy algorithms that allow fast addition and multiplication of the represented numbers but, somewhat mysteriously, are of no good use when trying to obtain the factors of, say, the product of two large primes. The information on the factors is encoded in the digits of the product, but cannot easily be extracted. Alternatively, a natural number can be represented by giving a list of its prime factors which could also be considered a number system on $\mathbb{N}$. In this setting multiplication and factorization are straight forward, but

in return addition is just as hard as factorization is in the other setting. That there appears to be no number system allowing for fast addition, multiplication and factorization all at once, is a phenomenon at the heart of many of the biggest open problems in mathematics today. The idea of defining number systems on arbitrary sets X by iterative application of some transformation on X led to the very general definition of *fibred systems* in [47] (cf. also [7]). Examples of fibred systems which have been the focus of extensive research in recent years and decades are *positional notation systems* (standard and non-standard), *double base number systems* [15, 14], *continued fractions*, *β-expansions* [45, 41, 9, 10, 18, 17, 39, 50], *canonical number systems (CNS)* [29, 42, 24, 22, 23, 31, 19, 44, 30, 32], and *shift radix systems* [1, 2, 3, 4, 12, 28, 55, 56, 43, 57].

In our setting the "names" of p-adic integers are of course obtained by taking the orbits modulo 2 which, in the case of F_2, yields the usual binary representation. The tables below show the initial parts of the orbits (which we will refer to as *sequences* in the following) of several natural numbers as well as the resulting "names" (*(digit)-expansions*).

1	1	2	1	2	$\cdots$
2	2	1	2	1	$\cdots$
3	3	5	8	4	$\cdots$
4	4	2	1	2	$\cdots$
5	5	8	4	2	$\cdots$
6	6	3	5	8	$\cdots$
7	7	11	17	26	$\cdots$
8	8	4	2	1	$\cdots$
9	9	14	7	11	$\cdots$
10	10	5	8	4	$\cdots$
11	11	17	26	13	$\cdots$
12	12	6	3	5	$\cdots$
13	13	20	10	5	$\cdots$
14	14	7	11	17	$\cdots$
15	15	23	35	53	$\cdots$
16	16	8	4	2	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\mathrm{S}(\mathrm{F}_C)$	0	1	2	3	$\cdots$

1	1	0	1	0	$\cdots$
2	0	1	0	1	$\cdots$
3	1	1	0	0	$\cdots$
4	0	0	1	0	$\cdots$
5	1	0	0	0	$\cdots$
6	0	1	1	0	$\cdots$
7	1	1	1	0	$\cdots$
8	0	0	0	1	$\cdots$
9	1	0	1	1	$\cdots$
10	0	1	0	0	$\cdots$
11	1	1	0	1	$\cdots$
12	0	0	1	1	$\cdots$
13	1	0	0	1	$\cdots$
14	0	1	1	1	$\cdots$
15	1	1	1	1	$\cdots$
16	0	0	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\mathrm{D}(\mathrm{F}_C)$	0	1	2	3	$\cdots$

1	1	0	0	0	$\cdots$
2	2	1	0	0	$\cdots$
3	3	1	0	0	$\cdots$
4	4	2	1	0	$\cdots$
5	5	2	1	0	$\cdots$
6	6	3	1	0	$\cdots$
7	7	3	1	0	$\cdots$
8	8	4	2	1	$\cdots$
9	9	4	2	1	$\cdots$
10	10	5	2	1	$\cdots$
11	11	5	2	1	$\cdots$
12	12	6	3	1	$\cdots$
13	13	6	3	1	$\cdots$
14	14	7	3	1	$\cdots$
15	15	7	3	1	$\cdots$
16	16	8	4	2	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\mathrm{S}(\mathrm{F}_2)$	0	1	2	3	$\cdots$

1	1	0	0	0	$\cdots$
2	0	1	0	0	$\cdots$
3	1	1	0	0	$\cdots$
4	0	0	1	0	$\cdots$
5	1	0	1	0	$\cdots$
6	0	1	1	0	$\cdots$
7	1	1	1	0	$\cdots$
8	0	0	0	1	$\cdots$
9	1	0	0	1	$\cdots$
10	0	1	0	1	$\cdots$
11	1	1	0	1	$\cdots$
12	0	0	1	1	$\cdots$
13	1	0	1	1	$\cdots$
14	0	1	1	1	$\cdots$
15	1	1	1	1	$\cdots$
16	0	0	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\mathrm{D}(\mathrm{F}_2)$	0	1	2	3	$\cdots$

TABLE 1. Sequences and expansions of natural numbers as given by F_C and F_2.

It can be seen that the tables of expansions of both F_C and F_2 admit a specific block structure which translates to a very natural condition on any number system on the p-adic integers:

(block) the first k elements of the expansions of m and n coincide $\Leftrightarrow$ $m \equiv n \mod p^k$.

It is this block structure which is the essential condition in the definition of p-adic systems. We will provide a formal definition in the upcoming section, but conclude this introduction by a verbal description and by a summary of the above observations: A p-adic system is a number system on p-adic integers which assigns an infinite string (expansion) over the alphabet $\{0, \ldots, p-1\}$ (the *digits*) to any element of $\mathbb{Z}_p$ such that the complete "table of expansions" satisfies the block property. The main goal of studying p-adic system is to understand which parameters control what kind of expansions one can get on specific subsets of $\mathbb{Z}_p$, such as the integers or rational numbers in $\mathbb{Z}_p$. Simple changes in the definition of a p-adic system (such as going from F_2 to F_C) can shift

questions on the resulting expansions from trivial to very hard. The hope is that by studying the entirety of p-adic systems one can find examples of intermediate difficulty which may shed some light on the true nature of the hard problems and help identify the "right questions to ask". A possible list of such examples and questions will be provided in the upcoming sections and it is the author's hope that they will arouse the curiosity of many and convince them to join in a common effort to approach them.

Structure. This manuscript is structured as follows:

Section 1 summarizes the motivation and philosophy behind p-adic systems.

Section 2 provides rigorous definitions of basic concepts and notions which are used throughout the paper, up to and including the central objects "p-adic systems".

Section 3 lists different interpretations ("ordinary functions on $\mathbb{Z}_p$ with block property", "p-digits tables with block property", and "p-adic permutations") of p-adic systems and outlines how to translate between these different viewpoints. Furthermore, a group structure on the set of p-adic systems is established and the notion of "trees of cycles" is introduced.

Section 4 provides a characterization of p-adic systems which considers the defining functions independently from one another. This allows for the complete characterization of all p-adic systems which are defined by polynomials in $\mathbb{Z}_p[x]$, $\mathbb{Q}_p[x]$ and certain rational functions on $\mathbb{Z}_p$. These classes provide a multitude of concrete examples of p-adic systems.

Section 5 shows how p-adic systems can be used to generalize Hensel's Lemma on polynomials to general functions on $\mathbb{Z}_p$ in two different ways. The notion of "p-fibred rational functions" is introduced and investigated here.

Section 6 provides general results on periodic and ultimately periodic digit expansions of "contractive" and "expansive" p-adic systems.

Section 7 studies the class of "linear-polynomial p-adic systems" which are closest to the original Collatz transformation. Several conjectures which generalize the Collatz conjecture within the framework of p-adic systems along with first related results are listed here.

Section 8 describes the relation between p-adic systems and permutation polynomials and analyzes properties of the trees of cycles of p-adic systems from different classes.

Section 9 provides a list of open questions and problems related to p-adic systems.

In the appendix a list and short summary of all theorems (lemmas, corollaries, examples, etc.) can be found, as well as a list of all used symbols in order of first appearance.

2. Notation and definitions

The purpose of this somewhat technical section is to provide a solid conceptual and notational foundation for the clear and efficient, but at the same time comprehensible discussion of p-adic systems.

Basic notation. For any set A and any set of predicates $\mathcal{P}$ we let

$$A(\mathcal{P}) := \{a \in A \mid \forall\, P \in \mathcal{P} : P(a)\} \tag{2.1}$$

denote the set of all elements of A which satisfy all predicates in $\mathcal{P}$. If $\mathcal{P} = \{P_1, \ldots, P_n\}$ for some $n \in \mathbb{N}_0$, we also define the shorter version $A(P_1, \ldots, P_n) := A(\mathcal{P})$. For $a, b \in \mathbb{R} \cup \{\pm\infty\}$ let

$$[\![a, b]\!] := \{n \in \mathbb{Z} \mid a \leq n \leq b\}\,, \qquad \underline{b} := [\![0, b-1]\!], \qquad \overline{b} := [\![0, b]\!]. \tag{2.2}$$

For sets A and B let B^A denote the *set of all mappings* from A to B, respectively the *set of all indexed families* with index set A and entries in B. For $n \in \mathbb{N}_0$ let also $B^n := B^{\underline{n}}$. For any set A we may identify elements of A, $\{\{a\} \mid a \in A\}$, and A^1 by

$$a \mapsto \{a\} \mapsto (a). \tag{2.3}$$

Throughout the paper we will make heavy use of the *modulo function* which shall be denoted by % (C++ notation). Specifically, for $0 \neq m \in \mathbb{Z}$ and $a \in \mathbb{Z}$, $a\%m$ denotes the unique element of

$\underline{|m|}$ satisfying $a - a\%m \equiv 0 \mod m$. Additionally, for any $2 \leq p \in \mathbb{N}$, $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ with $a_i \in \underline{p}$ for all $i \in \mathbb{N}_0$, and $k \in \mathbb{N}_0$ let $a\%p^k := \sum_{i=0}^{k-1} a_i p^i \in \underline{p^k}$.

Sequences. In order to deal with orbits and digit expansions, we introduce the notion of sequences: the elements of any set A^k, where A is a set and $k \in \mathbb{N}_0 \cup \{\infty\}$, are called *sequences*. The *class of all sequences* shall be denoted by $\mathbf{S}$. For any sequence $S \in A^k$ we set $|S| := k$, the *length* or *size* of S. For any set A we define $S[A]$ to be the subsequence of S consisting of the entries with indices in $A \cap \underline{|S|}$ in increasing order. Furthermore, for $i, j \in \mathbb{R} \cup \{\pm\infty\}$ we define the shorter version $S[i, j] := S[[\![i, j]\!]]$. Note that by Eqn. (2.3), $S[k]$ is defined for all $k \in \underline{|S|}$ $(k \mapsto \{k\})$ and may be interpreted as the subsequence of length 1 of S which consists of the entry of S with index k, or as this entry itself $(k \mapsto (k))$.
We define the following predicates on $\mathbf{S}$ ($S, T \in \mathbf{S}$, A set):

(2.4) $\mathrm{len}_A(S) \Leftrightarrow |S| \in A$ — S has *length in* A or, if $A = \{a\}$, S is *of length* a

(2.5) $\mathrm{fin}(S) \Leftrightarrow \mathrm{len}_{\mathbb{N}_0}(S)$ — S is *finite*, otherwise *infinite*

(2.6) $\mathrm{emp}(S) \Leftrightarrow \mathrm{len}_0(S)$ — S is *empty*, otherwise *non-empty*

(2.7) $\mathrm{bnd}_A(S) \Leftrightarrow \forall\, n \in \underline{|S|} : S[n] \in A$ — S is *A-bounded*

(2.8) $\mathrm{pre}_T(S) \Leftrightarrow S[\underline{|T|}] = T$ — S has *prefix* T

(2.9) $\mathrm{suf}_T(S) \Leftrightarrow S[|S| - |T|\,, |S| - 1] = T$ — S has *suffix* T

Multiplication $S \cdot T$ of two sequences S and T with S being finite is defined by concatenation. If S is infinite and T is empty we set $S \cdot T := S$ and $T \cdot S := S$. Being the neutral element of sequence multiplication, the empty sequence shall be the result of empty products. The *n-th power* S^n of a finite sequence S is the n-fold multiplication of S by itself. If $S \neq ()$, then S^∞ is the infinite periodic sequence with period S, otherwise we set $()^\infty := ()$. For an infinite sequence S we define $\mathcal{I}(S) \in \mathbf{S}$ to be the *initial part* of S and $\mathcal{P}(S) \in \mathbf{S}(\mathrm{fin})$ to be the *periodic part* of S, i.e. $\mathcal{I}(S)$ and $\mathcal{P}(S)$ are chosen shortest possible (with $\mathcal{I}(S)$ having the precedence) such that $S = \mathcal{I}(S) \cdot \mathcal{P}(S)^\infty$.
We define the following additional predicates on $\mathbf{S}$ ($S \in \mathbf{S}$):

(2.10) $\mathrm{per}(S) \Leftrightarrow \neg\mathrm{fin}(S) \wedge \mathrm{emp}(\mathcal{I}(S))$ — S is *(purely) periodic*

(2.11) $\mathrm{uper}(S) \Leftrightarrow \neg\mathrm{fin}(S) \wedge \mathrm{fin}(\mathcal{I}(S))$ — S is *ultimately periodic*

(2.12) $\mathrm{aper}(S) \Leftrightarrow \neg\mathrm{fin}(\mathcal{I}(S))$ — S is *aperiodic*

Any function $f : A \to B$ between arbitrary sets A and B extends naturally to $\mathbf{S}(\mathrm{bnd}_A)$ by $S \mapsto (f(S[k]))_{k \in \underline{|S|}} \in \mathbf{S}(\mathrm{bnd}_B)$ (*entry-wise application of* f *to* S).

Sequence tables. The entirety of orbits of a transformation will be collected in "tables" (cf. Table 1) which motivates the definition of sequence tables: the elements of any set $\mathbf{S}(\mathrm{bnd}_B, \mathrm{len}_k)^A$, where A and B are sets and $k \in \mathbb{N}_0 \cup \{\infty\}$, are called *sequence tables*. The *class of all sequence tables* shall be denoted by $\mathcal{S}$. For any sequence table $\mathrm{S} \in \mathbf{S}(\mathrm{bnd}_B, \mathrm{len}_k)^A$ we set $\mathrm{dom(S)} := A$, the *domain* of S, and $|\mathrm{S}| := k$, the *length* or *size* of S. For any $\mathrm{S} \in \mathcal{S}$ and any $n \in \mathrm{dom(S)}$ let $\mathrm{S}[n]$ denote the n-th entry of S (the *n-th row of* S or S-*sequence of* n). For any subset A of dom(S) we define $\mathrm{S}|_A := (\mathrm{S}[n])_{n \in A}$, the *restriction of* S *to* A, and for any arbitrary set A we define $\mathrm{S}[\![A]\!] := (\mathrm{S}[n][A])_{n \in \mathrm{dom(S)}}$. Furthermore, for $i, j \in \mathbb{R} \cup \{\pm\infty\}$ we define the shorter version $\mathrm{S}[\![i, j]\!] := \mathrm{S}[[\![i, j]\!]]$. *Multiplication* and *exponentiation* of sequences as well as *entry-wise applications of functions* to sequences carry over to sequence tables (row-wise).
We define the following predicates on $\mathcal{S}$ ($\mathrm{S} \in \mathcal{S}$, A set):

(2.13) $\mathrm{dom}_A(\mathrm{S}) \Leftrightarrow \mathrm{dom(S)} = A$ — S has *domain* A

(2.14) $\mathrm{len}_A(\mathrm{S}) \Leftrightarrow |\mathrm{S}| \in A$ — S has *length in* A or, if $A = \{a\}$, S is *of length* a

(2.15) $\mathrm{fin(S)} \Leftrightarrow \mathrm{len}_{\mathbb{N}_0}(\mathrm{S})$ — S is *finite*, otherwise *infinite*

(2.16) $\mathrm{emp(S)} \Leftrightarrow \mathrm{len}_0(\mathrm{S})$ — S is *empty*, otherwise *non-empty*

(2.17) $\mathrm{bnd}_A(\mathrm{S}) \Leftrightarrow \forall\, n \in \mathrm{dom(S)} : \mathrm{bnd}_A(\mathrm{S}[n])$ — S is *A-bounded*

p-digit tables. In addition to sequence tables, we define the specialised p-digit tables which will be used to represent collections of expansions. Let $2 \leq p \in \mathbb{N}$. An element D of any set $\mathcal{S}(\mathrm{dom}_A, \mathrm{bnd}_{\underline{p}})$, where $A \subseteq \mathbb{Z}_p$[1], is called *p-digit table* if it satisfies the condition

$$\forall\, n \in \mathrm{dom}(\mathrm{D}) : \mathrm{D}[n][0] = n\%p. \tag{2.18}$$

The *set of all p-digit tables* shall be denoted by $\mathcal{D}_p$. For any $\mathrm{D} \in \mathcal{D}_p$ and $n \in \mathrm{dom}(\mathrm{D})$ the D-*digit expansion of* n is given by $\mathrm{D}[n]$ and for $k \in \mathbb{N}_0$ the *k-th digit of n with respect to* D is given by $\mathrm{D}[n][k]$.
We define the following predicates on $\mathcal{D}_p$ ($\mathrm{D} \in \mathcal{D}_p$, $K \subseteq \mathbb{N}_0$) (cf. Table 1):

$$\text{(2.19)}\quad \text{w-block}_K(\mathrm{D}) \Leftrightarrow \forall\, k \in K : \forall\, m, n \in \mathrm{dom}(\mathrm{D}) : \quad m \equiv n \mod p^k \Rightarrow \mathrm{D}[m][\underline{k}] = \mathrm{D}[n][\underline{k}] \qquad \text{D has the } \textit{weak block property at } K$$

$$\text{(2.20)}\quad \text{w-block}(\mathrm{D}) \Leftrightarrow \text{w-block}_{\mathbb{N}_0}(\mathrm{D}) \qquad \text{D has the } \textit{weak block property}$$

$$\text{(2.21)}\quad \text{block}_K(\mathrm{D}) \Leftrightarrow \forall\, k \in K : \forall\, m, n \in \mathrm{dom}(\mathrm{D}) : \quad m \equiv n \mod p^k \Leftrightarrow \mathrm{D}[m][\underline{k}] = \mathrm{D}[n][\underline{k}] \qquad \text{D has the } \textit{block property at } K$$

$$\text{(2.22)}\quad \text{block}(\mathrm{D}) \Leftrightarrow \text{block}_{\mathbb{N}_0}(\mathrm{D}) \qquad \text{D has the } \textit{block property}$$

p-fibred functions. The transformations F_C and F_2 defined in the previous section are both piecewise functions on $\mathbb{Z}_2$ with branches for both residue classes modulo 2. Throughout the paper we will use a very useful notation for functions given in this way. Let $2 \leq p \in \mathbb{N}$. The elements of any set $\mathbf{S}(\mathrm{bnd}_{(\mathbb{Z}_p)^A}, \mathrm{len}_p)$, where $A \subseteq \mathbb{Z}_p$, are called *p-fibred functions*, i.e. a p-fibred function $\mathrm{F} = (\mathrm{F}[0], \ldots, \mathrm{F}[p-1])$ is a p-tuple of functions $\mathrm{F}[r] : A \to \mathbb{Z}_p$, $r \in \underline{p}$, on some fixed subset A of the p-adic integers. The *set of all p-fibred functions* shall be denoted by $\mathcal{F}_p$. For any p-fibred function $\mathrm{F} \in \mathbf{S}(\mathrm{bnd}_{(\mathbb{Z}_p)^A}, \mathrm{len}_p)$ we set $\mathrm{dom}(\mathrm{F}) := A$, the *domain of* F. We interpret F itself as a function on its domain in the following way:

$$\begin{aligned} \mathrm{F} : \mathrm{dom}(\mathrm{F}) &\to \mathbb{Z}_p \\ n &\mapsto \frac{\mathrm{F}[n\%p](n) - \mathrm{F}[n\%p](n)\%p}{p} \end{aligned} \tag{2.23}$$

where % is the modulo function (C++ notation). Note that the subtrahend in the numerator of the fraction above has the mere function to guarantee that the result is divisible by p. For any subset A of $\mathrm{dom}(\mathrm{F})$ we define $\mathrm{F}|_A := (\mathrm{F}[0]|_A, \ldots, \mathrm{F}[p-1]|_A)$, the *restriction of* F *to* A. For any ordinary function on a subset A of $\mathbb{Z}_p$ there is a p-fibred function showing the same behavior (i.e. the images of all elements of A under both the ordinary function and the p-fibred function coincide). If $f : A \to \mathbb{Z}_p$ is such an ordinary function, then one such p-fibred function showing the same behavior is given by

$$(pf, \ldots, pf). \tag{2.24}$$

In general (indeed, in any case) there are several different p-fibred functions representing a given ordinary function. "Representing the same ordinary function" defines an equivalence relation on $\mathcal{F}_p$:

$$\mathrm{F} \sim_p \mathrm{G} \quad \Leftrightarrow \quad \mathrm{dom}(\mathrm{F}) = \mathrm{dom}(\mathrm{G}) \wedge \forall\, n \in \mathrm{dom}(\mathrm{F}) : \mathrm{F}(n) = \mathrm{G}(n). \tag{2.25}$$

[1]Note that many authors define p-adic integers only for prime numbers p. The main reason is that if p has at least two different prime factors, then the ring $\mathbb{Z}_p$ is no domain anymore making it less useful in many situations. However, in the setting of this paper the existence of zero divisors does not cause any problems and we thus do not limit our definition to prime numbers. Note that $\mathbb{Z}_p \simeq \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_\ell}$ where $p_1, \ldots, p_\ell$ are the distinct prime factors of p. In the appendix a short discussion of the issue can be found.

For every equivalence class of $\sim_p$ there is a canonical representative fixed by the following predicate on $\mathcal{F}_p$ ($\mathrm{F} \in \mathcal{F}_p$):

$$\mathrm{canf}(\mathrm{F}) \Leftrightarrow \forall\, r \in \underline{p} : \forall\, n \in \mathrm{dom}(\mathrm{F}) : \qquad \mathrm{F}[r](n) \in \begin{cases} p\mathbb{Z}_p & \text{if } n \equiv r \mod p \\ \{0\} & \text{if } n \not\equiv r \mod p \end{cases} \tag{2.26}$$

F is *in canonical form*

The canonical representative of the equivalence class of a p-fibred function F is called the *canonical form* of F. In some cases it is useful to consider the following weaker predicate on $\mathcal{F}_p$ ($\mathrm{F} \in \mathcal{F}_p$):

$$\text{w-canf}(\mathrm{F}) \Leftrightarrow \forall\, r \in \underline{p} : \mathrm{F}[r]((r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})) \subseteq p\mathbb{Z}_p \tag{2.27}$$

F is *in weak canonical form*

If G is a p-fibred function in weak canonical form and $\mathrm{F} \sim_p \mathrm{G}$, then G is called a *weak canonical form* of F. If F is a p-fibred function in weak canonical form, the definition of its corresponding ordinary function simplifies to

$$\begin{aligned} \mathrm{F} : \mathrm{dom}(\mathrm{F}) &\to \mathbb{Z}_p. \\ n &\mapsto \frac{\mathrm{F}[n\%p](n)}{p} \end{aligned} \tag{2.28}$$

We define the following predicates on $\mathcal{F}_p$ ($\mathrm{F} \in \mathcal{F}_p$, A set):

$$\mathrm{dom}_A(\mathrm{F}) \Leftrightarrow \mathrm{dom}(\mathrm{F}) = A \tag{2.29}$$

F has *domain* A

$$\mathrm{bnd}_A(\mathrm{F}) \Leftrightarrow \mathrm{F}(\mathrm{dom}(\mathrm{F})) \subseteq A \tag{2.30}$$

F is *A-bounded*

$$\mathrm{closed}(\mathrm{F}) \Leftrightarrow \mathrm{bnd}_{\mathrm{dom}(\mathrm{F})}(\mathrm{F}) \tag{2.31}$$

F is *closed*

For any closed p-fibred function F we call $\mathrm{S}(\mathrm{F}) := \left(\left(\mathrm{F}^k(n)\right)_{k\in\mathbb{N}_0}\right)_{n\in\mathrm{dom}(\mathrm{F})} \in \mathcal{S}(\mathrm{dom}_{\mathrm{dom}(\mathrm{F})}, \neg\mathrm{fin})$ the F-*sequence table*, and $\mathrm{D}(\mathrm{F}) := \mathrm{S}(\mathrm{F})\%p \in \mathcal{D}_p(\mathrm{dom}_{\mathrm{dom}(\mathrm{F})}, \neg\mathrm{fin})$ the F-*digit table*. For $n \in \mathrm{dom}(\mathrm{F})$ the F-*sequence of* n is given by the S(F)-sequence of n, the F-*digit expansion of* n by the D(F)-digit expansion of n, and for $k \in \mathbb{N}_0$ the *k-th digit of n with respect to* F is given by the k-th digit of n with respect to D(F).
The predicates w-block$_K$, w-block, block$_K$, and block carry over to $\mathcal{F}_p$(closed) by D(F).

p-adic systems. We are now in the position to define our central object of interest. A *p-adic system* is a p-fibred function with domain $\mathbb{Z}_p$ (which implies that it is closed) which has the block property. The *set of all p-adic systems* is thus given by $\overline{\mathcal{F}}_p := \mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p}, \mathrm{block})$.

Following the definition above we are able to write

$$\mathrm{F}_C := (x, 3x+1) \tag{2.32}$$

$$\mathrm{F}_2 := (x, x-1) \sim_p (x, x). \tag{2.33}$$

$(x, x-1)$ is a weak canonical form of (x, x) and the canonical form of F_C is given by

$$(x(x \equiv 0 \mod 2\ ?\ 1 : 0), (3x+1)(x \equiv 1 \mod 2\ ?\ 1 : 0)) \tag{2.34}$$

where $(P(x)\ ?\ f(x) : g(x))$ is a function on $\mathbb{Z}_p$ which reads "if $P(x)$ then $f(x)$, else $g(x)$" (again, C++ notation). Both F_C and F_2 have the block property (as we will show later, Corollary 4.11 (2)) and are thus examples of p-adic systems.

3. Three and a half interpretations of p-adic systems

In this sections we will establish different ways to think about p-adic systems, all of which are valid interpretations in there own right along the one which we ultimately chose to be the formal definition. As with any introduction to a mathematical object, one has to decide which description to call "definition" and which "characterization" instead. Recall that the questions on p-adic systems we are most interested in are those on their ultimate behavior (such as whether the orbits of all natural numbers under F_C actually end up in 1). It is in this regard that the mentioned interpretations will be equivalent.

The formal definition: p-fibred functions with block property. We begin by repeating the formal definition which would be the first interpretation in our list of three and a half: A p-adic system is a p-fibred function F with domain $\mathbb{Z}_p$, i.e. a piecewise function on $\mathbb{Z}_p$ with branches for all residue classes modulo p, such that the p-digit table $\mathrm{D}(\mathrm{F})$ given by the F-digit expansions satisfies the block property: $\mathrm{D}(\mathrm{F})[m][\underline{k}] = \mathrm{D}(\mathrm{F})[n][\underline{k}]$ if and only if $m \equiv n \mod p^k$ for all $k \in \mathbb{N}_0$ and for all $m, n \in \mathbb{Z}_p$. According to this definition a p-adic system is a "dynamical object" as the property we are most interested in (the corresponding digit expansions) is defined by the dynamical process of repeatedly applying the p-adic system. We recall that $\sim_p$ (cf. Eqn. (2.25)) defines an equivalence relation on $\mathcal{F}_p$ (we provide a formal proof in the lemma below), where equivalent p-fibred functions show exactly the same dynamical behavior and thus define equal p-digit tables. Since the p-digit tables are what we really care about, one might consider a p-adic system to be a whole equivalence class of $\sim_p$ instead of a single p-fibred function.

Lemma 3.1. *Let $2 \leq p \in \mathbb{N}$ and $\mathrm{F} \in \mathcal{F}_p$. Then, there is a unique $\mathrm{F}_c \in \mathcal{F}_p$ such that F_c is a canonical form of F. In this case $\mathrm{S}(\mathrm{F}_c) = \mathrm{S}(\mathrm{F})$ and $\mathrm{D}(\mathrm{F}_c) = \mathrm{D}(\mathrm{F})$. If G is another p-fibred function and G_c its canonical form, then $\mathrm{F} \sim_p \mathrm{G}$ if and only if $\mathrm{F}_c = \mathrm{G}_c$. In particular, $\sim_p$ is an equivalence relation on $\mathcal{F}_p$ and every equivalence class contains a unique canonical form.*

Proof. Let $\mathrm{F}_c \in \mathcal{F}_p$ with

$$\mathrm{F}_c[r] : \mathrm{dom}(\mathrm{F}) \to \mathrm{dom}(\mathrm{F}) \tag{3.1}$$
$$n \mapsto \begin{cases} \mathrm{F}[r](n) - \mathrm{F}[r](n)\%p & \text{if } n \equiv r \mod p \\ 0 & \text{if } n \not\equiv r \mod p \end{cases}$$

for all $r \in \underline{p}$. Then, F_c is a canonical form of F and its uniqueness follows by construction. Clearly, $\mathrm{S}(\mathrm{F}_c) = \mathrm{S}(\mathrm{F})$ and hence $\mathrm{D}(\mathrm{F}_c) = \mathrm{D}(\mathrm{F})$.

Let $\mathrm{G} \in \mathcal{F}_p$. If $\mathrm{F} \sim_p \mathrm{G}$, then $\mathrm{dom}(\mathrm{F}) = \mathrm{dom}(\mathrm{G})$, and for all $r \in \underline{p}$ and all $n \in (r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})$ we get

$$\mathrm{F}_c[r](n) = \mathrm{F}[r](n) - \mathrm{F}[r](n)\%p = p\mathrm{F}(n) = p\mathrm{G}(n) = \mathrm{G}[r](n) - \mathrm{G}[r](n)\%p = \mathrm{G}_c[r](n) \tag{3.2}$$

and hence $\mathrm{F}_c = \mathrm{G}_c$.

If, however, $\mathrm{F}_c = \mathrm{G}_c$, then again $\mathrm{dom}(\mathrm{F}) = \mathrm{dom}(\mathrm{G})$ and for all $r \in \underline{p}$ and all $n \in (r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})$ we get

$$\mathrm{F}(n) = \frac{\mathrm{F}[r](n) - \mathrm{F}[r](n)\%p}{p} = \frac{\mathrm{F}_c[r](n)}{p} = \frac{\mathrm{G}_c[r](n)}{p} = \frac{\mathrm{G}[r](n) - \mathrm{G}[r](n)\%p}{p} = \mathrm{G}(n) \tag{3.3}$$

and hence $\mathrm{F} \sim_p \mathrm{G}$. □

From now on we identify elements of $\mathcal{F}_p$ and $\mathcal{F}_p/_{\sim_p}$ by $\mathrm{F} \mapsto [\mathrm{F}]_{\sim_p}$, e.g. $[\mathrm{F}]_{\sim_p}(n) = \mathrm{F}(n)$, $\mathrm{D}([\mathrm{F}]_{\sim_p}) = \mathrm{D}(\mathrm{F})$, etc.

Ordinary functions on $\mathbb{Z}_p$ with block property. This alternative interpretation accounts for the "half" in the title of this section and has already been mentioned in the formal definition of p-adic systems in the previous section. Any p-fibred function defines an ordinary function on its domain (Eqn. (2.23)) and, vice versa, any ordinary function on some subset of $\mathbb{Z}_p$ is equal to the ordinary function defined by some p-fibred function (Eqn. (2.24)). A class of the equivalence relation $\sim_p$ consists of exactly those p-fibred functions which represent the same ordinary function. For any $A \subseteq \mathbb{Z}_p$ there is thus a one-to-one correspondence between $\mathcal{F}_p(\mathrm{dom}_A)/_{\sim_p}$ and $(\mathbb{Z}_p)^A$. The distinction between p-fibred functions and ordinary functions is therefore only a matter of notation and the question that remains is: how does the block property of p-fibred functions translate to ordinary functions? The answer is given by the following Lemma.

Lemma 3.2. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \mathcal{F}_p(\mathrm{closed})$, and $k \in \mathbb{N} \cup \{\infty\}$. Then,*

(1) $(\forall\, \ell \in [\![1, k]\!] : \forall\, m, n \in \mathrm{dom}(\mathrm{F})$ *with* $m \equiv n \mod p : m \equiv n \mod p^\ell \Rightarrow \mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1})$
$\Rightarrow \text{w-block}_{\overline{k}}(\mathrm{F})$

(2) $(\forall\, \ell \in [\![1, k]\!] : \forall\, m, n \in \mathrm{dom}(\mathrm{F})$ *with* $m \equiv n \mod p : m \equiv n \mod p^\ell \Leftrightarrow \mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1})$
$\Leftrightarrow \mathrm{block}_{\overline{k}}(\mathrm{F})$.

Before we give a proof of the lemma, we analyze its meaning. (2) completely characterizes when an ordinary function $f : A \to A$, $A \subseteq \mathbb{Z}_p$ (which is the function given by the p-fibred function F in the lemma with $A = \mathrm{dom(F)}$) has the block property by only considering a single application of f. However, (1) only provides a sufficient condition for the weak block property as the following example shows.

Example 3.3. Let $\mathrm{F} \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{Z}_2})$ with $\mathrm{F}[0](n) = (n = 8\ ?\ 4 : 0)$ and $\mathrm{F}[1](n) = 2$ for all $n \in \mathbb{Z}_2$. Then, $\mathrm{D(F)} = ((n\%2)^\infty)_{n\in\mathbb{Z}_2}$ and, hence, w-block(F). At the same time we get $0 \equiv 8 \mod 2^3$ but $\mathrm{F}(0) = 0 \not\equiv 2 = \mathrm{F}(8) \mod 2^2$.

We will show later (Example 4.2) that no characterization of the weak block property of the above kind can exist that is both necessary and sufficient.

Proof of Lemma 3.2.
(1): We prove w-block$_\ell$(F) for all $\ell \in \overline{k}$ by induction on ℓ: clearly, w-block$_0$(F). Assume $\ell \in [\![1, k]\!]$ and that the statement holds for $\ell - 1$. Let $m, n \in \mathrm{dom(F)}$ with $m \equiv n \mod p^\ell$. Then $m \equiv n \mod p$ and thus

$$\mathrm{D(F)}[m][0] = \mathrm{D(F)}[n][0] \tag{3.4}$$

by definition of D(F). Furthermore,

$$m \equiv n \mod p^\ell \Rightarrow \mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1} \tag{3.5}$$
$$\text{(ind. hyp.)} \Rightarrow \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.6}$$
$$\Leftrightarrow \mathrm{D(F)}[m][0] \cdot \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[n][0] \cdot \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.7}$$
$$\Leftrightarrow \mathrm{D(F)}[m][\underline{\ell}] = \mathrm{D(F)}[n][\underline{\ell}] \tag{3.8}$$

which implies w-block$_\ell$(F).
(2): We prove " $\Rightarrow$" by showing block$_\ell$(F) for all $\ell \in \overline{k}$ by induction on ℓ: clearly, block$_0$(F). Assume $\ell \in [\![1, k]\!]$ and that the statement holds for $\ell - 1$. Let $m, n \in \mathrm{dom(F)}$ with $m \equiv n \mod p^\ell$. Then $m \equiv n \mod p$ and thus

$$\mathrm{D(F)}[m][0] = \mathrm{D(F)}[n][0] \tag{3.9}$$

as before. Furthermore,

$$m \equiv n \mod p^\ell \Leftrightarrow \mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1} \tag{3.10}$$
$$\text{(ind. hyp.)} \Leftrightarrow \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.11}$$
$$\Leftrightarrow \mathrm{D(F)}[m][0] \cdot \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[n][0] \cdot \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.12}$$
$$\Leftrightarrow \mathrm{D(F)}[m][\underline{\ell}] = \mathrm{D(F)}[n][\underline{\ell}] \tag{3.13}$$

which implies block$_\ell$(F).

For the proof of "$\Leftarrow$" let $m, n \in \mathrm{dom(F)}$ with $m \equiv n \mod p$. Then,

$$\mathrm{D(F)}[m][0] = \mathrm{D(F)}[n][0]. \tag{3.14}$$

Furthermore,

$$m \equiv n \mod p^\ell \Leftrightarrow \mathrm{D(F)}[m][\underline{\ell}] = \mathrm{D(F)}[n][\underline{\ell}] \tag{3.15}$$
$$\Leftrightarrow \mathrm{D(F)}[m][0] \cdot \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[n][0] \cdot \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.16}$$
$$\Leftrightarrow \mathrm{D(F)}[\mathrm{F}(m)][0, \ell-2] = \mathrm{D(F)}[\mathrm{F}(n)][0, \ell-2] \tag{3.17}$$
$$\Leftrightarrow \mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1}. \tag{3.18}$$

□

If we denote by $\overline{\mathcal{Z}}_p$ the set of all functions $f : \mathbb{Z}_p \to \mathbb{Z}_p$ which satisfy

$$\forall\, k \in \mathbb{N} : \forall\, m, n \in \mathbb{Z}_p : m \equiv n \mod p^k \Leftrightarrow f(m) \equiv f(n) \mod p^{k-1}, \tag{3.19}$$

as a consequence, there is a bijection between $\overline{\mathcal{F}}_p/_{\sim_p}$ and $\overline{\mathcal{Z}}_p$ given by

$$\begin{aligned} \overline{\mathcal{F}}_p/_{\sim_p} &\leftrightarrow \overline{\mathcal{Z}}_p. \\ \mathrm{F} &\mapsto (\mathrm{F} : \mathbb{Z}_p \to \mathbb{Z}_p) \\ (pf, \ldots, pf) &\leftarrow\!\shortmid f \end{aligned} \tag{3.20}$$

p-digit tables with block property. As argued above, both of the previous interpretations consider p-adic systems to be "dynamical objects". The dynamical behavior of a (closed) p-fibred function is used to define a "static object", the corresponding p-digit table, whose structure determines whether the p-fibred function is considered a p-adic system (which is the case precisely if the p-digit table has the block property). Surprisingly, it is also possible to go in the other direction, i.e. start out with the static object and use it to define a dynamical one. Indeed, there is a one-to-one correspondence between $\overline{\mathcal{F}}_p/_{\sim_p}$ and $\overline{\mathcal{D}}_p := \mathcal{D}_p(\mathrm{dom}_{\mathbb{Z}_p}, \neg\mathrm{fin}, \mathrm{block})$. Clearly, every p-adic system F defines an infinite p-digit table with block property by its F-digit table D(F) and any p-adic system that is equivalent to F defines the same p-digit table. The other two facts implied by the existence of the mentioned one-to-one correspondence are probably less obvious: the p-digit tables of two p-adic systems F and G are identical if and only if F and G are equivalent and every infinite p-digit table with domain $\mathbb{Z}_p$ and block property is the F-digit table of some p-adic system F. In the following we will prove just that and we begin by interpreting any p-digit table as a multivalued function on its domain. We will show that if D is infinite and has domain $\mathbb{Z}_p$ and the block property, then this function actually defines the p-adic system we are looking for. For any $\mathrm{D} \in \mathcal{D}_p$ let

$$\begin{aligned} \mathrm{D} : \mathrm{dom}(\mathrm{D}) &\to \mathcal{P}(\mathrm{dom}(\mathrm{D})) \\ n &\mapsto \{m \in \mathrm{dom}(\mathrm{D}) \mid \mathrm{D}[m][0, |\mathrm{D}| - 2] = \mathrm{D}[n][1, |\mathrm{D}| - 1]\} \end{aligned} \tag{3.21}$$

where $\mathcal{P}(A)$ denotes the power set of a set A. What D (as a function) does is, it takes an element n from its domain, drops the first entry (entry with index 0) from the D-digit expansion of n, and returns all elements of its domain which have the resulting sequence as their initial D-digit expansion. Using this notation we continue with a characterization of all p-fibred functions which define a given p-digit table.

Theorem 3.4. *Let $2 \leq p \in \mathbb{N}$ and $\mathrm{D} \in \mathcal{D}_p$. Then, for every $\mathrm{F} \in \mathcal{F}_p(\mathrm{dom}_{\mathrm{dom}(\mathrm{D})}, \mathrm{closed})$ we get $\mathrm{D}(\mathrm{F})[\![\underline{|\mathrm{D}|}]\!] = \mathrm{D}$ if and only if $\mathrm{F}(n) \in \mathrm{D}(n)$ for every $n \in \mathrm{dom}(\mathrm{D})$. In particular, there is a $\mathrm{F} \in \mathcal{F}_p(\mathrm{dom}_{\mathrm{dom}(\mathrm{D})}, \mathrm{closed})$ such that $\mathrm{D}(\mathrm{F})[\![\underline{|\mathrm{D}|}]\!] = \mathrm{D}$ if and only if $\mathrm{D}(n) \neq \emptyset$ for every $n \in \mathrm{dom}(\mathrm{D})$.*

Proof. For "$\Rightarrow$" let $n \in \mathrm{dom}(\mathrm{D})$ and observe that $\mathrm{D}(\mathrm{F})[n][1, \infty] = \mathrm{D}(\mathrm{F})[\mathrm{F}(n)]$ which implies that $\mathrm{D}[n][1, |\mathrm{D}| - 1] = \mathrm{D}(\mathrm{F})[n][1, |\mathrm{D}| - 1] = \mathrm{D}(\mathrm{F})[\mathrm{F}(n)][0, |\mathrm{D}| - 2] = \mathrm{D}[\mathrm{F}(n)][0, |\mathrm{D}| - 2]$. Therefore, $\mathrm{F}(n) \in \mathrm{D}(n)$.

To show "$\Leftarrow$" we prove $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}[\![\underline{k}]\!]$ for all $k \in [\![1, |\mathrm{D}|]\!]$ by induction on k. If $k = 1$ then this is clearly true by the definition of p-digit tables. Now assume $k \geq 2$ and let $n \in \mathrm{dom}(\mathrm{D})$. We get $\mathrm{D}(\mathrm{F})[\![\underline{k-1}]\!] = \mathrm{D}[\![\underline{k-1}]\!]$ by the induction hypothesis. Furthermore, $\mathrm{D}(\mathrm{F})[n][k-1] = \mathrm{D}(\mathrm{F})[\mathrm{F}(n)][k-2] = \mathrm{D}[\mathrm{F}(n)][k-2] = \mathrm{D}[n][k-1]$. Thus, $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}[\![\underline{k}]\!]$ and consequently $\mathrm{D}(\mathrm{F})[\![\underline{|\mathrm{D}|}]\!] = \mathrm{D}$. □

It is clear from the previous theorem that in order to get a better understanding of the relation between p-adic systems and p-digit tables with block property, we need to investigate the structure of the sets $\mathrm{D}(n)$. Before doing so, we need to prove two basic but useful lemmas on finite p-digit tables with block property at their lengths. From now on we interpret any complete residue system (CRS) $R \subseteq \mathbb{Z}_p$ modulo p^k (i.e. $|R| = p^k \in \mathbb{N}$ and no two distinct elements of R are congruent modulo p^k, e.g. $R = \underline{p^k}$) as a function $R : \mathbb{Z}_p \to R$ which maps any $n \in \mathbb{Z}_p$ to the unique $R(n) \in R$ with $n \equiv R(n) \mod p^k$.

Lemma 3.5. *Let $2 \leq p \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathrm{D} \in \mathcal{D}_p(\mathrm{len}_k, \mathrm{block}_k)$, $R \subseteq \mathrm{dom}(\mathrm{D})$ a CRS modulo p^k, and $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_k)$. Then there is a unique $n \in R$ such that $\mathrm{D}[n] = D$.*

Proof. Since $\left|\mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_k)\right| = |R| = p^k$ and $\mathrm{block}_k(\mathrm{D})$, every sequence in $\mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_k)$ occurs exactly once among the sequences $\mathrm{D}[r]$, $r \in R$. □

Lemma 3.6. *Let* $2 \leq p \in \mathbb{N}$, $k, \ell \in \mathbb{N}_0$ *with* $k < \ell$, $\mathrm{D} \in \mathcal{D}_p(\mathrm{len}_\ell, \mathrm{block}_\ell, \text{w-block}_k)$ *such that* $\mathrm{dom}(\mathrm{D})$ *contains a CRS modulo* p^ℓ. *Then* $\mathrm{block}_k(\mathrm{D})$.

Proof. Let $m, n \in \mathrm{dom}(\mathrm{D})$ such that $\mathrm{D}[m][\underline{k}] = \mathrm{D}[n][\underline{k}] =: D$ and assume $m \not\equiv n \mod p^k$. Furthermore, let $R \subseteq \mathrm{dom}(\mathrm{D})$ be a CRS modulo p^ℓ and

$$M := \left\{ r \in R \mid r \equiv m \mod p^k \vee r \equiv n \mod p^k \right\}. \tag{3.22}$$

Then $|M| = 2p^{\ell-k}$ and because of w-block$_k$(D), we get $\mathrm{D}[r][\underline{k}] = D$ for every $r \in M$. Thus, $\{\mathrm{D}[r] \mid r \in R\}$ can have at most $p^\ell - p^{\ell-k}$ elements, which contradicts Lemma 3.5 and hence implies block$_k$(D). □

The following theorem describes the structure of the sets $\mathrm{D}(n)$ in dependence of the structure of D.

Theorem 3.7. *Let* $2 \leq p \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathrm{D} \in \mathcal{D}_p(\mathrm{len}_k)$, $R, S \subseteq \mathrm{dom}(\mathrm{D})$ *CRSs modulo* p^k *and* p^{k-1} *respectively, and* $n \in \mathrm{dom}(\mathrm{D})$. *Then,*

(1) w-block$_k$(D) $\Rightarrow \mathrm{D}(n) = (\mathrm{D}(R(n)) \cap R + p^k\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D})$
In particular: (1) $\forall\, m \in (n + p^k\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D}) : \mathrm{D}(n) = \mathrm{D}(m)$
(2) $\mathrm{D}(n) = (\mathrm{D}(n) + p^k\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D})$

(2) w-block$_{\{k,k-1\}}$(D) $\Rightarrow \mathrm{D}(n) = (\mathrm{D}(R(n)) \cap S + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D})$
In particular: $\mathrm{D}(n) = (\mathrm{D}(n) + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D})$

(3) block$_k$(D) $\Rightarrow |\mathrm{D}(n) \cap R| = p$

(4) block$_k$(D) $\wedge$ w-block$_{k-1}$(D) $\Rightarrow \forall\, l, m \in \mathrm{D}(n) : l \equiv m \mod p^{k-1}$
In particular: $|\mathrm{D}(n) \cap S| = 1$ *and*
$\mathrm{D}(n) = (s_{R(n)} + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{D})$ *where*
$s_{R(n)}$ *is the unique element of* $\mathrm{D}(n) \cap S$.

Before we give a proof of the theorem, we will discuss its claims. (1) states that if D has the weak block property at k, then in order to know the structure of any $\mathrm{D}(n)$, it suffices to know the structures of $\mathrm{D}(r)$ within the finite set R alone, where $r \in R$ is again one element of only finitely many. In addition, the "In particular" part states that $\mathrm{D}(n)$ is closed under addition of multiples of p^k (if the result lands in the domain of D). (2) and (3) give even more precise information on the structure of $\mathrm{D}(n)$ if more is known on the structure of D. The results are stated in terms of arbitrary CRS R and S. To get a better understanding of the theorem, it is helpful to consider the most important special case $\mathrm{dom}(\mathrm{D}) \supseteq \mathbb{N}_0$, $R = \underline{p^k}$, $S = \underline{p^{k-1}}$, and hence $R(n) = n\%p^k$ for all $n \in \mathbb{Z}_p$. As examples consider the three 2-digit tables below which correspond to the three cases treated in the theorem. We get

$$\mathrm{D}_1(29) = (\mathrm{D}_1(5) \cap \underline{8} + 8\mathbb{Z}_2) \cap \mathbb{N}_0 = \{1, 3, 7\} + 8\mathbb{N}_0 \tag{3.23}$$

$$\mathrm{D}_2(29) = (\mathrm{D}_2(5) \cap \underline{8} + 8\mathbb{Z}_2) \cap \mathbb{N}_0 = \{0, 2\} + 8\mathbb{N}_0 \text{ (note: } |\{0, 2\}| = 2) \tag{3.24}$$

$$\mathrm{D}_3(29) = (\mathrm{D}_3(5) \cap \underline{4} + 4\mathbb{Z}_2) \cap \mathbb{N}_0 = 2 + 4\mathbb{N}_0 \tag{3.25}$$

just as claimed.

0	0	0	0
1	1	0	0
2	0	0	0
3	1	0	0
4	0	1	0
5	1	1	0
6	0	1	0
7	1	0	0
8	0	0	0
9	1	0	0
⋮	⋮	⋮	⋮
D_1	0	1	2

0	0	0	0
1	1	0	1
2	0	0	1
3	1	1	0
4	0	1	0
5	1	0	0
6	0	1	1
7	1	1	1
8	0	0	0
9	1	0	1
⋮	⋮	⋮	⋮
D_2	0	1	2

0	0	0	0
1	1	0	0
2	0	1	0
3	1	1	0
4	0	0	1
5	1	0	1
6	0	1	1
7	1	1	1
8	0	0	0
9	1	0	0
⋮	⋮	⋮	⋮
D_3	0	1	2

TABLE 2. Three 2-digit tables of length 3 with domain $\mathbb{N}_0$. The initial block of 8 rows is supposed to repeat periodically in all cases. They satisfy w-block$_3$(D_1), block$_3$(D_2), and block$_3$(D_3) $\wedge$ w-block$_2$(D_3).

Proof of Theorem 3.7.
(1):

$$\mathrm{D}(n) = \{m \in \mathrm{dom(D)} \mid \mathrm{D}[m][0,k-2] = \mathrm{D}[n][1,k-1]\} \tag{3.26}$$

$$(\text{w-block}_k(\mathrm{D})) = \{m \in \mathrm{dom(D)} \mid \mathrm{D}[R(m)][0,k-2] = \mathrm{D}[R(n)][1,k-1]\} \tag{3.27}$$

$$= \big(\{m \in R \mid \mathrm{D}[m][0,k-2] = \mathrm{D}[R(n)][1,k-1]\} + p^k\mathbb{Z}_p\big) \cap \mathrm{dom(D)} \tag{3.28}$$

$$= \big(\mathrm{D}(R(n)) \cap R + p^k\mathbb{Z}_p\big) \cap \mathrm{dom(D)}. \tag{3.29}$$

If $m \in (n + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)}$ then, $R(m) = R(n)$ and

$$\mathrm{D}(n) = (\mathrm{D}(R(n)) \cap R + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)} = (\mathrm{D}(R(m)) \cap R + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)} = \mathrm{D}(m) \tag{3.30}$$

which proves (1) of the "In particular" part. Furthermore, since $R(n) \in (n + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)}$, we get $\mathrm{D}(n) = \mathrm{D}(R(n))$ and thus

$$\mathrm{D}(n) = (\mathrm{D}(R(n)) \cap R + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)} = (\mathrm{D}(n) \cap R + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)} \tag{3.31}$$

$$= (\mathrm{D}(n) + p^k\mathbb{Z}_p) \cap \mathrm{dom(D)} \tag{3.32}$$

proving (2) of the "In particular" part.
(2): Analogously to Eqn. (3.26) – (3.29) we get

$$\mathrm{D}(n) = \{m \in \mathrm{dom(D)} \mid \mathrm{D}[m][0,k-2] = \mathrm{D}[n][1,k-1]\} \tag{3.33}$$

$$(\text{w-block}_{\{k,k-1\}}(\mathrm{D})) = \{m \in \mathrm{dom(D)} \mid \mathrm{D}[S(m)][0,k-2] = \mathrm{D}[R(n)][1,k-1]\} \tag{3.34}$$

$$= \big(\{m \in S \mid \mathrm{D}[m][0,k-2] = \mathrm{D}[R(n)][1,k-1]\} + p^{k-1}\mathbb{Z}_p\big) \cap \mathrm{dom(D)} \tag{3.35}$$

$$= (\mathrm{D}(R(n)) \cap S + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom(D)}. \tag{3.36}$$

For the "In particular" part we again observe that $\mathrm{D}(n) = \mathrm{D}(R(n))$, hence

$$\mathrm{D}(n) = (\mathrm{D}(R(n)) \cap S + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom(D)} = (\mathrm{D}(n) \cap S + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom(D)} \tag{3.37}$$

$$= (\mathrm{D}(n) + p^{k-1}\mathbb{Z}_p) \cap \mathrm{dom(D)}. \tag{3.38}$$

(3):

$$\mathrm{D}(n) \cap R = \{m \in R \mid \mathrm{D}[m][0,k-2] = \mathrm{D}[n][1,k-1]\} \tag{3.39}$$

$$= \{m \in R \mid \exists\, d \in \underline{p} : \mathrm{D}[m] = \mathrm{D}[n][1,k-1] \cdot (d)\}. \tag{3.40}$$

Thus, $\mathrm{block}_k(\mathrm{D})$ and Lemma 3.5 imply that $|\mathrm{D}(n) \cap R| = |\underline{p}| = p$.
(4): Let $l, m \in \mathrm{D}(n)$. Then, $\mathrm{D}[l][0,k-2] = \mathrm{D}[m][0,k-2]$ and hence $l \equiv m \mod p^{k-1}$ by $\mathrm{block}_k(\mathrm{D})$, $\text{w-block}_{k-1}(\mathrm{D})$, and Lemma 3.6 (which implies $\mathrm{block}_{k-1}(\mathrm{D})$). The "In particular" part then follows directly from (2). □

Using Theorem 3.4 and Theorem 3.7 we can completely characterize all 2-fibred functions which generate the finite 2-digit tables given in Table 2. If $\mathrm{F} \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{N}_0}, \text{closed})$ then

$$\mathrm{D(F)}[\![\underline{3}]\!] = \mathrm{D}_1 \Leftrightarrow \forall\, n \in \mathbb{N}_0 : \mathrm{F}(n) \in M_{n\%8} + 8\mathbb{N}_0 \text{ where} \tag{3.41}$$
$$M_0 := \{0,2\},\ M_1 := \{0,2\},\ M_2 := \{0,2\},\ M_3 := \{0,2\},$$
$$M_4 := \{1,3,7\},\ M_5 := \{1,3,7\},\ M_6 := \{1,3,7\},\ M_7 := \{0,2\}$$

$$\mathrm{D(F)}[\![\underline{3}]\!] = \mathrm{D}_2 \Leftrightarrow \forall\, n \in \mathbb{N}_0 : \mathrm{F}(n) \in M_{n\%8} + 8\mathbb{N}_0 \text{ where} \tag{3.42}$$
$$M_0 := \{0,2\},\ M_1 := \{4,6\},\ M_2 := \{4,6\},\ M_3 := \{1,5\},$$
$$M_4 := \{1,5\},\ M_5 := \{0,2\},\ M_6 := \{3,7\},\ M_7 := \{3,7\}$$

$$\mathrm{D(F)}[\![\underline{3}]\!] = \mathrm{D}_3 \Leftrightarrow \forall\, n \in \mathbb{N}_0 : \mathrm{F}(n) \in m_{n\%8} + 4\mathbb{N}_0 \text{ where} \tag{3.43}$$
$$m_0 := 0,\ m_1 := 0,\ m_2 := 1,\ m_3 := 1$$
$$m_4 := 2,\ m_5 := 2,\ m_6 := 3,\ m_7 := 3.$$

The rows of the F-digit table of a closed p-fibred function F are computed by iterative application of F. Actually performing these iterations can be a very difficult task if F is complicated or highly

expansive. The following corollary provides a useful method to actually compute p-digit tables of p-fibred functions that at least have the weak block property.

Corollary 3.8. *Let $2 \leq p \in \mathbb{N}$, $k \in \mathbb{N}$, $\mathrm{F}, \mathrm{G}_1, \mathrm{G}_2, \mathrm{H}_1, \mathrm{H}_2 \in \mathcal{F}_p(\text{closed})$ of equal domain, and $R, S, T \subseteq \mathbb{Z}_p$ CRSs modulo p^{k+1}, p^k, and p^k respectively, such that*

$$\mathrm{G}_1[r](n) = R(\mathrm{F}[r](n)) \tag{3.44}$$

$$\mathrm{G}_2[r](n) = R(\mathrm{F}[r](T(n))) \tag{3.45}$$

$$\mathrm{H}_1[r](n) = S(\mathrm{F}[r](n)) \tag{3.46}$$

$$\mathrm{H}_2[r](n) = S(\mathrm{F}[r](T(n))) \tag{3.47}$$

for all $r \in \underline{p}$ and all $n \in (r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})$, and

$$R' := \left\{ \frac{r - r\%p}{p} \mid r \in R \right\}, \qquad S' := \left\{ \frac{s - s\%p}{p} \mid s \in S \right\}. \tag{3.48}$$

Then,

(1) $\mathrm{bnd}_{R'}(\mathrm{G}_1)$, $\mathrm{bnd}_{R'}(\mathrm{G}_2)$, $\mathrm{bnd}_{S'}(\mathrm{H}_1)$, $\mathrm{bnd}_{S'}(\mathrm{H}_2)$
(2) $\text{w-block}_k(\mathrm{F}) \Rightarrow$
  $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G}_1)[\![\underline{k}]\!]$
  $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G}_2)[\![\underline{k}]\!]$, $\forall\, n \in \mathrm{dom}(\mathrm{F}) : \mathrm{G}_2(n) = \mathrm{G}_2(T(n))$
  $\text{w-block}_{\{k,k-1\}}(\mathrm{F}) \Rightarrow$
  $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{H}_1)[\![\underline{k}]\!]$
  $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{H}_2)[\![\underline{k}]\!]$, $\forall\, n \in \mathrm{dom}(\mathrm{F}) : \mathrm{H}_2(n) = \mathrm{H}_2(T(n))$
  $\mathrm{block}_k(\mathrm{F}) \wedge \text{w-block}_{k-1}(\mathrm{F})$ *and S' CRS modulo p^{k-1}* $\Rightarrow$
  $\forall\, n \in \mathrm{dom}(\mathrm{F}) : \mathrm{H}_1(n) = \mathrm{H}_1(T(n)) = \mathrm{H}_2(n)$.

We will prove a slightly stronger version of the last statement of (2) in a later part of the paper (Corollary 4.4 (3)).

As an example we consider $p = 3$, $k = 5$, $R = \underline{3^6}$, $S = T = \underline{3^5}$, and

$$\mathrm{F} = (7x^3 - 4x^2 + x - 6, 3x^7 - x + 1, x^2 + 6x + 2) \tag{3.49}$$

with $\mathrm{dom}(\mathrm{F}) = \mathbb{Z}_3$. Then, $\mathrm{block}(\mathrm{F})$ (as we will prove later, Corollary 4.11 (2)) and

$$\mathrm{H}_1(n) = (\mathrm{F}[0](n) \quad \%3^5, \mathrm{F}[1](n) \quad \%3^5, \mathrm{F}[2](n) \quad \%3^5) \tag{3.50}$$

$$\mathrm{H}_2(n) = (\mathrm{F}[0](n\%3^5)\%3^5, \mathrm{F}[1](n\%3^5)\%3^5, \mathrm{F}[2](n\%3^5)\%3^5) \tag{3.51}$$

for all $n \in \mathbb{Z}_3$. As claimed by the corollary, we get $\mathrm{H}_1(n) = \mathrm{H}_1(n\%3^5) = \mathrm{H}_2(n) \in \underline{3^4}$ for all $n \in \mathbb{Z}_3$ and

$$\mathrm{D}(\mathrm{F})[17][\underline{5}] = \mathrm{D}(\mathrm{H}_1)[17][\underline{5}] = (2, 2, 1, 2, 0) \tag{3.52}$$

but $\mathrm{S}(\mathrm{H}_1)[17][4] = 63$ while $\mathrm{S}(\mathrm{F})[17][4] = 2.51041\ldots \cdot 10^{52}$.

Proof of Corollary 3.8.
(1): Let $n \in \mathrm{dom}(\mathrm{F})$. Then,

$$\mathrm{G}_1(n) = \frac{\mathrm{G}_1[n\%p](n) - \mathrm{G}_1[n\%p](n)\%p}{p} = \frac{R(\mathrm{F}[n\%p](n)) - R(\mathrm{F}[n\%p](n))\%p}{p} \in R'. \tag{3.53}$$

The remaining statements can be proven analogously.
(2): We will prove

$$\mathrm{G}_1(n), \mathrm{G}_2(n), \mathrm{H}_1(n), \mathrm{H}_2(n) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n) \tag{3.54}$$

for all $n \in \mathrm{dom}(\mathrm{F})$ from which it follows by Theorem 3.4 that

$$\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G}_1)[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G}_2)[\![\underline{k}]\!] = \mathrm{D}(\mathrm{H}_1)[\![\underline{k}]\!] = \mathrm{D}(\mathrm{H}_2)[\![\underline{k}]\!]. \tag{3.55}$$

Let $n \in \mathrm{dom}(\mathrm{F})$. Then,

$$\mathrm{G}_1(n) = \frac{\mathrm{G}_1[n\%p](n) - \mathrm{G}_1[n\%p](n)\%p}{p} = \frac{R(\mathrm{F}[n\%p](n)) - R(\mathrm{F}[n\%p](n))\%p}{p} \tag{3.56}$$

$$\equiv \frac{\mathrm{F}[n\%p](n) - \mathrm{F}[n\%p](n)\%p}{p} = \mathrm{F}(n) \mod p^k. \tag{3.57}$$

In addition, $\mathrm{F}(n) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$ and thus $\mathrm{G}_1(n) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$ by w-block$_k$(F) and by (1) of the "In particular" part of Theorem 3.7 (1).

Analogously,

$$\mathrm{G}_2(n) = \frac{\mathrm{G}_2[n\%p](n) - \mathrm{G}_2[n\%p](n)\%p}{p} = \frac{R(\mathrm{F}[n\%p](T(n))) - R(\mathrm{F}[n\%p](T(n)))\%p}{p} \tag{3.58}$$

$$\equiv \frac{\mathrm{F}[n\%p](T(n)) - \mathrm{F}[n\%p](T(n))\%p}{p} = \mathrm{F}(T(n)) \mod p^k. \tag{3.59}$$

In addition, $\mathrm{F}(T(n)) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](T(n)) = \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$ by (2) of the "In particular" part of Theorem 3.7 (1) which again implies $\mathrm{G}_2(n) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$.

It can be shown in a completely analogous fashion that

$$\mathrm{H}_1(n) \equiv \mathrm{F}(n) \mod p^{k-1} \tag{3.60}$$

$$\mathrm{H}_2(n) \equiv \mathrm{F}(T(n)) \mod p^{k-1} \tag{3.61}$$

and hence $\mathrm{H}_1(n), \mathrm{H}_2(n) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$ by w-block$_{\{k,k-1\}}$(F) and by the "In particular" part of Theorem 3.7 (2) which completes the proof of Eqn. (3.55).

Clearly, $\mathrm{G}_2(n) = \mathrm{G}_2(T(n))$ and $\mathrm{H}_1(T(n)) = \mathrm{H}_2(n) = \mathrm{H}_2(T(n))$. We are thus left to show that $\mathrm{H}_1(n) = \mathrm{H}_1(T(n))$ if block$_k$(F), w-block$_{k-1}$(F), and S' is a CRS modulo p^{k-1}. We observe that $\mathrm{H}_1(T(n)) \equiv \mathrm{F}(T(n)) \mod p^{k-1}$ and thus $\mathrm{H}_1(T(n)) \in \mathrm{D}(\mathrm{F})[\![\underline{k}]\!](n)$. But then $\mathrm{H}_1(T(n)) \equiv \mathrm{H}_1(n) \mod p^{k-1}$ by Theorem 3.7 (4), and since both $\mathrm{H}_1(T(n))$ and $\mathrm{H}_1(n)$ are in S' by (1), they must be equal. □

Now that we know exactly how to generate a finite p-digit table using a p-fibred function, we are left with dealing with the infinite case which will finally establish the relation between p-adic systems and infinite p-digit tables with block property and prove the claimed existence of a one-to-one correspondence. We continue with two basic lemmas on infinite p-digit tables with block property and one corollary on p-adic systems.

Lemma 3.9. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{D} \in \mathcal{D}_p(\neg\mathrm{fin}, \mathrm{block})$, and $m, n \in \mathrm{dom}(\mathrm{D})$. Then, $m = n$ if and only if $\mathrm{D}[m] = \mathrm{D}[n]$.*

Proof.

$$m = n \Leftrightarrow \forall\, k \in \mathbb{N} : m \equiv n \mod p^k \Leftrightarrow \forall\, k \in \mathbb{N} : \mathrm{D}[m][\underline{k}] = \mathrm{D}[n][\underline{k}] \Leftrightarrow \mathrm{D}[m] = \mathrm{D}[n]. \tag{3.62}$$

□

From the previous lemma can be derived the following useful corollary on p-adic systems.

Corollary 3.10. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p$, and $n \in \mathbb{Z}_p$. Then, $|\mathcal{I}(\mathrm{S}(\mathrm{F})[n])| = |\mathcal{I}(\mathrm{D}(\mathrm{F})[n])|$ and $|\mathcal{P}(\mathrm{S}(\mathrm{F})[n])| = |\mathcal{P}(\mathrm{D}(\mathrm{F})[n])|$. In particular,* per$(\mathrm{S}(\mathrm{F})[n]) \Leftrightarrow$ per$(\mathrm{D}(\mathrm{F})[n])$, uper$(\mathrm{S}(\mathrm{F})[n]) \Leftrightarrow$ uper$(\mathrm{D}(\mathrm{F})[n])$, *and* aper$(\mathrm{S}(\mathrm{F})[n]) \Leftrightarrow$ aper$(\mathrm{D}(\mathrm{F})[n])$.

Proof. Let $k, \ell \in \mathbb{N}_0$. Then,

$$\mathrm{S}(\mathrm{F})[n][k+\ell, \infty] = \mathrm{S}(\mathrm{F})[n][k, \infty] \Leftrightarrow \mathrm{S}(\mathrm{F})[\mathrm{F}^{k+\ell}(n)] = \mathrm{S}(\mathrm{F})[\mathrm{F}^k(n)] \tag{3.63}$$

$$\Leftrightarrow \mathrm{F}^{k+\ell}(n) = \mathrm{F}^k(n) \tag{3.64}$$

$$\text{(by Lemma 3.9)} \Leftrightarrow \mathrm{D}(\mathrm{F})[\mathrm{F}^{k+\ell}(n)] = \mathrm{D}(\mathrm{F})[\mathrm{F}^k(n)] \tag{3.65}$$

$$\Leftrightarrow \mathrm{D}(\mathrm{F})[n][k+\ell, \infty] = \mathrm{D}(\mathrm{F})[n][k, \infty]. \tag{3.66}$$

If $k := |\mathcal{I}(\mathrm{S(F)}[n])|$ and $\ell := |\mathcal{P}(\mathrm{S(F)}[n])|$, then $\mathrm{S(F)}[n][k+\ell,\infty] = \mathrm{S(F)}[n][k,\infty]$ and hence $\mathrm{D(F)}[n][k+\ell,\infty] = \mathrm{D(F)}[n][k,\infty]$. Thus,

$$|\mathcal{I}(\mathrm{D(F)}[n])| \leq |\mathcal{I}(\mathrm{S(F)}[n])| \tag{3.67}$$

$$|\mathcal{P}(\mathrm{D(F)}[n])| \leq |\mathcal{P}(\mathrm{S(F)}[n])|. \tag{3.68}$$

Analogously, if $k := |\mathcal{I}(\mathrm{D(F)}[n])|$ and $\ell := |\mathcal{P}(\mathrm{D(F)}[n])|$, then $\mathrm{D(F)}[n][k+\ell,\infty] = \mathrm{D(F)}[n][k,\infty]$ and hence $\mathrm{S(F)}[n][k+\ell,\infty] = \mathrm{S(F)}[n][k,\infty]$. Thus,

$$|\mathcal{I}(\mathrm{S(F)}[n])| \leq |\mathcal{I}(\mathrm{D(F)}[n])| \tag{3.69}$$

$$|\mathcal{P}(\mathrm{S(F)}[n])| \leq |\mathcal{P}(\mathrm{D(F)}[n])|. \tag{3.70}$$

□

The following lemma is an analogue to the finite case treated in Lemma 3.5.

Lemma 3.11. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{D} \in \overline{\mathcal{D}}_p$, and $D \in \mathbf{S}(\mathrm{bnd}_p, \neg\mathrm{fin})$. Then, there is a unique $n \in \mathbb{Z}_p$ such that $\mathrm{D}[n] = D$. In particular, $|\mathrm{D}(n)| = 1$ for every $n \in \mathbb{Z}_p$.*

Proof. For every $i \in \mathbb{N}$ let r_i be the unique (by Lemma 3.5) element of $\underline{p^i}$ such that $\mathrm{D}[r_i][\underline{i}] = D[\underline{i}]$. Furthermore, let $n_0 := r_1 \in \underline{p}$, $n_i := (r_{i+1} - r_i)/p^i \in \underline{p}$ for all $i \in \mathbb{N}$, and $n := \sum_{i=0}^{\infty} n_i p^i \in \mathbb{Z}_p$. Then, $n \equiv \sum_{i=0}^{k-1} n_i p^i = s_k \mod p^k$ and hence $\mathrm{D}[n][\underline{k}] = \mathrm{D}[s_k][\underline{k}] = D[\underline{k}]$ for all $k \in \mathbb{N}$. The uniqueness of n follows directly from Lemma 3.9. □

Using the above lemmas we are finally able to establish the claimed relation between p-adic systems and infinite p-digit tables with block property.

Theorem 3.12. *Let $2 \leq p \in \mathbb{N}$ and $\mathrm{D} \in \overline{\mathcal{D}}_p$. Then, there is a unique $\mathrm{F_D} \in \mathcal{F}_p(\mathrm{canf})$ such that $\mathrm{D}(\mathrm{F_D}) = \mathrm{D}$. In particular, $\mathrm{F_D}$ is a p-adic system.*

Proof. From Lemma 3.11 we get $|\mathrm{D}(n)| = 1$ for every $n \in \mathbb{Z}_p$. Let $\mathrm{F_D} \in \mathcal{F}_p$ with

$$\mathrm{F_D}[r] : \mathbb{Z}_p \to \mathbb{Z}_p \qquad n \mapsto \begin{cases} p\mathrm{D}(n) & \text{if } n \equiv r \mod p \quad \text{(cf. Eqn. (2.3))} \\ 0 & \text{if } n \not\equiv r \mod p \end{cases} \tag{3.71}$$

for all $r \in \underline{p}$. Then, $\mathrm{canf}(\mathrm{F_D})$ and $\mathrm{D}(\mathrm{F_D}) = \mathrm{D}$ by Theorem 3.4. Furthermore, $\mathrm{F_D}$ is uniquely defined by this property by Lemma 3.1 and Theorem 3.4. □

Theorem 3.12 finally proves that there is a one-to-one correspondence between p-adic systems (modulo $\sim_p$) and infinite p-digit tables with block property given by

$$\begin{aligned} \overline{\mathcal{F}}_p/_{\sim_p} &\leftrightarrow \overline{\mathcal{D}}_p. \\ \mathrm{F} &\mapsto \mathrm{D(F)} \\ \mathrm{F_D} &\hookleftarrow \mathrm{D} \end{aligned} \tag{3.72}$$

In this sense we might as well define a p-adic system to be an infinite p-digit table with domain $\mathbb{Z}_p$ and block property and consider the corresponding p-fibred function to be its feature instead of interpreting it the other way around. The decision to choose the dynamical interpretation over the statical one in the definition (and thus fix a certain mindset) is somewhat arbitrary, but will be explained to some extent in the upcoming section. Nevertheless, we may choose to go back and forth between both interpretations if certain things are easier to see or prove in one setting or the other.

Considering the above theorem, a natural question to ask is whether all p-digit tables that only have the weak block property but not the the block property, can also be realized as the p-digit table of a closed p-fibred function. That this is not the case, is proven by the following counter-example.

Example 3.13. Let $\mathrm{D} := ((n \equiv 0 \mod 2\ ?\ (0)^\infty : (1,0)\cdot(1)^\infty))_{n\in\mathbb{Z}_2}$. Then, w-block(D) but, since $\mathrm{D}(1) = \emptyset$, Theorem 3.4 implies that there is no closed p-fibred function F such that $\mathrm{D(F)} = \mathrm{D}$.

As a first example of how the relation between p-adic systems and p-digit tables can be exploited, we show that any infinite p-digit table with block property whose domain is dense in $\mathbb{Z}_p$, can be extended to $\mathbb{Z}_p$ in a unique way such that the block property still holds. This implies an equal statement for p-adic systems: any p-fibred function with block property whose domain is dense in $\mathbb{Z}_p$, has a unique extension to a p-adic system (i.e. its domain can be extended to $\mathbb{Z}_p$ such that the block property is preserved).

Lemma 3.14. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{D}, \mathrm{E} \in \mathcal{D}_p(\text{w-block})$ *of equal domain such that* $\mathrm{D}|_A = \mathrm{E}|_A$ *for some set* $A \subseteq \mathrm{dom}(\mathrm{D})$ *that is dense in* $\mathbb{Z}_p$*. Then,* $\mathrm{D} = \mathrm{E}$*.*

Proof. Assume to the contrary that $\mathrm{D} \neq \mathrm{E}$. Then there is an $n \in \mathrm{dom}(\mathrm{D})$ and a $k \in \mathbb{N}_0$ such that $\mathrm{D}[n][k] \neq \mathrm{E}[n][k]$. Since A is dense in $\mathbb{Z}_p$, there is an $N \in A$ with $N \equiv n \mod p^{k+1}$. Then, w-block(D) and w-block(E) implies

$$\mathrm{D}[n][\overline{k}] = \mathrm{D}[N][\overline{k}] = \mathrm{E}[N][\overline{k}] = \mathrm{E}[n][\overline{k}]. \tag{3.73}$$

In particular, $\mathrm{D}[n][k] = \mathrm{E}[n][k]$, which is a contradiction. □

Lemma 3.15. *Let* $2 \leq p \in \mathbb{N}$*,* $\mathrm{D} \in \mathcal{D}_p(\text{w-block})$ *such that* $\mathrm{dom}(\mathrm{D})$ *is dense in* $\mathbb{Z}_p$*, and let* $\mathrm{E} \in \mathcal{D}_p(\mathrm{dom}_{\mathbb{Z}_p})$ *be defined in the following way: for* $n \in \mathbb{Z}_p$ *and* $k \in \mathbb{N}_0$ *let* $\mathrm{E}[n][k] := \mathrm{D}[N][k]$ *where* $N \in \mathrm{dom}(\mathrm{D})$ *such that* $N \equiv n \mod p^{k+1}$ *(well-defined due to* w-block(D)*). Then,* w-block(E) *and* $\mathrm{E}|_{\mathrm{dom}(\mathrm{D})} = \mathrm{D}$ *and* E *is uniquely defined by this property. Furthermore, if* block(D)*, then* block(E)*.*

Proof. Uniqueness follows directly from Lemma 3.14.

Let $n \in \mathbb{Z}_p$, $k \in \mathbb{N}$, and $N \in \mathrm{dom}(\mathrm{D})$ such that $N \equiv n \mod p^k$. Then $N \equiv n \mod p^{i+1}$ and hence $\mathrm{E}[n][i] = \mathrm{D}[N][i]$ for all $i \in \underline{k}$ which implies $\mathrm{E}[n][\underline{k}] = \mathrm{D}[N][\underline{k}]$. If $n \in \mathrm{dom}(\mathrm{D})$, this further implies that $\mathrm{E}[n][\underline{k}] = \mathrm{D}[N][\underline{k}] = \mathrm{D}[n][\underline{k}]$ and we conclude $\mathrm{E}|_{\mathrm{dom}(\mathrm{D})} = \mathrm{D}$.

Now let $m, n \in \mathbb{Z}_p$, $k \in \mathbb{N}$ with $m \equiv n \mod p^k$, and $M \in \mathrm{dom}(\mathrm{D})$ such that $M \equiv m \mod p^k$. Then, $M \equiv n \mod p^k$ and $\mathrm{E}[m][\underline{k}] = \mathrm{D}[M][\underline{k}] = \mathrm{E}[n][\underline{k}]$. Therefore, w-block(E).

Finally, assume that block(D) and let $m, n \in \mathbb{Z}_p$, $k \in \mathbb{N}$ with $\mathrm{E}[m][\underline{k}] = \mathrm{E}[n][\underline{k}]$, and $M, N \in \mathrm{dom}(\mathrm{D})$ such that $M \equiv m \mod p^k$ and $N \equiv n \mod p^k$. Then,

$$\mathrm{D}[M][\underline{k}] = \mathrm{E}[m][\underline{k}] = \mathrm{E}[n][\underline{k}] = \mathrm{D}[N][\underline{k}], \tag{3.74}$$

and since block(D), this implies that $m \equiv M \equiv N \equiv n \mod p^k$. Therefore, block(E). □

Corollary 3.16. *Let* $\mathrm{F} \in \mathcal{F}_p(\text{w-block})$ *with* $\mathrm{dom}(\mathrm{F})$ *dense in* $\mathbb{Z}_p$*,* $\mathrm{G} \in \mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p}, \text{w-block})$ *such that* $\mathrm{G}|_{\mathrm{dom}(\mathrm{F})} = \mathrm{F}$*, and* $\mathrm{E} \in \mathcal{D}_p(\mathrm{dom}_{\mathbb{Z}_p}, \text{w-block})$ *such that* $\mathrm{E}|_{\mathrm{dom}(\mathrm{F})} = \mathrm{D}(\mathrm{F})$ *(cf. Lemma 3.15). Then,* $\mathrm{E} = \mathrm{D}(\mathrm{G})$*.*

Proof. Follows directly from Lemma 3.15. □

By Lemma 3.14 and Lemma 3.15 a p-digit table with weak block property is uniquely defined by its restriction to any dense subset of its domain. Because of the nature of the weak block property, we can even go one step further and drop more redundant information to gain a minimal representation of a given p-digit table with weak block property that still allows to recover the full table. Looking at the examples given in Table 1, one can see that due to the repetition of blocks the full table can be reconstructed from the sequence gained by concatenating the rightmost rows in each block. Formally, if $2 \leq p \in \mathbb{N}$ and $k \in \mathbb{N} \cup \{\infty\}$, then there is a bijection between the set of all p-digit tables of length k that have domain $\mathbb{Z}_p$ and the weak block property and the set of all $\underline{p}$-bounded sequences of length $(p^{k+1}-1)/(p-1)-1$ with prefix $(0, \ldots, p-1)$ given by

$$\begin{aligned} \mathcal{D}_p(\mathrm{dom}_{\mathbb{Z}_p}, \mathrm{len}_k, \text{w-block}) &\leftrightarrow \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_{(p^{k+1}-1)/(p-1)-1}, \mathrm{pre}_{(0,\ldots,p-1)}) \\ \mathrm{D} &\mapsto \prod_{\ell=0}^{k-1} \prod_{n=0}^{p^{\ell+1}-1} (\mathrm{D}[n][\ell]) \\ \left(\left(D \left[\frac{p^{\ell+1}-1}{p-1} - 1 + n \% p^{\ell+1} \right] \right)_{\ell \in \underline{k}} \right)_{n \in \mathbb{Z}_p} &\hookleftarrow D \end{aligned} \tag{3.75}$$

where the product denotes a product of one-element sequences (i.e. their concatenation). In this interpretation the p-digit tables with weak block property correspond exactly to the $\underline{p}$-bounded sequences of a certain length (and a specific prefix necessary for technical reasons). The question arises how the stronger block property of p-digit tables (which makes them p-adic systems after all) translates to the corresponding sequences. In order to answer this question, we define the following two predicates on $\mathbf{S}$ ($2 \leq p \in \mathbb{N}$, $k \in \mathbb{N} \cup \{\infty\}$, $S \in \mathbf{S}$):

$$\begin{aligned}(3.76)\quad \text{w-block}_{p,k}(S) \Leftrightarrow\ & \text{bnd}_{\underline{p}}(S) && S \text{ has the } \textit{weak } (p,k)\textit{-block property}\\ & \text{len}_{(p^{k+1}-1)/(p-1)-1}(S)\\ & \text{pre}_{(0,\ldots,p-1)}(S)\end{aligned}$$

$$\begin{aligned}(3.77)\quad \text{block}_{p,k}(S) \Leftrightarrow\ & \text{w-block}_{p,k}(S) && S \text{ has the } (p,k)\textit{-block property}\\ & \forall\, \ell \in \underline{k} : \forall\, n \in (p^{\ell+1}-1)/(p-1) - 1 + \underline{p^\ell} : \left\{S[n+ip^\ell] \mid i \in \underline{p}\right\} = \underline{p}\end{aligned}$$

A quick check of the definitions shows that a sequence with the (p,k)-block property corresponds to (by the above mapping) a p-digit table that has the block property and vice versa. Therefore, the restriction of the above mapping also defines a bijection between $\mathcal{D}_p(\text{dom}_{\mathbb{Z}_p}, \text{len}_k, \text{block})$ and $\mathbf{S}(\text{block}_{p,k})$. This is true in particular for $k = \infty$, in which case we get a bijection between $\overline{\mathcal{D}}_p$ and $\mathbf{S}(\text{block}_{p,\infty})$.

As an example we consider the well-known Thue-Morse sequence

$$(3.78)\qquad T := (0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,0,1,1,0,1,0,0,1,\ldots)$$

which, according to its Wikipedia article, is "obtained by starting with 0 and successively appending the Boolean complement of the sequence obtained thus far". By slight modification of its beginning it is actually possible to make it satisfy the $(2,\infty)$-block property and thus define a 2-adic system. For that we set

$$(3.79)\qquad S := (0,1)\cdot T[4,\infty]$$

$$(3.80)\qquad = (0,1,1,0,0,1,1,0,0,1,0,1,1,0,1,0,0,1,0,1,1,0,0,1,1,0,1,0,0,1,\ldots).$$

The corresponding 2-adic system which generates this sequence can be found easily using the results of this subsection and is given by

$$(3.81)\qquad \mathrm{F} := (x+6-2(x\%8), x+3-2(x\%8)+2(x\%4)).$$

It can be readily verified that S is indeed equal to the sequence obtained from $D = \mathrm{D}(\mathrm{F})$ when using the bijection defined in Eqn. (3.75). Despite best efforts, the author was unable to find any reference to this method for defining the Thue-Morse sequence in the literature. Furthermore, it appears worth noting that the corresponding sequence of the even simpler 2-adic system

$$(3.82)\qquad \mathrm{G} := (x, x+3-2(x\%4))$$

coincides with $1 - T[2,\infty]$, the truncated Boolean complement of the Thue-Morse sequence.

Permutations of p-adic integers that respect congruence modulo powers of p. The last interpretation of p-adic systems we give in this section is that of permutations of $\mathbb{Z}_p$. Clearly, every p-adic system F defines a bijection between $\mathbb{Z}_p$ and $\mathbf{S}(\text{bnd}_{\underline{p}}, \neg\text{fin})$ by its F-digit table. We define

$$(3.83)\qquad \begin{aligned}\psi_{\mathrm{F}} : \mathbb{Z}_p &\to \mathbf{S}(\text{bnd}_{\underline{p}}, \neg\text{fin}).\\ n &\mapsto \mathrm{D}(\mathrm{F})[n]\end{aligned}$$

If one interprets an infinite sequence with entries in $\underline{p}$ as the usual base p expansion of a p-adic integer, then ψ_{F} also defines a permutation of $\mathbb{Z}_p$. This is a special case of the following idea: for two p-adic systems F and G let

$$(3.84)\qquad \pi_{\mathrm{F},\mathrm{G}} := {\psi_{\mathrm{G}}}^{-1} \circ \psi_{\mathrm{F}} : \mathbb{Z}_p \to \mathbb{Z}_p.$$

Then $\pi_{\mathrm{F},\mathrm{G}}$ clearly defines a permutation of $\mathbb{Z}_p$. Interpreting the infinite sequences that ψ_{F} yields as the usual base p expansions, corresponds to the choice $\mathrm{G} = \mathrm{F}_p = (x)^p = (x,\ldots,x)$ (cf. Eqn. (2.33)). As an example consider $\mathrm{F} := \mathrm{F}_C$ and $\mathrm{G} := \mathrm{F}_2$. Then we get $\mathrm{D}(\mathrm{F})[1] = (1,0)^\infty = \mathrm{D}(\mathrm{G})[-1/3]$ and hence $\pi_{\mathrm{F},\mathrm{G}}(1) = -1/3$.

Several properties of permutations of the form $\pi_{\mathrm{F,G}}$ are summarized in the following lemma.

Lemma 3.17. *Let $2 \leq p \in \mathbb{N}$, F and G two p-adic systems, $\pi := \pi_{\mathrm{F,G}}$, and $k \in \mathbb{N}_0$. Then,*

(1) $\forall\, m, n \in \mathbb{Z}_p : m \equiv n \mod p^k \Leftrightarrow \pi(m) \equiv \pi(n) \mod p^k$
In particular: π is measure preserving (and thus continuous) and it induces a permutation π_k of $\mathbb{Z}_p/p^k\mathbb{Z}_p$ by $[n] \mapsto [\pi(n)]$

(2) $\forall\, m, n \in \mathbb{Z}_p$ *with* $n \equiv \pi(m) \mod p^k : \forall\, M, N \in \mathbb{Z}_p$ *with* $N \equiv \pi(M) \mod p^{k+1}$:
$m \equiv M \mod p^k \Rightarrow n \equiv N \mod p^k$,
Note: $n \equiv \pi(m) \mod p^k \Leftrightarrow n \in \pi_k([m])$ and $N \equiv \pi(M) \mod p^{k+1} \Leftrightarrow N \in \pi_{k+1}([M])$

(3) $\pi^{-1} = \pi_{\mathrm{G,F}}$

(4) $\forall\, n \in \mathbb{Z}_p : \psi_{\mathrm{F}}(\mathrm{F}(n)) = \psi_{\mathrm{F}}(n)[1, \infty]$
In particular: $\forall\, \mathrm{D} \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \neg\mathrm{fin}) : \psi_{\mathrm{F}}(\mathrm{F}({\psi_{\mathrm{F}}}^{-1}(\mathrm{D}))) = \mathrm{D}[1, \infty]$

(5) $\forall\, n \in \mathbb{Z}_p : \pi(\mathrm{F}(n)) = \mathrm{G}(\pi(n))$ *and* $\mathrm{F}(\pi^{-1}(n)) = \pi^{-1}(\mathrm{G}(n))$.

Proof.
(1):

$$m \equiv n \mod p^k \Leftrightarrow \psi_{\mathrm{F}}(m)[\underline{k}] = \psi_{\mathrm{F}}(n)[\underline{k}] \ \ (\mathrm{block(F)}) \tag{3.85}$$

$$\Leftrightarrow \psi_{\mathrm{G}}({\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(m)))[\underline{k}] = \psi_{\mathrm{G}}({\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(n)))[\underline{k}] \tag{3.86}$$

$$(\mathrm{block(G)}) \Leftrightarrow {\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(m)) \equiv {\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(n)) \mod p^k \tag{3.87}$$

$$\Leftrightarrow \pi(m) \equiv \pi(n) \mod p^k. \tag{3.88}$$

(2): From $m \equiv M \mod p^k$ and (1) it follows that $n \equiv \pi(m) \equiv \pi(M) \equiv N \mod p^k$.
(3): Follows directly from the definitions.
(4): For every $n \in \mathbb{Z}_p$ we have

$$\psi_{\mathrm{F}}(\mathrm{F}(n)) = \mathrm{D}(\mathrm{F})[\mathrm{F}(n)] = \mathrm{D}(\mathrm{F})[n][1, \infty] = \psi_{\mathrm{F}}(n)[1, \infty]. \tag{3.89}$$

For the "In particular" part set $n := {\psi_{\mathrm{F}}}^{-1}(\mathrm{D})$. Then,

$$\psi_{\mathrm{F}}(\mathrm{F}({\psi_{\mathrm{F}}}^{-1}(\mathrm{D}))) = \psi_{\mathrm{F}}({\psi_{\mathrm{F}}}^{-1}(\mathrm{D}))[1, \infty] = \mathrm{D}[1, \infty]. \tag{3.90}$$

(5): From (4) it follows that

$$\psi_{\mathrm{G}}(\pi(\mathrm{F}(n))) = \psi_{\mathrm{G}}({\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(\mathrm{F}(n)))) = \psi_{\mathrm{F}}(n)[1, \infty] = \psi_{\mathrm{G}}(\mathrm{G}({\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(n)))) \tag{3.91}$$

$$= \psi_{\mathrm{G}}(\mathrm{G}(\pi(n))) \tag{3.92}$$

and hence $\pi(\mathrm{F}(n)) = \mathrm{G}(\pi(n))$. To see $\mathrm{F}(\pi^{-1}(n)) = \pi^{-1}(\mathrm{G}(n))$ just substitute n with $\pi^{-1}(n)$. □

In the previous paragraph we observed that p-digit tables coming from p-adic systems have a specific property (the block property). We then tried to answer the question if every p-digit table with block property can be recognized as the F-digit table of a p-adic system F and we found that this is indeed the case. We will now try to pursue the same strategy for permutations of p-adic integers, where the special property which we demand to hold is given by (1) of the previous lemma. Indeed, we call a permutation $\pi : \mathbb{Z}_p \to \mathbb{Z}_p$ of the p-adic integers a *p-adic permutation* if the following two properties hold:

$$\forall\, n \in \mathbb{Z}_p : \pi(n) \equiv n \mod p \tag{3.93}$$

$$\forall\, k \in \mathbb{N} : \forall\, m, n \in \mathbb{Z}_p : m \equiv n \mod p^k \Leftrightarrow \pi(m) \equiv \pi(n) \mod p^k. \tag{3.94}$$

The *set of p-adic permutations* shall be denoted by $\overline{\mathcal{P}}_p$. For every p-adic permutation π and every $k \in \mathbb{N}_0$ we define (cf. (1) of the previous lemma)

$$\pi_k : \mathbb{Z}_p/p^k\mathbb{Z}_p \to \mathbb{Z}_p/p^k\mathbb{Z}_p. \tag{3.95}$$
$$[n] \mapsto [\pi(n)]$$

Clearly, every permutation of the form $\pi = \pi_{\mathrm{F,G}}$ where F and G are p-adic systems is a p-adic permutation by the previous lemma (cf. also Eqn. (2.18)). The question is if every p-adic permutation can be expressed in this way and the answer is given in the following theorem.

Theorem 3.18. *Let $2 \leq p \in \mathbb{N}$, π a p-adic permutation, and* G *a p-adic system. Then there is a p-adic system* F *such that $\pi = \pi_{\mathrm{F,G}}$.* F *is uniquely defined up to $\sim_p$.*

Proof. Let

$$\mathrm{D} := (\psi_{\mathrm{G}}(\pi(n)))_{n\in\mathbb{Z}_p}. \tag{3.96}$$

We claim that D is a p-digit table. Then, Theorem 3.12 implies that there is a unique (up to $\sim_p$) p-adic system F such that $\mathrm{D} = \mathrm{D}(\mathrm{F})$ and we thus get

$$\psi_{\mathrm{F}}(n) = \mathrm{D}[n] = \psi_{\mathrm{G}}(\pi(n)) \tag{3.97}$$

for all $n \in \mathbb{Z}_p$, i.e. $\pi = \pi_{\mathrm{F,G}}$.

By Eqn. (3.93) and block(G) we get

$$\mathrm{D}[n][0] = \mathrm{D}(\mathrm{G})[\pi(n)][0] = \mathrm{D}(\mathrm{G})[n][0] = n\%p \tag{3.98}$$

for all $n \in \mathbb{Z}_p$. We are thus left to show block(D).

Let $k \in \mathbb{N}$ and $m, n \in \mathbb{Z}_p$. Then,

$$m \equiv n \mod p^k \Leftrightarrow \pi(m) \equiv \pi(n) \mod p^k \tag{3.99}$$

$$\text{(block(G))} \Leftrightarrow \psi_{\mathrm{G}}(\pi(m))[\underline{k}] = \mathrm{D}(\mathrm{G})[\pi(m)][\underline{k}] = \mathrm{D}(\mathrm{G})[\pi(n)][\underline{k}] = \psi_{\mathrm{G}}(\pi(n))[\underline{k}] \tag{3.100}$$

$$\Leftrightarrow \mathrm{D}[m][\underline{k}] = \mathrm{D}[n][\underline{k}] \tag{3.101}$$

which completes the proof. □

Just as with p-digit tables with block property we established a one-to-one correspondence between p-adic permutations and p-adic systems. If G is a fixed p-adic system then

$$\begin{aligned} \Pi_{\mathrm{G}} : \overline{\mathcal{F}}_p/_{\sim_p} &\to \overline{\mathcal{P}}_p \\ \mathrm{F} &\mapsto \pi_{\mathrm{F,G}} \end{aligned} \tag{3.102}$$

defines a bijection.

As with p-digit tables this relation can also be used to see and prove certain properties of p-adic systems more easily as the following theorem shows.

Theorem 3.19. *Let $2 \leq p \in \mathbb{N}$. Then the set of all p-adic permutations forms a subgroup of the set of all permutations of $\mathbb{Z}_p$ with respect to composition.*

Proof. Let π, π_1 and π_2 be p-adic permutations. Then, it follows directly from the definition that both $\pi_2 \circ \pi_1$ and π^{-1} are also p-adic permutations. □

We can now use Π_{G} to transport this group structure to the set $\overline{\mathcal{F}}_p$ of p-adic systems. We define

$$\mathrm{F}_1 \circ_{\mathrm{G}} \mathrm{F}_2 := {\Pi_{\mathrm{G}}}^{-1}(\Pi_{\mathrm{G}}(\mathrm{F}_1) \circ \Pi_{\mathrm{G}}(\mathrm{F}_2)) \tag{3.103}$$

for every pair $\mathrm{F}_1, \mathrm{F}_2$ of p-adic systems which makes $\left(\overline{\mathcal{F}}_p, \circ_{\mathrm{G}}\right)$ a group with neutral element ${\Pi_{\mathrm{G}}}^{-1}(\pi_{\mathrm{G,G}}) = \mathrm{G}$ and inverse element ${\Pi_{\mathrm{G}}}^{-1}(\pi_{\mathrm{G,F}})$ of $\mathrm{F} \in \overline{\mathcal{F}}_p$. Basic properties of these groups are summarized in the following lemma.

Lemma 3.20. *Let $2 \leq p \in \mathbb{N}$,* F, F_1, F_2, G, G_1, G_2 *p-adic systems, π a p-adic permutation, and $n \in \mathbb{Z}_p$. Then,*

1. Π_{G} *is an isomorphism and* $\left(\overline{\mathcal{F}}_p/_{\sim_p}, \circ_{\mathrm{G}}\right)$ *and* $\left(\overline{\mathcal{P}}_p, \circ\right)$ *are isomorphic*
   In particular: ${\Pi_{\mathrm{G}_2}}^{-1} \circ \Pi_{\mathrm{G}_1}$ *is an isomorphism and*
   $\left(\overline{\mathcal{F}}_p/_{\sim_p}, \circ_{\mathrm{G}_1}\right)$ *and* $\left(\overline{\mathcal{F}}_p/_{\sim_p}, \circ_{\mathrm{G}_2}\right)$ *are isomorphic*
2. $\Pi_{\mathrm{G}}(\mathrm{F})(n) = \pi_{\mathrm{F,G}}(n) = {\psi_{\mathrm{G}}}^{-1}(\psi_{\mathrm{F}}(n))$
3. ${\Pi_{\mathrm{G}}}^{-1}(\pi)(n) = \pi^{-1}(\mathrm{G}(\pi(n)))$
4. $\mathrm{F}_2 \circ_{\mathrm{G}} \mathrm{F}_1(n) = \pi_{\mathrm{G},\mathrm{F}_1}(\mathrm{F}_2(\pi_{\mathrm{F}_1,\mathrm{G}}(n)))$.

Proof.
(1) and (2): Follow directly from the definitions.
(3): Let $\mathrm{F} := {\Pi_\mathrm{G}}^{-1}(\pi)$. Then, $\pi = \pi_{\mathrm{F},\mathrm{G}}$ and

$$\pi^{-1}(\mathrm{G}(\pi(n))) = \pi_{\mathrm{G},\mathrm{F}}(\mathrm{G}(\pi_{\mathrm{F},\mathrm{G}}(n))) \text{ (Lemma 3.17 (3))} \tag{3.104}$$

$$= {\psi_\mathrm{F}}^{-1}(\psi_\mathrm{G}(\mathrm{G}({\psi_\mathrm{G}}^{-1}(\psi_\mathrm{F}(n))))) \tag{3.105}$$

$$\text{(Lemma 3.17 (4))} = {\psi_\mathrm{F}}^{-1}(\psi_\mathrm{F}(n)[1,\infty]) \tag{3.106}$$

$$= {\psi_\mathrm{F}}^{-1}(\mathrm{D}(\mathrm{F})[n][1,\infty]) = {\psi_\mathrm{F}}^{-1}(\mathrm{D}(\mathrm{F})[\mathrm{F}(n)]) = \mathrm{F}(n) = {\Pi_\mathrm{G}}^{-1}(\pi)(n). \tag{3.107}$$

(4):

$$\mathrm{F}_2 \circ_\mathrm{G} \mathrm{F}_1(n) = {\Pi_\mathrm{G}}^{-1}(\Pi_\mathrm{G}(\mathrm{F}_2) \circ \Pi_\mathrm{G}(\mathrm{F}_1))(n) \tag{3.108}$$

$$(3) = (\Pi_\mathrm{G}(\mathrm{F}_2) \circ \Pi_\mathrm{G}(\mathrm{F}_1))^{-1}(\mathrm{G}(\Pi_\mathrm{G}(\mathrm{F}_2) \circ \Pi_\mathrm{G}(\mathrm{F}_1)(n))) \tag{3.109}$$

$$= \Pi_\mathrm{G}(\mathrm{F}_1)^{-1}(\Pi_\mathrm{G}(\mathrm{F}_2)^{-1}(\mathrm{G}(\Pi_\mathrm{G}(\mathrm{F}_2)(\Pi_\mathrm{G}(\mathrm{F}_1)(n))))) \tag{3.110}$$

$$\text{(Lemma 3.17 (3))} = \pi_{\mathrm{G},\mathrm{F}_1}(\pi_{\mathrm{G},\mathrm{F}_2}(\mathrm{G}(\pi_{\mathrm{F}_2,\mathrm{G}}(\pi_{\mathrm{F}_1,\mathrm{G}}(n))))) \tag{3.111}$$

$$\text{(Lemma 3.17 (5))} = \pi_{\mathrm{G},\mathrm{F}_1}(\pi_{\mathrm{G},\mathrm{F}_2}(\pi_{\mathrm{F}_2,\mathrm{G}}(\mathrm{F}_2(\pi_{\mathrm{F}_1,\mathrm{G}}(n))))) \tag{3.112}$$

$$\text{(Lemma 3.17 (3))} = \pi_{\mathrm{G},\mathrm{F}_1}(\mathrm{F}_2(\pi_{\mathrm{F}_1,\mathrm{G}}(n))). \tag{3.113}$$

□

In order to see how $\circ_\mathrm{G}$ operates on $\overline{\mathcal{F}}_p$, consider the following example.

Example 3.21. Let $\mathrm{G} := (x, x-1)$, $\mathrm{F}_1 := (x, 3x+1)$, $\mathrm{F}_2 := \mathrm{F}_C = (5x, x+1)$, and $n := 5$. Then,

$$\psi_{\mathrm{F}_1}(5) = (1,0,0)\cdot(0,1)^\infty = \psi_\mathrm{G}(-13/3), \text{ hence } \pi_{\mathrm{F}_1,\mathrm{G}}(5) = -13/3, \tag{3.114}$$

$$\mathrm{F}_2(-13/3) = -5/3, \tag{3.115}$$

$$\psi_\mathrm{G}(-5/3) = (1,0)\cdot(0,1)^\infty = \psi_{\mathrm{F}_1}(7/3), \text{ hence } \pi_{\mathrm{G},\mathrm{F}_1}(-5/3) = 7/3. \tag{3.116}$$

Thus, Lemma 3.20 (4) implies $\mathrm{F}_2 \circ_\mathrm{G} \mathrm{F}_1(n) = 7/3$.

We close this paragraph with an analysis of the cycle structure of the induced permutations π_k of a p-adic permutation π which leads to the definition of the *tree of cycles* of π. In Section 8 we will use this tree of cycles to prove that two classes of p-adic systems (polynomial p-adic systems and p-permutation polynomials) are indeed distinct. The method used there is quite general and should work for other classes that may be found in the future as well.

We define the *cyclic shift function* on sequences by

$$\sigma : \mathbf{S} \times \mathbb{R} \to \mathbf{S}. \tag{3.117}$$

$$(S,s) \mapsto \begin{cases} S[\lfloor s \rfloor \,\%\, |S|\,, |S|-1] \cdot S[0, \lfloor s \rfloor \,\%\, |S| - 1] & \text{if } \mathrm{fin}(S) \\ S[\lfloor s \rfloor\,, \infty] & \text{if } \neg\mathrm{fin}(S) \end{cases}$$

For any permutation π of a finite set we denote by $\Sigma(\pi) \subseteq \mathbf{S}(\mathrm{fin})/_{\sim_\sigma}$ the *set of cycles* of π, where

$$S \sim_\sigma T \Leftrightarrow |S| = |T| \wedge \exists\, s \in \mathbb{Z} : \sigma(S,s) = T \tag{3.118}$$

for all $S, T \in \mathbf{S}(\mathrm{fin})$, e.g. $(0,1,2,3) \sim_\sigma (3,0,1,2)$, since $\sigma((0,1,2,3),3) = (3,0,1,2)$. We set $|[S]_{\sim_\sigma}| := |S|$ for all $[S]_{\sim_\sigma} \in \mathbf{S}(\mathrm{fin})/_{\sim_\sigma}$.

The following theorem is the basis of the definition of the tree of cycles of a p-adic permutation (and thus of p-adic systems).

Theorem 3.22. *Let $2 \leq p \in \mathbb{N}$, $\pi \in \overline{\mathcal{P}}_p$, $k \in \mathbb{N}_0$, and $S = [([a_0], \ldots, [a_{r-1}])]_{\sim_\sigma} \in \Sigma(\pi_k)$. Then there are $m \in [\![1, p]\!]$, $s_0, \ldots, s_{m-1} \in \mathbb{N}$ with $s_n/r \in [\![1,p]\!]$ for all $n \in \underline{m}$ and $\sum_{n=0}^{m-1} s_n/r = p$, and pairwise distinct $[([b_{0,0}], \ldots, [b_{0,s_0-1}])]_{\sim_\sigma}, \ldots, [([b_{m-1,0}], \ldots, [b_{m-1,s_{m-1}-1}])]_{\sim_\sigma} \in \Sigma(\pi_{k+1})$ (the* children of S*) such that*

$$\forall\, n \in \underline{m} : \forall\, i \in \underline{r} : \forall\, j \in \underline{s_n/r} : a_i \equiv b_{n,jr+i} \mod p^k. \tag{3.119}$$

In particular, $\Sigma(\pi_{k+1})$ is the disjoint union of the sets of children of all cycles in $\Sigma(\pi_k)$.

Proof. Let $b_{0,0} \in \{a_0 + ip^k \mid i \in \underline{p}\}$ and $[([b_{0,0}], \ldots, [b_{0,s_0-1}])]_{\sim_\sigma}$ be the cycle of π_{k+1} that contains $[b_{0,0}]$. Then Lemma 3.17 (2) implies that $a_{i\%r} \equiv b_{i\%s_0} \mod p^k$ for all $i \in \mathbb{Z}$ and hence $r \mid s_0$. If $s_0 = rp$ we are done. Otherwise we choose $b_{1,0} \in \{a_0 + ip^k \mid i \in \underline{p}\}$ such that $[b_{1,0}]$ does not occur among the entries of $[([b_{0,0}], \ldots, [b_{0,s_0-1}])]_{\sim_\sigma}$ and we consider the cycle $[([b_{1,0}], \ldots, [b_{1,s_1-1}])]_{\sim_\sigma}$ of π_{k+1} that contains $[b_{1,0}]$ which will again satisfy $a_{i\%r} \equiv b_{i\%s_1} \mod p^k$ for all $i \in \mathbb{Z}$ and $r \mid s_1$. After $m \leq p$ steps we have found the cycles $([([b_{0,0}], \ldots, [b_{0,s_0-1}])]_{\sim_\sigma}, \ldots, [([b_{m-1,0}], \ldots, [b_{m-1,s_{m-1}-1}])]_{\sim_\sigma})$ of π_{k+1} that have all the claimed properties. □

Corollary 3.23. *Let $2 \leq p \in \mathbb{N}$, $\pi \in \overline{\mathcal{P}}_p$, $k \in \mathbb{N}_0$, and $\sigma \in \Sigma(\pi_k)$. Then the prime factors of $|\sigma|$ are contained in $\overline{p}$.*

Proof. Follows directly from Theorem 3.22 and from the fact that $\pi_0 : \{\mathbb{Z}_p\} \to \{\mathbb{Z}_p\}$, $[0] \mapsto [0]$ and thus $\Sigma(\pi_0) = \{[([0])]_{\sim_\sigma}\}$. □

As indicated above, Theorem 3.22 implies the existence of a *tree of cycles*: for any $2 \leq p \in \mathbb{N}$ and $\pi \in \overline{\mathcal{P}}_p$ let

$$\mathcal{V}(\pi) := \{(k, \sigma) \mid k \in \mathbb{N}_0 \wedge \sigma \in \Sigma(\pi_k)\} \tag{3.120}$$

$$\begin{aligned} \mathcal{E}(\pi) := \big\{&((k, [([a_0], \ldots, [a_r])]_{\sim_\sigma}), (\ell, [([b_0], \ldots, [b_s])]_{\sim_\sigma})) \in \mathcal{V}(\pi)^2 \mid \\ &k + 1 = \ell \\ &\exists\, i \in \mathbb{Z} : \forall\, j \in \mathbb{Z} : a_{j\%r} \equiv b_{(i+j)\%s} \mod p^k\big\} \end{aligned} \tag{3.121}$$

$$\mathcal{G}(\pi) := (\mathcal{V}(\pi), \mathcal{E}(\pi)) \tag{3.122}$$

and

$$\begin{aligned} c(\pi) : \mathcal{E}(\pi) &\to [\![1, p]\!]. \\ ((k, \sigma), (k+1, \tau)) &\mapsto \frac{|\tau|}{|\sigma|} \end{aligned} \tag{3.123}$$

Corollary 3.24. *Let $2 \leq p \in \mathbb{N}$, $\pi \in \overline{\mathcal{P}}_p$, and $k \in \mathbb{N}_0$. Then $\mathcal{G}(\pi)$ is a directed, infinite, rooted tree with root $(0, [([0])]_{\sim_\sigma})$. The out-degrees of all vertices are contained in $[\![1, p]\!]$ and the out-degree of the root is p. The cycle decomposition of π_k is given by the k-th layer of $\mathcal{G}(\pi)$ (vertices of distance k from the root). Furthermore, $c(\pi)$ defines an edge labeling of $\mathcal{G}(\pi)$. The labels of all outgoing edges of a given vertex sum up to p and all edges going out of the root are labeled 1. For every vertex of $\mathcal{G}(\pi)$ the length of the represented cycle coincides with the product of all edge labels along the unique path connecting the vertex with the root.*

Proof. Follows directly from Theorem 3.22 and from the fact that

$$\Sigma(\pi_1) = \{[([0])]_{\sim_\sigma}, \ldots, [([p-1])]_{\sim_\sigma}\} \tag{3.124}$$

by Eqn. (3.93). □

Figure 1 below gives two examples of trees of cycles of p-adic permutations. For comparison we give the lists of all cycles of $\pi_0, \ldots, \pi_5$ for $\pi := \pi_{(x,3x+1),(5x+18,x-7)}$, i.e. the first of the two examples given in Figure 1 (to improve readability we omit the square brackets indicating equivalence classes, i.e. we write $(0, 2, 4, 6)$ for $[([0], [2], [4], [6])]_{\sim_\sigma}$):

$$\Sigma(\pi_0) : (\mathbf{0}) \tag{3.125}$$

$$\Sigma(\pi_1) : (\mathbf{0}),\ (\mathbf{1}) \tag{3.126}$$

$$\Sigma(\pi_2) : (\mathbf{0}, 2),\ (\mathbf{1}, 3) \tag{3.127}$$

$$\Sigma(\pi_3) : (\mathbf{0}, 2, 4, 6),\ (\mathbf{1}, 7),\ (\mathbf{5}, 3) \tag{3.128}$$

$$\Sigma(\pi_4) : (\mathbf{0}, 10, 4, 14),\ (\mathbf{8}, 2, 12, 6),\ (\mathbf{1}, 15, 9, 7),\ (\mathbf{5}, 11),\ (\mathbf{13}, 3) \tag{3.129}$$

$$\begin{aligned} \Sigma(\pi_5) : {}& (\mathbf{0}, 26, 4, 14, 16, 10, 20, 30),\ (\mathbf{8}, 2, 28, 22, 24, 18, 12, 6),\ (\mathbf{1}, 31, 25, 23),\ (\mathbf{17}, 15, 9, 7), \\ & (\mathbf{5}, 11),\ (\mathbf{21}, 27),\ (\mathbf{13}, 3, 29, 19). \end{aligned} \tag{3.130}$$

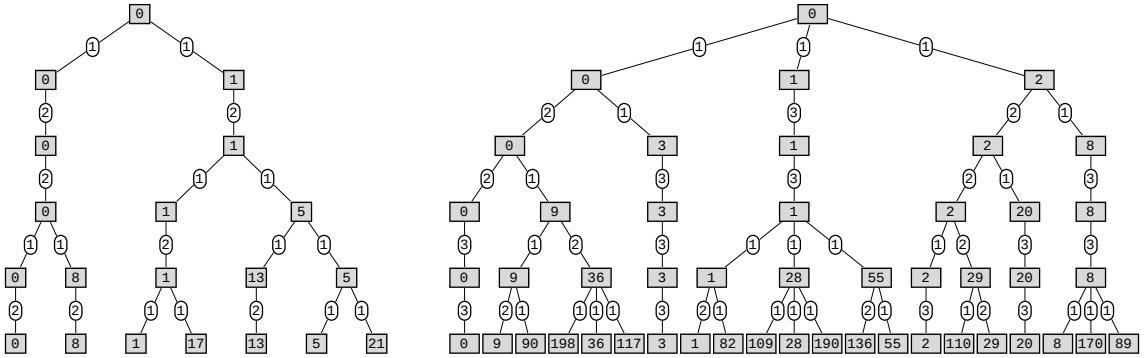

FIGURE 1. Layers 0 to 5 of the trees of cycles of the p-adic permutations $\pi_{(x,3x+1),(5x+18,x-7)}$ (left) and $\pi_{(-5x-3,5x+1,-x+5),(-4x+3,-x+1,-2x+4)}$ (right). The vertex labels are class representatives of possible starting points of the respective cycles.

Summary. In this section we have discussed several interpretations of p-adic systems. The relations we have established are summarized below.

$$\begin{array}{lll} \overline{\mathcal{F}}_p/_{\sim_p} \leftrightarrow \overline{\mathcal{Z}}_p, & \mathrm{D} : \overline{\mathcal{F}}_p/_{\sim_p} \leftrightarrow \overline{\mathcal{D}}_p, & \Pi_{\mathrm{G}}(\mathrm{F}) : \overline{\mathcal{F}}_p/_{\sim_p} \leftrightarrow \overline{\mathcal{P}}_p. \\ \mathrm{F} \mapsto (\mathrm{F} : \mathbb{Z}_p \to \mathbb{Z}_p) & \mathrm{F} \mapsto \mathrm{D}(\mathrm{F}) & \mathrm{F} \mapsto {\psi_{\mathrm{G}}}^{-1} \circ \psi_{\mathrm{F}} \\ (pf, \ldots, pf) \leftarrow\!\shortmid f & \mathrm{F}_{\mathrm{D}} \leftarrow\!\shortmid \mathrm{D} & \pi^{-1} \circ \mathrm{G} \circ \pi \leftarrow\!\shortmid \pi \end{array} \tag{3.131}$$

4. A useful characterization and many examples of p-adic systems

In the previous section we have discussed several interpretations of p-adic systems from which we ultimately chose "p-fibred functions with block property" to serve as their definition. As with any new mathematical object the obvious first question to ask is: do they exist? In the case of p-adic systems the question seems obsolete, as we already have given examples (F_C and F_2 from the introduction) and have also proven that there is a one-one-one correspondence between p-fibred systems and, say, p-digit tables with block property, the latter of which clearly exist in abundance. The real question to ask in this case is, thus, a slightly different one: do many of them occur "naturally" in their p-fibred function form (which we favored over the other forms in the definition after all) or are most of them clumsy and "artificial" when interpreted as p-fibred functions? The answer to this question (which is: yes, many occur naturally) will be given by the following very useful characterization. But before we need to define the following predicates on the set $(\mathbb{Z}_p)^A$ of all mappings from A to $\mathbb{Z}_p$, where $2 \le p \in \mathbb{N}$ and $A \subseteq \mathbb{Z}_p$ ($f \in (\mathbb{Z}_p)^A$, $r \in p$, $K \subseteq \mathbb{N}_0$):

$$\begin{aligned} &\text{(4.1)}\ \text{w-suit}_{p,r,K}(f) \Leftrightarrow \forall\, k \in K : \forall\, m, n \in (r + p\mathbb{Z}_p) \cap A : && f \text{ is } \textit{weakly } (p,r)\textit{-suitable at } K \\ &\qquad\qquad m \equiv n \mod p^k \Rightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k \\ &\text{(4.2)}\ \text{w-suit}_{p,r}(f) \Leftrightarrow \text{w-suit}_{p,r,\mathbb{N}_0}(f) && f \text{ is } \textit{weakly } (p,r)\textit{-suitable} \\ &\text{(4.3)}\ \text{suit}_{p,r,K}(f) \Leftrightarrow \forall\, k \in K : \forall\, m, n \in (r + p\mathbb{Z}_p) \cap A : && f \text{ is } (p,r)\textit{-suitable at } K \\ &\qquad\qquad m \equiv n \mod p^k \Leftrightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k \\ &\text{(4.4)}\ \text{suit}_{p,r}(f) \Leftrightarrow \text{suit}_{p,r,\mathbb{N}_0}(f) && f \text{ is } (p,r)\textit{-suitable} \end{aligned}$$

Note that any function $f : A \to \mathbb{Z}_p$ satisfying $f((r + p\mathbb{Z}_p) \cap A) \subseteq p\mathbb{Z}_p$ (cf. the definition of p-fibred functions being in weak canonical form, Eqn. (2.27)) is weakly (p,r)-suitable if and only if $f|_{(r+p\mathbb{Z}_p)\cap A}$ satisfies the 1-Lipschitz condition, and (p,r)-suitable if and only if $f|_{(r+p\mathbb{Z}_p)\cap A}$ is measure preserving (can be extended to a measure preserving function on $\mathbb{Z}_p$, to be exact) [59]. In this case one clearly gets $f(n)\%p = 0$ for all $n \in (r+p\mathbb{Z}_p)\cap A$ and thus the condition $(f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k$ simplifies to $f(m) \equiv f(n) \mod p^k$.

The following theorem summarizes how weakly (p,r)-suitable and (p,r)-suitable functions can be used to characterize closed p-fibred functions with weak block property and block property respectively.

Theorem 4.1. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \mathcal{F}_p(\text{closed})$, and $k \in \mathbb{N}$. Then,*

(1) $\forall\, r \in \underline{p} : \text{w-suit}_{p,r,\overline{k}}(\mathrm{F}[r]) \Rightarrow \text{w-block}_{\overline{k}}(\mathrm{F})$
In particular: $\forall\, r \in \underline{p} : \text{w-suit}_{p,r}(\mathrm{F}[r]) \Rightarrow \text{w-block}(\mathrm{F})$
(2) $\forall\, r \in \underline{p} : \text{suit}_{p,r,\overline{k}}(\mathrm{F}[r]) \Leftrightarrow \text{block}_{\overline{k}}(\mathrm{F})$
In particular: $\forall\, r \in \underline{p} : \text{suit}_{p,r}(\mathrm{F}[r]) \Leftrightarrow \text{block}(\mathrm{F})$.

Proof. Let $\ell \in \overline{k}$, $r \in \underline{p}$, and $m, n \in (r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})$. Then,

$$\mathrm{F}(m) \equiv \mathrm{F}(n) \mod p^{\ell-1} \Leftrightarrow \frac{\mathrm{F}[r](m) - \mathrm{F}[r](m)\%p}{p} \equiv \frac{\mathrm{F}[r](n) - \mathrm{F}[r](n)\%p}{p} \mod p^{\ell-1} \tag{4.5}$$

$$\Leftrightarrow \mathrm{F}[r](m) - \mathrm{F}[r](m)\%p \equiv \mathrm{F}[r](n) - \mathrm{F}[r](n)\%p \mod p^{\ell} \tag{4.6}$$

and the statements follow from Lemma 3.2. □

Despite the fact that the proof of this theorem is rather simple, it is quite remarkable. It states that the block property of a p-fibred function F does not depend on the relation between the functions $\mathrm{F}[0], \ldots, \mathrm{F}[p-1]$, but is only a question of whether each $\mathrm{F}[r]$ is "suitable" to be the r-th of the p entries of F. The p functions that define F can be chosen completely independently from one another.

The weak block property revisited. A similar characterization is given for the weak block property, but in contrast to the characterization of the block property in (2), the condition in (1) is only sufficient but not necessary. A natural question to ask is whether the weak block property also permits a necessary and sufficient characterization that only considers the functions $\mathrm{F}[0], \ldots, \mathrm{F}[p-1]$ independently from one another. The following example shows that this is not the case.

Example 4.2. Let $f, g, h : \mathbb{Z}_2 \to \mathbb{Z}_2$ with $f(n) = (n = 8\ ?\ 6 : 2)$, $g(n) = (n = 3\ ?\ -2 : (n \equiv 3 \mod 4\ ?\ 6 : 0))$, and $h(n) = 0$ for all $n \in \mathbb{Z}_2$. Furthermore, let $\mathrm{F} := (f,h)$, $\mathrm{G} := (h,g)$, and $\mathrm{H} := (f,g)$. Then $\mathrm{D}(\mathrm{H})[0][\underline{3}] = (0,1,0) \neq (0,1,1) = \mathrm{D}(\mathrm{H})[2^3][\underline{3}]$ which implies that H does not have the weak block property (at 3). At the same time we get $\mathrm{D}(\mathrm{F}) = ((n \equiv 0 \mod 2\ ?\ (0,1)^\infty : (1,0)^\infty))_{n\in\mathbb{Z}_2}$ and $\mathrm{D}(\mathrm{G}) = ((n \equiv 0 \mod 2\ ?\ (0)^\infty : (n \equiv 1 \mod 4\ ?\ (1)\cdot(0)^\infty : (1)^\infty))_{n\in\mathbb{Z}_2}$ which implies that both F and G have the weak block property. Note that $f(0) = 2 \not\equiv 2 + 2^2 = f(0+2^3) \mod 2^3$ and $g(3) = -2 \not\equiv -2 + 2^3 = g(3+2^4) \mod 2^4$ which means that neither f nor g are weakly $(2,0)$-, respectively weakly $(2,1)$-suitable.

f and g of the previous example can both be part of 2-fibred functions (F and G respectively) that have the weak block property, but the 2-fibred function H, which contains both f and g, does not have the weak block property. Thus, there cannot be a necessary and sufficient characterization of the weak block property which considers the entries of a p-fibred function independently.

A natural follow-up question is whether every p-digit table with weak block property that is the p-digit table of a p-fibred function can at least be realized as the p-digit table of a p-fibred function whose entries are weakly (p,r)-suitable functions. This is true for the 2-digit tables D(F) and D(G) of the previous example: if $f_0, f_1, g_0, g_1 : \mathbb{Z}_2 \to \mathbb{Z}_2$ with $f_0(n) = 2$, $f_1(n) = 0$, $g_0(n) = 0$, and $g_1(n) = (n \equiv 1 \mod 4\ ?\ 0 : 6)$ for all $n \in \mathbb{Z}_2$, then $\mathrm{D}(\mathrm{F}) = \mathrm{D}((f_0, f_1))$ and $\mathrm{D}(\mathrm{G}) = \mathrm{D}((g_0, g_1))$, and also $\text{w-suit}_{2,0}(f_0)$, $\text{w-suit}_{2,1}(f_1)$, $\text{w-suit}_{2,0}(g_0)$, and $\text{w-suit}_{2,1}(g_1)$. However, in general even this does not hold as the following example shows.

Example 4.3. Let $f_0, f_1 : \mathbb{Z}_2 \to \mathbb{Z}_2$ with $f_0(n) = (n\%16 = 8\ ?\ 6 : (n\%4 = 0\ ?\ 2 : 4))$ and $f_1(n) = (n\%4 = 1\ ?\ 4 : 0)$ for all $n \in \mathbb{Z}_2$. Furthermore, let $\mathrm{F} := (f_0, f_1)$, and $\mathrm{D} := \mathrm{D}(\mathrm{F})$. Then $\mathrm{D} = ((n \equiv 8 \mod 16\ ?\ (0,1,0,1) : (n \equiv 0 \mod 4\ ?\ (0,1) : (n \equiv 1 \mod 4\ ?\ (1) : (n \equiv 2 \mod 4\ ?\ () : (1,0,1)))))) \cdot (0)^\infty)_{n\in\mathbb{Z}_2}$ and hence D has the weak block property, but since $\mathrm{D}(0) = 1 + 4\mathbb{Z}_2$ and $\mathrm{D}(8) = 3 + 4\mathbb{Z}_2$, Theorem 3.4 implies that there cannot exist any 2-fibred

function $\mathrm{G} = (g_0, g_1)$ with $g_0 : \mathbb{Z}_2 \to \mathbb{Z}_2$ weakly $(2,0)$-suitable and $g_1 : \mathbb{Z}_2 \to \mathbb{Z}_2$ weakly $(2,1)$-suitable such that $\mathrm{D} = \mathrm{D}(\mathrm{G})$, because in this case $g_0(0) \in \{2,3\} + 8\mathbb{Z}_2$ and $g_0(8) \in \{6,7\} + 8\mathbb{Z}_2$ and hence $(g_0 - g_0\%2)(0) \not\equiv (g_0 - g_0\%2)(0 + 2^3) \mod 2^3$.

Example 3.13, Example 4.2, and Example 4.3 indicate that there are actually three levels of the weak block property of p-digit tables of different generality. The weakest form is given by the weak block property itself, the stronger version (as proven by Example 3.13) requires the p-digit table to come from some p-fibred function, while the even stronger version (as proven by Example 4.3) requires the entries of this p-fibred function to be weakly (p,r)-suitable.
We thus define the following predicates on $\mathcal{D}_p$ ($\mathrm{D} \in \mathcal{D}_p$, $K \subseteq \mathbb{N}_0$):

(4.7) $\text{w-block-F}_K(\mathrm{D}) \Leftrightarrow \exists\, \mathrm{F} \in \mathcal{F}_p(\text{w-block}_K) : \mathrm{D} = \mathrm{D}(\mathrm{F})$ — D has the *weak block property F at K*

(4.8) $\text{w-block-F}(\mathrm{D}) \Leftrightarrow \text{w-block-F}_{\mathbb{N}_0}(\mathrm{D})$ — D has the *weak block property F*

(4.9) $\text{w-block-S}_K(\mathrm{D}) \Leftrightarrow \exists\, \mathrm{F} \in \mathcal{F}_p(\text{w-block}_K) : \mathrm{D} = \mathrm{D}(\mathrm{F}) \wedge \forall\, r \in \underline{p} : \text{w-suit}_{p,r,K}(\mathrm{F}[r])$ — D has the *weak block property S at K*

(4.10) $\text{w-block-S}(\mathrm{D}) \Leftrightarrow \text{w-block-S}_{\mathbb{N}_0}(\mathrm{D})$ — D has the *weak block property S*

Clearly,

(4.11) $$\text{block}_K(\mathrm{D}) \Rightarrow \text{w-block-S}_K(\mathrm{D}) \Rightarrow \text{w-block-F}_K(\mathrm{D}) \Rightarrow \text{w-block}_K(\mathrm{D})$$

(4.12) $$\text{block}(\mathrm{D}) \Rightarrow \text{w-block-S}(\mathrm{D}) \Rightarrow \text{w-block-F}(\mathrm{D}) \Rightarrow \text{w-block}(\mathrm{D})$$

for all $\mathrm{D} \in \mathcal{D}_p$ and all $K \subseteq \mathbb{N}_0$ by definition but, as discussed above, neither of the converses of the four implications is true in general.

The predicates w-block-F_K and w-block-F carry over to $\mathcal{F}_p(\text{closed})$ by $\mathrm{D}(\mathrm{F})$ but we define the following alternative predicates on $\mathcal{F}_p(\text{closed})$ ($\mathrm{F} \in \mathcal{F}_p(\text{closed})$, $k \subseteq \mathbb{N}_0$):

(4.13) $\text{w-block-S}_K(\mathrm{F}) \Leftrightarrow \forall\, r \in \underline{p} : \text{w-suit}_{p,r,K}(\mathrm{F}[r])$ — F has the *weak block property S at K*

(4.14) $\text{w-block-S}(\mathrm{F}) \Leftrightarrow \text{w-block-S}_{\mathbb{N}_0}(\mathrm{F})$ — F has the *weak block property S*

It follows from the definitions and from Theorem 4.1 (2) that

(4.15) $$\text{block}_K(\mathrm{F}) \Rightarrow \text{w-block-S}_K(\mathrm{F}) \Rightarrow \text{w-block-S}_K(\mathrm{D}(\mathrm{F})) \Rightarrow \text{w-block-F}_K(\mathrm{F}) \Leftrightarrow \text{w-block}_K(\mathrm{F})$$

(4.16) $$\text{block}(\mathrm{F}) \Rightarrow \text{w-block-S}(\mathrm{F}) \Rightarrow \text{w-block-S}(\mathrm{D}(\mathrm{F})) \Rightarrow \text{w-block-F}(\mathrm{F}) \Leftrightarrow \text{w-block}(\mathrm{F})$$

for all $\mathrm{F} \in \mathcal{F}_p(\text{closed})$ and all $K \subseteq \mathbb{N}_0$ while, again, neither of the converses of the six implications is true in general.

In addition to being of general interest, this "refinement" of the weak block property has a first application as well in proving a stronger version of the last statement of Corollary 3.8 (2).

Corollary 4.4. *Under the assumptions of Corollary 3.8 we have*

(3) $\text{w-block-S}_k(\mathrm{F}) \wedge \text{w-block}_{k-1}(\mathrm{F})$ *and* S' *CRS modulo* $p^{k-1} \Rightarrow$
$\forall\, n \in \mathrm{dom}(\mathrm{F}) : \mathrm{H}_1(n) = \mathrm{H}_1(T(n)) = \mathrm{H}_2(n)$.

Proof. It follows from the assumptions that $\mathrm{H}_1[r](n) = S(\mathrm{F}[r](n)) \equiv \mathrm{F}[r](n) \mod p^k$ for all $r \in \underline{p}$ and all $n \in (r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{F})$. Thus, $\text{w-block-S}_k(\mathrm{F})$ implies that also $\text{w-block-S}_k(\mathrm{H}_1)$, i.e. $\text{w-suit}_{p,r,k}(\mathrm{H}_1[r])$ for all $r \in \underline{p}$.

Now let $n \in \mathrm{dom}(\mathrm{F})$. Clearly, $\mathrm{H}_1(T(n)) = \mathrm{H}_2(n)$. In addition, $T(n) \equiv n \mod p^k$ and hence

(4.17) $$p\mathrm{H}_1(T(n)) = \mathrm{H}_1[T(n)\%p](T(n)) - \mathrm{H}_1[T(n)\%p](T(n))\%p$$

(4.18) $$= \mathrm{H}_1[n\%p](T(n)) - \mathrm{H}_1[n\%p](T(n))\%p$$

(4.19) $$(\text{w-suit}_{p,n\%p,k}(\mathrm{H}_1[n\%p])) \equiv \mathrm{H}_1[n\%p](n) - \mathrm{H}_1[n\%p](n)\%p$$

(4.20) $$= p\mathrm{H}_1(n) \mod p^k.$$

We thus get $\mathrm{H}_1(T(n)) \equiv \mathrm{H}_1(n) \mod p^{k-1}$ and since both $\mathrm{H}_1(T(n))$ and $\mathrm{H}_1(n)$ are in S' by Corollary 3.8 (1), they must be equal. □

Properties of suitable functions. Since (p,r)-suitable functions are the building blocks of p-adic systems, we summarize some basic facts on them below.

Lemma 4.5. *Let $2 \leq p \in \mathbb{N}$, $A \subseteq \mathbb{Z}_p$, $r \in \underline{p}$, and $f : A \to \mathbb{Z}_p$ (p,r)-suitable. Then,*

(1) $f|_{(r+p\mathbb{Z}_p)\cap A}$ *is injective*
(2) $r + p\mathbb{Z}_p \subseteq A \wedge f(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p \Rightarrow f|_{r+p\mathbb{Z}_p}(r + p\mathbb{Z}_p) = p\mathbb{Z}_p$
In particular: $g : r + p\mathbb{Z}_p \to \mathbb{Z}_p$, $n \mapsto f(n)/p$ is bijective.

Proof.
(1): Assume to the contrary that $f|_{(r+p\mathbb{Z}_p)\cap A}$ is not injective and let $m, n \in (r + p\mathbb{Z}_p) \cap A$ with $m \neq n$ such that $f(m) = f(n)$. Then there is a $k \in \mathbb{N}$ such that $m \not\equiv n \mod p^k$, but $(f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k$ which is a contradiction.
(2): Let $g : \mathbb{Z}_p \to \mathbb{Z}_p$ be an arbitrary extension of f, $\mathrm{id}_{\mathbb{Z}_p}$ the identity function on $\mathbb{Z}_p$, and $\mathrm{F} := (\mathrm{id}_{\mathbb{Z}_p})^r \cdot (g) \cdot (\mathrm{id}_{\mathbb{Z}_p})^{p-r-1}$. Then $\mathrm{F} \in \overline{\mathcal{F}}_p$ by Theorem 4.1 (2) and hence Lemma 3.11 implies that for every $n \in \mathbb{Z}_p$ there is a unique $m \in \mathbb{Z}_p$ such that

$$\mathrm{D}(\mathrm{F})[m] = (r) \cdot \mathrm{D}(\mathrm{F})[n]. \tag{4.21}$$

It follows that

$$\mathrm{D}(\mathrm{F})[\mathrm{F}(m)] = \mathrm{D}(\mathrm{F})[n] \tag{4.22}$$

and hence $\mathrm{F}(m) = n$ by Lemma 3.9. Furthermore, $m \in r + pR$ and thus

$$f(m) = \mathrm{F}[r](m) = p\mathrm{F}(m) = pn. \tag{4.23}$$

We conclude that $f|_{r+p\mathbb{Z}_p}(r + p\mathbb{Z}_p) = p\mathbb{Z}_p$. Thus g is surjective and by (1) it is also injective. □

Corollary 4.6. *Let $2 \leq p \in \mathbb{N}$ and $\mathrm{F} \in \overline{\mathcal{F}}_p$. Then,*

(1) $\forall\, r \in \underline{p} : \mathrm{F}|_{r+p\mathbb{Z}_p} : r + p\mathbb{Z}_p \to \mathbb{Z}_p$ *is surjective and one-to-one (i.e. bijective)*
In particular: $\forall\, n \in \mathbb{Z}_p : \forall\, r \in \underline{p} : \left|\mathrm{F}^{-1}(n) \cap (r + p\mathbb{Z}_p)\right| = 1$
(2) $\mathrm{F} : \mathbb{Z}_p \to \mathbb{Z}_p$ *is surjective and p-to-one.*
In particular: $\forall\, n \in \mathbb{Z}_p : \left|\mathrm{F}^{-1}(n)\right| = p$.

Proof. By Lemma 3.1 we may assume without loss of generality that F is in canonical form. Then all statements follow directly from Theorem 4.1 (2), and Lemma 4.5. □

We may construct new (p,r)-suitable functions from existing ones by multiplying them with weakly (p,r)-suitable functions whose values are coprime to p. This fact will later be used to identify many rational functions that are (p,r)-suitable.

Theorem 4.7. *Let $2 \leq p \in \mathbb{N}$, $A \subseteq \mathbb{Z}_p$, $r \in \underline{p}$, $k \subseteq \mathbb{N}_0$, $f : A \to \mathbb{Z}_p$ with $f((r + p\mathbb{Z}_p) \cap A) \subseteq p\mathbb{Z}_p$, and $g : A \to \mathbb{Z}_p$ weakly (p,r)-suitable at $\overline{k}$ with $\gcd(p, g(n)\%p) = 1$ for all $n \in (r+p\mathbb{Z}_p)\cap A$. Then,*

(1) $\text{w-suit}_{p,r,\overline{k}}(f) \Leftrightarrow \text{w-suit}_{p,r,\overline{k}}(fg)$
(2) $\text{suit}_{p,r,\overline{k}}(f) \Leftrightarrow \text{suit}_{p,r,\overline{k}}(fg)$.

In particular, $1/g : A \to \mathbb{Z}_p$ exists and satisfies the same properties as g and thus f/g is (weakly) (p,r)-suitable at $\overline{k}$ as well if and only if f is (weakly) (p,r)-suitable at $\overline{k}$.

Proof. To prove "⇒" of (2) we need to show that

$$m \equiv n \mod p^\ell \quad \Leftrightarrow \quad ((fg) - (fg)\%p)(m) \equiv ((fg) - (fg)\%p)(n) \mod p^\ell \tag{4.24}$$

for all $\ell \in \overline{k}$ and $m, n \in (r + p\mathbb{Z}_p) \cap A$ which is equivalent to

$$m \equiv n \mod p^\ell \quad \Leftrightarrow \quad (fg)(m) \equiv (fg)(n) \mod p^\ell \tag{4.25}$$

since $f((r + p\mathbb{Z}_p) \cap A) \subseteq p\mathbb{Z}_p$.

We begin by proving "⇒", which is the easier direction. It follows from the assumptions that

$$m \equiv n \mod p^\ell \Rightarrow f(m) \equiv f(n) \mod p^\ell \quad \wedge \quad g(m) \equiv g(n) \mod p^\ell \tag{4.26}$$

$$\Rightarrow f(m)g(m) \equiv f(n)g(m) \mod p^\ell \quad \wedge \quad \frac{g(n) - g(m)}{p^\ell} \in \mathbb{Z}_p \tag{4.27}$$

$$\Rightarrow f(m)g(m) \equiv f(n)g(m) + f(n)\frac{g(n) - g(m)}{p^\ell}p^\ell \mod p^\ell \tag{4.28}$$

$$\Rightarrow (fg)(m) \equiv (fg)(n) \mod p^\ell. \tag{4.29}$$

Note that in the above deduction we only needed that f is weakly (p, r)-suitable at $\overline{k}$ (in the first implication), which implies that we have already proven "⇒" of (1).

For "⇐" we proceed by induction on ℓ. If $\ell = 0$, this is clearly true. Now assume that it is also true for some $\ell \in \underline{k}$ and that

$$(fg)(m) \equiv (fg)(n) \mod p^{\ell+1}. \tag{4.30}$$

Then,

$$(fg)(m) \equiv (fg)(n) \mod p^\ell \tag{4.31}$$

and thus

$$m \equiv n \mod p^\ell \tag{4.32}$$

by the induction hypothesis. Consequently, since g is weakly (p, r)-suitable at ℓ,

$$g(m) \equiv g(n) \mod p^\ell \tag{4.33}$$

and hence

$$f(n)g(m) \equiv f(n)g(n) \mod p^{\ell+1} \tag{4.34}$$

since $f(n) \in p\mathbb{Z}_p$. But then we get

$$(f(m) - f(n))g(m) = f(m)g(m) - f(n)g(m) \equiv f(n)g(n) - f(n)g(n) = 0 \mod p^{\ell+1}. \tag{4.35}$$

Since $\gcd(p, g(m)\%p) = 1$, we have $1/g(m) \in \mathbb{Z}_p$ and it follows that

$$f(m) - f(n) = (f(m) - f(n))g(m)\frac{1}{g(m)} \equiv 0 \mod p^{\ell+1}. \tag{4.36}$$

Consequently,

$$f(m) \equiv f(n) \mod p^{\ell+1} \tag{4.37}$$

and since f is (p, r)-suitable at $\ell + 1$, we finally get

$$m \equiv n \mod p^{\ell+1} \tag{4.38}$$

which proves that fg is (p, r)-suitable at $\ell + 1$.

For the "In particular" part we need to show that $1/g$ has the same properties as g, i.e. that $1/g$ is weakly (p, r)-suitable at $\overline{k}$ and $\gcd(p, (1/g)(n)\%p) = 1$ for all $n \in (r + p\mathbb{Z}_p) \cap A$. The latter part follows trivially from the fact that $\gcd(p, g(n)\%p) = 1$ and $g(n)(1/g)(n) = 1$ for all $n \in (r+p\mathbb{Z}_p)\cap A$. In order to prove that $1/g$ is weakly (p, r)-suitable at $\overline{k}$, let $\ell \in \overline{k}$ and $m, n \in (r + p\mathbb{Z}_p) \cap A$. Since $(g(m)g(n))\%p = ((g(m)\%p)(g(n)\%p))\%p = 1$, we have $1/(g(m)g(n)) \in \mathbb{Z}_p$. Thus,

$$m \equiv n \mod p^\ell \Rightarrow g(m) \equiv g(n) \mod p^\ell \tag{4.39}$$

$$\Rightarrow g(m)\frac{1}{g(m)g(n)} \equiv g(n)\frac{1}{g(m)g(n)} \mod p^\ell \tag{4.40}$$

$$\Rightarrow (1/g)(m) \equiv (1/g)(n) \mod p^\ell. \tag{4.41}$$

Using "⇒" of (1) and (2) and the "In particular" part, it is now straightforward to prove "⇐" of (1) and (2). As a result we have,

$$\text{w-suit}_{p,r,\overline{k}}(fg) \Rightarrow \text{w-suit}_{p,r,\overline{k}}(fg(1/g)) \Rightarrow \text{w-suit}_{p,r,\overline{k}}(f) \tag{4.42}$$

$$\text{suit}_{p,r,\overline{k}}(fg) \Rightarrow \text{suit}_{p,r,\overline{k}}(fg(1/g)) \Rightarrow \text{suit}_{p,r,\overline{k}}(f). \tag{4.43}$$

which completes the proof. □

Polynomial p-adic systems. In this paragraph we investigate the consequences of Theorem 4.1 for p-fibred systems defined by polynomials over $\mathbb{Z}_p$ and $\mathbb{Q}_p$. We will prove the surprising result that "most" polynomial p-fibred functions have the block property and thus provide a first big class of p-adic systems that have a rather natural representation as p-fibred functions.

Theorem 4.8. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}_p[x]$ (note that for the whole theorem we define $0^0 := 1$), and $k \in \mathbb{N}_0$. Then,*

(1) $\text{w-suit}_{p,r,k}(f)$
(2) $k \leq 1 \Rightarrow \text{suit}_{p,r,k}(f)$
(3) $k \geq 2 \Rightarrow$

$$\text{suit}_{p,r,k}(f) \Leftrightarrow \gcd(p, f'(r)\%p) = 1 \quad \textit{(note: } f'(r)\%p = \left(\textstyle\sum_{i=1}^{d}(a_i\%p)ir^{i-1}\right)\%p\textit{)}$$

In particular: if $a_0, a_2, \ldots, a_d$ are given then the set of all a_1 that make f (p,r)-suitable at k is given by $\left\{\left(a - \sum_{i=2}^{d}(a_i\%p)ir^{i-1}\right)\%p \mid a \in \underline{p} \wedge \gcd(p,a) = 1\right\} + p\mathbb{Z}_p$.

Proof. First we note that p is not a zero divisor of $\mathbb{Z}_p$ and therefore $a = b \Leftrightarrow pa = pb$ for all $a, b \in \mathbb{Z}_p$ (otherwise $a \neq b$ and $pa = pb$ for some $a, b \in \mathbb{Z}_p$ and hence $a - b \neq 0$ and $p(a-b) = 0$ which implies that p is a zero divisor). In particular,

$$p^k \mid pa \Leftrightarrow \exists\, b \in \mathbb{Z}_p : pp^{k-1}b = pa \Leftrightarrow \exists\, b \in \mathbb{Z}_p : p^{k-1}b = a \Leftrightarrow p^{k-1} \mid a \tag{4.44}$$

for all $a \in \mathbb{Z}_p$ and $k \in \mathbb{N}$. Let $k \in \mathbb{N}_0$, $m, n \in r + p\mathbb{Z}_p$, and $b_{m,n} \in \mathbb{Z}_p$ such that $m - n = pb_{m,n}$. If $k \leq 1$, then clearly $\text{suit}_{p,r,k}(f)$, which proves (2). Otherwise, we get

$$m \equiv n \mod p^k \Leftrightarrow p^k \mid m - n \Leftrightarrow p^k \mid pb_{m,n} \Leftrightarrow p^{k-1} \mid b_{m,n} \tag{4.45}$$

and

$$f(m) \equiv f(n) \mod p^k \Leftrightarrow p^k \mid \sum_{i=0}^{d} a_i m^i - \sum_{i=0}^{d} a_i n^i \tag{4.46}$$

$$\Leftrightarrow p^k \mid \sum_{i=1}^{d} a_i \left(m^i - n^i\right) \tag{4.47}$$

$$\Leftrightarrow p^k \mid (m-n) \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} m^j n^{i-1-j} \tag{4.48}$$

$$\Leftrightarrow p^k \mid pb_{m,n} \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} m^j n^{i-1-j} \tag{4.49}$$

$$\Leftrightarrow p^{k-1} \mid b_{m,n} \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} m^j n^{i-1-j} \tag{4.50}$$

$$\Leftrightarrow p^{k-1} \mid b_{m,n} \left(p \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} \frac{m^j n^{i-1-j} - r^{i-1}}{p} + \sum_{i=1}^{d} a_i i r^{i-1} \right) \tag{4.51}$$

$$\Leftrightarrow p^{k-1} \mid b_{m,n} \left(pc_{m,n} + s\right) \tag{4.52}$$

where

$$c_{m,n} := \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} (m^j n^{i-1-j} - r^{i-1})/p \tag{4.53}$$

$$s := \sum_{i=1}^{d} a_i i r^{i-1} \tag{4.54}$$

and $c_{m,n} \in \mathbb{Z}_p$, since $(m^j n^{i-1-j} - r^{i-1})\%p = (r^j r^{i-1-j} - r^{i-1})\%p = 0$ for all $i \in [\![1, d]\!]$ and $j \in \underline{i}$. Therefore, we get

$$\forall\, m, n \in r + p\mathbb{Z} : \big(m \equiv n \mod p^k \Rightarrow f(m) \equiv f(n) \mod p^k\big) \tag{4.55}$$

which proves (1).

In order to prove (3) we claim

$$\big(\forall\, m, n \in r + p\mathbb{Z}_p : p^{k-1} \mid b_{m,n}(pc_{m,n} + s) \Rightarrow p^{k-1} \mid b_{m,n}\big) \Leftrightarrow \gcd(p, s\%p) = 1 \tag{4.56}$$

for all $k \geq 2$.

For "$\Rightarrow$" assume to the contrary that $g := \gcd(p, s\%p) \neq 1$. Let $m := r$ and $n := r - p^k/g$. Then, $b_{m,n} = p^{k-1}/g$ and thus $p^{k-1} \nmid b_{m,n}$ since $g \neq 1$ (note: $p, g, b_{m,n} \in \mathbb{N}$). Next we claim that $g \mid s$. Then $b_{m,n}(pc_{m,n} + s) = p^{k-1}(p/gc_{m,n} + s/g)$ with $p/gc_{m,n} + s/g \in \mathbb{Z}_p$, and hence $p^{k-1} \mid b_{m,n}(pc_{m,n} + s)$ which is a contradiction. To prove the claim let $s = \sum_{i=0}^{\infty} s_i p^i$. Then

$$s/g = (s\%p)/g + \sum_{i=1}^{\infty} s_i p/g p^{i-1} = (s\%p)/g + \sum_{i=0}^{\infty} s_{i+1} p/g p^i \in \mathbb{Z}_p \tag{4.57}$$

and hence $g \mid s$.

For "$\Leftarrow$" we first claim that if $x = \sum_{i=0}^{\infty} x_i p^i$, $y = \sum_{i=0}^{\infty} y_i p^i \in \mathbb{Z}_p$ with $\gcd(p, y\%p) = 1$, and $\ell \in \mathbb{N}_0$ then

$$p^\ell \mid xy \Leftrightarrow p^\ell \mid x. \tag{4.58}$$

We have

$$xy = \left(x\%p^\ell + \frac{x - x\%p^\ell}{p^\ell} p^\ell\right)\left(y\%p^\ell + \frac{y - y\%p^\ell}{p^\ell} p^\ell\right) = \big(x\%p^\ell\big)\big(y\%p^\ell\big) + p^\ell d_{x,y,\ell} \tag{4.59}$$

where

$$d_{x,y,\ell} := \big(x\%p^\ell\big)\frac{y - y\%p^\ell}{p^\ell} + \frac{x - x\%p^\ell}{p^\ell}\big(y\%p^\ell\big) + \frac{x - x\%p^\ell}{p^\ell}\frac{y - y\%p^\ell}{p^\ell} p^\ell \in \mathbb{Z}_p. \tag{4.60}$$

Also, $\gcd\big(p^\ell, y\%p^\ell\big) = 1$, since $\gcd(p, y\%p) = 1$ and thus

$$p^\ell \mid xy \Leftrightarrow p^\ell \mid \big(x\%p^\ell\big)\big(y\%p^\ell\big) \Leftrightarrow p^\ell \mid x\%p^\ell \Leftrightarrow x\%p^\ell = 0 \Leftrightarrow p^\ell \mid x. \tag{4.61}$$

Now let $m, n \in r + p\mathbb{Z}_p$ with $p^{k-1} \mid b_{m,n}(pc_{m,n} + s)$. Then

$$\gcd(p, (pc_{m,n} + s)\%p) = \gcd(p, s\%p) = 1 \tag{4.62}$$

and thus $p^{k-1} \mid b_{m,n}$ by Eqn. (4.58).

For the "In particular" part we set $t := \sum_{i=2}^{d} (a_i\%p) i r^{i-1}$ and we claim that

$$\gcd(p, (a_1\%p + t)\%p) = 1 \Leftrightarrow \exists\, a \in \underline{p} : \exists\, b \in \mathbb{Z}_p : \gcd(p, a) = 1 \wedge a_1 = a - t + pb \tag{4.63}$$

for all $a_1 \in \mathbb{Z}_p$. For "$\Rightarrow$" we set $a := (a_1 + t)\%p$ and $b = \frac{a_1 + t - (a_1 + t)\%p}{p}$. Then clearly $a_1 = a - t + pb$ and

$$\gcd(p, a) = \gcd(p, (a_1 + t)\%p) = \gcd(p, (a_1\%p + t)\%p) = 1. \tag{4.64}$$

For "$\Leftarrow$" we compute

$$\gcd(p, (a_1\%p + t)\%p) = \gcd(p, ((a - t + pb)\%p + t)\%p) = \gcd(p, a) = 1. \tag{4.65}$$

□

It is possible to generalize the above result to functions defined by polynomials over $\mathbb{Q}_p$. Clearly, before we can ask the question of whether such a polynomial is (weakly) (p,r)-suitable, we first need to check if it even defines a function on $\mathbb{Z}_p$ in the first place. Consider the example where $p=2$, $r=1$, $f(x)=x/2+1/2\in\mathbb{Q}_2[x]$, and $g(x)=x/2+1\in\mathbb{Q}_2[x]$. In this situation we have $f(n)\in\mathbb{Z}_2$ for all $n\in 1+2\mathbb{Z}_2$ but $g(1)=3/2\notin\mathbb{Z}_2$. We define the following predicate on $\mathbb{Q}_p[x]$ which characterizes the decisive property that f has but g has not ($2\leq p\in\mathbb{N}$, $r\in\underline{p}$, $f\in\mathbb{Q}_p[x]$):

$$\text{integral}_{p,r}(f)\Leftrightarrow f(r+p\mathbb{Z}_p)\subseteq\mathbb{Z}_p \qquad f \text{ is } (p,r)\text{-integral} \tag{4.66}$$

The following lemma provides an easy characterization of (p,r)-integral polynomials. It involves a generalization of the p-adic valuation ν_p to the case where p is not a prime, which is discussed in the appendix.

Lemma 4.9. *Let $2\leq p\in\mathbb{N}$, $r\in\underline{p}$, $f=\sum_{i=0}^{d}a_ix^i\in\mathbb{Q}_p[x]$ (note that for the whole theorem we define $0^0:=1$), and*

$$K:=-\min(\{\nu_p(a_i)\mid i\in\overline{d}\}\cup\{0\}). \tag{4.67}$$

Then,

$$W:=\underline{p^K}\cap(r+p\mathbb{Z}_p) \tag{4.68}$$

is a finite witness set for f being (p,r)-integral, i.e. $\text{integral}_{p,r}(f)$ if and only if $f(W)\subseteq\mathbb{Z}_p$.

Proof. Let $n\in r+p\mathbb{Z}_p$ and $N:=n\%p^K\in W$. By definition of K we have $p^Kf\in\mathbb{Z}_p[x]$. Thus,

$$f(n)\in\mathbb{Z}_p\Leftrightarrow p^Kf(n)\in p^K\mathbb{Z}_p\Leftrightarrow p^Kf(N)\in p^K\mathbb{Z}_p\Leftrightarrow f(N)\in\mathbb{Z}_p. \tag{4.69}$$

□

Now that we have characterized possible candidates for (weakly) (p,r)-suitable polynomials over $\mathbb{Q}_p$, we are ready to formulate the following generalization of Theorem 4.8.

Theorem 4.10. *Let $2\leq p\in\mathbb{N}$, $r\in\underline{p}$, $f:\mathbb{Z}_p\to\mathbb{Z}_p$, $g=\sum_{i=0}^{d}a_ix^i\in\mathbb{Q}_p[x]$ (note that for the whole theorem we define $0^0:=1$) (p,r)-integral with $f(n)=g(n)$ for all $n\in r+p\mathbb{Z}_p$, $k\in\mathbb{N}_0$,*

$$W_\ell:=\underline{p^\ell}\cap(r+p\mathbb{Z}_p) \tag{4.70}$$

for all $\ell\in\mathbb{N}_0$, and

$$K:=-\min(\{\nu_p(a_i)\mid i\in\overline{d}\}\cup\{0\}). \tag{4.71}$$

Then, W_{K+k} is a finite witness set for f being (weakly) (p,r)-suitable at k, i.e.

(1) $\text{w-suit}_{p,r,k}(f)\Leftrightarrow$
$\forall\, m,n\in W_{K+k}: m\equiv n \mod p^k\Rightarrow(f-f\%p)(m)\equiv(f-f\%p)(n) \mod p^k$
(2) $\text{suit}_{p,r,k}(f)\Leftrightarrow$
$\forall\, m,n\in W_{K+k}: m\equiv n \mod p^k\Leftrightarrow(f-f\%p)(m)\equiv(f-f\%p)(n) \mod p^k$.

Furthermore,

(3) $\forall\,\ell\in[\![K+1,\infty]\!]:\text{w-suit}_{p,r,\ell}(f)\Rightarrow\text{w-suit}_{p,r,\ell+1}(f)$
In particular: $\text{w-suit}_{p,r,[\![K+1,\infty]\!]}(f)\Leftrightarrow\text{w-suit}_{p,r,K+1}(f)$
(4) $\forall\,\ell\in[\![K+2,\infty]\!]:(\text{w-suit}_{p,r,\ell}(f)\wedge\text{suit}_{p,r,\ell+1}(f))\Rightarrow\text{suit}_{p,r,\ell+2}(f)$
In particular: $\text{suit}_{p,r,[\![K+2,\infty]\!]}(f)\Leftrightarrow\text{suit}_{p,r,\{K+2,K+3\}}(f)$.

In particular,

(1) $\text{w-suit}_{p,r}(f)\Leftrightarrow\text{w-suit}_{p,r,\overline{K+1}}(f)\Leftrightarrow$
$\forall\,\ell\in\overline{K+1}:\forall\, m,n\in W_{K+\ell}: m\equiv n \mod p^\ell\Rightarrow(f-f\%p)(m)\equiv(f-f\%p)(n) \mod p^\ell$
(2) $\text{suit}_{p,r}(f)\Leftrightarrow\text{suit}_{p,r,\overline{K+3}}(f)\Leftrightarrow$
$\forall\,\ell\in\overline{K+3}:\forall\, m,n\in W_{K+\ell}: m\equiv n \mod p^\ell\Leftrightarrow(f-f\%p)(m)\equiv(f-f\%p)(n) \mod p^\ell$.

Proof.
(1) and (2): Let $m, n \in r + p\mathbb{Z}_p$, $M := m\%p^{K+k} \in W_{K+k}$, and $N := n\%p^{K+k} \in W_{K+k}$. Then,

$$m \equiv n \mod p^k \Leftrightarrow M \equiv N \mod p^k. \tag{4.72}$$

By definition of K we have $p^K g \in \mathbb{Z}_p[x]$. Thus,

$$(f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k \tag{4.73}$$

$$\Leftrightarrow g(m) - g(m)\%p - (g(n) - g(n)\%p) \in p^k\mathbb{Z}_p \tag{4.74}$$

$$\Leftrightarrow p^K g(m) - \left(p^K g(m)\right)\%p^{K+1} - \left(p^K g(n) - \left(p^K g(n)\right)\%p^{K+1}\right) \in p^{K+k}\mathbb{Z}_p \tag{4.75}$$

$$\Leftrightarrow p^K g(M) - \left(p^K g(M)\right)\%p^{K+1} - \left(p^K g(N) - \left(p^K g(N)\right)\%p^{K+1}\right) \in p^{K+k}\mathbb{Z}_p \tag{4.76}$$

$$\Leftrightarrow g(M) - g(M)\%p - (g(N) - g(N)\%p) \in p^k\mathbb{Z}_p \tag{4.77}$$

$$\Leftrightarrow (f - f\%p)(M) \equiv (f - f\%p)(N) \mod p^k \tag{4.78}$$

which completes the proof of (1) and (2).
(3): First we will prove

$$m \equiv n \mod p^{K+1} \Rightarrow f(m) \equiv f(n) \mod p \tag{4.79}$$

for all $m, n \in r + p\mathbb{Z}_p$. For that let $a \in \mathbb{Z}_p$, such that $n = m + ap^{K+1}$. Then,

$$f(m) - f(n) = \sum_{i=1}^{d} a_i \left(m^i - \left(m + ap^{K+1}\right)^i\right) \tag{4.80}$$

$$= \sum_{i=1}^{d} a_i \left(m^i - \sum_{j=0}^{i} \binom{i}{j} m^j \left(ap^{K+1}\right)^{i-j}\right) \tag{4.81}$$

$$= \sum_{i=1}^{d} a_i \sum_{j=0}^{i-1} \binom{i}{j} m^j a^{i-j} p^{(K+1)(i-j)} \tag{4.82}$$

$$= p \sum_{i=1}^{d} p^K a_i \sum_{j=0}^{i-1} \binom{i}{j} m^j a^{i-j} p^{(K+1)(i-j-1)} \in p\mathbb{Z}_p \tag{4.83}$$

and hence $f(m) \equiv f(n) \mod p$ as claimed.

Next we will show that

$$\frac{f\left(a + bvp^\ell\right) - f\left(a + (b+1)vp^\ell\right)}{-vp^\ell} - \frac{f\left(a + cvp^\ell\right) - f\left(a + (c+1)vp^\ell\right)}{-vp^\ell} \in p\mathbb{Z}_p \tag{4.84}$$

for all $a, b, c, v \in \mathbb{Z}_p$. We have,

$$f\left(a + bvp^\ell\right) - f\left(a + (b+1)vp^\ell\right) - \left(f\left(a + cvp^\ell\right) - f\left(a + (c+1)vp^\ell\right)\right) \tag{4.85}$$

$$= \sum_{i=0}^{d} a_i \left(a + bvp^\ell\right)^i - \sum_{i=0}^{d} a_i \left(a + (b+1)vp^\ell\right)^i - \tag{4.86}$$
$$\sum_{i=0}^{d} a_i \left(a + cvp^\ell\right)^i + \sum_{i=0}^{d} a_i \left(a + (c+1)vp^\ell\right)^i$$

$$= \sum_{i=0}^{d} a_i \sum_{j=0}^{i} \binom{i}{j} a^{i-j} b^j v^j p^{\ell j} - \sum_{i=0}^{d} a_i \sum_{j=0}^{i} \binom{i}{j} a^{i-j} (b+1)^j v^j p^{\ell j} - \tag{4.87}$$
$$\sum_{i=0}^{d} a_i \sum_{j=0}^{i} \binom{i}{j} a^{i-j} c^j v^j p^{\ell j} + \sum_{i=0}^{d} a_i \sum_{j=0}^{i} \binom{i}{j} a^{i-j} (c+1)^j v^j p^{\ell j}$$

$$= \sum_{i=0}^{d} a_i \sum_{j=0}^{i} \binom{i}{j} a^{i-j} \left(b^j - (b+1)^j - c^j + (c+1)^j\right) v^j p^{\ell j} \tag{4.88}$$

$$= \sum_{i=2}^{d} a_i \sum_{j=2}^{i} \binom{i}{j} a^{i-j} \left(b^j - (b+1)^j - c^j + (c+1)^j\right) v^j p^{\ell j} \tag{4.89}$$

$$= v^2 p^{2\ell-K} \sum_{i=2}^{d} a_i p^K \sum_{j=2}^{i} \binom{i}{j} a^{i-j} \left(b^j - (b+1)^j - c^j + (c+1)^j\right) v^{j-2} p^{\ell(j-2)} \tag{4.90}$$

$$\in v^2 p^{2\ell-K} \mathbb{Z}_p \tag{4.91}$$

and hence

$$\frac{f\left(a + bvp^\ell\right) - f\left(a + (b+1)vp^\ell\right)}{-vp^\ell} - \frac{f\left(a + cvp^\ell\right) - f\left(a + (c+1)vp^\ell\right)}{-vp^\ell} \in vp^{\ell-K}\mathbb{Z}_p. \tag{4.92}$$

Since $\ell \geq K+1$, it follows that $vp^{\ell-K}\mathbb{Z}_p \subseteq p\mathbb{Z}_p$.

Using the preliminary results above we will now prove (3). From Eqn. (4.79) it follows that

$$m \equiv n \mod p^\ell \Rightarrow f(m) \equiv f(n) \mod p^\ell \tag{4.93}$$

for all $m, n \in r + p\mathbb{Z}_p$ and by (1) and Eqn. (4.79) again we need to show that

$$m \equiv n \mod p^{\ell+1} \Rightarrow f(m) \equiv f(n) \mod p^{\ell+1} \tag{4.94}$$

for all $m, n \in W_{K+\ell+1}$. Let $m, n \in W_{K+\ell+1}$ such that $m \equiv n \mod p^\ell$. Our goal is to show that

$$\frac{f(m) - f(n)}{m-n} \in \mathbb{Z}_p, \tag{4.95}$$

because then $p^{\ell+1}$ divides $f(m) - f(n) = (m-n)\frac{f(m)-f(n)}{m-n}$ if $p^{\ell+1}$ divides $m-n$ (i.e. if $m \equiv n \mod p^{\ell+1}$). Assume without loss of generality that $m < n$ (clearly, if $m = n$, then $f(m) \equiv f(n) \mod p^{\ell+1}$) and let $a \in \mathbb{N}$ such that $n = m + ap^\ell$. We compute,

$$\frac{f(m) - f(n)}{m-n} = \frac{f(m) - f\left(m + ap^\ell\right)}{-ap^\ell} \tag{4.96}$$

$$= \frac{1}{a} \sum_{i=0}^{a-1} \frac{f\left(m + ip^\ell\right) - f\left(m + (i+1)p^\ell\right)}{-p^\ell}. \tag{4.97}$$

Since

$$m + ip^\ell \equiv m + (i+1)p^\ell \mod p^\ell \tag{4.98}$$

for all $i \in \underline{a}$, it follows from Eqn. (4.93) that

$$f\left(m + ip^\ell\right) \equiv f\left(m + (i+1)p^\ell\right) \mod p^\ell \tag{4.99}$$

and hence

$$\frac{f\left(m + ip^\ell\right) - f\left(m + (i+1)p^\ell\right)}{-p^\ell} \in \mathbb{Z}_p \tag{4.100}$$

for all $i \in \underline{a}$. Thus all of the a summands of Eqn. (4.97) are p-adic integers and by Eqn. (4.84) they are pairwise congruent modulo p. If $\gcd(p, a) = 1$, it would thus follow that $\frac{f(m)-f(n)}{m-n} \in \mathbb{Z}_p$ and we are done. If p and a are not coprime, let $q_0 \in \overline{p}$ be a common divisor of p and a and let $b_0 \in \mathbb{N}$ such that $a = b_0 q_0$. Then,

$$\frac{f(m) - f(n)}{m-n} = \frac{1}{b_0 q_0} \sum_{i=0}^{b_0 q_0 - 1} \frac{f\left(m + ip^\ell\right) - f\left(m + (i+1)p^\ell\right)}{-p^\ell} \tag{4.101}$$

$$= \frac{1}{b_0} \sum_{j=0}^{b_0-1} \frac{1}{q_0} \sum_{i=0}^{q_0-1} \frac{f\left(m + (jq_0 + i)p^\ell\right) - f\left(m + (jq_0 + i + 1)p^\ell\right)}{-p^\ell} \tag{4.102}$$

where all summands of the inner sum are p-adic integers that are pairwise congruent modulo p by Eqn. (4.84). Thus, the whole inner sum is divisible by q_0 and we get

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_0}\sum_{i=0}^{b_0-1}\frac{f\left(m+iq_0p^\ell\right)-f\left(m+(i+1)q_0p^\ell\right)}{-q_0p^\ell} \tag{4.103}$$

where all of the summands are again p-adic integers. As before, if $\gcd(p,b_0)=1$, we are done, and if p and b_0 are not coprime, we let $q_1\in\overline{p}$ be a common divisor of p and b_0, and $b_1\in\mathbb{N}$ such that $b_0=b_1q_1$. Then,

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_1q_1}\sum_{i=0}^{b_1q_1-1}\frac{f\left(m+iq_0p^\ell\right)-f\left(m+(i+1)q_0p^\ell\right)}{-q_0p^\ell} \tag{4.104}$$

$$= \frac{1}{b_1}\sum_{j=0}^{b_1-1}\frac{1}{q_1}\sum_{i=0}^{q_1-1}\frac{f\left(m+(jq_1+i)q_0p^\ell\right)-f\left(m+(jq_1+i+1)q_0p^\ell\right)}{-q_0p^\ell}. \tag{4.105}$$

where, again, all summands of the inner sum are p-adic integers that are pairwise congruent modulo p by Eqn. (4.84). Thus, the whole inner sum is divisible by q_1 and we get

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_1}\sum_{i=0}^{b_1-1}\frac{f\left(m+iq_1q_0p^\ell\right)-f\left(m+(i+1)q_1q_0p^\ell\right)}{-q_1q_0p^\ell} \tag{4.106}$$

where all of the summands are again p-adic integers. Continuing iteratively we find $u\in\mathbb{N}_0$ (since $a\in\mathbb{N}$ cannot be a zero divisor), $q_0,\ldots,q_{u-1}\in\overline{p}$, and $b_0,\ldots,b_{u-1}\in\mathbb{N}$ such that $a=b_0q_0$, $b_i=b_{i+1}q_{i+1}$ for all $i\in\underline{u-1}$, q_0 is a common divisor of p and a, q_{i+1} is a common divisor of p and b_i for all $i\in\underline{u-1}$. Furthermore,

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_{u-1}}\sum_{i=0}^{b_{u-1}-1}\frac{f\left(m+iq_{u-1}\cdots q_0p^\ell\right)-f\left(m+(i+1)q_{u-1}\cdots q_0p^\ell\right)}{-q_{u-1}\cdots q_0p^\ell}, \tag{4.107}$$

with all summands being p-adic integers, and $\gcd(p,b_{u-1})=1$. But then $\frac{f(m)-f(n)}{m-n}\in\mathbb{Z}_p$, which completes the proof of (3).

(4): From Eqn. (4.79) it follows that

$$m\equiv n \mod p^\ell \Rightarrow f(m)\equiv f(n) \mod p^\ell \tag{4.108}$$

$$m\equiv n \mod p^{\ell+1} \Leftrightarrow f(m)\equiv f(n) \mod p^{\ell+1} \tag{4.109}$$

for all $m,n\in r+p\mathbb{Z}_p$ and by (2), (3), and Eqn. (4.79) we need to show that

$$f(m)\equiv f(n) \mod p^{\ell+2} \Rightarrow m\equiv n \mod p^{\ell+2} \tag{4.110}$$

for all $m,n\in W_{K+\ell+2}$. Let $m,n\in W_{K+\ell+2}$ such that $f(m)\equiv f(n) \mod p^{\ell+1}$. Then $m\equiv n \mod p^{\ell+1}$ and we have $\frac{f(m)-f(n)}{m-n}\in\mathbb{Z}_p$ by Eqn. (4.95). Our goal is to show that

$$\gcd\left(p,\frac{f(m)-f(n)}{m-n}\%p\right)=1 \tag{4.111}$$

because then (cf. Eqn. (4.58)) $p^{\ell+2}$ divides $m-n$ if $p^{\ell+2}$ divides $f(m)-f(n)=(m-n)\frac{f(m)-f(n)}{m-n}$ (i.e. if $f(m)\equiv f(n) \mod p^{\ell+2}$). Assume without loss of generality that $m<n$ (clearly, if $m=n$, then $m\equiv n \mod p^{\ell+2}$) and let $a\in\mathbb{N}$ such that $n=m+ap^{\ell+1}$.

As a preliminary step we will prove that

$$\gcd\left(p,b_i\%p\right)=1, \tag{4.112}$$

for all $i\in\mathbb{Z}$, where

$$b_i := \frac{f\left(m+ip^\ell\right)-f\left(m+(i+1)p^\ell\right)}{-p^\ell} \tag{4.113}$$

which is in $\mathbb{Z}_p$ by Eqn. (4.95) (here we need w-suit$_{p,r,\ell}(f)$). For that assume to the contrary that there is a divisor $q \in [\![2,p]\!]$ of p such that

$$\exists\, i \in \mathbb{Z} : \gcd(p, b_i \% p) = q. \tag{4.114}$$

By Eqn. (4.84) the least significant digits of all b_i coincide, say $b_i \% p = s \in \underline{p}$ for all $i \in \mathbb{Z}$, which implies,

$$\forall\, i \in \mathbb{Z} : \gcd(p, b_i \% p) = \gcd(p, s) = q. \tag{4.115}$$

We compute

$$\frac{f(m) - f\left(m + p/qp^\ell\right)}{-p^\ell} = \sum_{i=0}^{p/q-1} b_i \tag{4.116}$$

$$= p \sum_{i=0}^{p/q-1} \frac{b_i - s + s}{p} \tag{4.117}$$

$$= p \left(\frac{s}{q} + \sum_{i=0}^{p/q-1} \frac{b_i - b_i \% p}{p} \right) \in p\mathbb{Z}_p \tag{4.118}$$

which implies that $f(m) \equiv f\left(m + p/qp^\ell\right) \mod p^{\ell+1}$. But then $m \equiv m + p/qp^\ell \mod p^{\ell+1}$ by suit$_{p,r,\ell+1}(f)$ which is a contradiction, since q divides p and $q \geq 2$. This completes the proof of Eqn. (4.112).

Furthermore, we need the following general fact:

$$\forall\, r \in \underline{p^2} : \forall\, a \in \mathbb{N},\, a \mid p \text{ (in } \mathbb{Z}_p) \;: \forall\, b_0, \ldots, b_{a-1} \in r + p^2\mathbb{Z}_p : \frac{1}{a} \sum_{i=0}^{a-1} b_i \equiv r \mod p. \tag{4.119}$$

In order to prove it let $c_i \in \mathbb{Z}_p$ such that $b_i = r + p^2 c_i$ for all $i \in \underline{a}$. Then,

$$\frac{1}{a} \sum_{i=0}^{a-1} b_i = \frac{1}{a} \sum_{i=0}^{a-1} \left(r + p^2 c_i\right) = r + p\frac{p}{a} \sum_{i=0}^{a-1} c_i \equiv r \mod p. \tag{4.120}$$

We continue with the proof of Eqn. (4.111) and compute

$$\frac{f(m) - f(n)}{m - n} = \frac{f(m) - f\left(m + ap^{\ell+1}\right)}{-ap^{\ell+1}} \tag{4.121}$$

$$= \frac{1}{a} \sum_{i=0}^{a-1} \frac{f\left(m + ip^\ell\right) - f\left(m + (i+1)p^\ell\right)}{-p^\ell}. \tag{4.122}$$

By Eqn. (4.112) it follows that the least significant digits of all summands of Eqn. (4.122) are coprime to p. Furthermore, they are all congruent modulo p^2 by Eqn. (4.92), since $\ell \geq K + 2$. If $\gcd(p, a) = 1$ (in which case a divides p in $\mathbb{Z}_p$), it would thus follow that $\gcd\left(p, \frac{f(m)-f(n)}{m-n} \% p\right) = 1$ due to Eqn. (4.119). If p and a are not coprime, let $q_0 \in \overline{p}$ be a common divisor of p and a and let $b_0 \in \mathbb{N}$ such that $a = b_0 q_0$. Then,

$$\frac{f(m) - f(n)}{m - n} = \frac{1}{b_0 q_0} \sum_{i=0}^{b_0 q_0 - 1} \frac{f\left(m + ip^\ell\right) - f\left(m + (i+1)p^\ell\right)}{-p^\ell} \tag{4.123}$$

$$= \frac{1}{b_0} \sum_{j=0}^{b_0-1} \frac{1}{q_0} \sum_{i=0}^{q_0-1} \frac{f\left(m + (jq_0 + i)p^\ell\right) - f\left(m + (jq_0 + i + 1)p^\ell\right)}{-p^\ell} \tag{4.124}$$

where all summands of the inner sum are p-adic integers that are pairwise congruent modulo p^2 by Eqn. (4.92), while their least significant digits are coprime to p. Thus, the least significant digits of the outer summands (i.e. the inner sum divided by q_0) are coprime to p by Eqn. (4.119), since q_0 divides p and we get

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_0}\sum_{i=0}^{b_0-1}\frac{f\left(m+iq_0p^\ell\right)-f\left(m+(i+1)q_0p^\ell\right)}{-q_0p^\ell} \tag{4.125}$$

where the least significant digits of the summands are coprime to p. As before, if $\gcd(p,b_0)=1$, we are done by Eqn. (4.119), and if p and b_0 are not coprime, we let $q_1 \in \overline{p}$ be a common divisor of p and b_0, and $b_1 \in \mathbb{N}$ such that $b_0 = b_1q_1$. Then,

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_1q_1}\sum_{i=0}^{b_1q_1-1}\frac{f\left(m+iq_0p^\ell\right)-f\left(m+(i+1)q_0p^\ell\right)}{-q_0p^\ell} \tag{4.126}$$

$$= \frac{1}{b_1}\sum_{j=0}^{b_1-1}\frac{1}{q_1}\sum_{i=0}^{q_1-1}\frac{f\left(m+(jq_1+i)q_0p^\ell\right)-f\left(m+(jq_1+i+1)q_0p^\ell\right)}{-q_0p^\ell}. \tag{4.127}$$

where, again, all summands of the inner sum are p-adic integers that are pairwise congruent modulo p^2 by Eqn. (4.92), and their least significant digits are coprime to p. Thus, the least significant digits of the outer summands (i.e. the inner sum divided by q_1) are coprime to p by Eqn. (4.119), since q_1 divides p and we get

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_1}\sum_{i=0}^{b_1-1}\frac{f\left(m+iq_1q_0p^\ell\right)-f\left(m+(i+1)q_1q_0p^\ell\right)}{-q_1q_0p^\ell} \tag{4.128}$$

where the least significant digits of the summands are coprime to p. Continuing iteratively we find $u \in \mathbb{N}_0$ (since $a \in \mathbb{N}$ cannot be a zero divisor), $q_0,\ldots,q_{u-1} \in \overline{p}$, and $b_0,\ldots,b_{u-1} \in \mathbb{N}$ such that $a = b_0q_0$, $b_i = b_{i+1}q_{i+1}$ for all $i \in \underline{u-1}$, q_0 is a common divisor of p and a, q_{i+1} is a common divisor of p and b_i for all $i \in \underline{u-1}$,

$$\frac{f(m)-f(n)}{m-n} = \frac{1}{b_{u-1}}\sum_{i=0}^{b_{u-1}-1}\frac{f\left(m+iq_{u-1}\cdots q_0p^\ell\right)-f\left(m+(i+1)q_{u-1}\cdots q_0p^\ell\right)}{-q_{u-1}\cdots q_0p^\ell} \tag{4.129}$$

with the least significant digits of the summands being coprime to p, and $\gcd(p,b_{u-1})=1$. But then $\gcd\left(p,\frac{f(m)-f(n)}{m-n}\%p\right)=1$ by Eqn. (4.119) which completes the proof of (4). □

The difference it makes to go from polynomials in $\mathbb{Z}_p[x]$ to (p,r)-integral polynomials in $\mathbb{Q}_p[x]$ in the context of p-adic systems is quite remarkable. While all polynomials in $\mathbb{Z}_p[x]$ are (p,r)-integral (trivially) and weakly (p,r)-suitable (Theorem 4.8) for all $2 \leq p \in \mathbb{N}$ and all $r \in \underline{p}$, both need to be checked algorithmically for polynomials in $\mathbb{Q}_p[x]$ (Lemma 4.9 and Theorem 4.10). $f(x) = 1/2x$ is an easy example of a polynomial that is $(2,0)$-integral but not weakly $(2,0)$-suitable at 2 ($f(0) = 0 \not\equiv 2 = f(2^2) \mod 2^2$). Furthermore, it is very easy to check whether a polynomial $f \in \mathbb{Z}_p[x]$ is (p,r)-suitable, as this only depends on the derivative of f in r (Theorem 4.8). For polynomials in $\mathbb{Q}_p[x]$ however, (p,r)-suitability needs to be checked algorithmically (Theorem 4.10). As an example consider $f(x) = 1/4x^3 + x^2 + x$ which is $(2,0)$-integral, weakly $(2,0)$-suitable, but not $(2,0)$-suitable at 2 ($f(0) = 0 \equiv 2^3 = f(2) \mod 2^2$) despite the fact that $f'(0) = 1$ is coprime to 2. $f(x) = 1/8x^3 + x^2 + x$ defines a polynomial that is not even weakly $(2,0)$-suitable at 2 ($f(2) = 7 \not\equiv 69 = f(2+2^2) \mod 2^2$) and yet again $f'(0) = 1$. Another difference is that for any p-adic system F defined by polynomials in $\mathbb{Z}_p[x]$ there exits a p-adic system G defined by polynomials in $\mathbb{Z}_p[x]$ that is a weak canonical form of F (e.g. $(x, 3x+1)$ which is a weak canonical form of $(x+1, 3x+2)$). For p-adic systems defined by polynomials in $\mathbb{Q}_p[x]$ this is no longer the case. Indeed, if $f(x) = 1/16x^4 + x^3 + 1/2x^2 + x + 1$, then f is $(2,0)$-integral (even $(2,0)$-suitable) but $f(0) = 1 \not\equiv 14 = f(2) \mod 2$, so the 2-adic system $\mathrm{F} := (f(x), x-1)$ does not have a weak canonical form that can be expressed with polynomials (a weak canonical form of F is given by

$((f - f\%2)(x), x - 1)$ but $f - f\%2$ is not a polynomial function). Further indications of the much more erratic behavior of polynomials in $Q_p[x]$ are given by the following examples. Let

$$f(x) = -3/512x^7 + 1/128x^5 + x^4 + 1/8x^2 + 1 \tag{4.130}$$

$$g(x) = 1/512x^7 + 1/128x^5 + x^4 + 1/8x^2 + 1 \tag{4.131}$$

$$h(x) = 1/32x^{11} + 1/2x^9 + 1/16x^8 + 1/16x^7 + 1/8x^6 + 1/16x^5 + 1/32x^4 + 1/8x^3 - 1/8x^2 + x + 1 \tag{4.132}$$

and $k \in \mathbb{N}$. Then f, g, and h are $(2,0)$-integral and we have

$$\text{w-suit}_{2,0,k}(f) \Leftrightarrow k \in \{1,3\} \tag{4.133}$$

$$\text{suit}_{2,0,k}(f) \Leftrightarrow k \in \{1\} \tag{4.134}$$

$$\text{w-suit}_{2,0,k}(g) \Leftrightarrow k \in \{1\} \cup [\![4,\infty]\!] \tag{4.135}$$

$$\text{suit}_{2,0,k}(g) \Leftrightarrow k \in \{1\} \tag{4.136}$$

$$\text{w-suit}_{2,0,k}(h) \Leftrightarrow k \in \{1\} \cup [\![3,\infty]\!] \tag{4.137}$$

$$\text{suit}_{2,0,k}(h) \Leftrightarrow k \in \{1,3\}\,. \tag{4.138}$$

Next, we will fix our notions in relation to p-adic systems defined by polynomials. We define the following predicates on $\mathcal{F}_p$ ($2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \mathcal{F}_p$, $A \subseteq \mathbb{Q}_p$, $D \subseteq \mathbb{N}_0 \cup \{-\infty\}$):

$$\begin{aligned} \text{poly}_{A,D}(\mathrm{F}) &\Leftrightarrow \text{dom}_{\mathbb{Z}_p}(\mathrm{F}) && \text{F is } \textit{A-polynomial with degree in D or, if } D = \{d\}, \\ &\quad \forall\, r \in \underline{p} : \mathrm{F}[r]|_{r+p\mathbb{Z}_p} \in A[x] && \text{F is } \textit{A-polynomial of degree d} \\ &\quad\quad \deg(\mathrm{F}[r]|_{r+p\mathbb{Z}_p}) \in D \end{aligned} \tag{4.139}$$

$$\text{poly}_A(\mathrm{F}) \Leftrightarrow \text{poly}_{A,\mathbb{N}_0\cup\{-\infty\}}(\mathrm{F}) \qquad \text{F is } \textit{A-polynomial} \tag{4.140}$$

$$\text{poly}(\mathrm{F}) \Leftrightarrow \text{poly}_{\mathbb{Q}_p,\mathbb{N}_0\cup\{-\infty\}}(\mathrm{F}) \qquad \text{F is } \textit{polynomial} \tag{4.141}$$

$$\text{lin-poly}_A(\mathrm{F}) \Leftrightarrow \text{poly}_{A,\{-\infty,0,1\}}(\mathrm{F}) \qquad \text{F is } \textit{A-linear-polynomial} \tag{4.142}$$

$$\text{lin-poly}(\mathrm{F}) \Leftrightarrow \text{poly}_{\mathbb{Q}_p,\{-\infty,0,1\}}(\mathrm{F}) \qquad \text{F is } \textit{linear-polynomial} \tag{4.143}$$

Using our new predicates it is easy to formulate the following corollary to Theorem 4.8.

Corollary 4.11. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{F} \in \mathcal{F}_p(\text{poly}_{\mathbb{Z}_p})$. *Then,*

(1) w-block-S(F)
(2) $\text{block}(\mathrm{F}) \Leftrightarrow \exists\, k \in [\![2,\infty]\!] : \text{block}_k(\mathrm{F})$.

Proof. Follows directly from Theorem 4.8. □

A similar corollary to Theorem 4.10 can also be formulated.

Corollary 4.12. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \mathcal{F}_p(\text{poly})$, *and* $K \in \mathbb{N}_0$ *such that* $-K$ *is the minimum of* 0 *and the p-adic valuations of all coefficients of the polynomials* $\mathrm{F}[r]|_{r+p\mathbb{Z}_p}$, $r \in \underline{p}$. *Then,*

(1) $\text{w-block-S}(\mathrm{F}) \Leftrightarrow \text{w-block-S}_{\overline{K+1}}(\mathrm{F})$
(2) $\text{block}(\mathrm{F}) \Leftrightarrow \text{block}_{\overline{K+3}}(\mathrm{F})$.

Proof. Follows directly from Theorem 4.10. □

Theorem 4.8 and Corollary 4.11 have a remarkable consequence: every $\mathbb{Z}_p$-polynomial p-fibred function has the weak block property and "almost all" of them also have the block property in the sense that if $P_0, \ldots, P_{p-1} \in \mathbb{Z}_p[x]$ are arbitrary, then there are $a_0, \ldots, a_{p-1} \in \underline{p}$ such that $(P_0(x) + a_0 x, \ldots, P_{p-1}(x) + a_{p-1}x)$ has the block property. In other words: every p-fibred function defined by polynomials over $\mathbb{Z}_p$ can be turned into a p-adic system by only modifying the linear coefficients! By Theorem 4.8 all of the following p-fibred functions are examples of p-adic systems:

- $(x)^p = (x, \ldots, x) \in \overline{\mathcal{F}}_p$ where $2 \leq p \in \mathbb{N}$ (standard base p)
- $(x, 3x+1) \in \overline{\mathcal{F}}_2$ (Collatz)
- $(7x^3 - 4x^2 + x - 6, 3x^7 - x + 1, x^2 + 6x + 2) \in \overline{\mathcal{F}}_3$
- $(\frac{32}{7}x^2 + \frac{5}{3}x - 4, \frac{13}{11}x + 5, \frac{1}{17}x + 2, 3x^2 + \frac{7}{19}x - \frac{14}{5}) \in \overline{\mathcal{F}}_4$
- $(\mathrm{i}x^2 + x, 5\mathrm{i}x^4 - 2 + 7, x + 3, -9x^3 + 12x + 7, -5\mathrm{i}x^2 + x + 1) \in \overline{\mathcal{F}}_5$ where $\mathrm{i}^2 = -1$, i.e. $\mathrm{i} \in \{\ldots 2431212, \ldots 2013233\} \subseteq \mathbb{Z}_5$
- $\left(\prod_{i=0}^{p-1}(x-i)\right)^p \in \overline{\mathcal{F}}_p$ where $p \in \mathbb{P}$.

Theorem 4.10 provides the following additional examples of p-adic systems:

- $(\frac{17}{4}x^6 + \frac{37}{16}x^5 - 107x^4 - \frac{15}{4}x^3 + 78x^2 + 3x - 2, -25x^6 + \frac{7}{4}x^5 - \frac{49}{2}x^4 - \frac{21}{2}x^3 + 5x^2 + \frac{79}{4}x + \frac{19}{2}) \in \overline{\mathcal{F}}_2$
- $(-\frac{23}{27}x^3 - 11x^2 + x - 20, -28x^4 + \frac{7}{9}x^3 + \frac{29}{3}x^2 + \frac{4}{3}x + \frac{11}{9}, -2x^4 - \frac{29}{9}x^3 - \frac{5}{3}x^2 - \frac{11}{3}x - \frac{2}{9}) \in \overline{\mathcal{F}}_3$.

A direct consequence of the fact that every $\mathbb{Z}_p$-polynomial p-fibred function has the weak block property is, that whenever we extend a p-fibred function F with domain $\mathbb{Z}$ that is defined by polynomial functions with integer coefficients (such as F_p or F_C) to $\mathbb{Z}_p$ by simply changing the domain from $\mathbb{Z}$ to $\mathbb{Z}_p$ while keeping the polynomials fixed (cf. Eqn. (1.1) and Eqn. (1.3)), the p-digit table of the new extended p-fibred function will coincide with the unique extension of the p-digit table of F as given by Lemma 3.15.

Corollary 4.13. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{G} \in \mathcal{F}_p(\mathrm{poly}_{\mathbb{Z}})$, $\mathrm{F} := \mathrm{G}|_{\mathbb{Z}}$, *and* $\mathrm{E} \in \mathcal{D}_p(\mathrm{dom}_{\mathbb{Z}_p}, \text{w-block})$ *such that* $\mathrm{E}|_{\mathbb{Z}} = \mathrm{D}(\mathrm{F})$ *(cf. Lemma 3.15 and note that* w-block(F) *by Corollary 4.11 (1)). Then,* $\mathrm{E} = \mathrm{D}(\mathrm{G})$.

Proof. Follows directly from Corollary 3.16 and Corollary 4.11 (1). □

It is possible to reduce the degrees of the polynomials defining a $\mathbb{Z}_p$-polynomial p-fibred function F to $k-1$ while keeping $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!]$ constant. In order to prove this we need the following lemma which utilizes the well-known notion of Vandermonde matrices.

Lemma 4.14. *Let* $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f \in \mathbb{Z}_p[x]$, *and* $k \in \mathbb{N}$. *Furthermore, let*

$$A := \left((r+ip)^j\right)_{i,j \in \underline{k}} = \begin{pmatrix} (r+(0\quad)p)^0 & \ldots & (r+(0\quad)p)^{k-1} \\ \vdots & & \vdots \\ (r+(k-1)p)^0 & \ldots & (r+(k-1)p)^{k-1} \end{pmatrix} \in \mathbb{N}^{k \times k} \tag{4.144}$$

$$b := \begin{pmatrix} f(r+(0\quad)p) \\ \vdots \\ f(r+(k-1)p) \end{pmatrix} \in \mathbb{Z}_p^k \tag{4.145}$$

(note that for the whole theorem we define $0^0 := 1$*). Then* A *is invertible,* $A^{-1} \cdot b \in \mathbb{Z}_p^k$, *and*

$$g(x) := \left((A^{-1} \cdot b)\%p^k\right) \cdot (1, x, \ldots, x^{k-1}) \tag{4.146}$$

satisfies $g(x) \in \underline{p^k}[x]$, $\deg(g) \leq k-1$, *and* $f(n) \equiv g(n) \mod p^k$ *for all* $n \in r + p\mathbb{Z}_p$.

Proof. We consider the following system of k equations in $a_0, \ldots, a_{k-1} \in \mathbb{Q}_p$

$$\begin{array}{rcl} a_0(r+(0\quad)p)^0 + \cdots + a_{k-1}(r+(0\quad)p)^{k-1} & = & f(r+(0\quad)p) \\ \vdots & & \\ a_0(r+(k-1)p)^0 + \cdots + a_{k-1}(r+(k-1)p)^{k-1} & = & f(r+(k-1)p) \end{array} \tag{4.147}$$

which is solved by $(a_0, \ldots, a_{k-1}) = A^{-1} \cdot b \in \mathbb{Q}_p^k$. It can be easily verified by induction on k that

$$\det(A) = \prod_{i=0}^{k-1} i! p^i \neq 0 \tag{4.148}$$

which implies that A^{-1} does indeed exist. To prove that $A^{-1} \cdot b \in \mathbb{Z}_p^k$ let $u, v \in \mathbb{Z}_p[x]$ with $\deg(v) < k$ such that

$$f(x) = \left(\prod_{i=0}^{k-1}(x - (r+ip))\right) u(x) + v(x). \tag{4.149}$$

Then $v(r+ip) = f(r+ip)$ for all $i \in \underline{k}$, which implies that the polynomial v of degree less than k interpolates the k points $(r+ip, f(r+ip))$, $i \in \underline{k}$ and thus is uniquely defined (within $\mathbb{Q}_p[x]$). In the same way the polynomial $(A^{-1}\cdot b)\cdot(1,x,\ldots,x^{k-1})$ is of degree less than k and interpolates the same points, which implies that $(A^{-1}\cdot b)\cdot(1,x,\ldots,x^{k-1}) = v(x) \in \mathbb{Z}_p[x]$ and hence $A^{-1}\cdot b \in \mathbb{Z}_p^k$.

We are left to show that $f(n) \equiv g(n) \mod p^k$ for all $n \in r+p\mathbb{Z}_p$ and compute

$$f(r+ap) - v(r+ap) = \left(\prod_{i=0}^{k-1}(r+ap-(r+ip))\right)u(r+ap) \tag{4.150}$$

$$= p^k\left(\prod_{i=0}^{k-1}(a-i)\right)u(r+ap) \tag{4.151}$$

$$\in p^k\mathbb{Z}_p \tag{4.152}$$

for all $a \in \mathbb{Z}_p$. Hence $f(n) \equiv v(n) \equiv g(n) \mod p^k$ for all $n \in r+p\mathbb{Z}_p$. □

Theorem 4.15. *For arbitrary $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f \in \mathbb{Z}_p[x]$, and $k \in \mathbb{N}$ let $g_{p,r,f,k} \in \underline{p^k}[x]$ denote the polynomial $g(x)$ in Lemma 4.14 for the given parameters p, r, f, k. Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p}, \mathrm{poly}_{\mathbb{Z}_p})$, and $k \in \mathbb{N}$. Furthermore, let $\mathrm{G} \in \mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p}, \mathrm{poly})$ such that $\mathrm{G}[r](x) = g_{p,r,\mathrm{F}[r],k}(x)$ for all $r \in \underline{p}$. Then $\mathrm{poly}_{\underline{p^k},\underline{k}}(\mathrm{G})$ and $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G})[\![\underline{k}]\!]$.*

Proof. Follows directly from Theorem 4.8 (1) ($\mathrm{F}[r]$ is weakly (p,r)-suitable for all $r \in \underline{p}$), Theorem 4.1 (1) (therefore F has the weak block property), Corollary 3.8 (2) (thus $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}((\mathrm{F}[0]\%p^k, \ldots, \mathrm{F}[p-1]\%p^k))[\![\underline{k}]\!]$), and Lemma 4.14 (thus $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G})[\![\underline{k}]\!]$). □

As an example consider the 2-adic system $\mathrm{F} := (-36x^9 - 67x^8 - 47x^7 - 35x^6 - 13x^5 + 79x^4 - 40x^3 + 95x^2 + 75x + 4, 15x^9 - x^8 - 58x^7 - 92x^6 - 68x^5 + 10x^4 - 54x^3 + 98x^2 - 10x + 48)$ and $k := 4$. By Theorem 4.15 the 2-adic system $\mathrm{G} := (8x^3 + 11x^2 + 11x + 4, 14x^2 + x + 1)$ satisfies $\mathrm{D}(\mathrm{F})[\![\underline{4}]\!] = \mathrm{D}(\mathrm{G})[\![\underline{4}]\!]$ and this is indeed the case.

p-adic systems defined by rational functions. Using the results from the previous subsection and Theorem 4.7, we can identify many rational functions that are (p,r)-suitable.

Theorem 4.16. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $g, h \in \mathbb{Z}_p[x]$ such that $\gcd(p, h(r)\%p) = 1$ and $f(n) = g(n)/h(n)$ for all $n \in r+p\mathbb{Z}_p$, and $k \in \mathbb{N}_0$. Then,*

(1) $\text{w-suit}_{p,r,k}(f)$
(2) $k \leq 1 \Rightarrow \mathrm{suit}_{p,r,k}(f)$
(3) $k \geq 2 \Rightarrow (\mathrm{suit}_{p,r,k}(f) \Leftrightarrow \mathrm{suit}_{p,r,k}(g - (f(r)\%p)h))$.

Note that $g - (f(r)\%p)h$ in (3) is a polynomial in $\mathbb{Z}_p[x]$, which implies that we can use Theorem 4.8 (3) to check whether it is (p,r)-suitable at k.

Proof of Theorem 4.16. (2) is clearly true for any function f. In order to prove (1) and (3) we first observe that

$$f(n) = \frac{g(n)}{h(n)} = \frac{g(n) - (f(r)\%p)h(n)}{h(n)} + f(r)\%p \tag{4.153}$$

for all $n \in r+p\mathbb{Z}_p$. Thus, f is (weakly) (p,r)-suitable if and only if

$$\hat{f} : \mathbb{Z}_p \to \mathbb{Z}_p \tag{4.154}$$
$$n \mapsto \begin{cases} \frac{g(n)-(f(r)\%p)h(n)}{h(n)} & \text{if } n \in r+p\mathbb{Z}_p \\ f(n) & \text{if } n \notin r+p\mathbb{Z}_p \end{cases}$$

is (weakly) (p,r)-suitable. Furthermore,

$$(g(n)h(r) - g(r)h(n))\%p = 0 \tag{4.155}$$

for all $n \in r+p\mathbb{Z}_p$, and hence

$$\hat{f}(n)\%p = (f(n) - f(r))\%p = \frac{g(n)h(r) - g(r)h(n)}{h(n)h(r)}\%p = 0 \tag{4.156}$$

for all $n \in r + p\mathbb{Z}_p$, since $\gcd(p, h(r)\%p) = 1$. Thus $\hat{f}$ (a quotient of two functions) satisfies all conditions of Theorem 4.7 and (1) and (3) follow from the "In particular" part and from Theorem 4.8 (in particular one needs that all polynomials are weakly (p,r)-suitable and also, for $k \geq 2$, that a polynomial is (p,r)-suitable at k if and only if it is (p,r)-suitable at $\overline{k}$). □

Since the question of (weak) suitability of the rational functions treated in Theorem 4.16 reduces to a questions of (weak) suitability of polynomial functions, as a result we get the following analogue of Corollary 4.11.

Corollary 4.17. *Let $2 \leq p \in \mathbb{N}$ and $\mathrm{F} \in \mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p})$ such that for all $r \in \underline{p}$ there are $g_r, h_r \in \mathbb{Z}_p[x]$ with $\gcd(p, h_r(r)\%p) = 1$ and $\mathrm{F}[r](n) = g_r(n)/h_r(n)$ for all $n \in r + p\mathbb{Z}_p$ (cf. the assumptions of Theorem 4.16). Then,*

(1) w-block-S(F)
(2) block(F) $\Leftrightarrow \exists\, k \in [\![2, \infty]\!] : \mathrm{block}_k(\mathrm{F})$.

Proof. Follows directly from Corollary 4.11 and Theorem 4.16. □

Given Theorem 4.16 all of the following p-fibred functions are examples of p-adic systems:

- $\left(\frac{1}{3x+1}, \frac{1}{x}\right) \in \overline{\mathcal{F}}_2$ (inverse Collatz)
- $\left(\frac{x^3-3x^2+7x-1}{5x^2-3}, \frac{6x^5+13x^4-9x+4}{19x^3-3x^2+1}\right) \in \overline{\mathcal{F}}_2$
- $\left(\frac{3x^3-x}{x-5}, \frac{1}{7x-2}, \frac{2x-9}{x-1}, \frac{5x-7}{x^2-2}, \frac{-2x+1}{x-3}, \frac{5x^2+x}{x^2-6}\right) \in \overline{\mathcal{F}}_6$.

One open problem is the characterization of all rational functions on $\mathbb{Z}_p$ that are (weakly) (p,r) suitable, i.e. dropping the assumption $\gcd(p, h(r)\%p) = 1$ in Theorem 4.16. This would also be a generalization of Theorem 4.10 which treats such rational functions requiring in return the function in the denominator to be constant. It appears likely that there is an analogue of Theorem 4.10 for this general situation, i.e. that one can find a finite witness set to check (weak) (p,r)-suitability at k and that it suffices to check (weak) (p,r)-suitability at k for finitely many k to get full (weak) (p,r)-suitability. An educated guess for the general situation might be given by the following conjecture (cf. Theorem 4.10).

Conjecture 4.18. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $g, h \in \mathbb{Z}_p[x]$ such that $f(n) = g(n)/h(n)$ for all $n \in r + p\mathbb{Z}_p$, $k \in \mathbb{N}_0$,*

$$W_\ell := \underline{p^\ell} \cap (r + p\mathbb{Z}_p) \tag{4.157}$$

for all $\ell \in \mathbb{N}_0$, and

$$K := \max(\{\nu_p(h(n)) \mid n \in r + p\mathbb{Z}_p\}) \in \mathbb{N}_0 \tag{4.158}$$

(note that this maximum exists and is in $\mathbb{N}_0$ because otherwise h would have a root in $r + p\mathbb{Z}_p$ which contradicts the assumption $f(n) = g(n)/h(n)$ for $n \in r + p\mathbb{Z}_p$).
Then, W_{K+k} is a finite witness set for f being (weakly) (p,r)-suitable at k, i.e.

(1) $\text{w-suit}_{p,r,k}(f) \Leftrightarrow$
$\forall\, m, n \in W_{K+k} : m \equiv n \mod p^k \Rightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k$
(2) $\mathrm{suit}_{p,r,k}(f) \Leftrightarrow$
$\forall\, m, n \in W_{K+k} : m \equiv n \mod p^k \Leftrightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^k$.

Furthermore,

(3) $\forall\, \ell \in [\![K+1, \infty]\!] : \text{w-suit}_{p,r,\ell}(f) \Rightarrow \text{w-suit}_{p,r,\ell+1}(f)$
In particular: $\text{w-suit}_{p,r,[\![K+1,\infty]\!]}(f) \Leftrightarrow \text{w-suit}_{p,r,K+1}(f)$
(4) $\forall\, \ell \in [\![K+2, \infty]\!] : (\text{w-suit}_{p,r,\ell}(f) \wedge \mathrm{suit}_{p,r,\ell+1}(f)) \Rightarrow \mathrm{suit}_{p,r,\ell+2}(f)$
In particular: $\mathrm{suit}_{p,r,[\![K+2,\infty]\!]}(f) \Leftrightarrow \mathrm{suit}_{p,r,\{K+2,K+3\}}(f)$.

In particular,

(1) $\text{w-suit}_{p,r}(f) \Leftrightarrow \text{w-suit}_{p,r,\overline{K+1}}(f) \Leftrightarrow$
$\forall\, \ell \in \overline{K+1} : \forall\, m,n \in W_{K+\ell} : m \equiv n \mod p^\ell \Rightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^\ell$
(2) $\text{suit}_{p,r}(f) \Leftrightarrow \text{suit}_{p,r,\overline{K+3}}(f) \Leftrightarrow$
$\forall\, \ell \in \overline{K+3} : \forall\, m,n \in W_{K+\ell} : m \equiv n \mod p^\ell \Leftrightarrow (f - f\%p)(m) \equiv (f - f\%p)(n) \mod p^\ell$.

Unfortunately, a general proof could not be given by now and will be subject of future work.

5. Generalizing Hensel's Lemma using p-adic systems

In this section we use p-adic systems to give a very easy and accessible proof of a surprisingly radical generalization of a famous lemma due to Kurt Hensel which has several equivalent formulations one of which reads as follows [21].

Lemma 5.1 (Hensel's Lemma)**.** *Let p be a prime, $r \in \underline{p}$, and $f \in \mathbb{Z}_p[x]$ such that $f(r)\%p = 0$ and $f'(r)\%p \neq 0$. Then, f has a unique root in $r + p\mathbb{Z}_p$.*

The generalization we will prove below is given by the following theorem.

Theorem 5.2. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, and $f \in (\mathbb{Z}_p)^{\mathbb{Z}_p}$ such that $f(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$ and $\text{suit}_{p,r}(f)$. Then, f has a unique root in $r + p\mathbb{Z}_p$.*

A comparison of the differing assumptions of Hensel's Lemma and the above theorem shows:

(1) $p \in \mathbb{P} \quad \rightarrow \quad 2 \leq p \in \mathbb{N}$
(2) $f \in \mathbb{Z}_p[x] \quad \rightarrow \quad f \in (\mathbb{Z}_p)^{\mathbb{Z}_p}$
(3) $f(r)\%p = 0 \quad \rightarrow \quad f(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p \quad (\Leftrightarrow f(r)\%p = 0 \text{ if } f \in \mathbb{Z}_p[x])$
(4) $f'(r)\%p \neq 0 \quad \rightarrow \quad \text{suit}_{p,r}(f) \quad (\Leftrightarrow f'(r)\%p \neq 0 \text{ if } p \in \mathbb{P} \text{ and } f \in \mathbb{Z}_p[x] \text{ by Theorem 4.8 (3)})$.

The generalizing aspect of Theorem 5.2 is entailed by (1) and (2), while (3) and (4) are necessary adaptations of the conditions on f. It can be seen that the theorem's conditions in (3) and (4) are equivalent to their corresponding versions in Hensel's Lemma if one assumes that p is prime and f is a polynomial function with coefficients in $\mathbb{Z}_p$. The most remarkable difference is probably given by (2), where the assumption that f is a polynomial function is dropped and arbitrary functions on $\mathbb{Z}_p$ are allowed. It should be noted that the idea of generalizing Hensel's Lemma by dropping the assumption that f is a polynomial function, is not new. A related result can be found in [60] which considers general functions on $\mathbb{Z}_p$, but only considers the case where p is prime. The further generalization which is given in the following subsection appears to be completely new, however. In order to prove Theorem 5.2 we need the following lemma.

Lemma 5.3. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $A \subseteq \mathbb{Z}_p$, $a, b \in \mathbb{Z}_p$, $f, g, h : A \to \mathbb{Z}_p$ such that*

$$g(n) = f(n) + an + b \tag{5.1}$$

$$h(n) = f(n) + apn + b \tag{5.2}$$

for all $n \in A$, and $k \in \mathbb{N}_0$. Then,

(1) $\text{w-suit}_{p,r,k}(f) \Rightarrow \text{w-suit}_{p,r,k}(g)$
(2) $\text{suit}_{p,r,\overline{k}}(f) \Rightarrow \text{suit}_{p,r,\overline{k}}(h)$.

Proof. The statements are clearly true if $a = 0$, hence we may assume without loss of generality that $b = 0$ and $f((r + p\mathbb{Z}_p) \cap A) \subseteq p\mathbb{Z}_p$.
(1): Let $m, n \in (r + p\mathbb{Z}_p) \cap A$. Then,

$$m \equiv n \mod p^k \Rightarrow m \equiv n \mod p^k \wedge f(m) \equiv f(n) \mod p^k \tag{5.3}$$

$$\Rightarrow f(m) + am \equiv f(n) + an \mod p^k \tag{5.4}$$

$$\Rightarrow g(m) \equiv g(n) \mod p^k. \tag{5.5}$$

(2): Let $m, n \in (r + p\mathbb{Z}_p) \cap A$. Then,

$$m \equiv n \mod p^k \Rightarrow h(m) \equiv h(n) \mod p^k \tag{5.6}$$

by (1) and we are left to show that

$$h(m) \equiv h(n) \mod p^k \Rightarrow m \equiv n \mod p^k. \tag{5.7}$$

Assume to the contrary that $h(m) \equiv h(n) \mod p^k$ and $m \not\equiv n \mod p^k$. Let

$$\ell := \max\left\{i \in \mathbb{N}_0 : m \equiv n \mod p^i\right\}. \tag{5.8}$$

Then $\ell < k$ and

$$\ell = \max\left\{i \in \mathbb{N}_0 : f(m) \equiv f(n) \mod p^i\right\} \tag{5.9}$$

since $\mathrm{suit}_{p,r,\overline{k}}(f)$. Let $c, d, e \in \mathbb{Z}_p$ such that $h(m) = h(n) + cp^k$, $m = n + dp^\ell$ and $f(m) = f(n) + ep^\ell$. Then,

$$f(m) + apm = f(n) + apn + cp^k \Leftrightarrow f(n) + ep^\ell + ap(n + dp^\ell) = f(n) + apn + cp^k \tag{5.10}$$

$$\Leftrightarrow ep^\ell + adp^{\ell+1} = cp^k \tag{5.11}$$

$$\Leftrightarrow e + adp = cp^{k-\ell} \tag{5.12}$$

$$\Leftrightarrow e = p(cp^{k-\ell-1} - ad) \tag{5.13}$$

where $cp^{k-\ell-1} - ad \in \mathbb{Z}_p$. Hence, $f(m) \equiv f(n) \mod p^{\ell+1}$ which is a contradiction. □

Note that the stronger version

$$\mathrm{suit}_{p,r,k}(f) \Rightarrow \mathrm{suit}_{p,r,k}(h) \tag{5.14}$$

of (2) is not true in general as the following example shows.

Example 5.4. Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ such that $f(n) = (n\%8 = 2\ ?\ 4 : (n\%8 = 4\ ?\ 2 : n\%8))$, $a = 1$, $b = 0$, and $h : \mathbb{Z}_2 \to \mathbb{Z}_2$ with $h(n) = f(n) + 2an + b = f(n) + 2n$ for all $n \in \mathbb{N}_2$. Then, $\mathrm{suit}_{2,0,3}(f)$ but $\neg\mathrm{suit}_{2,0,3}(h)$, since $0 \not\equiv 2 \mod 2^3$ but $h(0) = 0 \equiv 8 = h(2) \mod 2^3$. Note that $\neg\mathrm{suit}_{2,0,2}(f)$ since $0 \not\equiv 2 \mod 2^2$ but $f(0) = 0 \equiv 4 = f(2) \mod 2^2$, which is what makes the counter-example possible.

Proof of Theorem 5.2. Let $g \in (\mathbb{Z}_p)^{\mathbb{Z}_p}$ with $g(n) = f(n) + pn$ for all $n \in \mathbb{Z}_p$. Then, $\mathrm{suit}_{p,r}(g)$ by Lemma 5.3 (2) and also $g(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$. Let $\mathrm{id}_{\mathbb{Z}_p}$ denote the identity function on $\mathbb{Z}_p$ and $\mathrm{F} := (\mathrm{id}_{\mathbb{Z}_p})^r \cdot (g) \cdot (\mathrm{id}_{\mathbb{Z}_p})^{p-r-1}$. Then, $\mathrm{F} \in \overline{\mathcal{F}}_p$ by Theorem 4.1 (2) and thus there is a unique $n \in \mathbb{Z}_p$ such that $\mathrm{D(F)}[n] = (r)^\infty$ by Lemma 3.11. It follows that $n \in r + p\mathbb{Z}_p$ and $\mathrm{D(F)}[n] = \mathrm{D(F)}[\mathrm{F}(n)]$. Thus, $n = \mathrm{F}(n) = (g(n) - g(n)\%p)/p = g(n)/p$ by Lemma 3.9, i.e. $f(n) = g(n) - pn = 0$. If $m \in r + p\mathbb{Z}_p$ and $f(m) = 0$, then $\mathrm{F}(m) = g(m)/p = m$ and hence $\mathrm{D(F)}[m] = (r)^\infty$. Thus $m = n$, again by Lemma 3.9. □

An important application of Hensel's Lemma lies in proving that certain real or complex numbers that are defined by polynomial equations (such as $\sqrt{2}$ or i) have counterparts within $\mathbb{Z}_p$ for some $2 \leq p \in \mathbb{N}$. Examples are given below. Note that the polynomial function f always satisfies the conditions of Hensel's Lemma (respectively Theorem 5.2).

Example 5.5.

1) $p = 2$, $r = 1$, $f(x) = x^2 - x - 4 \ \rightarrow\ \pm\sqrt{17} \in \mathbb{Z}_2$
2) $p = 3$, $r \in \{1, 2\}$, $f(x) = x^2 + 2 \ \rightarrow\ \pm\sqrt{-2} \in \mathbb{Z}_3$
3) $p = 5$, $r \in \{2, 3\}$, $f(x) = x^2 + 1 \ \rightarrow\ \pm\mathrm{i} \in \mathbb{Z}_5$
4) $p = 7$, $r \in \{3, 4\}$, $f(x) = x^2 - 2 \ \rightarrow\ \pm\sqrt{2} \in \mathbb{Z}_7$
5) $p \in \mathbb{P}$, $r \in [\![1, p-1]\!]$, $f(x) = x^{p-1} - 1 \ \rightarrow\ \left|\left\{x \in \mathbb{Z}_p \mid x^{p-1} = 1\right\}\right| = p - 1$.

It is conceivable that the generalization of Hensel's Lemma given by Theorem 5.2 allows for similar deductions when applied to other classes of functions. Exploring such possibilities could be the subject of future research.

As we have seen above, (p, r)-suitable functions that map $r + p\mathbb{Z}_p$ to $p\mathbb{Z}_p$ have a unique root in $r + p\mathbb{Z}_p$. The following theorem examines the converse direction for polynomial functions.

Theorem 5.6. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, and $f \in \mathbb{Z}_p[x]$ such that $f(r)\%p = 0$. Then,* $\mathrm{suit}_{p,r}(f)$ *if and only if f has a unique root a in $r + p\mathbb{Z}_p$ and* $\gcd(p, g(r)\%p) = 1$, *where $g \in \mathbb{Z}_p[x]$ such that $f(x) = (x-a)g(x)$ for all $x \in \mathbb{Z}_p$.*

Proof. First we note that $\mathrm{suit}_{p,r}(f) \Leftrightarrow \gcd(p, f'(r)\%p) = 1$ by Theorem 4.8 (3).

Next we prove "$\Rightarrow$". f has a unique root a in $r + p\mathbb{Z}_p$ by Corollary 5.2. Let $g \in \mathbb{Z}_p[x]$ such that $f(x) = (x-a)g(x)$ for all $x \in \mathbb{Z}_p$. Then,

$$f'(x) = g(x) + (x-a)g'(x) \tag{5.15}$$

and hence

$$1 = \gcd(p, f'(r)\%p) = \gcd(p, (g(r) + (r-a)g'(r))\%p) = \gcd(p, g(r)\%p)\,. \tag{5.16}$$

To prove "$\Leftarrow$" we analogously compute

$$1 = \gcd(p, g(r)\%p) = \gcd(p, (g(r) + (r-a)g'(r))\%p) = \gcd(p, f'(r)\%p)\,. \tag{5.17}$$

□

Even if $p \in \mathbb{P}$, the condition $\gcd(p, g(r)\%p) = 1$ in the above theorem cannot be dropped which is shown by the following example.

Example 5.7. If $f(x) := (x-1)(x^2+1)$, then $\{x \in 1 + 2\mathbb{Z}_2 \mid f(x) = 0\} = \{1\}$ but $\neg\mathrm{suit}_{2,1}(f)$ (note that $g(x) = x^2 + 1$ here).

p-fibred rational functions and a further generalization of Hensel's Lemma. In the remaining part of this section we investigate another generalization of Hensel's Lemma which involves several (p,r)-suitable functions at once and allows for arbitrary compositions while keeping a unique root in a given residue class. Before we can formulate the results, we need to extend our framework by a new notion closely related to p-fibred functions which we formally defined in Section 2. Let $2 \leq p \in \mathbb{N}$. The elements of any set $\mathbf{S}(\mathrm{bnd}_{(\mathbb{Q}_p)^A}, \mathrm{len}_p)$ where $A \subseteq \mathbb{Q}_p$, are called *p-fibred rational functions*, i.e. a p-fibred rational function $\mathrm{R} = (\mathrm{R}[0], \ldots, \mathrm{R}[p-1])$ is a p-tuple of functions $\mathrm{R}[r] : A \to \mathbb{Q}_p$, $r \in \underline{p}$, on some fixed subset A of the p-adic numbers. The *set of all p-fibred rational functions* shall be denoted by $\mathcal{R}_p$. For any p-fibred rational function $\mathrm{R} \in \mathbf{S}(\mathrm{bnd}_{(\mathbb{Q}_p)^A}, \mathrm{len}_p)$ we set $\mathrm{dom}(\mathrm{R}) := A$, the *domain of* R. For any subset A of $\mathrm{dom}(\mathrm{R})$ we define $\mathrm{R}|_A := (\mathrm{R}[0]|_A, \ldots, \mathrm{R}[p-1]|_A)$, the *restriction of* R *to* A.
We define the following predicates on $\mathcal{R}_p$ ($\mathrm{R} \in \mathcal{R}_p$, A set):

(5.18)	$\mathrm{dom}_A(\mathrm{R}) \Leftrightarrow \mathrm{dom}(\mathrm{R}) = A$	R has *domain* A
(5.19)	$\mathrm{bnd}_A(\mathrm{R}) \Leftrightarrow \forall\, r \in \underline{p} : \mathrm{R}[r](\mathrm{dom}(\mathrm{R}))/p \subseteq A$	R is *A-bounded*
(5.20)	$\mathrm{closed}(\mathrm{R}) \Leftrightarrow \mathrm{bnd}_{\mathrm{dom}(\mathrm{R})}(\mathrm{R})$	R is *closed*
(5.21)	$\mathrm{integral}(\mathrm{R}) \Leftrightarrow \mathrm{dom}(\mathrm{R}) \subseteq \mathbb{Z}_p \wedge \mathrm{R}[r]((r + p\mathbb{Z}_p) \cap \mathrm{dom}(\mathrm{R})) \subseteq \mathbb{Z}_p$	R is *integral*

For any closed p-fibred rational function R and for any $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{fin})$ we define

$$\mathrm{R}_D : \mathrm{dom}(\mathrm{R}) \to \mathbb{Q}_p \qquad x \mapsto \begin{cases} x & \text{if } |D| = 0 \\ \frac{\mathrm{R}[D[|D|-1]]\left(\mathrm{R}_{D\lfloor |D|-1 \rfloor}(x)\right)}{p} & \text{if } |D| > 0 \end{cases} \tag{5.22}$$

and for any $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}})$ we call $\mathrm{S}_D(\mathrm{R}) := \left(\left(\mathrm{R}_{D[\underline{k}]}(n)\right)_{k \in \overline{|D|}}\right)_{n \in \mathrm{dom}(\mathrm{R})} \in \mathcal{S}(\mathrm{dom}_{\mathrm{dom}(\mathrm{R})}, \mathrm{len}_{|D|+1})$ the R-*sequence table with respect to* D. For $n \in \mathrm{dom}(\mathrm{R})$ the R-*sequence of* n *with respect to* D is given by the $\mathrm{S}_D(\mathrm{R})$-sequence of n.

We define the following additional predicates on $\mathcal{R}_p$ ($\mathrm{R} \in \mathcal{R}_p$, $A \subseteq \mathbb{Q}_p$, $D \subseteq \mathbb{N}_0 \cup \{-\infty\}$):

$$\begin{aligned}
(5.23)\ \mathrm{poly}_{A,D}(\mathrm{R}) &\Leftrightarrow \mathrm{dom}_{\mathbb{Q}_p}(\mathrm{R}) && \text{R is } A\text{-polynomial with degree in } D \text{ or, if } D = \{d\},\\
&\quad \forall\, r \in \underline{p} : \mathrm{R}[r](x) \in A[x] && \text{R is } A\text{-polynomial of degree } d\\
&\quad\ \ \deg(\mathrm{R}[r](x)) \in D &&\\
(5.24)\ \mathrm{poly}_A(\mathrm{R}) &\Leftrightarrow \mathrm{poly}_{A,\mathbb{N}_0\cup\{-\infty\}}(\mathrm{R}) && \text{R is } A\text{-polynomial}\\
(5.25)\ \mathrm{poly}(\mathrm{R}) &\Leftrightarrow \mathrm{poly}_{\mathbb{Q}_p,\mathbb{N}_0\cup\{-\infty\}}(\mathrm{R}) && \text{R is polynomial}\\
(5.26)\ \text{lin-poly}_A(\mathrm{R}) &\Leftrightarrow \mathrm{poly}_{A,\{-\infty,0,1\}}(\mathrm{R}) && \text{R is } A\text{-linear-polynomial}\\
(5.27)\ \text{lin-poly}(\mathrm{R}) &\Leftrightarrow \mathrm{poly}_{\mathbb{Q}_p,\{-\infty,0,1\}}(\mathrm{R}) && \text{R is linear-polynomial}
\end{aligned}$$

Furthermore, we establish a relation between $\mathcal{R}_p(\text{integral})$ and $\mathcal{F}_p$ by the bijection:

$$\begin{aligned}
(5.28)\qquad \mathrm{int} : \mathcal{R}_p(\text{integral}) &\to \mathcal{F}_p\\
\mathrm{R} &\mapsto (\mathrm{R}[0] : \mathrm{dom}(\mathrm{R}) \to \mathbb{Z}_p, \ldots, \mathrm{R}[p-1] : \mathrm{dom}(\mathrm{R}) \to \mathbb{Z}_p)
\end{aligned}$$

i.e. "int" changes the codomains of all $\mathrm{R}[r]$, $r \in \underline{p}$, from $\mathbb{Q}_p$ to $\mathbb{Z}_p$. Note that we cannot simply identify elements of $\mathcal{R}_p(\text{integral})$ and $\mathcal{F}_p$ by int since this would introduce ambiguities for the predicates "bnd_A" and "closed" which are defined differently for integral p-fibred rational functions and p-fibred functions and do not coincide in general.

The essential difference between p-fibred functions and p-fibred rational functions lies in the way they are considered to be functions on their respective domains (cf. Eqn. (2.23) and Eqn. (5.22)). While a p-fibred function F gets the information on which of the functions $\mathrm{F}[0], \ldots, \mathrm{F}[p-1]$ to apply to some $n \in \mathrm{dom}(\mathrm{F})$ from the residue class of n modulo p, a p-fibred rational function gets this information from the supplied "p-digit sequence" D. This difference also influences the definitions of the respective "bnd_A" and "closed" predicates. In both cases, the purpose of the "closed" predicate is to guarantee that application of a p-fibred function or p-fibred rational function in the sense of Eqn. (2.23) or Eqn. (5.22) respectively, yields elements of the domain again, rendering iterative application possible. Whenever a closed p-fibred rational function R "extends" a closed p-fibred function F in weak canonical form (which will be the main purpose of p-fibred rational functions), the different ways of applying them as functions coincide, however, if the supplied p-digit sequence D is the F-digit expansion of the argument n, as the following lemma shows.

Lemma 5.8. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{R} \in \mathcal{R}_p(\text{closed})$ *such that* $\text{integral}(\mathrm{R}|_{\mathbb{Z}_p \cap \mathrm{dom}(\mathrm{R})})$ *and such that* $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p \cap \mathrm{dom}(\mathrm{R})}) \in \mathcal{F}_p(\text{closed}, \text{w-canf})$. *Furthermore, let* $n \in \mathbb{Z}_p \cap \mathrm{dom}(\mathrm{R})$, $D := \mathrm{D}(\mathrm{F})[n]$, *and* $k \in \mathbb{N}_0$. *Then,*

$$\mathrm{F}^k(n) = \mathrm{R}_{D[\underline{k}]}(n). \tag{5.29}$$

In particular: $\mathrm{S}(\mathrm{F})[n] = \mathrm{S}_D(\mathrm{R})[n]$.

As an example consider the 2-fibred rational function $\mathrm{R} := (x, 3x+1) \in \mathcal{R}_2(\mathrm{dom}_{\mathbb{Q}_2}, \text{closed})$ and the corresponding 2-fibred function $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{Z}_2}, \text{closed}, \text{w-canf})$ (note that every p-tuple of polynomials in $\mathbb{Z}_p[x]$ may be regarded as an element of both $\mathcal{R}_p(\mathrm{dom}_{\mathbb{Q}_p}, \text{closed})$ and $\mathcal{F}_p(\mathrm{dom}_{\mathbb{Z}_p}, \text{closed})$, as the restriction to $\mathbb{Z}_p$ of every p-fibred rational function defined by polynomials in $\mathbb{Z}_p[x]$ is always integral). Then, $\mathrm{S}(\mathrm{F})[17] = (17, 26, 13, 20, 10, 5, 8, 4) \cdot (2, 1)^\infty$ and $D := \mathrm{D}(\mathrm{F})[17] = (1, 0, 1, 0, 0, 1, 0, 0) \cdot (0, 1)^\infty$. Furthermore, $\mathrm{F}^6(17) = 8 = \mathrm{R}_{D[\underline{6}]}(17)$ and $\mathrm{S}_D(\mathrm{R})[17] = (17, 26, 13, 20, 10, 5, 8, 4) \cdot (2, 1)^\infty$.

Proof of Lemma 5.8. We prove the statement by induction on k. If $k = 0$, then

$$\mathrm{F}^0(n) = n = \mathrm{R}_{()}(n) = \mathrm{R}_{D[\underline{0}]}(n). \tag{5.30}$$

Now we assume $\mathrm{F}^k(n) = \mathrm{R}_{D[\underline{k}]}(n)$ and compute

$$\mathrm{F}^{k+1}(n) = \mathrm{F}(\mathrm{F}^k(n)) = \frac{\mathrm{F}[\mathrm{F}^k(n)\%p](\mathrm{F}^k(n))}{p}\ (\Leftarrow \text{w-canf}(\mathrm{F})) \tag{5.31}$$

$$(\mathrm{F}^k(n) \in \mathbb{Z}_p)\ = \frac{\mathrm{R}[\mathrm{F}^k(n)\%p](\mathrm{F}^k(n))}{p} = \frac{\mathrm{R}[D[k]](\mathrm{R}_{D[\underline{k}]}(n))}{p} = \mathrm{R}_{D[\underline{k+1}]}(n). \tag{5.32}$$

□

The above lemma is basically "built into the DNA" of p-fibred rational functions: the way a p-fibred rational function is applied as a regular function is defined in the very way that would make the lemma true. However, under additional assumptions (namely that F has the block property and that for all $r \in \underline{p}$ the only elements of $\mathbb{Q}_p$ that are mapped into $p\mathbb{Z}_p$ by $\mathrm{R}[r]$ are those in $r + p\mathbb{Z}_p$), a much stronger version of the above lemma can be proven that is not built in by design. Before we state the new lemma, we reconsider the above example which happens to satisfy the additional assumptions: if $\mathrm{R} := (x, 3x+1) \in \mathcal{R}_2(\mathrm{dom}_{\mathbb{Q}_2}, \text{closed})$ and $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{Z}_2}, \text{w-canf})$ then $\mathrm{block}(\mathrm{F})$ and $\mathrm{R}[r](\mathbb{Q}_2 \setminus (r + 2\mathbb{Z}_2)) \cap 2\mathbb{Z}_2 = \emptyset$ for all $r \in \{0, 1\}$. Now, if n is any 2-adic integer, say $n := 17$, and $D := \mathrm{D}(\mathrm{F})[n][\underline{k}]$ is the initial part of length $k \in \mathbb{N}_0$ of the F-digit expansion of n, say $k = 6$ and hence $D = (1, 0, 1, 0, 0, 1)$, we know from the above lemma that $\mathrm{R}_D[n]$, the result of applying the functions $\frac{x}{2}$ and $\frac{3x+1}{2}$ iteratively to n in the order given by D, is equal to $\mathrm{F}^k(n)$, which is 8 in our case. In principle, the order given by D might not be the only one that would result in 17 being mapped to 8: could there be another $E \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \mathrm{fin})$ such that $\mathrm{R}_E[n]$ is also equal to $\mathrm{F}^k(n)$, i.e. $\mathrm{R}_E[17] = 8$? The answer, which is "no", is given by the following lemma, which basically states that if the mentioned additional assumptions hold, the only way a p-adic integer n can be mapped to another p-adic integer $\mathrm{R}_D(n)$ by R_D, is that $\mathrm{R}_D(n)$ is contained in the F-sequence of n, say the entry with index $k \in \mathbb{N}_0$, and D is equal to the initial part of length k of the F-digit expansion of n. Before we state the lemma, we define the following predicate on the set $(\mathbb{Q}_p)^A$ of all mappings from A to $\mathbb{Q}_p$, where $2 \leq p \in \mathbb{N}$ and $A \subseteq \mathbb{Q}_p$ ($f \in (\mathbb{Q}_p)^A$, $r \in \underline{p}$):

$$\mathrm{avoid}_{p,r}(f) \Leftrightarrow f((\mathbb{Q}_p \setminus (r + p\mathbb{Z}_p)) \cap A) \cap p\mathbb{Z}_p = \emptyset \qquad f \text{ is } (p,r)\textit{-avoiding} \tag{5.33}$$

Note that if $r + p\mathbb{Z}_p \subseteq A$, $f(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$, and $\mathrm{suit}_{p,r}(f)$ (e.g. if $f|_{\mathbb{Z}_p}$ is the entry with index r of a p-adic system in weak canonical form, cf. Theorem 4.1 (2)), then $f(r + p\mathbb{Z}_p) = p\mathbb{Z}_p$ by Lemma 4.5 (2). In this case the condition for f to be (p, r)-avoiding can also be written as $f((\mathbb{Q}_p \setminus (r + p\mathbb{Z}_p)) \cap A) \cap f(r + p\mathbb{Z}_p) = \emptyset$ or even as $f(\mathbb{Q}_p \setminus (r + p\mathbb{Z}_p)) \cap f(r + p\mathbb{Z}_p) = \emptyset$ if $A = \mathbb{Q}_p$. Additionally, we define the following predicate on $\mathcal{R}_p$ ($\mathrm{R} \in \mathcal{R}_p$):

$$\mathrm{avoid}(\mathrm{R}) \Leftrightarrow \forall\, r \in \underline{p} : \mathrm{avoid}_{p,r}(\mathrm{R}[r]) \qquad \mathrm{R} \text{ is } \textit{avoiding} \tag{5.34}$$

A p-fibred function is said to be *avoiding* if the correspondig p-fibred rational function is avoiding. Using the new predicates we now formulate the lemma.

Lemma 5.9. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{R} \in \mathcal{R}_p(\text{closed}, \mathrm{avoid}(\mathrm{R}))$ *with* $\mathbb{Z}_p \subseteq \mathrm{dom}(\mathrm{R})$ *such that* $\mathrm{integral}(\mathrm{R}|_{\mathbb{Z}_p})$, *and* $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \overline{\mathcal{F}}_p(\text{w-canf})$. *Furthermore, let* $n \in \mathbb{Z}_p$, $k \in \mathbb{N}_0$, *and* $D \in \mathbf{S}(\mathrm{bnd}_p, \mathrm{len}_k)$ *such that* $\mathrm{R}_D(n) \in \mathbb{Z}_p$. *Then,* $\mathrm{S}(\mathrm{F})[n][\overline{k}] = \mathrm{S}_D(\mathrm{R})[n]$ *and* $\mathrm{D}(\mathrm{F})[n][\underline{k}] = D$. *In particular.* $\mathrm{F}^k(n) = \mathrm{R}_D(n)$.

Proof. Let m be the unique element of $\mathbb{Z}_p$ such that $\mathrm{D}(\mathrm{F})[m] = D \cdot \mathrm{D}(\mathrm{F})[\mathrm{R}_D(n)]$ (cf. Lemma 3.11). Then,

$$\mathrm{D}(\mathrm{F})[\mathrm{F}^k(m)] = \mathrm{D}(\mathrm{F})[m][k, \infty] = \mathrm{D}(\mathrm{F})[\mathrm{R}_D(n)] \tag{5.35}$$

and hence

$$\mathrm{F}^k(m) = \mathrm{R}_D(n) \tag{5.36}$$

by Lemma 3.9. Also,

$$\mathrm{D}(\mathrm{F})[m][\underline{k}] = D. \tag{5.37}$$

We claim that $\mathrm{S}(\mathrm{F})[m][k - \ell] = \mathrm{S}_D(\mathrm{R})[n][k - \ell]$ for all $\ell \in \overline{k}$ (which in particular implies that $m = n$) and proceed by induction on ℓ. If $\ell = 0$, then

$$\mathrm{S}(\mathrm{F})[m][k - \ell] = \mathrm{S}(\mathrm{F})[m][k] = \mathrm{F}^k(m) = \mathrm{R}_D(n) = \mathrm{S}_D(\mathrm{R})[n][k] = \mathrm{S}_D(\mathrm{R})[n][k - \ell]. \tag{5.38}$$

Now assume that $\mathrm{S(F)}[m][k-\ell] = \mathrm{S}_D(\mathrm{R})[n][k-\ell]$ for some $\ell \in \underline{k}$. Then,

$$\mathrm{R}[D[k-(\ell+1)]](\mathrm{S}_D(\mathrm{R})[n][k-(\ell+1)]) = \mathrm{R}[D[k-(\ell+1)]](\mathrm{R}_{D[\underline{k-(\ell+1)}]}(n)) \tag{5.39}$$

$$= p\mathrm{R}_{D[\underline{k-\ell}]}(n) \tag{5.40}$$

$$= p\mathrm{S}_D(\mathrm{R})[n][k-\ell] \tag{5.41}$$

$$= p\mathrm{S(F)}[m][k-\ell] \in p\mathbb{Z}_p. \tag{5.42}$$

Thus, it follows from $\mathrm{R}[D[k-(\ell+1)]](\mathbb{Q}_p \setminus (D[k-(\ell+1)] + p\mathbb{Z}_p)) \cap p\mathbb{Z}_p = \emptyset$ that

$$\mathrm{S}_D(\mathrm{R})[n][k-(\ell+1)] \in D[k-(\ell+1)] + p\mathbb{Z}_p. \tag{5.43}$$

In addition,

$$\mathrm{S(F)}[m][k-(\ell+1)]\%p = \mathrm{D(F)}[m][k-(\ell+1)] = \mathrm{D(F)}[m][\underline{k}][k-(\ell+1)] = D[k-(\ell+1)] \tag{5.44}$$

and hence

$$\mathrm{S(F)}[m][k-(\ell+1)] \in D[k-(\ell+1)] + p\mathbb{Z}_p. \tag{5.45}$$

But then,

$$\mathrm{F}[D[k-(\ell+1)]](\mathrm{S}_D(\mathrm{R})[n][k-(\ell+1)]) = \mathrm{R}[D[k-(\ell+1)]](\mathrm{S}_D(\mathrm{R})[n][k-(\ell+1)]) \tag{5.46}$$

$$= p\mathrm{S(F)}[m][k-\ell] \tag{5.47}$$

$$= p\mathrm{F}^{k-\ell}(m) \tag{5.48}$$

$$= p\mathrm{F}(\mathrm{F}^{k-(\ell+1)}(m)) \tag{5.49}$$

$$= p\mathrm{F}(\mathrm{S(F)}[m][k-(\ell+1)]) \tag{5.50}$$

$$= \mathrm{F}[D[k-(\ell+1)]](\mathrm{S(F)}[m][k-(\ell+1)]) \tag{5.51}$$

and hence Theorem 4.1 (2) and Lemma 4.5 (1) imply that

$$\mathrm{S(F)}[m][k-(\ell+1)] = \mathrm{S}_D(\mathrm{R})[n][k-(\ell+1)]. \tag{5.52}$$

□

One could assume that if the entries of R are polynomials, the assumptions of the lemma (i.e. that R is avoiding) could be loosened. The following examples show that this is not the case.

Example 5.10.

- Let $\mathrm{R} := (2x^2-5x+2, x+3) \in \mathcal{R}_2(\mathrm{dom}_{\mathbb{Q}_2}, \mathrm{closed})$ and $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{Z}_2}, \text{w-canf}, \mathrm{block})$. Then, $\mathrm{S}_{(1,0)}(\mathrm{R})[-2] = (-2, \frac{1}{2}, 0)$, but $\mathrm{S(F)}[-2][\overline{2}] = (-2, 10, 76)$ and $\mathrm{D(F)}[-2][\underline{2}] = (0,0)$ (note: $\mathrm{S(F)}[1][\overline{2}] = (1,2,0)$ and $\mathrm{D(F)}[1][\underline{2}] = (1,0)$).
- Let $\mathrm{R} := (x^2+x, x^2-x) \in \mathcal{R}_2(\mathrm{dom}_{\mathbb{Q}_2}, \mathrm{closed})$ and $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \mathcal{F}_2(\mathrm{dom}_{\mathbb{Z}_2}, \text{w-canf}, \mathrm{block})$. Then, $\mathrm{S}_{(0,1)}(\mathrm{R})[1] = (1,1,0)$, but $\mathrm{S(F)}[1][\overline{2}] = (1,0,0)$ and $\mathrm{D(F)}[1][\underline{2}] = (1,0)$. Therefore, even for polynomials the condition $\mathrm{R}[r](\mathbb{Q}_p \setminus (r + p\mathbb{Z}_p)) \cap p\mathbb{Z}_p = \emptyset$ in Lemma 5.9 is necessary and cannot even be reduced to $\mathrm{R}[r](\mathbb{Q}_p \setminus \mathbb{Z}_p) \cap p\mathbb{Z}_p = \emptyset$.

Using the above lemma we are able to prove the promised generalization of Theorem 5.2 which is a further generalization of Hensel's Lemma.

Theorem 5.11. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{R} \in \mathcal{R}_p(\mathrm{closed}, \mathrm{avoid}(\mathrm{R}))$ *with* $\mathbb{Z}_p \subseteq \mathrm{dom}(\mathrm{R})$ *such that* $\mathrm{integral}(\mathrm{R}|_{\mathbb{Z}_p})$, *and* $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) \in \overline{\mathcal{F}}_p(\text{w-canf})$. *Furthermore, let* $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_{\mathbb{N}})$. *Then,* R_D *has a unique fixed point in* $\mathbb{Z}_p$.

A comparison of the assumptions of Theorem 5.2 and Theorem 5.11 shows that the latter is not a pure generalization of the first, as the p-fibred rational function R in Theorem 5.11 is required to be avoiding, whereas the function f in Theorem 5.2 is not required to be (p,r)-avoiding. However, if this is the case, the unique root of Theorem 5.2 corresponds to the unique fixed point in Theorem 5.11 if $|D| = 1$ (cf. Lemma 5.3). What Theorem 5.11 generalizes is thus the length of D.

Proof of Theorem 5.11. Let $k := |D|$ and n be the unique element of $\mathbb{Z}_p$ such that $\mathrm{D(F)}[n] = D^\infty$ (cf. Lemma 3.11). Then, $\mathrm{R}_D(n) = \mathrm{F}^k(n)$ by Lemma 5.8. In addition,

$$\mathrm{D(F)}[\mathrm{F}^k(n)] = \mathrm{D(F)}[n][k,\infty] = D^\infty[k,\infty] = D^\infty = \mathrm{D(F)}[n] \tag{5.53}$$

and hence $\mathrm{F}^k(n) = n$ by Lemma 3.9. Therefore, n is a fixed point of R_D.

If $m \in \mathbb{Z}_p$ is a fixed point of R_D, then $\mathrm{R}_D(m) = m \in \mathbb{Z}_p$ and Lemma 5.9 implies that $\mathrm{S(F)}[m][\overline{k}] = \mathrm{S}_D\mathrm{(R)}[m]$ and $\mathrm{D(F)}[m][\underline{k}] = D$. In particular, $\mathrm{F}^k(m) = \mathrm{R}_D(m) = m$ and therefore $\mathrm{D(F)}[m] = D^\infty$. But then Lemma 3.9 implies that $m = n$. □

Just as Theorem 4.8 characterizes polynomials in $\mathbb{Z}_p[x]$ that are (p,r)-suitable (i.e. suitable to be the building blocks of p-adic systems), we will now try to characterize polynomials that are (p,r)-avoiding (i.e. suitable to be the building blocks of avoiding p-fibred rational functions). For this purpose we need an analogue of the p-adic valuation ν_p for the case where p is not a prime. These and other technicalities of p-adic numbers are discussed in the appendix. Using the definitions and facts presented there, we are able to characterize (p,r)-avoiding polynomials.

Theorem 5.12. *Let $2 \leq p \in \mathbb{N}$, $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}_p[x]$ (note that for the whole theorem we define $0^0 := 1$ and assume $d = 0$, $a_0 = 0$ if $f = 0$), and $r \in \underline{p}$. Furthermore, let $s \in \mathbb{N}$, $q_1, \ldots, q_s \in \mathbb{P}$ the distinct prime factors of p, and for all $q \in \{q_1, \ldots, q_s\}$ let $t_q \in \overline{d+1}$ and $i_{q,1}, \ldots, i_{q,t_q} \in \overline{d}$ be the longest possible strictly increasing sequence of indices satisfying $\nu_q(a_{i_{q,j}}) \neq \infty$ for all $j \in [\![1, t_q]\!]$. We set*

(5.54)

$$K := \max\left(\left\{\frac{\nu_q(a_{i_{q,j+1}}) - \nu_q(a_{i_{q,j}}) + i_{q,j+1}(\nu_q(p)-1)}{(i_{q,j+1} - i_{q,j})\nu_q(p)} \;\middle|\; q \in \{q_1,\ldots,q_s\} \wedge j \in [\![1, t_q - 1]\!]\right\} \cup \right.$$
$$\left.\left\{\frac{\nu_q(a_{i_{q,t_q}}) - \nu_q(p) + i_{q,t_q}(\nu_q(p)-1)}{i_{q,t_q}\nu_q(p)} \;\middle|\; q \in \{q_1,\ldots,q_s\} \wedge t_q \geq 1 \wedge i_{q,t_q} \geq 1\right\} \cup \{1\}\right).$$

Then,

$$W := (\underline{p} \setminus \{r\}) \cup \left\{a/p^k \mid k \in [\![1, K]\!] \wedge a \in \underline{p^{dk+1}}\right\} \tag{5.55}$$

is a finite witness set for f being (p,r)-avoiding, i.e. $\mathrm{avoid}_{p,r}(f)$ *if and only if $f(W) \cap p\mathbb{Z}_p = \emptyset$.*

Proof. We need to show

$$\exists\, n \in \mathbb{Q}_p \setminus (r + p\mathbb{Z}_p) : f(n) \in p\mathbb{Z}_p \quad \Rightarrow \quad \exists\, w \in W : f(w) \in p\mathbb{Z}_p. \tag{5.56}$$

Clearly, if $f(n) \in p\mathbb{Z}_p$ for some $n \in \mathbb{Z}_p \setminus (r + p\mathbb{Z}_p)$, then $w = n\%p \in W$ and $f(w) \in p\mathbb{Z}_p$. We are thus left to show that

$$\exists\, n \in \mathbb{Q}_p \setminus \mathbb{Z}_p : f(n) \in p\mathbb{Z}_p \quad \Rightarrow \quad \exists\, w \in W : f(w) \in p\mathbb{Z}_p. \tag{5.57}$$

For that let $n \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, $\ell := -\nu_p(n) \in \mathbb{N}$, and $m := np^\ell \in \mathbb{Z}_p$ and assume that $f(n) \in p\mathbb{Z}_p$. Then,

$$f(n) = f(m/p^\ell) = \sum_{i=0}^{d} a_i \left(m/p^\ell\right)^i = \sum_{i=0}^{d} a_i m^i / p^{i\ell} = 1/p^{d\ell} \sum_{i=0}^{d} a_i m^i p^{(d-i)\ell} \tag{5.58}$$

and thus

$$f(n)p^{d\ell} = \sum_{i=0}^{d} a_i m^i p^{(d-i)\ell} \in p^{d\ell+1}\mathbb{Z}_p. \tag{5.59}$$

We may thus reformulate our goal as

$$\exists\, v \in \mathbb{Q}_p \setminus \mathbb{Z}_p : -\nu_p(v) \leq K \wedge f(v) \in p\mathbb{Z}_p, \tag{5.60}$$

because for any such v it follows analogously that

$$f(v)p^{dk} = \sum_{i=0}^{d} a_i u^i p^{(d-i)k} \in p^{dk+1}\mathbb{Z}_p, \tag{5.61}$$

where $k := -\nu_p(v)$ and $u := vp^k$, and $w := (u\%p^{dk+1})/p^k \in W$ thus satisfies $f(w) \in p\mathbb{Z}_p$. To prove this new goal we distinguish three cases:

Case 1: $\exists\, q \in \{q_1, \dots, q_s\} : t_q = 0$.
Let $v := \varphi_p^{-1}((0, \dots, 0, 1/p, 0, \dots, 0)) \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ where the "$1/p$" is at the j-th position if $q = q_j$. Then $k = 1 \leq K$ and $f(v) = 0 \in p\mathbb{Z}_p$.

Case 2: $\forall\, q \in \{q_1, \dots, q_s\} : t_q \geq 1$
$\forall\, q \in \{q_1, \dots, q_s\} : \nu_q(m) \neq \infty \Rightarrow i_{q,t_q} = 0$.
In this case as a result we get

$$\nu_q\left(a_i m^i p^{(d-i)\ell}\right) = \nu_q(a_i) + i\nu_q(m) + (d-i)\ell\nu_q(p) = \infty \tag{5.62}$$

for all $q \in \{q_1, \dots, q_s\}$ and $i \in [\![1, d]\!]$, and hence $f(mp^c) = a_0 \in p\mathbb{Z}_p$ for all $c \in \mathbb{Z}$. Setting $v := m/p$ thus implies $k = 1 \leq K$ and $f(v) \in p\mathbb{Z}_p$.

Case 3: $\forall\, q \in \{q_1, \dots, q_s\} : t_q \geq 1$
$\exists\, q \in \{q_1, \dots, q_s\} : \nu_q(m) \neq \infty \wedge i_{q,t_q} \geq 1$.
We may assume without loss of generality that there is no $a \in \mathbb{Z}_p \setminus (r + p\mathbb{Z}_p)$ such that $f(a) \in p\mathbb{Z}_p$, because we already treated this case at the beginning of the proof. But then it follows that

$$\exists\, q \in \{q_1, \dots, q_s\} : \nu_q(m) < \ell\nu_q(p) \wedge i_{q,t_q} \geq 1, \tag{5.63}$$

because otherwise we could find an $a \in \mathbb{Z}_p \setminus (r + p\mathbb{Z}_p)$ with $f(a) \in p\mathbb{Z}_p$ in the following way: set $b := \varphi_p^{-1}((b_1, \dots, b_s))$ and $c := \varphi_p^{-1}((1 - b_1, \dots, 1 - b_s))$ with $b_j = (i_{q_j,t_{q_j}} = 0\ ?\ 0, 1)$ for all $j \in [\![1, s]\!]$. Then $c \neq 0$ (otherwise $\nu_q(m) \geq \ell\nu_q(p) \geq \nu_q(p)$ for all q in $\{q_1, \dots, q_s\}$, hence $m \in p\mathbb{Z}_p$ which is a contradiction), bn and $bn + c$ are in $\mathbb{Z}_p$; they are not congruent modulo p, and both satisfy $f(bn) = f(bn + c) = f(n) \in p\mathbb{Z}_p$. Thus $a = bn$ or $a = bn + c$ contradicts our assumption that no such a exists.

Now let $v := bn \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, $k := -\nu_p(v)$, and $u := vp^k$. Then $f(v) = f(n) \in p\mathbb{Z}_p$ and we claim that $k \leq K$ which would complete the proof. Assume to the contrary that $k > K$ and let $q \in \{q_1, \dots, q_s\}$ such that $\nu_q(u) \in \underline{\nu_q(p)}$ (such a q exists because $\nu_p(u) = 0$). Then $i_{q,t_q} \geq 1$ (otherwise $\nu_q(u) = \infty$ by $u = bnp^k$ and by the definition of b) and

$$\nu_q\left(a_i u^i p^{(d-i)k}\right) = \nu_q(a_i) + i\nu_q(k) + (d-i)k\nu_q(p) \tag{5.64}$$

$$\in \nu_q(a_i) + (d-i)k\nu_q(p) + i\underline{\nu_q(p)} \tag{5.65}$$

for all $i \in \overline{d}$. By assumption we have

$$\frac{\nu_q(a_{i_{q,j+1}}) - \nu_q(a_{i_{q,j}}) + i_{q,j+1}(\nu_q(p) - 1)}{(i_{q,j+1} - i_{q,j})\nu_q(p)} \leq K < k \tag{5.66}$$

or equivalently

$$\nu_q(a_{i_{q,j+1}}) + (d - i_{q,j+1})k\nu_q(p) + i_{q,j+1}(\nu_q(p) - 1) < \nu_q(a_{i_{q,j}}) + (d - i_{q,j})k\nu_q(p) \tag{5.67}$$

for all $j \in [\![1, t_q - 1]\!]$ and hence

$$\nu_q\left(a_{i_{q,j_1}} u^{i_{q,j_1}} p^{(d-i_{q,j_1})k}\right) \neq \nu_q\left(a_{i_{q,j_2}} u^{i_{q,j_2}} p^{(d-i_{q,j_2})k}\right) \tag{5.68}$$

for all distinct $j_1, j_2 \in [\![1, t_q]\!]$. Furthermore, we have, again by assumption and by $t_q \geq 1$ and $i_{q,t_q} \geq 1$,

$$\frac{\nu_q(a_{i_{q,t_q}}) - \nu_q(p) + i_{q,t_q}(\nu_q(p) - 1)}{i_{q,t_q}\nu_q(p)} \leq K < k \tag{5.69}$$

or equivalently

$$\nu_q(a_{i_{q,t_q}}) + (d - i_{q,t_q})k\nu_q(p) + i_{q,t_q}(\nu_q(p) - 1) < (dk + 1)\nu_q(p). \tag{5.70}$$

Thus we get

$$\nu_q\left(f(v)p^{dk}\right) = \inf\left\{\nu_q\left(a_{i_{q,j}}u^{i_{q,j}}p^{(d-i_{q,j})k}\right) \;\middle|\; j \in [\![1,t_q]\!]\right\} \tag{5.71}$$

$$= \nu_q\left(a_{i_{q,t_q}}u^{i_{q,t_q}}p^{(d-i_{q,t_q})k}\right) \tag{5.72}$$

$$\leq \nu_q(a_{i_{q,t_q}}) + (d-i_{q,t_q})k\nu_q(p) + i_{q,t_q}(\nu_q(p)-1) \tag{5.73}$$

$$< (dk+1)\nu_q(p) \tag{5.74}$$

which contradicts $f(v)p^{dk} \in p^{dk+1}\mathbb{Z}_p$. □

As an example consider the following polynomials: $f_0(x) := 7x^3-4x^2+x-6$, $f_1(x) := 3x^7-x+1$, $f_2(x) := 5x^4+4x-1$. By Theorem 5.12 all of the f_r are $(3,r)$-avoiding, and by Theorem 4.8 they are $(3,r)$-suitable. Thus $\mathrm{R} := (f_0,f_1,f_2) \in \mathcal{R}_3$ is avoiding by definition and $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p}) = (f_0,f_1,f_2) \in \mathcal{F}_3$ has the block property by Theorem 4.1 (2). In addition, R is clearly closed and F is in weak canonical form. Thus the conditions of Theorem 5.11 are met and R_D has a unique fixed point in $\mathbb{Z}_p$ for every $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_{\mathbb{N}})$. Stripping off the machinery of p-fibred functions this implies that for every polynomial of the form $g_{r_1}\circ\ldots\circ g_{r_\ell}$, where $g_r := f_r/3$ for every $r \in \{0,1,2\}$, $\ell \in \mathbb{N}$, and $r_1,\ldots,r_\ell \in \{0,1,2\}$, there is a unique $n \in \mathbb{Z}_p$ satisfying $g_{r_1}\circ\ldots\circ g_{r_\ell}(n) = n$.

6. Periodic and ultimately periodic digit expansions

One problem about p-adic systems we are particularly interested in concerns the characterization of the sets of all p-adic integers which have periodic or ultimately periodic digit expansions with respect to a given p-adic system. It is a natural generalization of the very specific question asked in the Collatz conjecture which claims that all natural numbers have periodic digit expansions with period $(1,0)$. If one could characterize the set of all 2-adic integers having ultimately periodic F_C-digit expansions, one would probably find what numerous experiments suggest, namely that it is exactly the set $\mathbb{Q}\cap\mathbb{Z}_2$ of rational numbers with odd denominators. By Corollary 3.10 this would automatically prove that orbits of natural numbers under F_C cannot diverge, which would be a significant step in proving the Collatz conjecture.

For $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p$, and $n \in \mathbb{Z}_p$ we say that n is a *periodic*, *ultimately periodic*, or *aperiodic point* of F if $\mathrm{D}(\mathrm{F})[n]$ is periodic, ultimately periodic, or aperiodic, respectively. Note that by Corollary 3.10 we could replace $\mathrm{D}(\mathrm{F})[n]$ by $\mathrm{S}(\mathrm{F})[n]$ to get equivalent definitions. We define the sets

$$\mathrm{PerP}(\mathrm{F}) := \{n \in \mathbb{Z}_p \mid \mathrm{per}(\mathrm{D}(\mathrm{F})[n])\} \tag{6.1}$$

$$\mathrm{UPerP}(\mathrm{F}) := \{n \in \mathbb{Z}_p \mid \mathrm{uper}(\mathrm{D}(\mathrm{F})[n])\} \tag{6.2}$$

$$\mathrm{APerP}(\mathrm{F}) := \{n \in \mathbb{Z}_p \mid \mathrm{aper}(\mathrm{D}(\mathrm{F})[n])\} \tag{6.3}$$

of periodic, ultimately periodic, and aperiodic points of F. Furthermore, for every logical expression E in the three unknown sets PerP, UPerP, and APerP we define the following predicate on $\overline{\mathcal{F}}_p$ $(2 \leq p \in \mathbb{N}, \mathrm{F} \in \overline{\mathcal{F}}_p)$:

$$[E](\mathrm{F}) \Leftrightarrow E[\mathrm{PerP} \to \mathrm{PerP}(\mathrm{F}), \mathrm{UPerP} \to \mathrm{UPerP}(\mathrm{F}), \mathrm{APerP} \to \mathrm{APerP}(\mathrm{F})] \qquad \mathrm{F}\ \textit{satisfies}\ E \tag{6.4}$$

where $E[\mathrm{PerP} \to \mathrm{PerP}(\mathrm{F}), \mathrm{UPerP} \to \mathrm{UPerP}(\mathrm{F}), \mathrm{APerP} \to \mathrm{APerP}(\mathrm{F})]$ is the logical expression obtained by substituting PerP with $\mathrm{PerP}(\mathrm{F})$, UPerP with $\mathrm{UPerP}(\mathrm{F})$, and APerP with $\mathrm{APerP}(\mathrm{F})$ in E, e.g. $[\mathrm{UPerP} = \mathbb{Q}\cap\mathbb{Z}_2](\mathrm{F}_C) \Leftrightarrow \mathrm{UPerP}(\mathrm{F}_C) = \mathbb{Q}\cap\mathbb{Z}_2$.
Additionally, we define the following predicates on $\overline{\mathcal{F}}_p$ $(2 \leq p \in \mathbb{N}, \mathrm{F} \in \overline{\mathcal{F}}_p, A$ set):

$$\text{per-on}_A(\mathrm{F}) \Leftrightarrow [\mathrm{PerP} = A](\mathrm{F}) \qquad \mathrm{F}\ \textit{is periodic on}\ A \tag{6.5}$$

$$\text{uper-on}_A(\mathrm{F}) \Leftrightarrow [\mathrm{UPerP} = A](\mathrm{F}) \qquad \mathrm{F}\ \textit{is ultimately periodic on}\ A \tag{6.6}$$

$$\text{aper-on}_A(\mathrm{F}) \Leftrightarrow [\mathrm{APerP} = A](\mathrm{F}) \qquad \mathrm{F}\ \textit{is aperiodic on}\ A \tag{6.7}$$

Using $\pi_{\mathrm{F},\mathrm{G}}$ we can characterize when two p-adic systems F and G are periodic, ultimately periodic, or aperiodic on the same sets.

Lemma 6.1. *Let* $2 \le p \in \mathbb{N}$, $\mathrm{F}, \mathrm{G} \in \overline{\mathcal{F}}_p$, $B \subseteq \mathbf{S}(\mathrm{bnd}_p, \neg\mathrm{fin})$, $A_\mathrm{F} := \{n \in \mathbb{Z}_p \mid \mathrm{D}(\mathrm{F})[n] \in B\}$, *and* $A_\mathrm{G} := \{n \in \mathbb{Z}_p \mid \mathrm{D}(\mathrm{G})[n] \in B\}$. *Then,*

$$A_\mathrm{F} = A_\mathrm{G} \Leftrightarrow \pi_{\mathrm{F},\mathrm{G}}(A_\mathrm{F}) = A_\mathrm{F}. \tag{6.8}$$

In particular,

(1) $\mathrm{PerP}(\mathrm{F}) = \mathrm{PerP}(\mathrm{G}) \Leftrightarrow \pi_{\mathrm{F},\mathrm{G}}(\mathrm{PerP}(\mathrm{F})) = \mathrm{PerP}(\mathrm{F})$
(2) $\mathrm{UPerP}(\mathrm{F}) = \mathrm{UPerP}(\mathrm{G}) \Leftrightarrow \pi_{\mathrm{F},\mathrm{G}}(\mathrm{UPerP}(\mathrm{F})) = \mathrm{UPerP}(\mathrm{F})$
(3) $\mathrm{APerP}(\mathrm{F}) = \mathrm{APerP}(\mathrm{G}) \Leftrightarrow \pi_{\mathrm{F},\mathrm{G}}(\mathrm{APerP}(\mathrm{F})) = \mathrm{APerP}(\mathrm{F})$.

Proof. First we observe that $A_\mathrm{F} = \psi_\mathrm{F}^{-1}(B)$ and $A_\mathrm{G} = \psi_\mathrm{G}^{-1}(B)$ by definition of ψ_F and ψ_G. Since ψ_F and ψ_G are bijective it follows that

$$A_\mathrm{F} = A_\mathrm{G} \Leftrightarrow \psi_\mathrm{G}(A_\mathrm{F}) = \psi_\mathrm{G}(A_\mathrm{G}) = \psi_\mathrm{G}(\psi_\mathrm{G}^{-1}(B)) = B = \psi_\mathrm{F}(\psi_\mathrm{F}^{-1}(B)) = \psi_\mathrm{F}(A_\mathrm{F}) \tag{6.9}$$

$$\Leftrightarrow A_\mathrm{F} = \psi_\mathrm{G}^{-1}(\psi_\mathrm{G}(A_\mathrm{F})) = \psi_\mathrm{G}^{-1}(\psi_\mathrm{F}(A_\mathrm{F})) = \pi_{\mathrm{F},\mathrm{G}}(A_\mathrm{F}). \tag{6.10}$$

The "In particular" part follows directly if one sets $B := \big\{S \in \mathbf{S}(\mathrm{bnd}_p, \neg\mathrm{fin}) \mid \mathrm{per}(S)\big\}$, $B := \big\{S \in \mathbf{S}(\mathrm{bnd}_p, \neg\mathrm{fin}) \mid \mathrm{uper}(S)\big\}$, or $B := \big\{S \in \mathbf{S}(\mathrm{bnd}_p, \neg\mathrm{fin}) \mid \mathrm{aper}(S)\big\}$ respectively. □

In the upcoming section we will prove direct formulas for $\pi_{\mathrm{F},\mathrm{G}}(n)$, $n \in \mathbb{Z}_p$ for several combinations of p-adic systems F and G. For example, Theorem 7.14 implies that $\pi_{(x,3x+1),(x,3x+c)}(n) = cn$ for all odd integers c. Since the mapping $n \mapsto cn$ maps $\mathbb{Q} \cap \mathbb{Z}_2$ to itself, it follows from the "In particular" part of Lemma 6.1 that $(x, 3x+1)$ is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$ if and only if $(x, 3x+c)$ is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$. It thus suffices to prove that $(x, 3x+c)$ is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$ for any c to automatically prove it for all c. Furthermore, if a 2-adic system G could be found which can be proven to be ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$ and for which $\pi_{(x,3x+1),\mathrm{G}}(n)$ can be directly computed by a formula, such that $\pi_{(x,3x+1),\mathrm{G}}(\mathbb{Q} \cap \mathbb{Z}_2) = \mathbb{Q} \cap \mathbb{Z}_2$ can be demonstrated, it would again follow from the "In particular" part of Lemma 6.1 that $(x, 3x+1)$ is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$. Unfortunately, such a G could not be found so far, but further investigations in this direction are made in the upcoming section.

Contractive and expansive p-adic systems. In the special cases where a p-adic system F is either *contractive* or *expansive* we can easily characterize $\mathrm{PerP}(\mathrm{F}) \cap \mathbb{Q}$ and $\mathrm{UPerP}(\mathrm{F}) \cap \mathbb{Q}$ respectively.
We define the following predicates on $\overline{\mathcal{F}}_p$ ($2 \le p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p$):

$$\mathrm{contr}(\mathrm{F}) \Leftrightarrow \mathrm{F}(\mathbb{Q} \cap \mathbb{Z}_p) \subseteq \mathbb{Q} \cap \mathbb{Z}_p \qquad \text{F is } \textit{contractive} \tag{6.11}$$
$$\exists\, 0 \le M \in \mathbb{R} : \forall\, n \in \mathbb{Q} \cap \mathbb{Z}_p : |n| > M \Rightarrow |\mathrm{F}(n)| < |n|$$

$$\mathrm{exp}(\mathrm{F}) \Leftrightarrow \mathrm{F}(\mathbb{Q} \cap \mathbb{Z}_p) \subseteq \mathbb{Q} \cap \mathbb{Z}_p \qquad \text{F is } \textit{expansive} \tag{6.12}$$
$$\exists\, 0 \le M \in \mathbb{R} : \forall\, n \in \mathbb{Q} \cap \mathbb{Z}_p : |n| > M \Rightarrow |\mathrm{F}(n)| > |n|$$

$$\mathrm{mix}(\mathrm{F}) \Leftrightarrow \mathrm{F}(\mathbb{Q} \cap \mathbb{Z}_p) \subseteq \mathbb{Q} \cap \mathbb{Z}_p \qquad \text{F is } \textit{of mixed type} \tag{6.13}$$
$$\neg\mathrm{contr}(\mathrm{F}) \wedge \neg\mathrm{exp}(\mathrm{F})$$

$$\text{d-contr}(\mathrm{F}) \Leftrightarrow \forall\, a/b \in \mathbb{Q} \cap \mathbb{Z}_p \text{ with } (a,b) \in \mathbb{Z} \times \mathbb{N} \text{ coprime} : \qquad \mathrm{F} \textit{ contracts denominators} \tag{6.14}$$
$$\exists\, (c,d) \in \mathbb{Z} \times \mathbb{N} \text{ coprime} : \mathrm{F}(a/b) = c/d \wedge d \le b$$

$$\text{d-exp}(\mathrm{F}) \Leftrightarrow \forall\, a/b \in \mathbb{Q} \cap \mathbb{Z}_p \text{ with } (a,b) \in \mathbb{Z} \times \mathbb{N} \text{ coprime} : \qquad \mathrm{F} \textit{ expands denominators} \tag{6.15}$$
$$\exists\, (c,d) \in \mathbb{Z} \times \mathbb{N} \text{ coprime} : \mathrm{F}(a/b) = c/d \wedge d > b$$

$$\text{d-mix}(\mathrm{F}) \Leftrightarrow \mathrm{F}(\mathbb{Q} \cap \mathbb{Z}_p) \subseteq \mathbb{Q} \cap \mathbb{Z}_p \qquad \mathrm{F} \textit{ mixes denominators} \tag{6.16}$$
$$\neg\text{d-contr}(\mathrm{F}) \wedge \neg\text{d-exp}(\mathrm{F})$$

Note that d-contr(F) and d-exp(F) both imply $\mathrm{F}(\mathbb{Q} \cap \mathbb{Z}_p) \subseteq \mathbb{Q} \cap \mathbb{Z}_p$.

If a p-fibred function is contractive or expansive, this has the following consequences for periodic and ultimately periodic digit expansions.

Lemma 6.2. *Let* $2 \le p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p$, $0 \le M \in \mathbb{R}$ *as in the definition above, and* $A := \{n \in \mathbb{Q} \cap \mathbb{Z}_p \mid |n| \le M\}$. *Then,*

(1) contr(F) $\Rightarrow$ $\mathrm{PerP}(\mathrm{F}) \cap \mathbb{Q} \subseteq \bigcup_{k=0}^{\infty} \mathrm{F}^k(A)$
In particular: Every period of F *that contains a rational number also contains an element of* A

(2) contr(F) $\wedge$ d-contr(F) $\Rightarrow$ $\mathrm{UPerP}(\mathrm{F}) \cap \mathbb{Q} = \mathbb{Q} \cap \mathbb{Z}_p$
In particular: $\mathrm{UPerP}(\mathrm{F}) \subseteq \mathbb{Q} \Rightarrow \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$

(3) exp(F) $\Rightarrow$ $\mathrm{UPerP}(\mathrm{F}) \cap \mathbb{Q} \subseteq A$
In particular: $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$

(4) d-exp(F) $\Rightarrow$ $\mathrm{UPerP}(\mathrm{F}) \cap \mathbb{Q} = \emptyset$
In particular: $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$.

Proof.
(1): Let $n \in \mathrm{PerP}(\mathrm{F}) \cap \mathbb{Q}$. Then, $\left|\mathrm{F}^{\ell+1}(n)\right| \geq \left|\mathrm{F}^{\ell}(n)\right|$ for some $\ell \in \mathbb{N}_0$ (otherwise n cannot be a periodic point of F) and thus $\left|\mathrm{F}^{\ell}(n)\right| \leq M$ by definition of M which proves the "In particular" part. Also, $n = \mathrm{F}^k(\mathrm{F}^{\ell}(n))$ for some $k \in \mathbb{N}_0$ and thus we get $n \in \bigcup_{k=0}^{\infty} \mathrm{F}^k(A)$ as claimed.
(2): Let $n = a/b \in \mathbb{Q} \cap \mathbb{Z}_p$ with $(a, b) \in \mathbb{Z} \times \mathbb{N}$ coprime and

$$B := \{c/d \in \mathbb{Q} \mid (c, d) \in \mathbb{Z} \times \mathbb{N} \wedge d \leq b\}. \tag{6.17}$$

Then, contr(F) and d-contr(F) imply that $\left\{\mathrm{F}^k(n) \mid k \in \mathbb{N}_0\right\}$ is contained in $\bigcup_{k=0}^{\infty} \mathrm{F}^k(A \cap B)$ which is a finite set. Thus n is an ultimately periodic point of F.
(3) and (4) follow directly from the definitions. □

An important class of p-adic systems that are expansive (and thus cannot be ultimately periodic on $\mathbb{Q}\cap\mathbb{Z}_p$) is given by $(\mathbb{Q}\cap\mathbb{Z}_p)$-polynomial p-adic systems where each polynomial is either of degree 2 or higher or has a linear coefficient greater than p in absolute value.

Theorem 6.3. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{F}, \mathrm{G} \in \overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$ *such that* $\mathrm{F}[r]$ *either is of degree* 2 *or higher or* $\mathrm{F}[r] = a_r + b_r x$ *with* $|b_r| > p$ *for all* $r \in \underline{p}$. *Then,*

(1) exp(F)
In particular: $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$

(2) contr(G) $\Rightarrow$ lin-poly(G).

Note that by Theorem 4.1 (2) and Theorem 4.8 (3) we get $\overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Q}\cap\mathbb{Z}_p}) = \overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Q}\cap\mathbb{Z}_p,[\![1,\infty]\!]})$.

Proof of Theorem 6.3.
(1): For every $r \in \underline{p}$, $\mathrm{F}[r]$ is a polynomial function (on $r + p\mathbb{Z}_p$) with coefficients in $\mathbb{Q}\cap\mathbb{Z}_p$. Thus we clearly have $\mathrm{F}(\mathbb{Q}\cap\mathbb{Z}_p) \subseteq \mathbb{Q}\cap\mathbb{Z}_p$ and for all $r \in \underline{p}$ there is an $0 \leq M_r \in \mathbb{R}$ such that

$$|\mathrm{F}[r](n) - \mathrm{F}[r](n)\%p| > p\,|n| \tag{6.18}$$

for all $n \in \mathbb{Q} \cap (r + p\mathbb{Z}_p)$ with $|n| > M_r$ (note that $\mathrm{F}[r](n)\%p \in \underline{p}$) by the additional assumptions. Let $M := \max\{M_0, \ldots, M_{p-1}\}$, $n \in \mathbb{Q}\cap\mathbb{Z}_p$ with $|n| > M$, and $r := n\%p$. Then,

$$|\mathrm{F}(n)| = \left|\frac{\mathrm{F}[r](n) - \mathrm{F}[r](n)\%p}{p}\right| > |n| \tag{6.19}$$

which implies that F is expansive.
(2): Clearly, if $\mathrm{G}[r]$ is of degree 2 or higher for at least one $r \in \underline{p}$, then G cannot be contractive. □

7. Linear-polynomial p-adic systems and the question of ultimate periodicity

In the following we investigate linear-polynomial p-adic systems such as $\mathrm{F}_p = (x)^p$ (standard base p) or $\mathrm{F}_C = (x, 3x + 1)$ (Collatz).

Basic facts. We begin by applying results from previous sections to characterize linear polynomials with special properties.

Lemma 7.1. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $f = a + bx \in \mathbb{Z}_p[x]$, and $k \in \mathbb{N}_0$. Then,*

(1) $\text{w-suit}_{p,r}(f)$
(2) $\text{suit}_{p,r}(f) \Leftrightarrow \gcd(p, b\%p) = 1$
(3) $\text{suit}_{p,r}(f) \Rightarrow (\text{avoid}_{p,r}(f) \Leftrightarrow f(r) \in p\mathbb{Z}_p)$.

Note that by (3) and Theorem 4.1 (2) it follows that every linear-polynomial p-adic system in weak canonical form is avoiding when interpreted as the p-fibred rational function defined by the same polynomials.

Proof of Lemma 7.1. (1) and (2) follow directly from Theorem 4.8. For the proof of (3) we assume $\text{suit}_{p,r}(f)$ which is equivalent to $\gcd(p, b\%p) = 1$ by (2). Thus, $f(\mathbb{Q}_p \setminus \mathbb{Z}_p) \cap p\mathbb{Z}_p = \emptyset$ and $f(\underline{p})\%p = \underline{p}$. But then

$$\text{avoid}_{p,r}(f) \Leftrightarrow f(\underline{p} \setminus \{r\}) \cap p\mathbb{Z}_p = \emptyset \Leftrightarrow f(r) \in p\mathbb{Z}_p \tag{7.1}$$

by Theorem 5.12. □

A formula for R_D. Next we give a direct formula for R_D if R is a linear-polynomial p-fibred rational function. Note that for the special case $\mathrm{R} = (x, 3x + 1)$ this formula can be found in many publications on the original Collatz conjecture, such as [11, 48, 5, 6]. For any sequence S and any a we denote by $\text{pos}(S, a)$ the increasing sequence of all indices $i \in \underline{|S|}$ for which $S[i] = a$ and set $\text{cnt}(S, a) := |\text{pos}(S, a)|$. Furthermore, for $\mathrm{F} := (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1} x) \in \mathcal{F}_p(\text{lin-poly}) \cup \mathcal{R}_p(\text{lin-poly})$ and $D \in \mathbf{S}(\text{bnd}_{\underline{p}}, \text{fin})$ we define

$$A_{\mathrm{F}}(D) := \sum_{i=0}^{|D|-1} a_{D[i]} p^i \prod_{j=i+1}^{|D|-1} b_{D[j]} \tag{7.2}$$

$$B_{\mathrm{F}}(D) := \prod_{i=0}^{|D|-1} b_{D[i]}. \tag{7.3}$$

By collecting the "a_i"s and "b_i"s it follows that

$$A_{\mathrm{F}}(D) = \sum_{r=0}^{p-1} a_r \sum_{i=0}^{\text{cnt}(D,r)-1} p^{\text{pos}(D,r)[i]} \prod_{s=0}^{p-1} b_s^{\text{cnt}(D[\text{pos}(D,r)[i]+1, |D|-1], s)} \tag{7.4}$$

$$B_{\mathrm{F}}(D) = \prod_{r=0}^{p-1} b_r^{\text{cnt}(D,r)}. \tag{7.5}$$

Theorem 7.2. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{R} \in \mathcal{R}_p(\text{lin-poly})$, $D \in \mathbf{S}(\text{bnd}_{\underline{p}}, \text{fin})$, and $n \in \mathbb{Q}_p$. Then,*

$$\mathrm{R}_D(n) = \frac{A_{\mathrm{R}}(D) + nB_{\mathrm{R}}(D)}{p^{|D|}}. \tag{7.6}$$

In particular: $\mathrm{R}_D(x) \in \mathbb{Q}_p[x]$ is a linear polynomial.

Proof. Let $a_0, b_0, \ldots, a_{p-1}, b_{p-1} \in \mathbb{Q}_p$ such that $\mathrm{R} = (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1} x)$. We prove the formula by induction on the length of D. If $|D| = 0$, then $\mathrm{R}_D(n) = n$ as claimed. Now assume that the formula is true for D and let $E := D \cdot (e) \in \mathbf{S}(\text{bnd}_{\underline{p}}, \text{fin})$ where $e \in \underline{p}$. We compute

$$\mathrm{R}_E(n) = \frac{\mathrm{R}[E[|E|-1]]\left(\mathrm{R}_{E[\underline{|E|-1}]}(n)\right)}{p} = \frac{\mathrm{R}[e]\left(\mathrm{R}_D(n)\right)}{p} \tag{7.7}$$

$$= \left(a_e + b_e \left(n \cdot \prod_{i=0}^{|D|-1} b_{D[i]} + \sum_{i=0}^{|D|-1} a_{D[i]} p^i \prod_{j=i+1}^{|D|-1} b_{D[j]} \right) \frac{1}{p^{|D|}} \right) \frac{1}{p} \tag{7.8}$$

$$= \left(a_{E[|E|-1]} + b_{E[|E|-1]} \left(n \cdot \prod_{i=0}^{|E|-2} b_{E[i]} + \sum_{i=0}^{|E|-2} a_{E[i]} p^i \prod_{j=i+1}^{|E|-2} b_{E[j]} \right) \frac{1}{p^{|E|-1}} \right) \frac{1}{p} \tag{7.9}$$

$$= \left(n \cdot \prod_{i=0}^{|E|-1} b_{E[i]} + a_{E[|E|-1]} p^{|E|-1} + \sum_{i=0}^{|E|-2} a_{E[i]} p^i \prod_{j=i+1}^{|E|-1} b_{E[j]} \right) \frac{1}{p^{|E|}} \tag{7.10}$$

$$= \left(n \cdot \prod_{i=0}^{|E|-1} b_{E[i]} + \sum_{i=0}^{|E|-1} a_{E[i]} p^i \prod_{j=i+1}^{|E|-1} b_{E[j]} \right) \frac{1}{p^{|E|}}. \tag{7.11}$$

□

Find the number that has a given expansion. Theorem 7.2 has several consequences, one of them being that all ultimately periodic points of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems are rational numbers. This follows from a general formula for the unique p-adic integer that has a given ultimately periodic digit expansion with respect to a given linear-polynomial p-adic system.

Corollary 7.3. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly})$, $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{uper})$, *and* n *the unique element of* $\mathbb{Z}_p$ *satisfying* $\mathrm{D}(\mathrm{F})[n] = D$ *(cf. Lemma 3.11). Then,*

$$n = \left(\frac{A_{\mathrm{F}}(\mathcal{P}(D))}{p^{|\mathcal{P}(D)|} - B_{\mathrm{F}}(\mathcal{P}(D))} p^{|\mathcal{I}(D)|} - A_{\mathrm{F}}(\mathcal{I}(D)) \right) \frac{1}{B_{\mathrm{F}}(\mathcal{I}(D))}. \tag{7.12}$$

In particular,

$$\mathrm{PerP}(\mathrm{F}) = \left\{ \frac{A_{\mathrm{F}}(D_P)}{p^{|D_P|} - B_{\mathrm{F}}(D_P)} \mid D_P \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{fin}) \right\} \tag{7.13}$$

$$\mathrm{UPerP}(\mathrm{F}) = \left\{ \left(\frac{A_{\mathrm{F}}(D_P)}{p^{|D_P|} - B_{\mathrm{F}}(D_P)} p^{|D_I|} - A_{\mathrm{F}}(D_I) \right) \frac{1}{B_{\mathrm{F}}(D_I)} \mid D_I, D_P \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{fin}) \right\} \tag{7.14}$$

and if $\text{lin-poly}_{\mathbb{Q} \cap \mathbb{Z}_p}(\mathrm{F})$, *then* $[\mathrm{UPerP} \subseteq \mathbb{Q} \cap \mathbb{Z}_p](\mathrm{F})$.

Proof. Let $a_0, b_0, \ldots, a_{p-1}, b_{p-1} \in \mathbb{Z}_p$ and $\mathrm{R} := (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1} x) \in \mathcal{R}_p(\text{lin-poly})$. Then, $\mathrm{F} = \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p})$ and thus

$$\mathrm{F}^k(n) = \mathrm{R}_{D[\underline{k}]}(n) \tag{7.15}$$

for all $k \in \mathbb{N}_0$ by Lemma 5.8. Furthermore, let $m := \mathrm{F}^{|\mathcal{I}(D)|}(n)$. Then, $\mathrm{D}(\mathrm{F})[m] = \mathcal{P}(D)^\infty$ and hence

$$\mathrm{F}^k(m) = \mathrm{R}_{(\mathcal{P}(D)^\infty)[\underline{k}]}(m) \tag{7.16}$$

for all $k \in \mathbb{N}_0$, again by Lemma 5.8. Thus, Corollary 3.10 and Theorem 7.2 imply

$$m = \mathrm{F}^{|\mathcal{I}(D)|}(n) = \mathrm{R}_{D[|\underline{\mathcal{I}(D)}|]}(n) = \mathrm{R}_{\mathcal{I}(D)}(n) = \frac{A_{\mathrm{R}}(\mathcal{I}(D)) + nB_{\mathrm{R}}(\mathcal{I}(D))}{p^{|\mathcal{I}(D)|}} \tag{7.17}$$

$$m = \mathrm{F}^{|\mathcal{P}(D)|}(m) = \mathrm{R}_{(\mathcal{P}(D)^\infty)[|\underline{\mathcal{P}(D)}|]}(m) = \mathrm{R}_{\mathcal{P}(D)}(m) = \frac{A_{\mathrm{R}}(\mathcal{P}(D)) + mB_{\mathrm{R}}(\mathcal{P}(D))}{p^{|\mathcal{P}(D)|}}. \tag{7.18}$$

Solving the second equation for m and plugging in the result into the first equation yields

$$m = \frac{A_{\mathrm{F}}(\mathcal{P}(D))}{p^{|\mathcal{P}(D)|} - B_{\mathrm{F}}(\mathcal{P}(D))} \tag{7.19}$$

$$n = \left(\frac{A_{\mathrm{F}}(\mathcal{P}(D))}{p^{|\mathcal{P}(D)|} - B_{\mathrm{F}}(\mathcal{P}(D))} p^{|\mathcal{I}(D)|} - A_{\mathrm{F}}(\mathcal{I}(D)) \right) \frac{1}{B_{\mathrm{F}}(\mathcal{I}(D))}. \tag{7.20}$$

The inclusion "$\subseteq$" in Eqn. (7.13) and Eqn. (7.14) of the "In particular" part follows directly from what we just proved. For the other inclusion let $D_I, D_P \in \mathbf{S}(\mathrm{bnd}_p, \mathrm{fin})$ and set

$$m := \frac{A_{\mathrm{F}}(D_P)}{p^{|D_P|} - B_{\mathrm{F}}(D_P)} \in \mathbb{Z}_p \tag{7.21}$$

$$n := \left(\frac{A_{\mathrm{F}}(D_P)}{p^{|D_P|} - B_{\mathrm{F}}(D_P)} p^{|D_I|} - A_{\mathrm{F}}(D_I)\right) \frac{1}{B_{\mathrm{F}}(D_I)} \in \mathbb{Z}_p. \tag{7.22}$$

Then $\mathrm{R}_{D_I}(n) = m \in \mathbb{Z}_p$ and $\mathrm{R}_{D_P}(m) = m \in \mathbb{Z}_p$, and since R is avoiding (cf. the remark after Lemma 7.1), we get $\mathrm{F}^{|D_I|}(n) = \mathrm{R}_{D_I}(n) = m$, and $\mathrm{F}^{|D_P|}(m) = \mathrm{R}_{D_P}(m) = m$ by Lemma 5.9. Thus, $m \in \mathrm{PerP}(\mathrm{F})$ and $n \in \mathrm{UPerP}(\mathrm{F})$.

Clearly, if lin-poly$_{\mathbb{Q}\cap\mathbb{Z}_p}$(F), i.e. $a_0, b_0, \ldots, a_{p-1}, b_{p-1} \in \mathbb{Q} \cap \mathbb{Z}_p$, then

$$A_{\mathrm{F}}(\mathcal{I}(D)), A_{\mathrm{F}}(\mathcal{P}(D)), B_{\mathrm{F}}(\mathcal{I}(D)), B_{\mathrm{F}}(\mathcal{P}(D)) \in \mathbb{Q} \cap \mathbb{Z}_p \tag{7.23}$$

and hence $n \in \mathbb{Q} \cap \mathbb{Z}_p$. □

Another consequence of Theorem 7.2 is a complete characterization of those p-adic integers whose digit-expansions with respect to a given linear-polynomial p-adic system have a given beginning.

Corollary 7.4. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly})$, $D \in \mathbf{S}(\mathrm{bnd}_p, \mathrm{fin})$, and n the unique element of $\underline{p^{|D|}}$ satisfying $\mathrm{D}(\mathrm{F})[n][\lfloor \underline{D} \rfloor] = D$ (cf. Lemma 3.5). Then,*

$$n = (bA_{\mathrm{F}}(D)) \,\%p^{|D|} \tag{7.24}$$

where $b \in \mathbb{Z}$ such that

$$p^{|D|}a - \left(B_{\mathrm{F}}(D)\%p^{|D|}\right) b = 1 \tag{7.25}$$

for some $a \in \mathbb{Z}$ (find b with extended Euclidean algorithm). In particular,

$$\{m \in \mathbb{Z}_p \mid \mathrm{D}(\mathrm{F})[m][\lfloor \underline{D} \rfloor] = D\} = n + p^{|D|}\mathbb{Z}_p \tag{7.26}$$

by block(F).

Proof. Let $A := A_{\mathrm{F}}(D)$ and $B := B_{\mathrm{F}}(D)$. If we interpret F as the p-fibred rational function that is defined by the same polynomials as the p-adic system F, we have avoid(F) according to the remark after Lemma 7.1. Thus, Lemma 5.9 and Theorem 7.2 imply that

$$\mathrm{D}(\mathrm{F})[m][\lfloor \underline{D} \rfloor] = D \Leftrightarrow \frac{A + mB}{p^{|D|}} = \mathrm{F}_D(m) \in \mathbb{Z}_p \tag{7.27}$$

$$\Leftrightarrow A + mB \in p^{|D|}\mathbb{Z}_p \tag{7.28}$$

$$\Leftrightarrow A\%p^{|D|} + \left(m\%p^{|D|}\right)\left(B\%p^{|D|}\right) \in p^{|D|}\mathbb{Z} \tag{7.29}$$

$$\Leftrightarrow \exists\, a \in \mathbb{Z} : A\%p^{|D|} + \left(m\%p^{|D|}\right)\left(B\%p^{|D|}\right) = ap^{|D|} \tag{7.30}$$

$$\Leftrightarrow \exists\, a \in \mathbb{Z} : p^{|D|}a - \left(B\%p^{|D|}\right)\left(m\%p^{|D|}\right) = A\%p^{|D|} \tag{7.31}$$

for all $m \in \mathbb{Z}_p$. Since $\gcd\left(p^{|D|}, B\%p^{|D|}\right) = 1$ by Lemma 7.1 (2), the equation

$$p^{|D|}a - \left(B\%p^{|D|}\right) b = 1 \tag{7.32}$$

has a solution $a, b \in \mathbb{Z}$ by Bézout's Lemma. For any such $a, b \in \mathbb{Z}$ we get

$$p^{|D|}a\left(A\%p^{|D|}\right) - \left(B\%p^{|D|}\right) b \left(A\%p^{|D|}\right) = A\%p^{|D|} \tag{7.33}$$

$$\Leftrightarrow p^{|D|}a\left(A\%p^{|D|}\right) - \left(B\%p^{|D|}\right)\left(p^{|D|}\frac{b\left(A\%p^{|D|}\right) - (bA)\,\%p^{|D|}}{p^{|D|}} + (bA)\,\%p^{|D|}\right) = A\%p^{|D|} \tag{7.34}$$

$$\Leftrightarrow p^{|D|}C - \left(B\%p^{|D|}\right)\left((bA)\,\%p^{|D|}\right) = A\%p^{|D|} \tag{7.35}$$

where

$$C := a\left(A\%p^{|D|}\right) - \left(B\%p^{|D|}\right)\frac{b\left(A\%p^{|D|}\right) - (bA)\,\%p^{|D|}}{p^{|D|}} \in \mathbb{Z}. \tag{7.36}$$

Thus,

$$\mathrm{D(F)}[bA][\lfloor \underline{D} \rfloor] = D \tag{7.37}$$

and consequently $n = (bA)\%p^{|D|}$. □

Inverse problem: given a number and expansion, find a system. Corollary 7.3 allows to compute the unique p-adic integer that has a given ultimately periodic F-digit expansion for a given linear-polynomial p-adic system F in weak canonical form. In the other direction one might try to find one or even all linear-polynomial p-adic systems for which a given p-adic integer has a given ultimately periodic digit expansion. The characterization of these p-adic systems is given in the following corollary which is another consequence of Theorem 7.2.

Corollary 7.5. *Let* $2 \leq p \in \mathbb{N}$, $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{uper})$, $r := D[0]$, $n \in r + p\mathbb{Z}_p$, *and* $\mathrm{F} = (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly})$. *Furthermore, let*

$$k := |\mathcal{I}(D)| \tag{7.38}$$

$$\ell := |\mathcal{P}(D)| \tag{7.39}$$

$$c_s := \sum_{i=0}^{\mathrm{cnt}(\mathcal{I}(D),s)-1} p^{\mathrm{pos}(\mathcal{I}(D),s)[i]} \prod_{t=0}^{p-1} b_t^{\mathrm{cnt}(\mathcal{I}(D)[\mathrm{pos}(\mathcal{I}(D),s)[i]+1,k-1],t)},\ s \in \underline{p} \tag{7.40}$$

$$d_s := \sum_{i=0}^{\mathrm{cnt}(\mathcal{P}(D),s)-1} p^{\mathrm{pos}(\mathcal{P}(D),s)[i]} \prod_{t=0}^{p-1} b_t^{\mathrm{cnt}(\mathcal{P}(D)[\mathrm{pos}(\mathcal{P}(D),s)[i]+1,\ell-1],t)},\ s \in \underline{p} \tag{7.41}$$

$$c := B_{\mathrm{F}}(\mathcal{I}(D)) \tag{7.42}$$

$$d := B_{\mathrm{F}}(\mathcal{P}(D)). \tag{7.43}$$

If $a_0, \ldots, a_{r-1}, a_{r+1}, \ldots, a_{p-1}, b_0, \ldots, b_{p-1}$ *are fixed, then there is a unique choice for* a_r *such that* $\mathrm{D(F)}[n] = D$. *This choice is given by*

$$a_r = \left(cn - \sum_{s \in \underline{p}\setminus\{r\}} a_s \left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right) \Bigg/ \left(\frac{d_r p^k}{p^\ell - d} - c_r\right). \tag{7.44}$$

Proof. By rearranging the formula for n in Corollary 7.3 it follows that if a_r can be chosen such that $\mathrm{D(F)}[n] = D$ holds, a_r must satisfy Eqn. (7.44). We are thus left to show that a_r as given in Eqn. (7.44) is an element of $-rb_r + p\mathbb{Z}_p$ and thus defines a valid linear-polynomial p-adic system in weak canonical form (within F). This would follow in particular if we could demonstrate that

$$\gcd\left(p, \left(\frac{d_r p^k}{p^\ell - d} - c_r\right)\%p\right) = 1 \tag{7.45}$$

and

$$cn - \sum_{s \in \underline{p}\setminus\{r\}} a_s \left(\frac{d_s p^k}{p^\ell - d} - c_s\right) \in -rb_r \left(\frac{d_r p^k}{p^\ell - d} - c_r\right) + p\mathbb{Z}_p \tag{7.46}$$

which is what we will do.

We begin by showing Eqn. (7.45) and use the fact $D[0] = r$ and Lemma 7.1 (2) to compute

$$\gcd\left(p, \left(\frac{d_r p^k}{p^\ell - d} - c_r\right)\%p\right) \tag{7.47}$$

$$= \gcd\left(p, \left(k = 0\ ?\ \frac{d_r}{p^\ell - d} : -c_r\right)\%p\right) \tag{7.48}$$

$$= \gcd\left(p, \left(k = 0\ ?\ \frac{\prod_{t=0}^{p-1} b_t^{\mathrm{cnt}(\mathcal{P}(D)[1,\ell-1],t)}}{p^\ell - \prod_{t=0}^{p-1} b_t^{\mathrm{cnt}(\mathcal{P}(D),t)}} : -\prod_{t=0}^{p-1} b_t^{\mathrm{cnt}(\mathcal{I}(D)[1,k-1],t)}\right)\%p\right) \tag{7.49}$$

$$= 1. \tag{7.50}$$

To show Eqn. (7.46) let m be the unique element of $r + p\mathbb{Z}_p$ satisfying $\mathrm{D}(\mathrm{G})[m] = D$ (cf. Lemma 3.11) where $\mathrm{G} \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly})$ is given by

$$\mathrm{G} := (a_0 + b_0 x, \ldots, a_{r-1} + b_{r-1}x, -rb_r + b_r x, a_{r+1} + b_{r+1}x, \ldots, a_{p-1} + b_{p-1}x). \tag{7.51}$$

Then by Corollary 7.3 we get

$$m = \frac{1}{c}\left(-rb_r\left(\frac{d_r p^k}{p^\ell - d} - c_r\right) + \sum_{s \in \underline{p}\setminus\{r\}} a_s\left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right) \tag{7.52}$$

which implies

$$\left(cn - \sum_{s \in \underline{p}\setminus\{r\}} a_s\left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right)\%p = \left(cm - \sum_{s \in \underline{p}\setminus\{r\}} a_s\left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right)\%p \tag{7.53}$$

$$= \left(-rb_r\left(\frac{d_r p^k}{p^\ell - d} - c_r\right)\right)\%p. \tag{7.54}$$

□

The above corollary indeed characterizes all weak canonical linear-polynomial p-adic systems for which a given p-adic integer n has a given ultimately periodic digit expansion D: simply pick all coefficients at random apart from the constant coefficient of $\mathrm{F}[n\%p]$ which is fixed uniquely by the other coefficients and can be computed by the formula given in the corollary. A further corollary of Theorem 7.2 which will answer a similar question is proven next.

Corollary 7.6. *Let $2 \leq p \in \mathbb{N}$, $r \in \underline{p}$, $D \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{uper})$, and $\mathrm{F} = (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly})$. Furthermore, let $k, \ell, c_0, \ldots, c_{p-1}, d_0, \ldots, d_{p-1}, c, d$ as in Corollary 7.5 and*

$$K := (\mathrm{cnt}\,(D, r) \neq 0\ ?\ \mathrm{pos}\,(D, r)[0] + 1 : -\infty) \tag{7.55}$$

$$A_1 := (-rb_r)\%p \tag{7.56}$$

$$B_1 := \frac{1}{c}\left(A_1\left(\frac{d_r p^k}{p^\ell - d} - c_r\right) + \sum_{s \in \underline{p}\setminus\{r\}} a_s\left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right) \tag{7.57}$$

$$C_1 := \left(\mathrm{cnt}\,(D, r) \neq 0\ ?\ \frac{1}{cp^{K-1}}\left(\frac{d_r p^k}{p^\ell - d} - c_r\right) : 1\right) \tag{7.58}$$

$$A_2 := \left(\mathrm{cnt}\,(D, r) \neq 0\ ?\ A_1 - \frac{B_1 - B_1\%p^K}{C_1 p^{K-1}} : A_1\right) \tag{7.59}$$

$$B_2 := \left(\mathrm{cnt}\,(D, r) \neq 0\ ?\ B_1\%p^K, B_1\right) \tag{7.60}$$

$$C_2 := \frac{1}{C_1}. \tag{7.61}$$

If $a_0, \ldots, a_{r-1}, a_{r+1}, \ldots, a_{p-1}, b_0, \ldots, b_{p-1}$ are fixed, then

(1) $\left\{(a_r,n)\in(\mathbb{Z}_p)^2 \mid \mathrm{D}(\mathrm{F})[n]=D\right\}=\left\{\left(A_1+mp,B_1+mC_1p^K\right)\mid m\in\mathbb{Z}_p\right\}$
$=\left\{\left(A_2+mC_2p,B_2+mp^K\right)\mid m\in\mathbb{Z}_p\right\}$
where $A_1,B_1,C_1,A_2,B_2,C_2\in\mathbb{Z}_p$, $A_1\in\underline{p}$, $B_2\in\underline{p^K}$ *if* $\mathrm{cnt}\,(D,r)\neq 0$, *and* $\gcd(p,C_1\%p)=\gcd(p,C_2\%p)=1$

(2) *If* $\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$ *and* K_1,L_1,K_2,L_2 *are the denominators of* B_1,C_1,A_2,C_2 *respectively then,*
$\left\{(a_r,n)\in\mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n]=D\right\}\neq\emptyset\Leftrightarrow K_1\mid L_1$
$\Leftrightarrow K_2\mid L_2\wedge B_2\in\mathbb{Z}$
In this case:
$\left\{(a_r,n)\in\mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n]=D\right\}$
$=\left\{\left(A_1+(S_1B_1+m)L_1p,B_1+(S_1B_1+m)L_1C_1p^K\right)\mid m\in\mathbb{Z}\right\}$
$=\left\{\left(A_2+(S_2A_2+m)L_2C_2p,B_2+(S_2A_2+m)L_2p^K\right)\mid m\in\mathbb{Z}\right\}$
where $S_1,S_2\in\mathbb{Z}$ *such that*
$L_1R_1-L_1C_1p^KS_1=1$
$L_2R_2-L_2C_2pS_2=1$
for some $R_1,R_2\in\mathbb{Z}$ *(find* S_1,S_2 *with extended Euclidean algorithm).*

Proof.
(1): Clearly, $A_1,B_1,A_2,B_2\in\mathbb{Z}_p$, $A_1\in\underline{p}$, and $B_2\in\underline{p^K}$ if $\mathrm{cnt}\,(D,r)\neq 0$. In addition, if $\mathrm{cnt}\,(D,r)=0$, then $C_1,C_2=1\in\mathbb{Z}_p$ and $\gcd(p,C_1\%p)=\gcd(p,C_2\%p)=\gcd(p,1)=1$. If, however, $\mathrm{cnt}\,(D,r)\neq 0$ then either $\mathrm{pos}\,(D,r)[0]<|\mathcal{I}\,(D)|$ or $\mathrm{pos}\,(D,r)[0]\geq|\mathcal{I}\,(D)|$. In the first case we get $K-1=\mathrm{pos}\,(D,r)[0]=\mathrm{pos}\,(\mathcal{I}\,(D),r)[0]$,

$$C_1=\frac{1}{cp^{K-1}}\left(\frac{d_rp^k}{p^\ell-d}-c_r\right) \tag{7.62}$$

$$=\frac{p^{|\mathcal{I}(D)|}}{p^{\mathrm{pos}(D,r)[0]}}\frac{d_r}{c(p^\ell-d)}-\frac{1}{c}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{I}(D)[\mathrm{pos}(\mathcal{I}(D),r)[0]+1,k-1],t)}- \tag{7.63}$$
$$\frac{1}{c}\sum_{i=1}^{\mathrm{cnt}(\mathcal{I}(D),r)-1}\frac{p^{\mathrm{pos}(\mathcal{I}(D),r)[i]}}{p^{\mathrm{pos}(\mathcal{I}(D),r)[0]}}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{I}(D)[\mathrm{pos}(\mathcal{I}(D),r)[i]+1,k-1],t)}$$

$$\in\mathbb{Z}_p \tag{7.64}$$

and

$$\gcd(p,C_1\%p)=\gcd\left(p,\left(\frac{1}{c}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{I}(D)[\mathrm{pos}(\mathcal{I}(D),r)[0]+1,k-1],t)}\right)\%p\right) \tag{7.65}$$

$$=1 \tag{7.66}$$

by Lemma 7.1 (2). In the second case we get $K-1=\mathrm{pos}\,(D,r)[0]=|\mathcal{I}\,(D)|+\mathrm{pos}\,(\mathcal{P}\,(D),r)[0]$,

$$C_1=\frac{1}{cp^{K-1}}\left(\frac{d_rp^k}{p^\ell-d}-c_r\right) \tag{7.67}$$

$$=\frac{1}{c(p^\ell-d)}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{P}(D)[\mathrm{pos}(\mathcal{P}(D),r)[0]+1,\ell-1],t)}+ \tag{7.68}$$
$$\frac{1}{c(p^\ell-d)}\sum_{i=1}^{\mathrm{cnt}(\mathcal{P}(D),r)-1}\frac{p^{\mathrm{pos}(\mathcal{P}(D),r)[i]}}{p^{\mathrm{pos}(\mathcal{P}(D),r)[0]}}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{P}(D)[\mathrm{pos}(\mathcal{P}(D),r)[i]+1,\ell-1],t)}$$

$$\in\mathbb{Z}_p \tag{7.69}$$

and

$$\gcd(p,C_1\%p)=\gcd\left(p,\left(\frac{1}{c(p^\ell-d)}\prod_{t=0}^{p-1}b_t^{\mathrm{cnt}(\mathcal{P}(D)[\mathrm{pos}(\mathcal{P}(D),r)[0]+1,\ell-1],t)}\right)\%p\right) \tag{7.70}$$

$$=1 \tag{7.71}$$

again by Lemma 7.1 (2). We thus proved that, in any case, $C_1, C_2 \in \mathbb{Z}_p$ and $\gcd(p, C_1\%p) = \gcd(p, C_2\%p) = 1$.

If $a_r = A_1 + mp = (-rb_r)\%p + mp$ for some $m \in \mathbb{Z}_p$ (which exactly covers all possible candidates for a_r for F to be in weak canonical form), then by Corollary 7.3 there is a unique $n \in \mathbb{Z}_p$ satisfying $\mathrm{D(F)}[n] = D$ which is given by

$$n = \left(\frac{A_{\mathrm{F}}(\mathcal{P}(D))}{p^{|\mathcal{P}(D)|} - B_{\mathrm{F}}(\mathcal{P}(D))} p^{|\mathcal{I}(D)|} - A_{\mathrm{F}}(\mathcal{I}(D))\right) \frac{1}{B_{\mathrm{F}}(\mathcal{I}(D))} \tag{7.72}$$

$$= \frac{1}{c} \sum_{r=0}^{p-1} a_r \left(\frac{d_r p^k}{p^\ell - d} - c_r\right) \tag{7.73}$$

$$= \frac{1}{c} \left((A_1 + mp)\left(\frac{d_r p^k}{p^\ell - d} - c_r\right) + \sum_{s \in \underline{p} \setminus \{r\}} a_s \left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right) \tag{7.74}$$

$$= B_1 + mp \frac{1}{c} \left(\frac{d_r p^k}{p^\ell - d} - c_r\right) \tag{7.75}$$

$$= B_1 + \left(\mathrm{cnt}(D, r) \neq 0 \; ? \; mp^K \frac{1}{cp^{K-1}} \left(\frac{d_r p^k}{p^\ell - d} - c_r\right) : 0\right) \tag{7.76}$$

$$= B_1 + mC_1 p^K. \tag{7.77}$$

Thus, $\left\{(a_r, n) \in (\mathbb{Z}_p)^2 \mid \mathrm{D(F)}[n] = D\right\} = \left\{\left(A_1 + mp, B_1 + mC_1 p^K\right) \mid m \in \mathbb{Z}_p\right\}$.

If, however, $a_r = A_2 + mC_2 p$ for some $m \in \mathbb{Z}_p$ (which again exactly covers all possible candidates for a_r for F to be in weak canonical form since $\gcd(p, C_2\%p) = 1$), then again by Corollary 7.3 there is a unique $n \in \mathbb{Z}_p$ satisfying $\mathrm{D(F)}[n] = D$ which is given by

$$n = \frac{1}{c} \left((A_2 + mC_2 p)\left(\frac{d_r p^k}{p^\ell - d} - c_r\right) + \sum_{s \in \underline{p} \setminus \{r\}} a_s \left(\frac{d_s p^k}{p^\ell - d} - c_s\right)\right) \tag{7.78}$$

$$= B_1 - \frac{1}{c} \left(\mathrm{cnt}(D, r) \neq 0 \; ? \; \left(\frac{B_1 - B_1\%p^K}{C_1 p^{K-1}} - \frac{mp}{C_1}\right)\left(C_1 c p^{K-1}\right) : 0\right) \tag{7.79}$$

$$= B_2 + mp^K. \tag{7.80}$$

Thus, $\left\{(a_r, n) \in (\mathbb{Z}_p)^2 \mid \mathrm{D(F)}[n] = D\right\} = \left\{\left(A_2 + mC_2 p, B_2 + mp^K\right) \mid m \in \mathbb{Z}_p\right\}$.

(2): First we observe that $c_0, \ldots, c_{p-1}, d_0, \ldots, d_{p-1}, c, d, A_1, B_1, C_1, K_1, L_1, A_2, B_2, C_2, K_2, L_2 \in \mathbb{Q} \cap \mathbb{Z}_p$ by (1) and their respective definitions. Moreover, from (1) it follows that

$$\left\{(a_r, n) \in \mathbb{Z}^2 \mid \mathrm{D(F)}[n] = D\right\} \tag{7.81}$$

$$= \left\{\left(A_1 + mp, B_1 + mC_1 p^K\right) \mid m \in \mathbb{Z}_p\right\} \cap \mathbb{Z}^2 \tag{7.82}$$

$$= \left\{\left(A_1 + mp, B_1 + mC_1 p^K\right) \mid m \in \mathbb{Z} \wedge B_1 + mC_1 p^K \in \mathbb{Z}\right\} \tag{7.83}$$

$$= \left\{\left(A_1 + yp, B_1 + yC_1 p^K\right) \mid y \in \mathbb{Z} \wedge \exists\, x \in \mathbb{Z} : Lx - LC_1 p^K y = LB_1\right\} \tag{7.84}$$

where $L := \mathrm{lcm}(K_1, L_1)$. Bézout's Lemma implies that the equation $Lx - LC_1 p^K y = LB_1$ has a solution $x, y \in \mathbb{Z}$ if and only if $\gcd\left(L, LC_1 p^K\right)$ divides LB_1, which in return is true if and only if $\gcd\left(L, LC_1 p^K\right) = 1$, or equivalently $L = L_1$, respectively $K_1 \mid L_1$. In this case the set of all solutions is given by

$$\left\{(x, y) \in \mathbb{Z}^2 \mid Lx - LC_1 p^K y = LB_1\right\} = \left\{((R_1 B_1 + mC_1 p^K)L_1, (S_1 B_1 + m)L_1) \mid m \in \mathbb{Z}\right\} \tag{7.85}$$

where $R_1, S_1 \in \mathbb{Z}$ such that $L_1 R_1 - L_1 C_1 p^K S_1 = 1$. Consequently,

$$\left\{(a_r, n) \in \mathbb{Z}^2 \mid \mathrm{D(F)}[n] = D\right\} \tag{7.86}$$

$$= \left\{\left(A_1 + (S_1 B_1 + m)L_1 p, B_1 + (S_1 B_1 + m)L_1 C_1 p^K\right) \mid m \in \mathbb{Z}\right\}. \tag{7.87}$$

Analogously we get,

$$\{(a_r,n)\in\mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n]=D\} \tag{7.88}$$

$$=\{(A_2+mC_2p,B_2+mp^K) \mid m\in\mathbb{Z}_p\}\cap\mathbb{Z}^2 \tag{7.89}$$

$$=\{(A_2+mC_2p,B_2+mp^K) \mid m\in\mathbb{Z}\wedge A_2+mC_2p\in\mathbb{Z}\wedge B_2\in\mathbb{Z}\} \tag{7.90}$$

$$=\{(A_2+yC_2p,B_2+yp^K) \mid y\in\mathbb{Z}\wedge\exists\, x\in\mathbb{Z}: Lx-LC_2py=LA_2\wedge B_2\in\mathbb{Z}\} \tag{7.91}$$

where $L:=\operatorname{lcm}(K_2,L_2)$. As before Bézout's Lemma implies that the equation $Lx-LC_2py=LA_2$ has a solution $x,y\in\mathbb{Z}$ if and only if $\gcd(L,LC_2p)$ divides LA_2, which in return is true if and only if $\gcd(L,LC_2p)=1$, or equivalently $L=L_2$, respectively $K_2\mid L_2$. In this case the set of all solutions is given by

$$\{(x,y)\in\mathbb{Z}^2 \mid Lx-LC_2py=LA_2\}=\{((R_2A_2+mC_2p)L_2,(S_2A_2+m)L_2) \mid m\in\mathbb{Z}\} \tag{7.92}$$

where $R_2,S_2\in\mathbb{Z}$ such that $L_2R_2-L_2C_2pS_2=1$. Consequently,

$$\{(a_r,n)\in\mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n]=D\} \tag{7.93}$$

$$=\{(A_2+(S_2A_2+m)L_2C_2p,B_2+(S_2A_2+m)L_2p^K) \mid m\in\mathbb{Z}\}. \tag{7.94}$$

□

As an example consider $\mathrm{F}:=\mathrm{F}_C=(x,3x+1)$, $r=1$, and $D=(P)^\infty\in\mathbf{S}(\mathrm{bnd}_{\underline{2}},\mathrm{per})$ and let

$$U_0:=\sum_{i=0}^{\mathrm{cnt}(P,0)-1}2^{\mathrm{pos}(P,0)[i]}3^{\mathrm{cnt}(P,1)-\mathrm{pos}(P,0)[i]+i} \tag{7.95}$$

$$U_1:=\sum_{i=0}^{\mathrm{cnt}(P,1)-1}2^{\mathrm{pos}(P,1)[i]}3^{\mathrm{cnt}(P,1)-i-1} \tag{7.96}$$

$$V:=2^{|P|}-3^{\mathrm{cnt}(P,1)}. \tag{7.97}$$

Then $a_0=0$, $b_0=1$, and $b_1=3$. Furthermore, if $D\neq(0)^\infty$, simplifying all expressions in Corollary 7.6 then yields,

$$K=\mathrm{pos}(P,1)[0]+1,\quad A_1=1,\quad B_1=\frac{U_1}{V},\quad C_1=\frac{U_1}{V}\frac{1}{2^{K-1}},\quad L_1=\frac{|V|}{\gcd(U_1,V)}, \tag{7.98}$$

and $R_1,S_1\in\mathbb{Z}$ such that

$$\frac{V}{\gcd(U_1,V)}R_1-\frac{2U_1}{\gcd(U_1,V)}S_1=\operatorname{sgn}(V). \tag{7.99}$$

Furthermore,

$$\{(a_1,n)\in\mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n]=D\} \tag{7.100}$$

$$=\{(A_1+(S_1B_1+m)L_12,B_1+(S_1B_1+m)L_1C_12^K) \mid m\in\mathbb{Z}\} \tag{7.101}$$

$$=\left\{\left(1+\left(S_1\frac{U_1}{V}+m\right)\frac{2|V|}{\gcd(U_1,V)},\frac{U_1}{V}+\left(S_1\frac{U_1}{V}+m\right)\frac{2|V|}{\gcd(U_1,V)}\frac{U_1}{V}\right) \mid m\in\mathbb{Z}\right\} \tag{7.102}$$

$$=\left\{\left(1,\frac{U_1}{V}\right)\left(1+\operatorname{sgn}(V)\left(S_1\frac{2U_1}{\gcd(U_1,V)}+2m\frac{V}{\gcd(U_1,V)}\right)\right) \mid m\in\mathbb{Z}\right\} \tag{7.103}$$

$$=\left\{\left(1,\frac{U_1}{V}\right)(2m+R_1)\frac{|V|}{\gcd(U_1,V)} \mid m\in\mathbb{Z}\right\} \tag{7.104}$$

$$=\left\{\left(1,\frac{U_1}{V}\right)(2m+1)\frac{V}{\gcd(U_1,V)} \mid m\in\mathbb{Z}\right\} \tag{7.105}$$

$$=\left\{\left(\frac{V}{\gcd(U_1,V)},\frac{U_1}{\gcd(U_1,V)}\right)(2m+1) \mid m\in\mathbb{Z}\right\}. \tag{7.106}$$

Analogously, if $r = 0$ and $D \neq (1)^\infty$, then $a_1 = 1$, $b_0 = 1$, $b_1 = 3$,

$$K = \operatorname{pos}(P, 0)[0] + 1, \quad A_1 = 0, \quad B_1 = \frac{U_1}{V}, \quad C_1 = \frac{U_0}{V}\frac{1}{2^{K-1}}, \quad L_1 = \frac{|V|}{\gcd(U_0, V)}, \tag{7.107}$$

and $R_1, S_1 \in \mathbb{Z}$ such that

$$\frac{V}{\gcd(U_0, V)} R_1 - \frac{2U_0}{\gcd(U_0, V)} S_1 = \operatorname{sgn}(V). \tag{7.108}$$

In addition,

$$\left\{(a_0, n) \in \mathbb{Z}^2 \mid \mathrm{D}(\mathrm{F})[n] = D\right\} = \left\{ \left(\frac{V}{\gcd(U_0, V)}, \frac{U_0}{\gcd(U_0, V)} \right) (2m+1) - 1 \mid m \in \mathbb{Z} \right\}. \tag{7.109}$$

Note that $U_0 - U_1 = V$ and $\gcd(U_0, V) = \gcd(U_1, V) = \gcd(U_0, U_1)$. A consequence of both Eqn. (7.106) and Eqn. (7.109) is that the Collatz conjecture is equivalent to

$$\mathbb{N} \subseteq \mathrm{UPerP}(\mathrm{F}) \quad \wedge \quad \exists\, m \in \mathbb{N} : mV = U_0 \Rightarrow \mathcal{P}(D) \in \{(0), (0,1), (1,0)\} \tag{7.110}$$

and respectively

$$\mathbb{N} \subseteq \mathrm{UPerP}(\mathrm{F}) \quad \wedge \quad \exists\, m \in \mathbb{N} : mV = U_1 \Rightarrow \mathcal{P}(D) \in \{(0,1), (1,0)\}. \tag{7.111}$$

Variants of this result can be found in several publications on the original Collatz conjecture, such as [48].

When do all rational numbers have ultimately periodic digit expansions? Conjectures. In Corollary 7.3 we proved that all ultimately periodic points of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems are rational numbers. The converse question whether all rational numbers have ultimately periodic digit expansions with respect to a given $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic system F, i.e. whether F is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_p$, is incredibly difficult in general and sits right at the heart of the Collatz conjecture. The general framework of p-adic systems might help to shed some light on the true nature of the underlying difficulty, as it allows to discuss the question in a broader context. In this context we are able to formulate conjectures of increasing generality which are backed by computer experiments to a varying degree. Several generalizations of the original Collatz transformation which have been considered in the literature (cf. e.g. [13, 52, 53, 8]) are covered by these general conjectures.

We begin by revisiting the Collatz conjecture itself.

Conjecture 7.7 (Collatz)**.** *Let* $\mathrm{F}_C := (x, 3x+1) \in \overline{\mathcal{F}}_2(\text{lin-poly}_{\mathbb{Z}})$*. Then,*

$$\forall\, n \in \mathbb{N} : \exists\, k \in \mathbb{N} : \mathrm{D}(\mathrm{F}_C)[n][k] = 1. \tag{7.112}$$

A slightly stronger version is given by

Conjecture 7.8. *Let* $\mathrm{F}_C := (x, 3x+1) \in \overline{\mathcal{F}}_2(\text{lin-poly}_{\mathbb{Z}})$*. Then,*

(1) $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{F}_C)$
(2) $\forall\, n \in \mathbb{N} : (\text{uper}(\mathrm{D}(\mathrm{F}_C)[n]) \Rightarrow \exists\, k \in \mathbb{N} : \mathrm{D}(\mathrm{F}_C)[n][k] = 1)$.

Considering both parts of the conjecture separately, there are several ways to generalize. The seemingly most arbitrary element is the definition of F_C. Why should $(x, 3x+1)$ be in any way special among linear-polynomial 2-adic systems? Experiments show that it probably isn't if we weaken (2).

Conjecture 7.9. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Z}})$*, and* $B \in \mathbb{Z}$ *the product of all leading coefficients of the polynomials* $\mathrm{F}[r](x)$*,* $r \in \underline{p}$*. Then,*

(1) $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \quad \Leftrightarrow \quad |B| < p^p$
(2) $|\{\mathcal{P}(\mathrm{D}(\mathrm{F})[n]) \mid n \in \mathbb{Z}\}| < \infty$.

For this conjecture numerous computer experiments have been performed by the author and while it may take quite a long time for digit expansions to become periodic (especially for larger p), they all did eventually. One of the experiments that were done was the computation of the maximal

lengths of the initial and periodic parts of the expansions of all integers in $\overline{1000}$ for all $\mathbb{Z}$-linear-polynomial p-adic systems satisfying $|B| < p^p$ where all constant coefficients are equal to 0, i.e. the computation of

$$m_I(p) := \max\left\{|\mathcal{I}\left(\mathrm{D}(\mathrm{F})[n]\right)| \mid \mathrm{F} = (b_0x, \ldots, b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Z}}) \wedge |b_0 \ldots b_{p-1}| < p^p \wedge n \in \overline{1000}\right\} \tag{7.113}$$

$$m_P(p) := \max\left\{|\mathcal{P}\left(\mathrm{D}(\mathrm{F})[n]\right)| \mid \mathrm{F} = (b_0x, \ldots, b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Z}}) \wedge |b_0 \ldots b_{p-1}| < p^p \wedge n \in \overline{1000}\right\}. \tag{7.114}$$

For $p \in \{2, 3, 4\}$ these values and the corresponding p-adic systems and starting values generating them are

$$m_I(2) = 160 \quad \text{for } \mathrm{F} = (-3x, -x), \quad n = 284 \tag{7.115}$$

$$m_P(2) = 19 \quad \text{for } \mathrm{F} = (x, -3x), \quad n = 609 \tag{7.116}$$

$$m_I(3) = 52401 \quad \text{for } \mathrm{F} = (x, -26x, -x), \quad n = 796 \tag{7.117}$$

$$m_P(3) = 3905 \quad \text{for } \mathrm{F} = (-13x, -x, 2x), \quad n = 608 \tag{7.118}$$

$$m_I(4) = 18481661 \quad \text{for } \mathrm{F} = (5x, -x, -51x, -x), \quad n = 818 \tag{7.119}$$

$$m_P(4) = 3291996 \quad \text{for } \mathrm{F} = (-51x, -x, -5x, x), \quad n = 416. \tag{7.120}$$

Note that the conjecture states in particular that the constant coefficients of the polynomials have no influence on the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$. On this aspect of the problem some results could be achieved which are presented further down in this section.

A further generalization, the status of which is less clear, considers more general coefficients for the linear polynomials defining the p-adic system.

Conjecture 7.10. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$, and $B \in \mathbb{Q} \cap \mathbb{Z}_p$ the product of all leading coefficients of the polynomials $\mathrm{F}[r](x)$, $r \in \underline{p}$. Then,*

(1) $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \quad \Leftrightarrow \quad B \in \mathbb{Z} \wedge |B| < p^p$
(2) $|\{\mathcal{P}\left(\mathrm{D}(\mathrm{F})[n]\right) \mid n \in \mathbb{Z}\}| < \infty$.

One of the observations often pointed out as being a first hint that the Collatz conjecture is indeed very hard to prove, is the fact that 27 takes 70 steps to reach 1 under $\mathrm{F}_C = (x, 3x + 1)$. In the context of the conjecture above we can do "much worse" as the following examples show. Let

$$\mathrm{F}_1 := (3/11x + 2, -11x + 1) \tag{7.121}$$

$$\mathrm{F}_2 := (1/7x + 2, 21x + 1) \tag{7.122}$$

$$\mathrm{F}_3 := (1/5x - 4, -15x + 3). \tag{7.123}$$

Then,

$$|\mathcal{I}\left(\mathrm{D}(\mathrm{F}_1)[27]\right)| = 816179238 \qquad |\mathcal{P}\left(\mathrm{D}(\mathrm{F}_1)[27]\right)| = 5890445 \tag{7.124}$$

$$|\mathcal{I}\left(\mathrm{D}(\mathrm{F}_2)[27]\right)| = 312815429 \qquad |\mathcal{P}\left(\mathrm{D}(\mathrm{F}_2)[27]\right)| = 22014805908 \tag{7.125}$$

$$|\mathcal{I}\left(\mathrm{D}(\mathrm{F}_3)[27]\right)| = 18966150 \qquad |\mathcal{P}\left(\mathrm{D}(\mathrm{F}_3)[27]\right)| = 122858925930. \tag{7.126}$$

Furthermore,

$$\mathcal{P}\left(\mathrm{S}(\mathrm{F}_1)[27]\right)[0] = \frac{292064}{11^3} \qquad d_I(\mathrm{F}_1) = 11^{25086} \qquad d_P(\mathrm{F}_1) = 11^{2912} \tag{7.127}$$

$$\mathcal{P}\left(\mathrm{S}(\mathrm{F}_2)[27]\right)[0] = \frac{197828}{7^3} \qquad d_I(\mathrm{F}_2) = 7^{9154} \qquad d_P(\mathrm{F}_2) = 7^{170632} \tag{7.128}$$

$$\mathcal{P}\left(\mathrm{S}(\mathrm{F}_3)[27]\right)[0] = \frac{101772}{5^6} \qquad d_I(\mathrm{F}_3) = 5^{3008} \qquad d_P(\mathrm{F}_3) = 5^{320048} \tag{7.129}$$

where $d_I(\mathrm{F}_i)$ and $d_P(\mathrm{F}_i)$ denote the largest denominators occurring in the initial and periodic parts of the sequence $\mathrm{S}(\mathrm{F}_i)[27]$ for $i \in \{1,2,3\}$. Another 2-adic system that was considered in computer experiments is

$$\mathrm{F}_4 := (21/5x, 5/7x+1) \tag{7.130}$$

which satisfies $|\mathcal{I}(\mathrm{D}(\mathrm{F}_4)[27])| > 10^{10}$. The denominator of $\mathrm{D}(\mathrm{F}_4)^{(10^{10})}(n)$ is $5^{12806}7^{119930} \approx 4.1477678 \cdot 10^{110303}$. Its numerator is approximately $8.2260293 \cdot 10^{110305}$ which makes the entire fraction approximately equal to 0.0050422. It appears hard to even guess whether $\mathrm{D}(\mathrm{F}_4)[27]$ is ultimately periodic. Figure 2 and Figure 3 below show the developments of the magnitudes of the denominators in the sequences $\mathrm{S}(\mathrm{F}_i)[27]$, $i \in \{1,2,3,4\}$. While for $\mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ these magnitudes can increase and decrease at any time, in the case of F_4 there is a tradeoff between the 5-adic and 7-adic valuations of the denominators of successive entries of the sequence $\mathrm{S}(\mathrm{F}_4)[27]$. If the 5- and 7-adic valuations of the denominator are both positive and $\mathrm{F}_4[0]$ is applied, then the 5-adic valuation of the denominator increases by 1 while the 7-adic valuation decreases by 1. If, however, $\mathrm{F}_4[1]$ is applied, it is the other way around. This means that the sum of the 5- and 7-adic valuations of the denominator can only ever change if one of the two is equal to 0 which explains the shape of the graph showing this sum in Figure 3. The consequence of this observation is that on the one hand the denominators of the sequence $\mathrm{S}(\mathrm{F}_4)[27]$ get large, which makes it unlikely that a period occurs, but on the other hand the sums of the 5- and 7-adic valuations of the denominator stay constant for a large number of steps, which increases the chances for the occurrence of a period. Which of these effects is stronger in the (infinitely) long run, remains an open question.

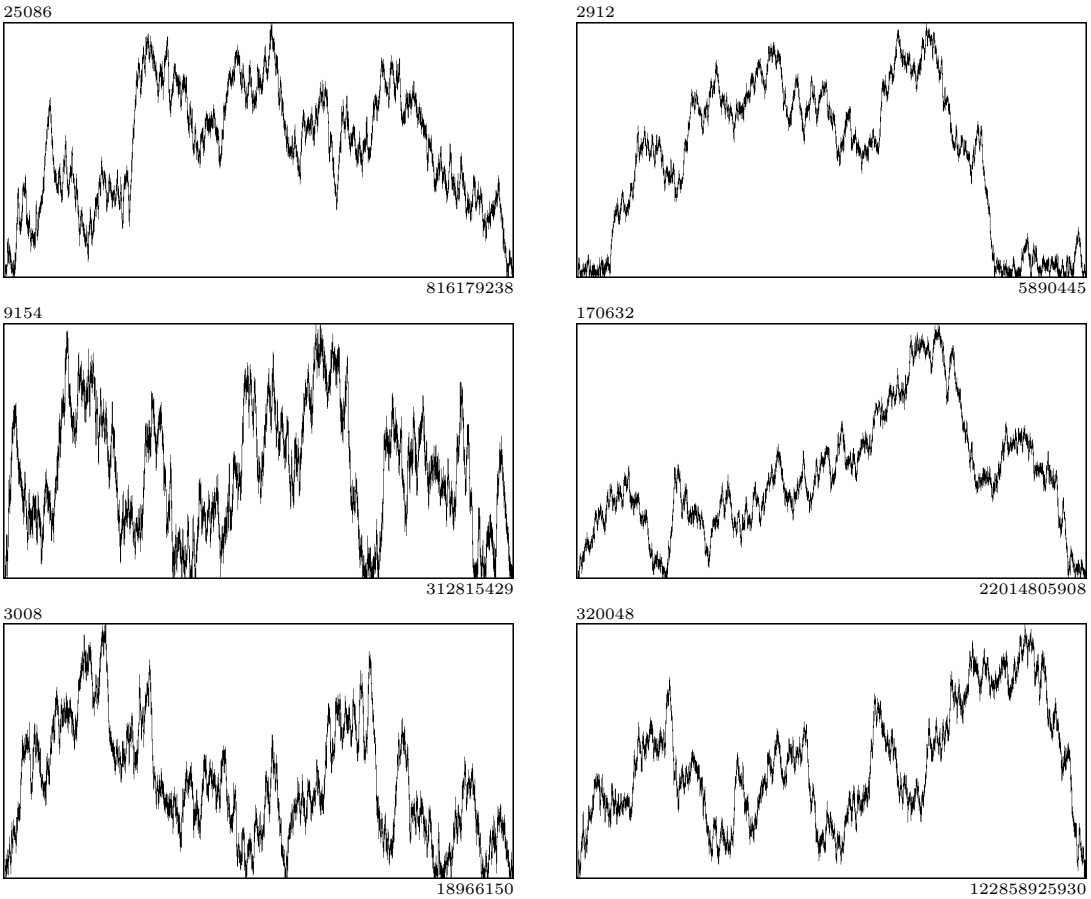

FIGURE 2. The magnitudes (i.e. the 11-, 7-, and 5-adic valuations respectively) of the denominators in the sequences $\mathrm{S}(\mathrm{F}_1)[27]$ (top row), $\mathrm{S}(\mathrm{F}_2)[27]$ (middle row), and $\mathrm{S}(\mathrm{F}_3)[27]$ (bottom row). The left column shows the initial parts and the right column shows the periodic parts of the respective sequences.

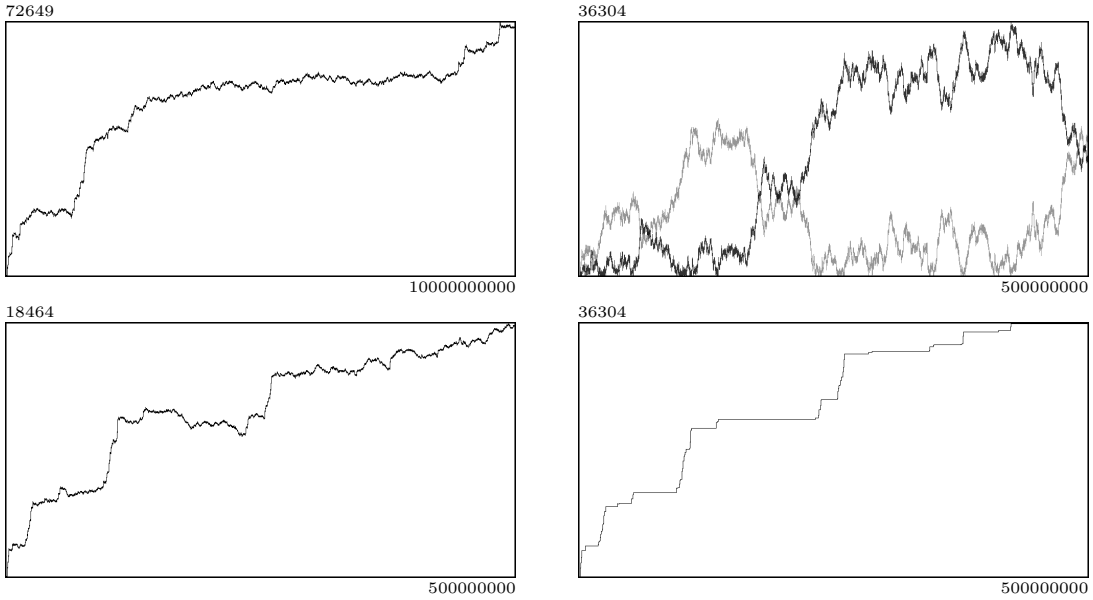

FIGURE 3. The two images in the left column show the magnitudes (i.e. the number of digits in base 35) of the denominators of the first 10^{10} and $5 \cdot 10^8$ entries of the sequences $\mathrm{S}(\mathrm{F}_4)[27]$ respectively. The top right image shows the 5- (dark gray) and 7-adic valuations (light gray) of the denominators and the bottom right image shows their sums. It can be seen that changes (which are mostly increases) in the sum only occur, if one of the two valuations is equal to 0.

Comparing the two conditions

$$B \in \mathbb{Z} \tag{7.131}$$

$$|B| < p^p \tag{7.132}$$

of Conjecture 7.10 (1) one can see that there is a conceptual difference between them that might be significant in explaining the difference between $\mathrm{F}_1, \mathrm{F}_2, \mathrm{F}_3$ on the one hand and F_4 on the other. While the second condition does not include the extremal case $|B| = p^p$ (indeed, by Lemma 7.1 (2) it could not even occur), the first condition does, in the sense explained above. It thus might be necessary to replace the condition $B \in \mathbb{Z}$ by a slightly stronger one which excludes the extremal case in some way. The condition $B \in \mathbb{Z}$ may be understood as a placeholder for a possibly slightly modified condition "in the same spirit", i.e. a condition which also involves only the absolute values of the linear coefficients of the polynomials in a "simple" way.

The following two conjectures state that we do not gain anything by increasing the degrees of the polynomials ...

Conjecture 7.11. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$, *and* $B \in \mathbb{Z}_p$ *the product of all leading coefficients of the polynomials* $\mathrm{F}[r](x)$, $r \in \underline{p}$. *Then,*

(1) $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \quad \Leftrightarrow \quad \mathrm{F} \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}) \wedge B \in \mathbb{Z} \wedge |B| < p^p$
(2) $|\{\mathcal{P}(\mathrm{D}(\mathrm{F})[n]) \mid n \in \mathbb{Z}\}| < \infty$.

... or by further extending the set from where to take the coefficients of the polynomials.

Conjecture 7.12. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} \in \overline{\mathcal{F}}_p(\mathrm{poly})$, *and* $B \in \mathbb{Z}_p$ *the product of all leading coefficients of the polynomials* $\mathrm{F}[r](x)$, $r \in \underline{p}$. *Then,*

(1) $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \quad \Leftrightarrow \quad \mathrm{F} \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}) \wedge B \in \mathbb{Z} \wedge |B| < p^p$
(2) $|\{\mathcal{P}(\mathrm{D}(\mathrm{F})[n]) \mid n \in \mathbb{Z}\}| < \infty$.

An overview of the conjectures above is given in Figure 4 below.

Note that if $\mathrm{F} \in \overline{\mathcal{F}}_p$, then

$$\text{lin-poly}(\mathrm{F}) \Leftrightarrow \mathrm{poly}_{\mathbb{Z}_p,1}(\mathrm{F}) \tag{7.133}$$

by Theorem 4.1 (2) and Lemma 7.1 (2), and if $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{w-canf}, \text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$, then

$$\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \tag{7.134}$$

$$\Leftrightarrow [\mathbb{Q}\cap\mathbb{Z}_p \subseteq \text{UPerP}](\mathrm{F}) \tag{7.135}$$

$$\Leftrightarrow \left\{ \left(\frac{A_\mathrm{F}(D_P)}{p^{|D_P|} - B_\mathrm{F}(D_P)} p^{|D_I|} - A_\mathrm{F}(D_I) \right) \frac{1}{B_\mathrm{F}(D_I)} \mid D_I, D_P \in \mathbf{S}(\text{bnd}_p, \text{fin}) \right\} = \mathbb{Q}\cap\mathbb{Z}_p \tag{7.136}$$

by the "In particular" part of Corollary 7.3. By the same argument the original Collatz conjecture (Conjecture 7.7) is equivalent to the following divisibility question (cf. Eqn. (7.110)):

$$\mathbb{N} \subseteq \text{UPerP}(\mathrm{F}) \quad \wedge \quad \left\{ D \in \mathbf{S}(\text{bnd}_p, \text{fin}) \mid \frac{A_{\mathrm{F}_C}(D)}{p^{|D|} - B_{\mathrm{F}_C}(D)} \in \mathbb{N} \right\} = \{(0,1),(1,0)\}\,. \tag{7.137}$$

Non-rational coefficients. A first general result on the question of ultimate periodicity on $\mathbb{Q}\cap\mathbb{Z}_p$ of polynomial p-adic systems where at least one coefficient of the polynomials is not a rational number, is given by the following theorem. It implies in particular that Conjecture 7.11 (1) and Conjecture 7.12 (1) are equivalent.

Theorem 7.13. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{poly}, \neg\text{poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$. *Then,* $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$.

Proof. Assume to the contrary that $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$ and let $r \in \underline{p}$ such that

$$\mathrm{F}[r] = a_0 + a_1 x + \cdots + a_d x^d \notin (\mathbb{Q}\cap\mathbb{Z}_p)[x]. \tag{7.138}$$

If $\mathrm{F}[r](a) = b$ for some $a \in \mathbb{Q}\cap(r+p\mathbb{Z}_p)$ and $b \in \mathbb{Z}_p\setminus\mathbb{Q}$, then $a \in \text{UPerP}(\mathrm{F})$ by $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$ and hence $(b-b\%p)/p = \mathrm{F}(a) \in \text{UPerP}(\mathrm{F})$ which contradicts $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$, since $(b-b\%p)/p \in \mathbb{Z}_p\setminus\mathbb{Q}$. Thus, $\mathrm{F}[r](\mathbb{Q}\cap(r+p\mathbb{Z}_p)) \subseteq \mathbb{Q}\cap\mathbb{Z}_p$. In particular,

$$b_i \;:=\; \mathrm{F}[r](r+ip) = a_0 + a_1(r+ip) + \cdots + a_d(r+ip)^d \in \mathbb{Q}\cap\mathbb{Z}_p \tag{7.139}$$

for all $i \in [\![1, d+1]\!]$. Thus, $a_0, \ldots, a_d$ solve a system of $d+1$ independent linear equations with coefficients in $\mathbb{Q}\cap\mathbb{Z}_p$. The unique solution of this system (which is $a_0, \ldots, a_d$) can be computed using Gaussian elimination which expresses the solution in terms of the coefficients of the linear equations using only the four basic arithmetical operations. Thus, $a_0, \ldots, a_d \in \mathbb{Q}\cap\mathbb{Z}_p$ which is a contradiction. □

Note that the proof actually shows $[\text{UPerP} \not\subseteq \mathbb{Q}\cap\mathbb{Z}_p](\mathrm{F})$ which of course implies $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$. In addition, one might conjecture that $[\mathbb{Q}\cap\mathbb{Z}_p \not\subseteq \text{UPerP}](\mathrm{F})$ also holds under the assumptions of the theorem but a proof appears to be much harder.

The constant coefficients. A consequence of Theorem 7.2 is that, at least for $(\mathbb{Q}\cap\mathbb{Z}_2)$-linear-polynomial 2-adic system, the constant coefficients of the linear polynomials have no influence on the question of whether all rational numbers have ultimately periodic digit expansions.

Theorem 7.14. *Let* $\mathrm{F} = (a'_0 + b_0 x, a'_1 + b_1 x), \mathrm{G} = (a''_0 + b_0 x, a''_1 + b_1 x) \in \overline{\mathcal{F}}_2(\text{w-canf}, \text{lin-poly})$. *Then,*

$$\pi_{\mathrm{F},\mathrm{G}}(n) = \frac{a'_0 a''_1 - a'_1 a''_0 + n((b_0-2)a''_1 - (b_1-2)a''_0)}{(b_0-2)a'_1 - (b_1-2)a'_0} \tag{7.140}$$

for all $n \in \mathbb{Z}_2$. *In particular, if* $\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{F})$ *and* $\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{G})$, *then* $\pi_{\mathrm{F},\mathrm{G}}(\mathbb{Q}\cap\mathbb{Z}_2) = \mathbb{Q}\cap\mathbb{Z}_2$ *and consequently*

$$\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{F}) \Leftrightarrow \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{G}) \tag{7.141}$$

by the "In particular" part of Lemma 6.1.

Proof. First we observe that it is sufficient to prove Eqn. (7.140) on a dense subset of $\mathbb{Z}_2$, since $\pi_{\mathrm{F},\mathrm{G}}$ is a continuous function by Lemma 3.17 (1) (and so is the right-hand side of Eqn. (7.140)). The subset we will consider is given by the set of all 2-adic integers which have a periodic F-digit expansion which is dense in $\mathbb{Z}_2$, because F has the block property.

Let $D \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \neg\mathrm{emp}, \mathrm{fin})$, and m, n the unique elements of $\mathbb{Z}_p$ satisfying

$$\mathrm{D}(\mathrm{F})[m] = D^{\infty} \tag{7.142}$$

$$\mathrm{D}(\mathrm{G})[n] = D^{\infty} \tag{7.143}$$

(cf. Lemma 3.11). Then, $\pi_{\mathrm{F},\mathrm{G}}(m) = {\psi_{\mathrm{G}}}^{-1} \circ \psi_{\mathrm{F}}(m) = n$ by definition of $\pi_{\mathrm{F},\mathrm{G}}(n)$, and

$$m = \frac{A_{\mathrm{F}}(D)}{2^{|D|} - B_{\mathrm{F}}(D)} \tag{7.144}$$

$$n = \frac{A_{\mathrm{G}}(D)}{2^{|D|} - B_{\mathrm{G}}(D)} \tag{7.145}$$

by Corollary 7.3. We are left to show that

$$\frac{a'_0 a''_1 - a'_1 a''_0 + m((b_0 - 2)a''_1 - (b_1 - 2)a''_0)}{(b_0 - 2)a'_1 - (b_1 - 2)a'_0} = n \tag{7.146}$$

and respectively

$$\begin{aligned} &a'_0 a''_1 (2^{|D|} - B) + A_{\mathrm{F}}(D)((b_0 - 2)a''_1 - (b_1 - 2)a''_0) \\ &\quad = a'_1 a''_0 (2^{|D|} - B) + A_{\mathrm{G}}(D)((b_0 - 2)a'_1 - (b_1 - 2)a'_0) \end{aligned} \tag{7.147}$$

where

$$e \;:=\; \mathrm{cnt}\,(D, 0) \tag{7.148}$$

$$o \;:=\; \mathrm{cnt}\,(D, 1) \tag{7.149}$$

$$B \;:=\; B_{\mathrm{F}}(D) = B_{\mathrm{G}}(D) = \prod_{r=0}^{1} b_r^{\mathrm{cnt}(D,r)} = b_0^{\mathrm{cnt}(D,0)} b_1^{\mathrm{cnt}(D,1)} = {b_0}^e {b_1}^o. \tag{7.150}$$

We compute

$$A_{\mathrm{F}}(D) = \sum_{r=0}^{1} a'_r \sum_{i=0}^{\mathrm{cnt}(D,r)-1} 2^{\mathrm{pos}(D,r)[i]} \prod_{s=0}^{1} b_s^{\mathrm{cnt}(D[\mathrm{pos}(D,r)[i]+1,|D|-1],s)} \tag{7.151}$$

$$\begin{aligned} &= a'_0 \sum_{i=0}^{\mathrm{cnt}(D,0)-1} 2^{\mathrm{pos}(D,0)[i]} b_0^{\mathrm{cnt}(D[\mathrm{pos}(D,0)[i]+1,|D|-1],0)} b_1^{\mathrm{cnt}(D[\mathrm{pos}(D,0)[i]+1,|D|-1],1)} + \\ &\quad a'_1 \sum_{i=0}^{\mathrm{cnt}(D,1)-1} 2^{\mathrm{pos}(D,1)[i]} b_0^{\mathrm{cnt}(D[\mathrm{pos}(D,1)[i]+1,|D|-1],0)} b_1^{\mathrm{cnt}(D[\mathrm{pos}(D,1)[i]+1,|D|-1],1)} \end{aligned} \tag{7.152}$$

$$\begin{aligned} &= a'_0 \sum_{i=0}^{\mathrm{cnt}(D,0)-1} 2^{\mathrm{pos}(D,0)[i]} b_0^{\mathrm{cnt}(D,0)-i-1} b_1^{\mathrm{cnt}(D,1)-\mathrm{pos}(D,0)[i]+i} + \\ &\quad a'_1 \sum_{i=0}^{\mathrm{cnt}(D,1)-1} 2^{\mathrm{pos}(D,1)[i]} b_0^{\mathrm{cnt}(D,0)-\mathrm{pos}(D,1)[i]+i} b_1^{\mathrm{cnt}(D,1)-i-1} \end{aligned} \tag{7.153}$$

$$= a'_0 \sum_{i=0}^{e-1} 2^{E_i} b_0^{e-i-1} b_1^{o-E_i+i} + a'_1 \sum_{i=0}^{o-1} 2^{O_i} b_0^{e-O_i+i} b_1^{o-i-1} \tag{7.154}$$

where

$$E_i \;:=\; \mathrm{pos}\,(D, 0)[i] \text{ for all } i \in \underline{e} \tag{7.155}$$

$$O_i \;:=\; \mathrm{pos}\,(D, 1)[i] \text{ for all } i \in \underline{o}. \tag{7.156}$$

Analogously, we get

$$A_{\mathrm{G}}(D) = a''_0 \sum_{i=0}^{e-1} 2^{E_i} b_0^{e-i-1} b_1^{o-E_i+i} + a''_1 \sum_{i=0}^{o-1} 2^{O_i} b_0^{e-O_i+i} b_1^{o-i-1}. \tag{7.157}$$

Let

$$S_e := \sum_{i=0}^{e-1} 2^{E_i} b_0^{e-i-1} b_1^{o-E_i+i} \tag{7.158}$$

$$S_o := \sum_{i=0}^{o-1} 2^{O_i} b_0^{e-O_i+i} b_1^{o-i-1}. \tag{7.159}$$

Then, our goal Eqn. (7.147) is equivalent to

$$\begin{aligned} &a_0' a_1''(2^{|D|} - B) + (a_0' S_e + a_1' S_o)\left((b_0-2)a_1'' - (b_1-2)a_0''\right) \\ &\quad = a_1' a_0''(2^{|D|} - B) + (a_0'' S_e + a_1'' S_o)\left((b_0-2)a_1' - (b_1-2)a_0'\right) \end{aligned} \tag{7.160}$$

which is again equivalent to

$$(2^{|D|} - B + (b_0-2)S_e + (b_1-2)S_o)(a_0' a_1'' - a_1' a_0'') = 0. \tag{7.161}$$

Since we may assume without loss of generality that $a_0' a_1'' - a_1' a_0'' \neq 0$ (and $\mathbb{Z}_2$ has no zero divisors), we need to show that

$$2^{|D|} - B + (b_0-2)S_e + (b_1-2)S_o = 0 \tag{7.162}$$

which we will prove to be true for every $D \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \mathrm{fin})$ by induction on the length of D.

If $|D| = 0$ then $e = 0$, $o = 0$ and hence $B = 1$, $S_e = 0$, and $S_o = 0$. Altogether, Eqn. (7.162) is clearly true.

Now assume that Eqn. (7.162) holds for some $D \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \mathrm{fin})$ and let $D' \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \mathrm{fin})$ such that $D' = D \cdot (d)$ where $d \in \{0, 1\}$. Furthermore, let

$$e' := \mathrm{cnt}\,(D', 0),\ o' := \mathrm{cnt}\,(D', 1),\ B' := {b_0}^{e'} {b_1}^{o'} \tag{7.163}$$

$$E_i' := \mathrm{pos}\,(D', 0)[i] \text{ for all } i \in \underline{e'},\ O_i' := \mathrm{pos}\,(D', 1)[i] \text{ for all } i \in \underline{o'} \tag{7.164}$$

$$S_e' := \sum_{i=0}^{e'-1} 2^{E_i'} b_0^{e'-i-1} b_1^{o'-E_i'+i},\ S_o' := \sum_{i=0}^{o'-1} 2^{O_i'} b_0^{e'-O_i'+i} b_1^{o'-i-1}. \tag{7.165}$$

On the one hand, if $d = 0$, then

$$e' = e+1,\ o' = o,\ B' = b_0 B, \tag{7.166}$$

$$E_i' = E_i \text{ for all } i \in \underline{e},\ E_e' = |D|\,,\ O_i' = O_i \text{ for all } i \in \underline{o}, \tag{7.167}$$

$$S_e' = b_0 S_e + 2^{|D|},\ S_o' = b_0 S_o \tag{7.168}$$

and

$$\begin{aligned} &2^{|D'|} - B' + (b_0-2)S_e' + (b_1-2)S_o' \\ &\quad = 2 \cdot 2^{|D|} - b_0 B + (b_0-2)\left(b_0 S_e + 2^{|D|}\right) + (b_1-2) b_0 S_o \end{aligned} \tag{7.169}$$

$$= 2 \cdot 2^{|D|} + b_0\left(-B + (b_0-2)S_e + 2^{|D|} + (b_1-2)S_o\right) - 2 \cdot 2^{|D|} \tag{7.170}$$

$$= 0. \tag{7.171}$$

On the other hand, if $d = 1$, then

$$e' = e,\ o' = o+1,\ B' = b_1 B, \tag{7.172}$$

$$E_i' = E_i \text{ for all } i \in \underline{e},\ O_i' = O_i \text{ for all } i \in \underline{o},\ O_o' = |D|\,, \tag{7.173}$$

$$S_e' = b_1 S_e,\ S_o' = b_1 S_o + 2^{|D|} \tag{7.174}$$

and

$$2^{|D'|} - B' + (b_0 - 2)S'_e + (b_1 - 2)S'_o \tag{7.175}$$

$$= 2 \cdot 2^{|D|} - b_1 B + (b_0 - 2)b_1 S_e + (b_1 - 2)\left(b_1 S_o + 2^{|D|}\right) \tag{7.176}$$

$$= 2 \cdot 2^{|D|} + b_1\left(-B + (b_0 - 2)S_e + (b_1 - 2)S_o + 2^{|D|}\right) - 2 \cdot 2^{|D|} \tag{7.177}$$

$$= 0$$

which completes the proof of Eqn. (7.140).

For the "In particular" part we observe that $b_0 \equiv b_1 \equiv 1 \mod 2$, $a'_0 \equiv a''_0 \equiv 0 \mod 2$, and $a'_1 \equiv a''_1 \equiv 1 \mod 2$ by Theorem 4.1 (2) and Lemma 7.1 (2) (note that $\mathrm{F}, \mathrm{G} \in \overline{\mathcal{F}}_2(\text{w-canf})$). Thus

$$a'_0 a''_1 - a'_1 a''_0 \equiv 0 \mod 2 \tag{7.178}$$

$$(b_0 - 2)a''_1 - (b_1 - 2)a''_0 \equiv 1 \mod 2 \tag{7.179}$$

$$(b_0 - 2)a'_1 - (b_1 - 2)a'_0 \equiv 1 \mod 2 \tag{7.180}$$

and hence

$$\pi : \mathbb{Q} \cap \mathbb{Z}_2 \to \mathbb{Q} \cap \mathbb{Z}_2 \tag{7.181}$$

$$n \mapsto \frac{a'_0 a''_1 - a'_1 a''_0 + n((b_0 - 2)a''_1 - (b_1 - 2)a''_0)}{(b_0 - 2)a'_1 - (b_1 - 2)a'_0}$$

is bijective. □

A natural follow-up question is whether the "In particular" part of the previous theorem is true for general $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems, i.e. if the constant coefficients of the linear polynomials which define the p-adic systems can always be neglected when dealing with the question of whether the p-adic system is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_p$. If true, this would be a first step in proving the general conjectures 7.9 – 7.12. At least for $p = 2$, which includes the Collatz case, this first step has already been made. For $p \geq 3$ the situation becomes more difficult as there doesn't seem to exist a simple formula for $\pi_{\mathrm{F},\mathrm{G}}(n)$ in general. Nevertheless, we state the following conjecture which would probably be a good start for future work on this matter.

Conjecture 7.15. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{F} = (a'_0 + b_0 x, \ldots, a'_{p-1} + b_{p-1}x), \mathrm{G} = (a''_0 + b_0 x, \ldots, a''_{p-1} + b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$. *Then,* $\pi_{\mathrm{F},\mathrm{G}}(\mathbb{Q} \cap \mathbb{Z}_p) = \mathbb{Q} \cap \mathbb{Z}_p$ *and consequently*

$$\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \Leftrightarrow \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{G}) \tag{7.182}$$

by the "In particular" part of Lemma 6.1.

Swapping polynomials. In the last subsection we have established that, at least in the case $p = 2$, the constant coefficients of the linear polynomials defining a $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic system F have no influence on whether F is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_p$. Here we will prove, again for $p = 2$, that the specific positions of the linear coefficients can also be neglected, which is another step closer to the proof of the general conjectures 7.9 – 7.12. Before we can formulate our result, we need to add a little flexibility to the definition of $\pi_{\mathrm{F},\mathrm{G}}$ in that we allow the digits of the F-digit expansions to be permuted before interpreting them as G-digit expansions. For two p-adic systems F and G and for a bijective function $\sigma : \underline{p} \to \underline{p}$ (which extends naturally to $\mathbf{S}(\mathrm{bnd}_{\underline{p}})$, cf. the end of the subsection on sequences in Section 2) let

$$\pi_{\mathrm{F},\sigma,\mathrm{G}} := {\psi_{\mathrm{G}}}^{-1} \circ \sigma \circ \psi_{\mathrm{F}} : \mathbb{Z}_p \to \mathbb{Z}_p. \tag{7.183}$$

If σ is the identity function, then clearly $\pi_{\mathrm{F},\sigma,\mathrm{G}} = \pi_{\mathrm{F},\mathrm{G}}$. Note that here we formulate our result for a specific choice for the constant coefficients. In combination with Theorem 7.14 a general result involving arbitrary constant coefficients can easily be achieved since $\pi_{\mathrm{G},\tau,\mathrm{H}} \circ \pi_{\mathrm{F},\sigma,\mathrm{G}} = \pi_{\mathrm{F},\tau\circ\sigma,\mathrm{H}}$.

Theorem 7.16. *Let* $\mathrm{F} = (b_0 x, 1 + b_1 x), \mathrm{G} = (b_1 x, 1 + b_0 x) \in \overline{\mathcal{F}}_2(\text{lin-poly})$*, and* $\sigma : \{0,1\} \to \{0,1\}$*,* $0 \mapsto 1$*,* $1 \mapsto 0$*. Then,*

$$\pi_{\mathrm{F},\sigma,\mathrm{G}}(n) = \frac{1 + n(b_1 - 2)}{2 - b_0} \tag{7.184}$$

for all $n \in \mathbb{Z}_2$*. In particular, if* $\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$ *and* $\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{G})$*, then* $\pi_{\mathrm{F},\sigma,\mathrm{G}}(\mathbb{Q}\cap\mathbb{Z}_2) = \mathbb{Q}\cap\mathbb{Z}_2$ *and consequently,*

$$\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{F}) \Leftrightarrow \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}(\mathrm{G}) \tag{7.185}$$

by the "In particular" part of Lemma 6.1.

Note that we actually need a slight generalization of Lemma 6.1 to account for the permutation σ in $\pi_{\mathrm{F},\sigma,\mathrm{G}}$. The proof can easily be adapted to show that the lemma also holds if $\pi_{\mathrm{F},\mathrm{G}}$ is replaced by $\pi_{\mathrm{F},\sigma,\mathrm{G}}$, if the set B from the assumptions is stable under σ, i.e. if $\sigma(B) = B$. For $B := \left\{S \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}) \mid \mathrm{per}(S)\right\}$, $B := \left\{S \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}) \mid \mathrm{uper}(S)\right\}$, and $B := \left\{S \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}) \mid \mathrm{aper}(S)\right\}$ this is true for every σ which implies that the "In particular" part of the lemma holds for $\pi_{\mathrm{F},\sigma,\mathrm{G}}$ without additional assumptions.

Proof of Theorem 7.16. As we did in the proof of Theorem 7.14, we again only consider a dense subset of $\mathbb{Z}_2$ (clearly, $\pi_{\mathrm{F},\sigma,\mathrm{G}}$ and the right-hand side of Eqn. (7.184) are also continuous functions) which will again be the set of all 2-adic integers which have a periodic F-digit expansion.

Let $D \in \mathbf{S}(\mathrm{bnd}_{\underline{2}}, \neg\mathrm{emp}, \mathrm{fin})$, and m, n the unique elements of $\mathbb{Z}_p$ satisfying

$$\mathrm{D}(\mathrm{F})[m] = D^\infty \tag{7.186}$$

$$\mathrm{D}(\mathrm{G})[n] = \sigma(D^\infty) \tag{7.187}$$

(cf. Lemma 3.11). Then, $\pi_{\mathrm{F},\sigma,\mathrm{G}}(m) = {\psi_{\mathrm{G}}}^{-1} \circ \sigma \circ \psi_{\mathrm{F}}(m) = n$ by definition of $\pi_{\mathrm{F},\sigma,\mathrm{G}}(n)$, and

$$m = \frac{A_{\mathrm{F}}(D)}{2^{|D|} - B_{\mathrm{F}}(D)} \tag{7.188}$$

$$n = \frac{A_{\mathrm{G}}(\sigma(D))}{2^{|D|} - B_{\mathrm{G}}(\sigma(D))} \tag{7.189}$$

by Corollary 7.3. Note that,

$$B_{\mathrm{F}}(D) = b_0^{\mathrm{cnt}(D,0)} b_1^{\mathrm{cnt}(D,1)} = b_1^{\mathrm{cnt}(\sigma(D),0)} b_0^{\mathrm{cnt}(\sigma(D),1)} = B_{\mathrm{G}}(\sigma(D)). \tag{7.190}$$

We are thus left to show that

$$\frac{1 + m(b_1 - 2)}{2 - b_0} = n \tag{7.191}$$

and respectively

$$2^{|D|} - {b_0}^e {b_1}^o + (b_0 - 2)A_{\mathrm{G}}(\sigma(D)) + (b_1 - 2)A_{\mathrm{F}}(D) = 0 \tag{7.192}$$

where

$$e := \mathrm{cnt}\,(D, 0) \tag{7.193}$$

$$o := \mathrm{cnt}\,(D, 1). \tag{7.194}$$

As in the proof of Theorem 7.14 we compute

$$A_{\mathrm{F}}(D) = \sum_{i=0}^{o-1} 2^{O_i} b_0^{e - O_i + i} b_1^{o-i-1} \tag{7.195}$$

$$A_{\mathrm{G}}(\sigma(D)) = \sum_{i=0}^{e-1} 2^{E_i} b_0^{e-i-1} b_1^{o - E_i + i} \tag{7.196}$$

where

$$E_i := \mathrm{pos}\,(D, 0)[i] \text{ for all } i \in \underline{e} \tag{7.197}$$

$$O_i := \mathrm{pos}\,(D, 1)[i] \text{ for all } i \in \underline{o}. \tag{7.198}$$

Thus, our goal Eqn. (7.192) is equivalent to

$$2^{|D|} - {b_0}^e {b_1}^o + (b_0 - 2)\sum_{i=0}^{e-1} 2^{E_i} b_0^{e-i-1} b_1^{o-E_i+i} + (b_1 - 2)\sum_{i=0}^{o-1} 2^{O_i} b_0^{e-O_i+i} b_1^{o-i-1} = 0 \tag{7.199}$$

which is identical to Eqn. (7.162) which we already proved. □

As we did after Theorem 7.14, we again formulate a conjecture on how to generalize the previous theorem.

Conjecture 7.17. *Let $2 \leq p \in \mathbb{N}$, $\sigma : \underline{p} \to \underline{p}$ a bijective function, and $\mathrm{F} = (b_0 x, \ldots, b_{p-1} x), \mathrm{G} = (b_{\sigma(0)} x, \ldots, b_{\sigma(p-1)} x) \in \overline{\mathcal{F}}_p(\text{lin-poly})$. Then, $\pi_{\mathrm{F},\sigma,\mathrm{G}}(\mathbb{Q} \cap \mathbb{Z}_p) = \mathbb{Q} \cap \mathbb{Z}_p$ and consequently,*

$$\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F}) \Leftrightarrow \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{G}) \tag{7.200}$$

by the "In particular" part of (the mentioned generalization of) Lemma 6.1.

We give an example which combines the statements of Theorem 7.14 and Theorem 7.16 to illustrate how to compute $\pi_{\mathrm{F},\sigma,\mathrm{G}}(n)$ in a general situation.

Example 7.18. Let $\mathrm{F}_1 := (5x + 4, -7x + 19)$, $\mathrm{F}_2 := (5x, -7x + 1)$, $\mathrm{F}_3 := (-7x, 5x + 1)$, $\mathrm{F}_4 := (-7x - 12, 5x + 3)$, and $\sigma : \{0, 1\} \to \{0, 1\}$, $0 \mapsto 1$, $1 \mapsto 0$. Then, Theorem 7.14 and Theorem 7.16 imply that

$$\pi_{\mathrm{F}_1,\mathrm{F}_2}(n) = \frac{4 + 3n}{93}, \qquad \pi_{\mathrm{F}_2,\sigma,\mathrm{F}_3}(n) \qquad = \frac{-1 + 9n}{3}, \qquad \pi_{\mathrm{F}_3,\mathrm{F}_4}(n) = \frac{-12 - 9n}{9} \tag{7.201}$$

and consequently

$$\pi_{\mathrm{F}_1,\sigma,\mathrm{F}_4}(n) = \pi_{\mathrm{F}_3,\mathrm{F}_4}(n) \circ \pi_{\mathrm{F}_2,\sigma,\mathrm{F}_3}(n) \circ \pi_{\mathrm{F}_1,\mathrm{F}_2}(n) = \frac{-35 - 3n}{31}. \tag{7.202}$$

Indeed, if $m := \frac{156065447}{59288775}$ and $n := -\frac{847767822}{612650675}$, then $\frac{-35-3m}{31} = n$ and

$$\mathrm{F}_1(m) = (1, 0, 1, 0) \cdot (1, 1, 0, 1, 0, 0, 0, 1)^\infty \tag{7.203}$$

$$\mathrm{F}_4(n) = (0, 1, 0, 1) \cdot (0, 0, 1, 0, 1, 1, 1, 0)^\infty. \tag{7.204}$$

The contractive and expansive cases. In the previous subsections we have proven for $p = 2$ and conjectured for $p \geq 3$ that neither the constant coefficients nor the order of the linear coefficients of the polynomials defining a $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic system matter when it comes to the question of whether the p-adic system is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_p$. These observations are closely related to the conjectures 7.9 – 7.12 which essentially state that the answer to this question only depends on the product of the linear coefficients. In the special cases where the $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic system is either contractive or expansive, we can even go further and prove some of the conjectures under these additional constraints. Among other things the following theorem characterizes contractive and expansive $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems.

Theorem 7.19. *Let $2 \leq p \in \mathbb{N}$, $\mathrm{F} = (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1} x) \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$. Then,*

(1) $\text{contr}(\mathrm{F}) \quad \Leftrightarrow \quad \forall\, r \in \underline{p} : |b_r| < p$
(2) $\exp(\mathrm{F}) \quad \Leftrightarrow \quad \forall\, r \in \underline{p} : |b_r| > p.$
(3) $\text{mix}(\mathrm{F}) \quad \Leftrightarrow \quad \exists\, r \in \underline{p} : |b_r| < p \wedge \exists\, r \in \underline{p} : |b_r| > p$
(4) $\text{d-contr}(\mathrm{F}) \quad \Leftrightarrow \quad \forall\, r \in \underline{p} : a_r, b_r \in \mathbb{Z}$
(5) $\neg\text{d-exp}(\mathrm{F})$.

Proof. Let

$$M := \max\left\{ \left| \frac{|a_r| + p - 1}{|b_r| - p} \right| \mid r \in \underline{p} \right\}. \tag{7.205}$$

Note that M is well-defined since $|b_r| \neq p$ for all $r \in \underline{p}$ by Theorem 4.1 (2) and Lemma 7.1 (2).
(1), "⇒": Assume to the contrary that $|b_r| > p$ for some $r \in \underline{p}$ and let $m \in \mathbb{N}$ such that

$$m > \frac{|a_r| + p - 1 - r(|b_r| - p)}{p(|b_r| - p)} \quad \left(\Leftrightarrow \frac{|b_r|\,(mp + r) - |a_r| - p + 1}{p} > mp + r \right). \tag{7.206}$$

Then,

$$|\mathrm{F}(mp+r)| = \left|\frac{a_r + b_r(mp+r) - (a_r + b_r(mp+r))\%p}{p}\right| \tag{7.207}$$

$$\geq \frac{|b_r|\,(mp+r) - |a_r| - p + 1}{p} \tag{7.208}$$

$$> mp + r = |mp+r| \tag{7.209}$$

and hence F cannot be contractive.
(1), "⇐": We compute

$$|n| > M \Rightarrow |n|\,\big||b_{n\%p}| - p\big| > |a_{n\%p}| + p - 1 \tag{7.210}$$

$$\Leftrightarrow |n|\,(p - |b_{n\%p}|) > |a_{n\%p}| + p - 1 \tag{7.211}$$

$$\Leftrightarrow |n|\,p > |a_{n\%p}| + |b_{n\%p}n| + p - 1 \tag{7.212}$$

$$\Rightarrow |n|\,p > |a_{n\%p}| + |b_{n\%p}n| + (a_{n\%p} + b_{n\%p}n)\%p \tag{7.213}$$

$$\Rightarrow |n| > \left|\frac{a_{n\%p} + b_{n\%p}n - (a_{n\%p} + b_{n\%p}n)\%p}{p}\right| = \mathrm{F}(n). \tag{7.214}$$

(2), "⇒": Assume to the contrary that $|b_r| < p$ for some $r \in \underline{p}$ and let $m \in \mathbb{N}$ such that

$$m > \frac{|a_r| + p - 1 - r(p - |b_r|)}{p(p - |b_r|)} \quad \left(\Leftrightarrow \frac{|b_r|\,(mp+r) + |a_r| + p - 1}{p} < mp + r\right). \tag{7.215}$$

Then,

$$|\mathrm{F}(mp+r)| = \left|\frac{a_r + b_r(mp+r) - (a_r + b_r(mp+r))\%p}{p}\right| \tag{7.216}$$

$$\leq \frac{|b_r|\,(mp+r) + |a_r| + p - 1}{p} \tag{7.217}$$

$$< mp + r = |mp+r| \tag{7.218}$$

and hence F cannot be expansive.
(2), "⇐": We compute

$$|n| > M \Rightarrow |n|\,\big||b_{n\%p}| - p\big| > |a_{n\%p}| + p - 1 \tag{7.219}$$

$$\Leftrightarrow |n|\,(|b_{n\%p}| - p) > |a_{n\%p}| + p - 1 \tag{7.220}$$

$$\Leftrightarrow |n|\,p < -|a_{n\%p}| + |b_{n\%p}n| - p + 1 \tag{7.221}$$

$$\Rightarrow |n|\,p < -|a_{n\%p}| + |b_{n\%p}n| - (a_{n\%p} + b_{n\%p}n)\%p \tag{7.222}$$

$$\Rightarrow |n| < \left|\frac{a_{n\%p} + b_{n\%p}n - (a_{n\%p} + b_{n\%p}n)\%p}{p}\right| = \mathrm{F}(n). \tag{7.223}$$

Note that we also could have referred to Theorem 6.3 as (2), "⇐" is a special case of the theorem.
(3): Follows directly from (1) and (2).
(4), "⇒": Assume to the contrary that $a_r = a/b$ with $(a,b) \in \mathbb{Z} \times \mathbb{N}$ coprime, $b_r = c/d$ with $(c,d) \in \mathbb{Z} \times \mathbb{N}$ coprime for some $r \in \underline{p}$, and $(b,d) \neq (1,1)$. Since $a/b = a_r \in \mathbb{Z}_p$ and a and b are coprime it follows that also p and b are coprime. Thus, there are $x, y \in \mathbb{Z}$ such that $xp + yb = 1$ by Bézout's Lemma.

First we consider the case $d \neq 1$. Let $n := r - rxp = ryb \in \mathbb{Z}$. Then, $n \in (r + p\mathbb{Z}) \cap b\mathbb{Z}$ and we get

$$\mathrm{F}(n) = \frac{an/b + c/d - (an/b + c/d)\%p}{p} \tag{7.224}$$

with $an/b - (an/b + c/d)\%p \in \mathbb{Z}$ and $c/d \in \mathbb{Q} \setminus \mathbb{Z}$ (since $d \neq 1$). Thus, $\mathrm{F}(n) \in \mathbb{Q} \setminus \mathbb{Z}$ but $n \in \mathbb{Z}$ which contradicts d-contr(F).

For the case $d = 1$ let $n := r - rxp + p = ryb + p$. Then, $n \in (r + p\mathbb{Z})$ but $n \notin b\mathbb{Z}$ (since $b \neq 1$ and p and b are coprime) and we get $c/d - (an/b + c/d)\%p \in \mathbb{Z}$ and $an/b \in \mathbb{Q} \setminus \mathbb{Z}$ (since $n \notin b\mathbb{Z}$ and a and b are coprime). Thus, $\mathrm{F}(n) \in \mathbb{Q} \setminus \mathbb{Z}$ but $n \in \mathbb{Z}$, which again contradicts d-contr(F).
(4), "$\Leftarrow$": Follows directly from the definitions.
(5): Let $(a, b) \in \mathbb{Z} \times \mathbb{N}$ coprime with $a_0 = a/b$ and $(c, d) \in \mathbb{Z} \times \mathbb{N}$ coprime with $b_0 = c/d$. Furthermore, let $u, v \in \mathbb{Z}$ such that

$$apu + c \equiv 0 \mod \gcd(b, d) \tag{7.225}$$

$$\gcd(\gcd(b, d)v + u, d/\gcd(b, d)) = 1. \tag{7.226}$$

Such u and v exist because of two basic facts from elementary number theory, namely

$$\forall\, m \in \mathbb{N} : \forall\, a, b \in \mathbb{Z} : \quad (\exists\, x \in \mathbb{Z} : a + bx \equiv 0 \mod m \quad \Leftrightarrow \quad \gcd(m, b) \mid a) \tag{7.227}$$

$$\forall\, a, b \in \mathbb{Z} : \forall\, 0 \neq c \in \mathbb{Z} : \quad (\exists\, x \in \mathbb{Z} : \gcd(a + bx, c) = 1 \quad \Leftrightarrow \quad \gcd(a, b, c) = 1)\,. \tag{7.228}$$

To see that the conditions of these two statements are satisfied, note that $\gcd(p, b) = 1$ by Lemma 7.1, and hence $\gcd(\gcd(b, d), ap) = 1 \mid c$, and that $\gcd(\gcd(b, d), u) = 1$ (because the equation $c + ux \equiv 0 \mod \gcd(b, d)$ has a solution, viz. ap, and $\gcd(\gcd(b, d), c) = 1$) and hence $\gcd(u, \gcd(b, d), d/\gcd(b, d)) = 1$. Using u and v we set

$$n := \frac{p(u + v\gcd(b, d))b/\gcd(b, d)}{d/\gcd(b, d)} \in \mathbb{Q} \cap p\mathbb{Z}_p. \tag{7.229}$$

By definition of u and v we get $\gcd(p(u + v\gcd(b, d))b/\gcd(b, d), d/\gcd(b, d)) = 1$, which implies that n as given above is in lowest terms. Since $n\%p = 0$ we get

$$\mathrm{F}(n) = \frac{1}{p}\left(\frac{an}{b} + \frac{c}{d} - \left(\frac{an}{b} + \frac{c}{d}\right)\%p\right) \tag{7.230}$$

$$= \frac{1}{p}\left(\frac{(apu + c)/\gcd(b, d) + apv}{d/\gcd(b, d)} - \left(\frac{an}{b} + \frac{c}{d}\right)\%p\right). \tag{7.231}$$

Thus, the denominator of $\mathrm{F}(n)$ in lowest terms is at most (in absolute value) $d/\gcd(b, d)$ (since $\gcd(b, d)$ divides $apu + c$ by definition of u) which is the denominator of n in lowest terms. □

For contractive $\mathbb{Z}$-linear-polynomial- and for expansive $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems this settles the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$ (cf. Conjecture 7.9).

Corollary 7.20. *Let* $2 \leq p \in \mathbb{N}$, $\mathrm{F} = (a_0 + b_0x, \ldots, a_{p-1} + b_{p-1}x) \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$. *Then,*

(1) $\forall\, r \in \underline{p} : a_r, b_r \in \mathbb{Z} \wedge |b_r| < p \quad \Rightarrow \quad \text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$
(2) $\forall\, r \in \underline{p} : |b_r| > p \quad \Rightarrow \quad \neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$.

Proof. Follows from Theorem 7.19, Lemma 6.2, and the "In particular" part of Corollary 7.3. □

The mixed case. There are two mixed cases to be considered: a $(\mathbb{Q}\cap\mathbb{Z}_p)$-linear-polynomial p-adic system F could be of mixed type (i.e. mix(F)) or mixing denominators (i.e. d-mix(F)). To the best knowledge of the author the question for ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$ has not been settled for even a single such F. The most famous example is of course given by $\mathrm{F}_C = (x, 3x+1)$ of the Collatz conjecture which is of mixed type by Theorem 7.19 (3). While it appears to be completely out of reach to answer whether or not $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_2}$ holds for F_C at the moment, the general framework that is p-adic systems, might provide examples that are easier to tackle without being "trivial" like in the contractive (e.g. $\mathrm{F}_p = (x, \ldots, x)$, standard base p) or expansive (e.g. $\mathrm{F} = (3x, 3x + 1)$) cases which are settled by Corollary 7.20. Before we list some of these examples we will summarize what has already been achieved in this and in the previous section.

Corollary 7.21. *Let* $2 \leq p \in \mathbb{N}$ *and* $\mathrm{F} \in \overline{\mathcal{F}}_p(\text{poly}_{\mathbb{Q}\cap\mathbb{Z}_p})$. *Then,*

(1) *If* $\mathrm{F}[r] = a_r + b_rx$ *with* $a_r, b_r \in \mathbb{Z}$ *and* $|b_r| < p$ *for all* $r \in \underline{p}$, *then* $\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$
(2) *If either* $\mathrm{F}[r]$ *is of degree* 2 *or higher or* $\mathrm{F}[r] = a_r + b_rx$ *with* $|b_r| > p$ *for all* $r \in \underline{p}$, *then* $\neg\text{uper-on}_{\mathbb{Q}\cap\mathbb{Z}_p}(\mathrm{F})$.

Proof. Follows directly from Theorem 6.3, Theorem 7.19, and Corollary 7.20. □

Progress on conjectures: summary and open questions. Figure 4 below gives an overview of the status of the conjectures 7.9 – 7.12 and the mixed case. Related results and conjectures are given in Theorem 7.14, Conjecture 7.15, Theorem 7.16, Conjecture 7.17, Theorem 7.19, and Corollary 7.21.

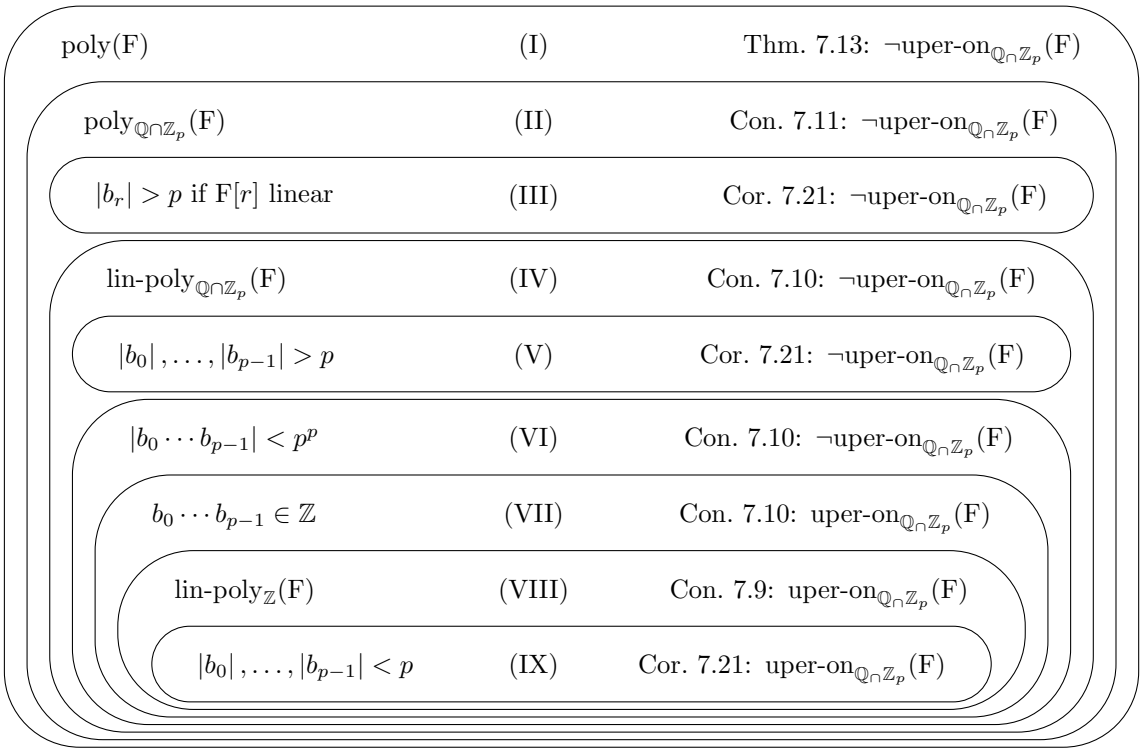

FIGURE 4. Overview of settled and open cases on the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$ of a p-adic system F, where b_r is the linear coefficient of the polynomial F[r] for $r \in \underline{p}$.

Referring to the different regions in Figure 4 we give a list of possibly interesting examples of p-adic systems, some of which only just fall into the respective cases.

(I) $\mathrm{F} = (a_0 + b_0x, a_1 + b_1x)$, where $\{1\} \neq \{a_0, b_0, a_1, b_1\} \subseteq \{1, \sqrt{17}, -\sqrt{17}\}$
$\mathrm{F} = (a_0 + b_0x, \ldots, a_2 + b_2x)$, where $\{1\} \neq \{a_0, b_0, \ldots, a_2, b_2\} \subseteq \{1, \sqrt{-2}, -\sqrt{-2}\}$
$\mathrm{F} = (a_0 + b_0x, \ldots, a_4 + b_4x)$, where $\{1\} \neq \{a_0, b_0, \ldots, a_4, b_4\} \subseteq \{1, \mathrm{i}, -\mathrm{i}\}$

(II) $\mathrm{F} = (x^2 + x) \cdot (x)^{p-1}$
$\mathrm{F} = (x^{ap} + x)^{p-1} \cdot ((p-1)x)$, where $a \in \mathbb{N}$ (say, $a = 1000$)

(III) $\mathrm{F} = (3x, x^2 + x)$
$\mathrm{F} = (x^2 + x, 3x)$
$\mathrm{F} = (x^2 + x, x^2 + x)$

(IV) $\mathrm{F} = ((p^p + 1)x) \cdot (x)^{p-1}$
$\mathrm{F} = ((p + (p = 2\ ?\ 3 : 1))x)^{p-1}((p-1)x)$

(V) $\mathrm{F} = ((p+1)x)^p$
$\mathrm{F} = ((p^p + 1)x)^p$

(VI) $\mathrm{F} = (1/(p+1)x, (p-1)x) \cdot (x)^{p-2}$
$\mathrm{F} = (1/(p+1)x)^{\lfloor p/2 \rfloor + 1} \cdot ((p+1)x)^{\lceil p/2 \rceil - 1}$

(VII) $\mathrm{F} = (1/(p+1)x, (p+1)x) \cdot (x)^{p-2}$
$\mathrm{F} = (1/(p+1)x)^{\lfloor p/2 \rfloor} \cdot ((p+1)x)^{\lceil p/2 \rceil}$

(VIII) $\mathrm{F} = ((p+1)x) \cdot (x)^{p-1}$

$$\begin{aligned}
&\mathrm{F} = ((p+1)x)^{\lfloor p/2\rfloor} \cdot ((p-1)x)^{\lceil p/2\rceil}\\
&\mathrm{F} = ((p^p-1)x)\cdot(x)^{p-1}\\
\text{(IX)}\quad &\mathrm{F} = (x)^p \text{ (standard base } p)\\
&\mathrm{F} = ((p-1)x)^p.
\end{aligned}$$

Note that (cf. Example 5.5),

$$\sqrt{17} \in \{\ldots 0010111, \ldots 1101001\} \subseteq \mathbb{Z}_2 \tag{7.232}$$

$$\sqrt{-2} \in \{\ldots 0200211, \ldots 2022012\} \subseteq \mathbb{Z}_3 \tag{7.233}$$

$$\mathrm{i} \in \{\ldots 2431212, \ldots 2013233\} \subseteq \mathbb{Z}_5. \tag{7.234}$$

Generalizations. The previous subsections of this section deal with the question of ultimate periodicity on a specific set ($\mathbb{Q}\cap\mathbb{Z}_p$) for a specific kind of p-adic systems (mostly ($\mathbb{Q}\cap\mathbb{Z}_p$)-linear-polynomial ones). While the set $\mathbb{Q}$ of rational numbers is certainly special among all dense subsets of $\mathbb{Z}_p$ and polynomial functions are also special among all functions on $\mathbb{Z}_p$, there is no obvious reason why this combination of "subset of $\mathbb{Z}_p$" and "class of functions on $\mathbb{Z}_p$" should be the only one to result in interesting patterns and relations. Analyzing previous results, the following generalization appears to be natural: for $2 \le p \in \mathbb{N}$ and $A \subseteq \overline{\mathcal{F}}_p$ let

$$\mathrm{PerP}(A) := \bigcup_{\mathrm{F}\in A} \mathrm{PerP}(\mathrm{F}),\ \mathrm{UPerP}(A) := \bigcup_{\mathrm{F}\in A} \mathrm{UPerP}(\mathrm{F}),\ \mathrm{APerP}(A) := \bigcup_{\mathrm{F}\in A} \mathrm{APerP}(\mathrm{F}). \tag{7.235}$$

We say that an element F of A *generates the periodic, ultimately periodic, or aperiodic points of* A, if $\mathrm{PerP}(\mathrm{F}) = \mathrm{PerP}(A)$, $\mathrm{UPerP}(\mathrm{F}) = \mathrm{UPerP}(A)$, or $\mathrm{APerP}(\mathrm{F}) = \mathrm{APerP}(A)$ respectively, and denote by PerP-Gen(A), UPerP-Gen(A), and APerP-Gen(A) the respective sets of all these $\mathrm{F} \in A$.
By the "In particular" part of Corollary 7.3 we get

$$\mathrm{UPerP}(\overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})) = \mathbb{Q}\cap\mathbb{Z}_p \tag{7.236}$$

and Conjecture 7.10 can be expressed as

$$\begin{aligned}
\mathrm{UPerP\text{-}Gen}(\overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p})) \stackrel{?}{=} \Big\{ &\mathrm{F} \in \overline{\mathcal{F}}_p(\text{lin-poly}_{\mathbb{Q}\cap\mathbb{Z}_p}) \mid\\
&\mathrm{F} = (a_0 + b_0 x, \ldots, a_{p-1} + b_{p-1}x)\\
&b_0 \cdots b_{p-1} \in \mathbb{Z}\\
&|b_0 \cdots b_{p-1}| < p^p \Big\}.
\end{aligned} \tag{7.237}$$

Related results and conjectures are given in Theorem 7.14, Conjecture 7.15, Theorem 7.16, Conjecture 7.17, Theorem 7.19, and Corollary 7.20. Generalizing Conjecture 7.10 one might try to study any of the sets PerP(A), UPerP(A), APerP(A), PerP-Gen(A), UPerP-Gen(A), or APerP-Gen(A) for other classes A of p-adic systems, such as $\overline{\mathcal{F}}_p(\mathrm{poly}_{C,D})$ where C is a (possibly dense) subset of $\mathbb{Z}_p$, and $D \subseteq \mathbb{N}_0$ is a set of allowed degrees, some class of rational functions on $\mathbb{Z}_p$ (Section 4), p-adic systems defined by certain permutation polynomials (Section 8), etc.

8. Permutation polynomials and trees of cycles

In Section 4 we proved that "almost all" $\mathbb{Z}_p$-polynomial p-fibred functions are actually p-fibred systems (cf. Theorem 4.1 and Theorem 4.8) giving us a multitude of examples. In addition to this class, the different interpretations of p-adic systems discussed in Section 3 allow us to find even more p-adic systems that are essentially different from those we already know. This new class is again defined by polynomials but in a very different way. It turns out that p-adic permutations, which we proved to be just a different interpretation of p-adic systems (cf. Theorem 3.18), can be polynomial functions and are thus defined by a single polynomial in $\mathbb{Z}_p[x]$ in this case (in the following we will use the terms "polynomial" and "polynomial function" interchangeably). These polynomials are exactly what is commonly known as permutation polynomials. A polynomial

$f \in \mathbb{Z}_p[x]$ is called a *p-permutation polynomial*, where $2 \leq p \in \mathbb{N}$, if the following holds:

$$f_1 \text{ is the identity on } \mathbb{Z}_p/p\mathbb{Z}_p \tag{8.1}$$

$$\forall\, k \in \mathbb{N} : f_k \text{ is bijective,} \tag{8.2}$$

where

$$\begin{aligned} f_k : \mathbb{Z}_p/p^k\mathbb{Z}_p &\to \mathbb{Z}_p/p^k\mathbb{Z}_p. \\ x + p^k\mathbb{Z}_p &\mapsto f(x) + p^k\mathbb{Z}_p \end{aligned} \tag{8.3}$$

Please note that we slightly adapted the usual notion of permutation polynomials (cf. [26, 37, 38, 49]) which usually are required only to satisfy the second condition but not the first. We need the first condition because p-adic permutations must satisfy Eqn. (3.93). Using the following lemma which can also be found in [26], it is very easy to test whether a given polynomial is a p-permutation polynomial.

Lemma 8.1. *Let $2 \leq p \in \mathbb{N}$ and $f \in \mathbb{Z}_p[x]$. Then f is a p-permutation polynomial if and only if f_1 is the identity on $\mathbb{Z}_p/p\mathbb{Z}_p$ and f_2 is bijective.*

If $\pi := f$, then Eqn. (8.1) and Eqn. (8.2) are clearly equivalent to Eqn. (3.93) and Eqn. (3.94) respectively which proves the following theorem.

Theorem 8.2. *Let $2 \leq p \in \mathbb{N}$ and $f \in \mathbb{Z}_p[x]$. Then f is a p-permutation polynomial if and only if f is a p-adic permutation (i.e. $f \in \overline{\mathcal{P}}_p$).*

Theorem 3.18 thus implies that for every p-permutation polynomial f and every p-adic system G there is a p-adic system F such that $f = \pi_{\mathrm{F,G}}$. A natural follow-up question to this observation is whether all p-adic permutations are actually polynomial functions, i.e. p-permutation polynomials. The following example shows that this is not the case even if F and G are $\mathbb{Z}$-linear-polynomial.

Example 8.3. Let $\mathrm{F} := \mathrm{F}_C = (x, 3x+1)$, $\mathrm{G} := \mathrm{F}_2 = (x, x-1)$, and $\pi := \pi_{\mathrm{F,G}}$. Then $\pi \in \overline{\mathcal{P}}_2$ (since F and G are in $\overline{\mathcal{F}}_2$), $\pi(n) = -n/3$ for all $n \in \left\{2^k \mid k \in \mathbb{N}\right\}$, and $\pi(n) = -23n/9$ for all $n \in \left\{2^k + 2^{k-1} \mid k \in \mathbb{N}\right\}$. If we assume that π is a polynomial function then both $\pi(x) + x/3$ and $\pi(x) + 23x/9$ have infinitely many roots. This implies (since $\mathbb{Q}_2$ does not contain zero divisors) that both polynomials are equal to 0. But then $x/3$ is equal to $23x/9$ (as polynomials) which is a contradiction.

In the other direction one might ask if every p-permutation polynomial f can be written as $f = \pi_{\mathrm{F,G}}$ where both F and G are $\mathbb{Z}_p$-polynomial p-adic systems. This is not the case either, but there does not seem to be a proof as easy as the one given above for the other direction. Instead we will make use of the tree of cycles introduced at the end of Section 3 to demonstrate that certain p-permutation polynomials cannot be represented in this way. The method we will use is quite general in nature and can probably be adapted to show that other classes of p-adic systems which may be found in the future, are also distinct from classes known up to this point.

Cycle trees. For a general p-adic permutation $\pi \in \overline{\mathcal{P}}_p$ we recall some of the properties of its tree of cycles $\mathcal{G}(\pi) = (\mathcal{V}(\pi), \mathcal{E}(\pi))$ and the corresponding edge labeling $c(\pi) : \mathcal{E}(\pi) \to \underline{p}$ as given in Corollary 3.24:

- $\mathcal{G}(\pi)$ is a directed, infinite, rooted tree,
- the out-degrees of all vertices are contained in $[\![1, p]\!]$ and the out-degree of the root is p,
- the labels of all outgoing edges of a given vertex sum up to p.

We call any edge labeled tree satisfying all of the above properties a *p-cycle tree*.

The first natural question in the context of p-adic systems that arises is whether every p-cycle tree can be realized as the tree of cycles of some p-adic permutation. This is indeed the case as the following theorem shows.

Theorem 8.4. *Let $2 \leq p \in \mathbb{N}$ and $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a p-cycle tree with edge labeling $c : \mathcal{E} \to [\![1, p]\!]$. Let $o \in \mathcal{V}$ denote the root of $\mathcal{G}$ and for every vertex $o \neq v \in \mathcal{V}$ let $p(v) \in \mathcal{V}$ denote the predecessor of v, i.e. the unique vertex satisfying $p(v)v \in \mathcal{E}$. Furthermore, for every $v \in \mathcal{V}$ let $S(v) \in \mathbf{S}(\mathrm{bnd}_{\mathcal{V}})$*

be a minimal sequence of all successors of v in an arbitrary but fixed order, i.e. $vS(v)[i] \in \mathcal{E}$ for all $i \in \underline{|S(v)|}$, $\{u \in \mathcal{V} \mid vu \in \mathcal{E}\} = \{S(v)[i] \mid i \in \underline{|S(v)|}\}$, and $|\{u \in \mathcal{V} \mid vu \in \mathcal{E}\}| = |S(v)|$. We label the vertices of $\mathcal{G}$ by the following function (which we will also call c as there is no danger of ambiguity),

$$c : \mathcal{V} \to [\![1, p]\!]. \tag{8.4}$$
$$v \mapsto \begin{cases} 1 & \text{if } v = o \\ c(p(v)v) & \text{if } v \neq o \end{cases}$$

Furthermore, we define the functions o (which stands for "offset" and, again, is not at risk of being confused with the identically named root), P (standing for "positions"), and E (standing for "entries"),

$$o : \mathcal{V} \to \underline{p} \tag{8.5}$$
$$v \mapsto \begin{cases} 0 & \text{if } v = o \\ \sum_{i=0}^{\mathrm{pos}(S(p(v)),v)-1} c(S(p(v))[i]) & \text{if } v \neq o \end{cases}$$
$$P : \mathcal{V} \to \mathbf{S}(\mathrm{bnd}_{\mathbb{N}_0}) \tag{8.6}$$
$$v \mapsto \begin{cases} (0) & \text{if } v = o \\ \prod_{i=0}^{c(v)-1} \left(P(p(v)) + (o(v)+i)p^{k(v)-1}\right) & \text{if } v \neq o \end{cases}$$
$$E : \mathcal{V} \to \mathbf{S}(\mathrm{bnd}_{\underline{p}}) \tag{8.7}$$
$$v \mapsto \begin{cases} (0) & \text{if } v = o \\ \prod_{i=0}^{c(v)-1} (o(v)+i)^{|E(p(v))|-1} \cdot (o(v) + (i+1)\%c(v)) & \text{if } v \neq o \end{cases}$$

where the products mean products of sequences (i.e. their concatenation) and $k(v)$ denotes the layer of v, i.e. its distance from the root, i.e.,

$$k : \mathcal{V} \to \mathbb{N}_0. \tag{8.8}$$
$$v \mapsto \begin{cases} 0 & \text{if } v = o \\ k(p(v)) + 1 & \text{if } v \neq o \end{cases}$$

Using P and E we define an infinite p-digit table $\mathrm{D} \in \overline{\mathcal{D}}_p$ with domain $\mathbb{Z}_p$ and block property by writing the entries in E at positions P in the following way:

$$\mathrm{D}\left[P(v)[i] + ap^{k(v)}\right]\left[k(v) - 1\right] = E(v)[i] \tag{8.9}$$

for all $o \neq v \in \mathcal{V}$, $i \in \underline{|P(v)|}$, and $a \in \mathbb{Z}_p$. Let $\mathrm{F} \in \overline{\mathcal{F}}_p(\mathrm{canf})$ be the p-adic system corresponding to D according to Eqn. (3.131), $\pi := \pi_{\mathrm{F},(x)^p} \in \overline{\mathcal{P}}_p$, and

$$\varphi : \mathcal{V} \to \mathcal{V}(\pi). \tag{8.10}$$
$$v \mapsto (k(v), [([P(v)[0]], \ldots, [P(v)[|P(v)| - 1]])]_{\sim_\sigma})$$

Then, φ is an isomorphism between $\mathcal{G}$ and $\mathcal{G}(\pi)$ that respects the labelings c and $c(\pi)$. In particular, $(\mathcal{G}, c)$ and $(\mathcal{G}(\pi), c(\pi))$ are isomorphic.

To illustrate the workings of the theorem consider the example given in Figure 5 below.

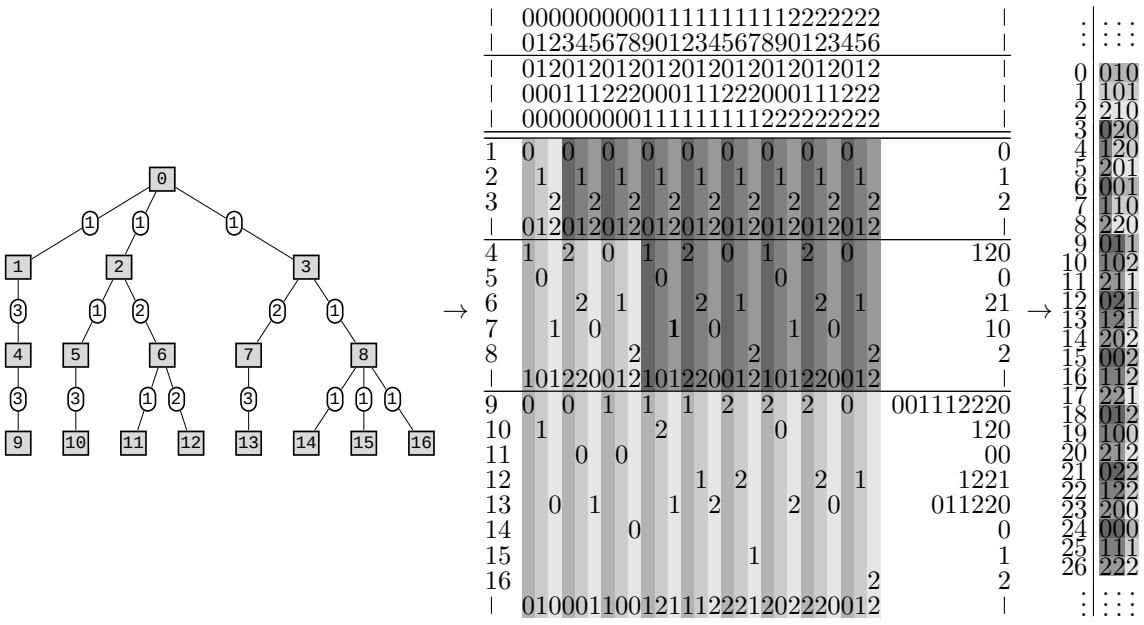

FIGURE 5. The image to the left shows layers 0 to 3 of a 3-cycle tree. The table in the middle shows the corresponding sequences of entries $E(v)$ (right part) and the sequences of positions $P(v)$ (colored center part) for all 16 vertices (excluding the root). For convenience, the top part of the table contains the indices of the respective positions in base 10 and base 3. The table to the right shows the resulting 3-digit table D (cf. also Eqn. (3.75)).

The 3-adic system F corresponding to D in Figure 5 satisfies

$$\mathrm{F}(\underline{3^3})\%3^2 = (1,0,1,5,5,0,0,1,5,7,3,7,2,2,3,3,4,2,4,6,4,8,8,6,6,7,8) \tag{8.11}$$

(cf. Corollary 3.8 (2)), and the resulting 3-adic permutation π thus has the cycles (to improve readability we omit the square brackets indicating equivalence classes, i.e. we write $(0,3,6)$ for $[([0],[3],[6])]_{\sim_\sigma}$)

$$\Sigma(\pi_0):\ (0) \tag{8.12}$$

$$\Sigma(\pi_1):\ (0),\ (1),\ (2) \tag{8.13}$$

$$\Sigma(\pi_2):\ (0,3,6),\ (1),\ (4,7),\ (2,5),\ (8) \tag{8.14}$$

$$\Sigma(\pi_3):\ (0,3,6,9,12,15,18,21,24),\ (1,10,19),\ (4,7),\ (13,16,22,25),\ (2,5,11,14,20,23),\ (8),\ (17),\ (26) \tag{8.15}$$

which coincide with the sequences $P(v)$ and also define the same tree as the one given in Figure 5.

Proof of Theorem 8.4. We will prove the theorem by induction on the layer. It may be helpful to consult Figure 5 when following the argument. In the following we denote the set of vertices contained in the k-th layer of $\mathcal{G}$, $k \in \mathbb{N}_0$, by $\mathcal{V}_k = \{v \in \mathcal{V} \mid k(v) = k\}$ (analogously we set $\mathcal{V}(\pi)_k = \{(\ell,\sigma) \in \mathcal{V}(\pi) \mid \ell = k\}$).

The first thing we observe is that the k-th layer of the graph $\mathcal{G}(\pi)$ only depends on $\mathrm{D}[\![\underline{k}]\!]$, i.e. the columns 0 to $k-1$ of D. Additionally, by definition of D the k-th column $\mathrm{D}[\![k-1]\!]$ of D (note that we start at 0 when indexing columns) is completely determined by "the first p^k entries" of the column, i.e. the entries $\mathrm{D}[0][k-1],\dots,\mathrm{D}[p^k-1][k-1]$ (the quotation marks are due to the fact that a column of D technically has entries for all p-adic integers on which the notion "first" does not make sense as there is no natural order on $\mathbb{Z}_p$). We thus define the sequence

$$S_k \ :=\ (\mathrm{D}[0][k-1],\dots,\mathrm{D}[p^k-1][k-1]) \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_{p^k}) \tag{8.16}$$

for all $k \in \mathbb{N}$ (in the example given in Figure 5 these sequences are the lighter shaded parts of the columns of the rightmost table, i.e. $S_1 = (0,1,2)$, $S_2 = (1,0,1,2,2,0,0,1,2)$, and $S_3 = (0,1,0,0,0,1,1,0,0,1,2,1,1,1,2,2,2,1,2,0,2,2,2,0,0,1,2)$). By definition of D we thus get

$$S_k[j] = \mathrm{D}\,[P(v)[i]]\,[k-1] = E(v)[i] \tag{8.17}$$

for all $k \in \mathbb{N}$ and $j \in \underline{p^k}$ where $v \in \mathcal{V}_k$ and $i \in \underline{|P(v)|}$ are the unique elements satisfying $j = P(v)[i]$ and whose existence and uniqueness we will prove in the following.

For that we first observe that $P(v)$ is $\underline{p^{k(v)}}$-bounded for all $v \in \mathcal{V}$ which can easily be shown by induction on k using the fact that the labels of all vertices that share a parent vertex, sum up to p. In the same way it can be readily verified that $\sum_{v\in\mathcal{V}_k} |P(v)| = p^k$ for all $k \in \mathbb{N}_0$. We are thus left to show that for all $k \in \mathbb{N}_0$, $P(v)$ and $P(w)$ don't have any common entries if v and w are distinct elements of $\mathcal{V}_k$. This follows again by induction on k (in order to conclude that $P(v)$ and $P(w)$ don't share any entries if v and w have distinct parent vertices) and by definition of the offset function o (in order to conclude that $P(v)$ and $P(w)$ don't share any entries if v and w have the same parent vertex). Altogether we just have proven that for all $k \in \mathbb{N}_0$ and $j \in \underline{p^k}$ there is a unique $v \in \mathcal{V}_k$ and $i \in \underline{|P(v)|}$ satisfying $j = P(v)[i]$. Together with the fact that $|P(v)| = |E(v)|$ for all $v \in \mathcal{V}$ this implies that the sequences S_k, $k \in \mathbb{N}$ and consequently D are well-defined.

Next we note that the concatenation $S := \prod_{k=1}^{\infty} S_k$ of all sequences S_k is exactly the infinite sequence corresponding to D in the sense of Eqn. (3.75). Again by induction on the layer k and by the definition of o it can be shown that S has the (p,k)-block property and thus $\mathrm{D} \in \overline{\mathcal{D}}_p$.

We are now ready to proceed with the induction argument to show that φ is an isomorphism between $(\mathcal{G}(\pi), c(\pi))$ (which we now know to be well-defined) and $(\mathcal{G}, c)$. Clearly, the zeroth layers of $(\mathcal{G}, c)$ and $(\mathcal{G}(\pi), c(\pi))$ only consist of the respective roots which are mapped to each other by φ. Now assume that φ is an isomorphism between the layers 0 to $k-1$ of $(\mathcal{G}, c)$ and $(\mathcal{G}(\pi), c(\pi))$ for some $k \in \mathbb{N}$ and let $v \in \mathcal{V}_{k-1}$ and $v' := \varphi(v)$. Then it follows from the induction hypothesis that $v' = (k-1, P(v)) \in \mathcal{V}(\pi)_{k-1}$ (to economize notation we will identify $P(v)$ and $[([P(v)[0]], \ldots, [P(v)[|P(v)|-1]])]_{\sim_\sigma}$). We are left to show that φ maps the children of v exactly to the children of v' and also preserves the labels of all edges between v and its children. For that let $w \in \mathcal{V}_k$ such that $vw \in \mathcal{E}$. We need to show that $w' := \varphi(w) = (k, P(w)) \in \mathcal{V}(\pi)$, $v'w' \in \mathcal{E}(\pi)$ and $|P(w)| \,/\, |P(v)| = c(w) = c(vw)$. The latter part follows directly from the definition of P. To prove the other two statements we observe that

$${\psi_{(x)^p,k-1}}^{-1} \circ \psi_{\mathrm{F},k-1}(P(v)[i]) = \pi_{k-1}(P(v)[i]) = P(v)[(i+1)\,\%\,|P(v)|] \tag{8.18}$$

for all $i \in \underline{|P(v)|}$, where

$$\begin{aligned} \psi_{\mathrm{F},k} : \mathbb{Z}_p/p^k\mathbb{Z}_p &\to \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \mathrm{len}_k) \\ n &\mapsto \psi_{\mathrm{F}}(n)[\underline{k}] \end{aligned} \tag{8.19}$$

for any p-adic system F and $k \in \mathbb{N}_0$ (again we omit the square brackets indicating equivalence classes to improve readability). Rearranging Eqn. (8.18) results in

$$\psi_{\mathrm{F},k-1}(P(v)[i]) = \psi_{(x)^p,k-1}\left(P(v)[(i+1)\,\%\,|P(v)|]\right) \tag{8.20}$$

for all $i \in \underline{|P(v)|}$, i.e. the first $k-1$ digits of the standard base p expansion of $P(v)[(i+1)\,\%\,|P(v)|] \in \underline{p^{k-1}}$. Furthermore, from the definitions of P and E it follows that

$$P(w) = \prod_{i=0}^{c(w)-1} \left(P(v) + (o(w)+i)p^{k-1}\right) \tag{8.21}$$

$$E(w) = \prod_{i=0}^{c(w)-1} (o(w)+i)^{|P(v)|-1} \cdot (o(w) + (i+1)\%c(w)). \tag{8.22}$$

We thus get

$$\psi_{\mathrm{F},k}(P(w)[i]) = \mathrm{D}[P(w)[i]][\underline{k}] \tag{8.23}$$
$$= \mathrm{D}[P(v)[i\%\,|P(v)|][\underline{k-1}] \cdot (E[w][i]) \tag{8.24}$$
$$= \psi_{\mathrm{F},k-1}\,(P(v)[i\%\,|P(v)|]) \cdot (E(w)[i]) \tag{8.25}$$
$$= \psi_{(x)^p,k-1}\,(P(v)[(i+1)\%\,|P(v)|]) \cdot (o(w) + (\lfloor i/\,|P(v)|\rfloor + (i\%\,|P(v)| \neq |P(v)| - 1\ ?\ 0 : 1))\%c(w)) \tag{8.26}$$
$$= \psi_{(x)^p,k-1}\,(P(v)[(i+1)\%\,|P(v)|]) \cdot (o(w) + \lfloor (i+1)/\,|P(v)|\rfloor\,\%c(w)) \tag{8.27}$$
$$= \psi_{(x)^p,k}\,(P(w)[(i+1)\%\,|P(w)|]) \tag{8.28}$$

for all $i \in \underline{|P(w)|}$, or equivalently,

$$\pi_k(P(w)[i]) = {\psi_{(x)^p,k}}^{-1} \circ \psi_{\mathrm{F},k}(P(w)[i]) = P(w)[(i+1)\%\,|P(w)|]. \tag{8.29}$$

Since all elements of $P(w)$ are mutually distinct modulo p^k, $P(w)$ is a cycle of π_k and consequently $w' \in \mathcal{V}(\pi)$. In addition, $P[w]\%p^{k-1} = P[v]^{c(w)}$ and thus $v'w' \in \mathcal{E}(\pi)$ which completes the proof. □

The following theorem characterizes completely the sets of all isomorphism classes of trees with up to 4 layers which may occur as subtrees of trees of cycles of 2-adic permutations defined by $\mathbb{Z}_2$-polynomial 2-adic systems or 2-permutation polynomials. This will allow also to show that the sets of all p-adic permutations defined by $\mathbb{Z}_p$-polynomial p-adic systems and p-permutation polynomials respectively, have both exclusive elements (that the two sets are not disjoint either follows from the simple observation that $\pi_{\mathrm{F},\mathrm{F}}(n) = n$ for all p-adic systems F and $n \in \mathbb{Z}_p$).

Theorem 8.5. *For $2 \leq p \in \mathbb{N}$ and $k \in \mathbb{N}_0$ let*

$$S_{p,k} := \big\{\textit{isomorphism class of } T \mid \mathrm{F},\mathrm{G} \in \overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Z}_p}) \quad T \textit{ full } k\textit{-layer rooted subtree of } (\mathcal{G}(\pi_{\mathrm{F},\mathrm{G}}), c(\pi_{\mathrm{F},\mathrm{G}}))\big\} \tag{8.30}$$
$$T_{p,k} := \big\{\textit{isomorphism class of } T \mid \mathrm{F},\mathrm{G} \in \overline{\mathcal{F}}_p(\mathrm{poly}_{\mathbb{Z}_p}) \quad T \textit{ full } k\textit{-layer rooted subtree of } (\mathcal{G}(\pi_{\mathrm{F},\mathrm{G}}), c(\pi_{\mathrm{F},\mathrm{G}})) \quad |\sigma| > 1 \textit{ for root } (\ell,\sigma) \textit{ of } T\big\} \tag{8.31}$$
$$U_{p,k} := \big\{\textit{isomorphism class of } T \mid f \in \mathbb{Z}_p[x] \textit{ } p\textit{-permutation polynomial} \quad T \textit{ full } k\textit{-layer rooted subtree of } (\mathcal{G}(f), c(f))\big\} \tag{8.32}$$
$$V_{p,k} := \big\{\textit{isomorphism class of } T \mid f \in \mathbb{Z}_p[x] \textit{ } p\textit{-permutation polynomial} \quad T \textit{ full } k\textit{-layer rooted subtree of } (\mathcal{G}(f), c(f)) \quad |\sigma| > 1 \textit{ for root } (\ell,\sigma) \textit{ of } T\big\}. \tag{8.33}$$

Then,

$$|S_{2,2}| = 5 \qquad |S_{2,3}| = 20 \qquad |S_{2,4}| = 71 \tag{8.34}$$
$$|T_{2,2}| = 5 \qquad |T_{2,3}| = 12 \qquad |T_{2,4}| = 50 \tag{8.35}$$
$$|U_{2,2}| = 5 \qquad |U_{2,3}| = 18 \qquad |U_{2,4}| = 83 \tag{8.36}$$
$$|V_{2,2}| = 3 \qquad |V_{2,3}| = 5 \qquad |V_{2,4}| = 7 \tag{8.37}$$

and all these sets are given in Figure 6 where membership in the respective sets is indicated by the black boxes below each graph in the order S, T, U, V.

Note that Figure 6 lists all possible isomorphism classes of 2-, 3-, and 4-layer rooted trees with out-degrees in $\{1,2\}$ of which there are 5, 20, and 230 respectively. Also note that the edge labels are not shown as they are uniquely fixed by the graph itself in the case $p = 2$.

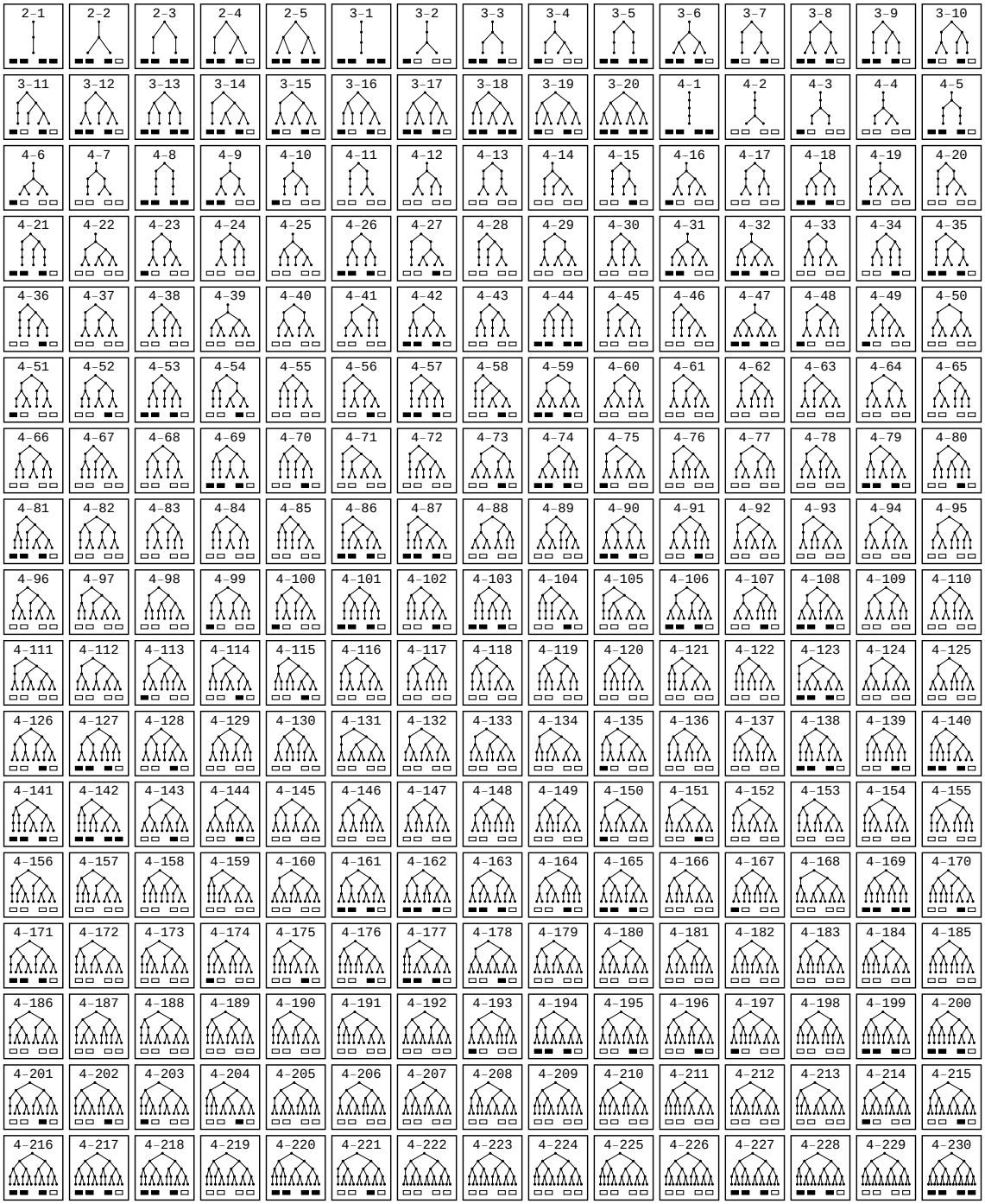

FIGURE 6. The sets $S_{p,k}$, $T_{p,k}$, $U_{p,k}$, and $V_{p,k}$ for $p = 2$ and $k \in \{2, 3, 4\}$.

Proof of Theorem 8.5. We begin with the easier part of the proof and show that all the isomorphism classes marked by black boxes in Figure 6 actually are elements of the respective sets by listing examples of 2-adic permutations $\pi_{\mathrm{F,G}}$, where F and G are $\mathbb{Z}_2$-polynomial 2-adic systems, and 2-adic permutations defined by 2-permutation polynomials whose trees of cycles contain the given isomorphism classes as subtrees. These examples are summarized in the following table, where the $\mathbb{Z}_2$-polynomial 2-adic system F (for $S_{2,k}$ and $T_{2,k}$) and the 2-permutation polynomial f (for

$U_{2,k}$ and $V_{2,k}$) are given and $\mathrm{G} := (x, x-1) \in \overline{\mathcal{F}}_2$ is supposed to be fixed. Note that all claimed subtrees are found within the layers 0 to 8 of $\mathcal{G}(\pi_{\mathrm{F,G}})$ and $\mathcal{G}(f)$ respectively.

Subtree	$\mathbf{S_{2,k}}$, F = ...	$\mathbf{T_{2,k}}$, F = ...	$\mathbf{U_{2,k}}$, **f** = ...	$\mathbf{V_{2,k}}$, **f** = ...
$2-1:$	$(x+2, x+1)$	$(x+2, x+1)$	$x+2$	$x+2$
$2-2:$	$(x, x+1)$	$(3x+2, x+1)$	$3x$	
$2-3:$	$(x+2, x+1)$	$(3x+2, 3x+3)$	$x+2$	$3x$
$2-4:$	$(x, x+1)$	$(3x, x+1)$	$3x$	
$2-5:$	$(3x, x+1)$	$(x, x+1)$	x	$2x^2+3x+2$
$3-1:$	$(x+2, x+1)$	$(x+2, x+1)$	$x+2$	$x+2$
$3-2:$	$(3x+2, x+1)$			
$3-3:$	$(x+4, x+1)$	$(3x+2, x+3)$	$3x$	
$3-4:$	$(3x, x+1)$			
$3-5:$	$(x+2, x+1)$	$(x+4, x+1)$	$x+2$	$3x$
$3-6:$	$(x, x+1)$	$(3x+2, x+1)$	$2x^2+3x+2$	
$3-7:$	$(3x+2, x+1)$		$2x^3+3x+2$	
$3-8:$	$(3x+2, 3x+3)$	$(2x^2+x+4, x^2+x)$	$2x^2+3x+2$	
$3-9:$	$(3x+4, 3x+3)$	(x^2+x+2, x^2+x)	$2x^2+x+2$	
$3-10:$	$(3x+4, x+1)$		$2x^3+x+4$	
$3-11:$	$(3x+2, x+3)$		$2x^3+x+2$	
$3-12:$	$(x, x+1)$	$(x+2, 3x+1)$	$3x$	
$3-13:$	$(x+4, x+3)$	$(3x+2, 3x+3)$	$x+4$	$2x^2+3x+2$
$3-14:$	$(3x, 3x+1)$	$(3x, x+1)$	$2x^2+x$	
$3-15:$	$(3x, x+1)$		$2x^3+x$	
$3-16:$	$(3x, x+1)$		$2x^3+3x$	
$3-17:$	$(3x, 3x+1)$	$(2x^2+x, x^2+x)$	$2x^2+3x$	
$3-18:$	$(x, x+3)$	(x^2+3x, x^2+x)	$2x^2+x$	x^4+3x^2+x+2
$3-19:$	$(x, 3x+1)$		$2x^3+3x+4$	
$3-20:$	$(2x^2+x, x^2+x+2)$	$(x, x+1)$	x	$2x^3+2x^2+3x+2$
$4-1:$	$(x+2, x+1)$	$(x+2, x+1)$	$x+2$	$x+2$
$4-3:$	$(3x+2, x+3)$			
$4-5:$	$(x+4, x+1)$	$(3x+2, x+3)$	$3x$	
$4-6:$	$(3x, x+1)$			
$4-8:$	$(x+2, x+1)$	$(x+4, x+1)$	$x+2$	$3x$
$4-9:$	$(3x+4, x+3)$	$(3x+4, x+3)$		
$4-10:$	$(3x, x+1)$			
$4-15:$			$2x^3+3x+2$	
$4-16:$	$(3x, x+1)$			
$4-18:$	$(3x+2, 3x+3)$	$(4x^2+x+4, x^2+x)$	$7x$	
$4-19:$	$(3x, x+1)$			
$4-21:$	$(x+4, 3x+1)$	$(x+4, 3x+1)$	$2x^2+x+2$	
$4-23:$	$(3x, x+1)$			
$4-26:$	$(3x^2+3x+4, x^2+x)$	$(2x^2+x, x^2+x+2)$	$4x^3+2x^2+7x+2$	
$4-27:$			$2x^3+7x+2$	
$4-31:$	$(3x+2, x+1)$	$(3x+2, x+1)$		
$4-32:$	$(3x+4, x+1)$	$(3x+4, x+1)$	x^4+x^2+x+6	
$4-34:$			$2x^3+x+4$	
$4-35:$	$(3x, 3x+1)$	$(2x^2+3x+4, x^2+x)$	$x^4+2x^3+x^2+3x+4$	
$4-36:$			x^4+x^2+x+4	
$4-42:$	$(x, 3x+3)$	$(x, 3x+3)$	$2x^2+3x+2$	
$4-44:$	$(x+4, x+3)$	$(3x+2, 3x+3)$	$x+4$	$2x^2+3x+2$
$4-47:$	$(x, x+1)$	$(x+2, 3x+3)$	$2x^2+3x$	
$4-48:$	$(3x+2, x+3)$			
$4-49:$	$(x, 3x+3)$			
$4-51:$	$(3x+4, x+1)$			
$4-52:$			x^4+x^2+x+2	
$4-53:$	$(3x+4, x+3)$	$(3x+4, x+3)$	$x^4+2x^3+3x^2+x+6$	
$4-54:$			$2x^3+5x+4$	
$4-56:$			$2x^3+x+2$	
$4-57:$	$(2x^2+3x, x^2+x+2)$	$(2x^2+3x, x^2+x+2)$	$2x^2+x+6$	
$4-58:$			x^4+x^2+x	
$4-59:$	$(3x+2, 3x+1)$	$(2x^2+x, x^2+x)$	$4x^3+2x^2+3x+2$	
$4-69:$	$(2x^2+x+4, x^2+x+2)$	$(4x^2+3x+2, x^2+x+2)$	x^5+3x^3+5x+4	
$4-70:$			$x^5+x^3+2x^2+x+4$	
$4-73:$			x^4+3x^2+3x+4	
$4-74:$	$(2x^2+3x+4, x^2+x)$	$(2x^2+3x+4, x^2+x)$	$x^4+2x^3+3x^2+x+2$	
$4-75:$	$(3x+4, x+3)$			
$4-79:$	$(x+4, x+1)$	$(x+2, 3x+1)$	$3x$	
$4-80:$			$4x^4+2x^3+6x^2+7x+6$	
$4-81:$	$(x, 3x+1)$	$(x, 3x+1)$	$x^4+2x^3+3x^2+x$	
$4-86:$	$(3x, x+1)$	$(3x, x+1)$	$x^4+2x^3+x^2+3x$	
$4-87:$	$(2x^2+x+4, x^2+x)$	$(4x^2+x, x^2+x)$	$2x^2+x$	
$4-90:$	(x^2+3x+4, x^2+x+2)	$(3x^2+3x+2, 2x^2+3x+3)$	$x^4+2x^3+3x^2+3x+4$	

$4-91:$			x^4+x^2+3x+4	
$4-99:$	$(3x^2+x+4, x^2+x+2)$			
$4-100:$	$(3x+4, x+3)$			
$4-101:$	(x^2+3x+2, x^2+x+2)	$(2x^2+3x, x^2+3x)$	$x^4+2x^3+x^2+x+4$	
$4-102:$			$2x^3+3x$	
$4-103:$	$(3x+4, 3x+3)$	$(3x+4, 3x+3)$	$4x^2+x+4$	
$4-104:$			$x^5+x^3+2x^2+5x+4$	
$4-106:$	$(x, x+1)$	$(x+4, 3x+1)$	$7x$	
$4-107:$			$4x^4+6x^3+6x^2+3x+6$	
$4-108:$	$(x+4, 3x+3)$	$(x+4, 3x+3)$	$x^4+2x^3+3x^2+x+4$	
$4-113:$	$(3x, x+1)$			
$4-114:$			x^4+3x^2+3x	
$4-115:$			$6x^3+5x$	
$4-123:$	$(3x+4, x+1)$	$(3x+4, x+1)$	$2x^2+5x$	
$4-126:$			x^5+x^3+3x	
$4-127:$	$(2x^2+3x+4, x^2+3x+4)$	$(3x^2+3x+2, 2x^2+3x+1)$	$x^5+5x^4+x^3+7x^2+7x+4$	
$4-128:$			x^4+x^2+7x+4	
$4-135:$	$(3x, x+1)$			
$4-138:$	$(3x+4, x+1)$	$(3x+4, x+1)$	$x^5+3x^3+2x^2+3x$	
$4-139:$			$x^5+5x^4+7x^3+7x^2+x+4$	
$4-140:$	$(3x, x+1)$	$(3x, x+1)$	$x^4+2x^3+x^2+5x$	
$4-141:$	$(2x^2+x+4, x^2+x)$	$(2x^2+3x+2, x^2+x)$	x^5+3x^3+x+4	
$4-142:$	$(x, x+3)$	$(3x+4, 3x+3)$	$5x$	x^4+3x^2+x+2
$4-143:$			x^4+x^2+x+6	
$4-144:$			$2x^3+5x$	
$4-150:$	$(x, 3x+1)$			
$4-151:$			$2x^3+x$	
$4-161:$	(x^2+3x, x^2+x+2)	$(3x^2+3x+2, 4x^2+3x+1)$	$x^4+2x^3+3x^2+7x$	
$4-162:$	$(4x^2+x, x^2+x+2)$	$(2x^2+3x+2, 2x^2+x+3)$	x^5+3x^3+x	
$4-163:$	$(2x^2+x+4, x^2+x)$	$(2x^2+x+4, x^2+x)$	$2x^2+3x$	
$4-164:$			$2x^3+7x$	
$4-165:$	$(2x^2+x+2, x^2+x+2)$	$(4x^2+x+2, x^2+3x+4)$	$x^5+3x^3+2x^2+3x+4$	
$4-167:$	(x^2+x+2, x^2+x+2)			
$4-169:$	$(3x^2+x+2, 3x^2+3x+4)$	$(3x^2+x+2, 3x^2+3x+4)$	$2x^2+3x$	$2x^2+3x$
$4-170:$			$x^5+5x^4+3x^3+7x^2+5x+4$	
$4-171:$	$(3x+2, x+1)$	$(3x+2, x+1)$	$x^4+2x^3+x^2+x$	
$4-174:$	$(2x^2+3x, x^2+x+2)$			
$4-175:$			x^4+x^2+7x	
$4-176:$			$x^5+x^3+2x^2+5x$	
$4-177:$	(x^2+3x, x^2+x)	(x^2+3x, x^2+x)	$2x^2+x$	
$4-178:$			$6x^3+x$	
$4-193:$	$(x, 3x+1)$			
$4-194:$	$(2x^2+x, x^2+x+2)$	$(x^2+3x+2, 2x^2+3x+1)$	$x^5+3x^3+4x^2+5x$	
$4-195:$			x^5+x^3+3x+4	
$4-196:$			$2x^3+3x+4$	
$4-197:$	$(3x^2+x, x^2+x)$			
$4-199:$	(x^2+x+2, x^2+x)	(x^2+x+2, x^2+x)	$3x^5+x^4+7x^3+7x^2+7x$	
$4-200:$	$(3x^2+3x, x^2+x)$	$(3x^2+3x, x^2+x)$	$4x^3+5x$	
$4-201:$			x^4+x^2+3x	
$4-202:$			$x^5+x^3+6x^2+5x$	
$4-203:$	(x^2+x, x^2+x)			
$4-204:$			$x^5+x^3+6x^2+x$	
$4-214:$	$(x, 3x+1)$			
$4-215:$			$2x^3+2x^2+5x$	
$4-216:$	$(3x^2+x+4, x^2+x)$	$(3x^2+x+4, x^2+x)$	$x^4+2x^3+3x^2+3x$	
$4-217:$	$(2x^2+3x+2, x^2+x+2)$	$(2x^2+3x+2, x^2+x+2)$	$x^5+3x^3+4x^2+x$	
$4-218:$	(x^2+3x, x^2+x)	(x^2+3x, x^2+x)	$2x^2+5x$	
$4-220:$	(x^2+x+4, x^2+3x)	(x^2+x+4, x^2+3x)	$2x^2+x$	$2x^3+2x^2+3x+2$
$4-221:$			$x^5+x^3+2x^2+x$	
$4-227:$	$(2x^2+x, x^2+x+2)$	$(2x^2+3x+2, 3x^2+x+4)$	x^5+3x^3+5x	
$4-228:$	(x^2+x+2, x^2+3x)	$(2x^2+x+2, x^2+3x+2)$	$4x^3+4x^2+x$	
$4-230:$	$(x, x+1)$	$(x, x+1)$	x	$2x^3+x+2$

In the other direction we need to show that all isomorphism classes not marked by black boxes cannot be realized as the isomorphism class of a subtree of the tree of cycles of a 2-adic permutation of the respective type. To do so we define the auxiliary function

$$\varphi_{\pi,k} : \mathbb{Z}_2 \to \{0,1\} \qquad n \mapsto \psi_{\mathrm{F}_2,k+1}(\pi_{k+1}(n))[k] = \mathrm{D}((x,x-1))[\pi(n)][k] \tag{8.38}$$

for all 2-adic permutations π and all $k \in \mathbb{N}_0$, i.e. $\varphi_{\pi,k}(n)$ is the k-th digit (the digit corresponding to 2^k) in the base 2 expansion of $\pi(n)$ (note, $\mathrm{F}_2 = (x, x-1)$ and we omit the square brackets

indicating equivalence classes to improve readability). Also, by Eqn. (3.94) we get

$$\varphi_{\pi,k}(n) = 1 - \varphi_{\pi,k}(n + 2^k) \tag{8.39}$$

$$= \varphi_{\pi,k}(n + 2^{k+1}) \tag{8.40}$$

for all $k \in \mathbb{N}_0$ and $n \in \mathbb{Z}_2$.

For arbitrary $\mathbb{Z}_2$-polynomial 2-adic systems F and G, 2-permutation polynomial f, and $k \in \mathbb{N}_0$ we will prove the relations

(1) $\varphi_{\pi,k+2}(n_{000}) + \varphi_{\pi,k+2}(n_{010}) + \varphi_{\pi,k+3}(n_{100}) + \varphi_{\pi,k+3}(n_{110}) + \varphi_{\pi,k+3}(n_{101}) + \varphi_{\pi,k+3}(n_{111}) \equiv \varphi_{\pi,k+1}(n_{000}) + \varphi_{\pi,k+1}(n_{100}) \mod 2$
(2) $\varphi_{f,k+2}(n_{000}) + \varphi_{f,k+2}(n_{010}) + \varphi_{f,k+3}(n_{000}) + \varphi_{f,k+3}(n_{010}) + \varphi_{f,k+3}(n_{001}) + \varphi_{f,k+3}(n_{011}) \equiv 0 \mod 2$
(3) $k \geq 1 \Rightarrow$
$\varphi_{f,k+1}(n_{000}) + \varphi_{f,k+2}(n_{000}) + \varphi_{f,k+3}(n_{010}) + \varphi_{f,k+3}(n_{011}) \equiv 0 \mod 2$
(4) $k \geq 1 \Rightarrow$
$(\varphi_{f,k+1}(n_{000}) + \varphi_{f,k+2}(n_{010}) + \varphi_{f,k+3}(n_{000}) \in \{0,3\} \ ? \ 0 : 1) \equiv$
$\varphi_{f,k}(n_{000}) + \varphi_{f,k+1}(n_{100}) + \varphi_{f,k+2}(n_{000}) + \varphi_{f,k+3}(n_{010}) + \varphi_{f,k+4}(n_{000}) + \varphi_{f,k+4}(n_{001}) \mod 2$

for all $n \in \mathbb{Z}_2$, where $\pi := \pi_{\mathrm{F,G}}$ and $n_{(a_0 2^0 + \cdots + a_\ell 2^\ell)} := n_{a_0 \ldots a_\ell} := n + a_0 2^{k+0} + \cdots + a_\ell 2^{k+\ell}$ for all $\ell \in \mathbb{N}_0$ and $a_0, \ldots, a_\ell \in \{0,1\}$.

To prove (1) we first show that if arbitrary 2-adic permutations π, π_1, π_2 satisfy (1), then so do π^{-1} and $\pi_2 \circ \pi_1$. For all $n \in \mathbb{Z}_2$ there is an $s_n \in \underline{2^4}$ such that

$$\psi_{\mathrm{F}_2,k+4}(n_{(r)}) = \psi_{\mathrm{F}_2,k}(n) \cdot \psi_{\mathrm{F}_2,4}(r + s_n) \tag{8.41}$$

for all $r \in \underline{2^4}$. Furthermore, if π is a 2-adic permutation it follows from the definition that there are unique $m_{\pi,n,[0]}, \ldots, m_{\pi,n,[15]} \in \underline{2^4}$ such that

$$\psi_{\mathrm{F}_2,k+4}(\pi(n_{(r)})) = \psi_{\mathrm{F}_2,k}(\pi(n)) \cdot \psi_{\mathrm{F}_2,4}(m_{\pi,n,r}) \tag{8.42}$$

for all $r \in \underline{2^4}$ and the $m_{\pi,n,r}$ satisfy

$$r \equiv s \mod 2^\ell \Leftrightarrow m_{\pi,n,r} \equiv m_{\pi,n,s} \mod 2^\ell \tag{8.43}$$

for all $\ell \in \overline{4}$ and $r, s \in \underline{2^\ell}$. Thus there is a bijective function

$$\pi_{(n)} : \mathbb{Z}_2/2^4\mathbb{Z}_2 \to \mathbb{Z}_2/2^4\mathbb{Z}_2 \tag{8.44}$$
$$r \mapsto m_{\pi,n,r-s_n}$$

satisfying $\pi_{(n)}(r + s_n) = m_{\pi,n,r}$ for all $r \in \underline{2^4}$ and

$$r \equiv s \mod 2^\ell \Leftrightarrow \pi_{(n)}(r) \equiv \pi_{(n)}(s) \mod 2^\ell \tag{8.45}$$

for all $\ell \in \overline{4}$ and $r, s \in \underline{2^\ell}$. Thus we get

$$\forall\, n \in \mathbb{Z}_2 : \forall\, r \in \underline{2^4} : \psi_{\mathrm{F}_2,k+4}(n_{(r)}) = \psi_{\mathrm{F}_2,k}(n) \cdot \psi_{\mathrm{F}_2,4}(r + s_n) \tag{8.46}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(\pi(n))) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(\pi(n))) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(\pi_{(n)}(s_n))) \tag{8.47}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(n)) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(n)) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(\pi_{(\pi^{-1}(n))}(s_{\pi^{-1}(n)}))) \tag{8.48}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(n)) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(n)) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(m_{\pi,\pi^{-1}(n),0})) \tag{8.49}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(n)) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(n)) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(s_n)) \tag{8.50}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \forall\, r \in \underline{2^4} : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(n_{(r)})) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(n)) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(s_{n_{(r)}})) \tag{8.51}$$

$$\Rightarrow \forall\, n \in \mathbb{Z}_2 : \forall\, r \in \underline{2^4} : \psi_{\mathrm{F}_2,k+4}(\pi^{-1}(n_{(r)})) = \psi_{\mathrm{F}_2,k}(\pi^{-1}(n)) \cdot \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(r + s_n)). \tag{8.52}$$

By the definitions we have the following identities

$$\varphi_{\pi,k+\ell}(n_{(r)}) = \psi_{\mathrm{F}_2,4}(\pi_{(n)}(r + s_n))[\ell] \tag{8.53}$$

$$\varphi_{\pi^{-1},k+\ell}(n_{(r)}) = \psi_{\mathrm{F}_2,4}(\pi_{(\pi^{-1}(n))}^{-1}(r + s_n))[\ell] \tag{8.54}$$

for all $n \in \mathbb{Z}_p$, $r \in \underline{2^4}$, and $\ell \in \overline{3}$. The condition that π satisfies (1) is thus equivalent to

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}(0+s_n))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(2+s_n))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(1+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(3+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(5+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(7+s_n))[3] \equiv \tag{8.55}$$

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}(1+s_n))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(3+s_n))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(0+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(2+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(4+s_n))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(6+s_n))[3] \equiv \tag{8.56}$$

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}(0+s_n))[1] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}(1+s_n))[1] \mod 2 \tag{8.57}$$

for all $n \in \mathbb{Z}_2$, and the condition that π^{-1} satisfies (1) is equivalent to

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(0+s_{\pi^{-1}(n)}))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(2+s_{\pi^{-1}(n)}))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(1+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(3+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(5+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(7+s_{\pi^{-1}(n)}))[3] \equiv \tag{8.58}$$

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(1+s_{\pi^{-1}(n)}))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(3+s_{\pi^{-1}(n)}))[2] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(0+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(2+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(4+s_{\pi^{-1}(n)}))[3] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(6+s_{\pi^{-1}(n)}))[3] \equiv \tag{8.59}$$

$$\psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(0+s_{\pi^{-1}(n)}))[1] + \psi_{\mathrm{F}_2,4}(\pi_{(n)}^{-1}(1+s_{\pi^{-1}(n)}))[1] \mod 2 \tag{8.60}$$

for all $n \in \mathbb{Z}_2$ (note that since the condition must be satisfied for all $n \in \mathbb{Z}_2$ and $\pi : \mathbb{Z}_2 \to \mathbb{Z}_2$ is bijective, we may interchange n and $\pi^{-1}(n)$ which is what we did here). There are only finitely many options for $\pi_{(n)} : \mathbb{Z}_2/2^4\mathbb{Z}_2 \to \mathbb{Z}_2/2^4\mathbb{Z}_2$ which satisfy Eqn. (8.45) (16384, to be precise) and among those there are 8192 which also satisfy Eqn. (8.55) – (8.57) for at least one choice for $s_n \in \underline{2^4}$. It can be easily checked using a computer that any of those 8192 choices for $\pi_{(n)}$ satisfy Eqn. (8.58) – (8.60) for all choices for $s_{\pi^{-1}(n)} \in \underline{2^4}$. This completes the proof that if π satisfies (1), then so does π^{-1}. On the other hand, if $\pi = \pi_2 \circ \pi_1$ (which is a 2-adic permutation by Theorem 3.19) then

$$\psi_{\mathrm{F}_2,k+4}(\pi_2 \circ \pi_1(n_{(r)})) = \psi_{\mathrm{F}_2,k}(\pi_2 \circ \pi_1(n)) \cdot \psi_{\mathrm{F}_2,4}((\pi_2)_{(\pi_1(n))} \circ (\pi_1)_{(n)}(r+s_n)) \tag{8.61}$$

and thus

$$\varphi_{\pi_2\circ\pi_1,k+\ell}(n_{(r)}) = \psi_{\mathrm{F}_2,4}((\pi_2)_{(\pi_1(n))} \circ (\pi_1)_{(n)}(r+s_n))[\ell] \tag{8.62}$$

for all $n \in \mathbb{Z}_p$, $r \in \underline{2^4}$, and $\ell \in \overline{3}$. Thus, if we set $\pi_{(n)} := (\pi_2)_{(\pi_1(n))} \circ (\pi_1)_{(n)}$ for all $n \in \mathbb{Z}_2$, the condition that $\pi_2 \circ \pi_1$ satisfies (1) reads exactly as Eqn. (8.55) – (8.57) and we can again verify using a computer that if $(\pi_1)_{(n)}$ and $(\pi_2)_{(\pi_1(n))}$ are chosen among the 8192 possible options mentioned above, then $\pi_{(n)} = (\pi_2)_{(\pi_1(n))} \circ (\pi_1)_{(n)}$ satisfies Eqn. (8.55) – (8.57) for all choices for $s_n \in \underline{2^4}$. This completes the proof that if π_1 and π_2 satisfies (1), then so does $\pi_2 \circ \pi_1$. Thus it suffices to prove (1) for the case where $\mathrm{G} = \mathrm{F}_2$, because a general $\pi = \pi_{\mathrm{F,G}}$ can always be written as $\pi = \pi_{\mathrm{G,F}_2}^{-1} \circ \pi_{\mathrm{F,F}_2}$ (cf. also Lemma 3.17 (3)).

If $\mathrm{G} = \mathrm{F}_2$, then

$$\varphi_{\pi,k}(n) = \psi_{\mathrm{F}_2,k+1}(\pi_{k+1}(n))[k] = \psi_{\mathrm{F}_2,k+1}({\psi_{\mathrm{F}_2,k+1}}^{-1}(\psi_{\mathrm{F},k+1}(n)))[k] = \psi_{\mathrm{F},k+1}(n)[k] \tag{8.63}$$

$$= \mathrm{D(F)}[n][k]. \tag{8.64}$$

Thus (1) simplifies to

$$\mathrm{D(F)}[n_{000}][k+2] + \mathrm{D(F)}[n_{010}][k+2] + \mathrm{D(F)}[n_{100}][k+3] + \mathrm{D(F)}[n_{110}][k+3] + \mathrm{D(F)}[n_{001}][k+3] + \mathrm{D(F)}[n_{011}][k+3] \equiv \tag{8.65}$$

$$\mathrm{D(F)}[n_{000}][k+1] + \mathrm{D(F)}[n_{100}][k+1] \mod 2. \tag{8.66}$$

The first step will be to prove the statement for the case $k = 0$. This can easily be done with the aid of a computer, since Theorem 4.15 implies that it suffices to check the statement for all $\underline{2^4}$-polynomial 2-adic systems with degree in $\underline{4}$. The next step is to prove the auxiliary property

$$\mathrm{F}^k(n) - \mathrm{F}^k(n+2^{k+\ell}) \equiv \mathrm{F}^k(n+2^k) - \mathrm{F}^k(n+2^k+2^{k+\ell}) \mod 2^{\ell+2} \tag{8.67}$$

for all $k, \ell \in \mathbb{N}_0$ and $n \in \mathbb{Z}_2$ which we will do by induction on k. The statement is clearly true for $k = 0$. Assume that it is also true for $k \in \mathbb{N}_0$. Then,

$$\mathrm{F}^k(n) - \mathrm{F}^k(n + 2^{k+\ell+1}) \equiv \mathrm{F}^k(n + 2^k) - \mathrm{F}^k(n + 2^k + 2^{k+\ell+1}) \tag{8.68}$$

$$\equiv \mathrm{F}^k(n + 2^{k+1}) - \mathrm{F}^k(n + 2^{k+1} + 2^{k+\ell+1}) \mod 2^{\ell+3}. \tag{8.69}$$

If $A := \mathrm{F}^k(n)$, $B := \mathrm{F}^k(n + 2^{k+\ell+1})$, $C := \mathrm{F}^k(n + 2^{k+1})$, and $D := \mathrm{F}^k(n + 2^{k+1} + 2^{k+\ell+1})$ then

$$A - B - C + D \equiv 0 \mod 2^{\ell+3} \tag{8.70}$$

by definition, and

$$A \equiv B \equiv C \equiv D \mod 2 \tag{8.71}$$

$$A \equiv B \mod 2^{\ell+1} \tag{8.72}$$

$$C \equiv D \mod 2^{\ell+1} \tag{8.73}$$

by Theorem 4.8 (1). Consequently,

$$\mathrm{F}(A) - \mathrm{F}(B) - \mathrm{F}(C) + \mathrm{F}(D) = \frac{1}{2} \sum_{i=1}^{d} a_i (A^i - B^i - C^i + D^i) \tag{8.74}$$

where $\mathrm{F}[A\%2] = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}_2[x]$ (note that for the whole theorem we define $0^0 := 1$ and we assume without loss of generality that F is in weak canonical form). Our goal is to show that $\mathrm{F}(A) - \mathrm{F}(B) - \mathrm{F}(C) + \mathrm{F}(D) \equiv 0 \mod 2^{\ell+2}$ which obviously would follow if we could prove

$$A^i - B^i - C^i + D^i \equiv 0 \mod 2^{\ell+3} \tag{8.75}$$

for all $i \in \mathbb{N}$ which we will do by induction on i. The statement is clearly true for $i = 1$. Now assume that it is also true for some $i \in \mathbb{N}$ and let $S, T, U, V, W, X, Y \in \mathbb{Z}_2$ such that,

$$2^{\ell+3} S = A - B - C + D \tag{8.76}$$

$$2^{\ell+3} T = A^i - B^i - C^i + D^i \tag{8.77}$$

$$2^{\ell+1} U = A - B \tag{8.78}$$

$$2^{\ell+1} V = C - D \tag{8.79}$$

$$2W = B - C \tag{8.80}$$

$$2^{\ell+1} X = A^i - B^i \tag{8.81}$$

$$2^{\ell+1} Y = C^i - D^i. \tag{8.82}$$

It is easy to show that,

$$i = 1 \Rightarrow U = X \tag{8.83}$$

$$i \neq 1 \Rightarrow (X\%2 = 1 \Rightarrow B\%2 = i\%2 = 1 \Rightarrow U\%2 = X\%2) \tag{8.84}$$

which implies

$$X + U \sum_{j=0}^{i-1} B^j (B - 2W)^{i-1-j} \equiv 0 \mod 2. \tag{8.85}$$

If we let $Z \in \mathbb{Z}_2$ such that

$$2Z = X + U \sum_{j=0}^{i-1} B^j (B - 2W)^{i-1-j} \tag{8.86}$$

then

$$A^{i+1} - B^{i+1} - C^{i+1} + D^{i+1} = 2^{\ell+3}(TD + WZ + SC^i + 2^{\ell-1} X(U + V)) \in 2^{\ell+3}\mathbb{Z}_2 \tag{8.87}$$

which completes the proof of Eqn. (8.67) and thus also the proof of Eqn. (8.75). Using the fact that Eqn. (8.65) – Eqn. (8.66) is true for $k = 0$ together with Eqn. (8.67), we are now able to prove

Eqn. (8.65) – Eqn. (8.66) for general k which will complete the proof of relation (1). We do so again by using a computer to verify that

$$\mathrm{D}[a][2]+\mathrm{D}[c][2]+\mathrm{D}[b][3]+\mathrm{D}[d][3]+\mathrm{D}[f][3]+\mathrm{D}[h][3]\equiv \mathrm{D}[a][1]+\mathrm{D}[b][1] \mod 2. \tag{8.88}$$

for all $\mathrm{D}\in\mathcal{D}_2(\mathrm{len}_4,\mathrm{block})$ satisfying Eqn. (8.65) – Eqn. (8.66) for $k=0$ (if $\mathrm{D}(\mathrm{F})=\mathrm{D}$ there) and all $a,b,c,d,e,f,g,h\in\underline{2^4}$ satisfying

$$a\not\equiv b\not\equiv c\not\equiv d\not\equiv e\not\equiv f\not\equiv g\not\equiv h \mod 2 \tag{8.89}$$

$$a\not\equiv c\not\equiv e\not\equiv g,\quad b\not\equiv d\not\equiv f\not\equiv h \mod 2^2 \tag{8.90}$$

$$a\not\equiv e,\quad b\not\equiv f,\quad c\not\equiv g,\quad d\not\equiv h \mod 2^3 \tag{8.91}$$

$$a-c\equiv b-d\equiv c-e\equiv d-f\equiv e-g\equiv f-h\equiv g-a\equiv h-b \mod 2^3 \tag{8.92}$$

$$a-e\equiv b-f\equiv c-g\equiv d-h\equiv e-a\equiv f-b\equiv g-c\equiv h-d \mod 2^4. \tag{8.93}$$

Note that the first three conditions correspond to the block property and the last two correspond to Eqn. (8.67) for $\ell=1$ and $\ell=2$ if $a,\dots,h=\mathrm{F}^k(n_{000}),\dots,\mathrm{F}^k(n_{111})$. This completes the proof of relation (1).

To prove (2) we assume $k\geq 1$ (we leave it to the reader to verify (2) for $k=0$ by, for example, using an adapted version of Lemma 4.14 to bound the degree of f), $f(x)=\sum_{i=0}^d a_i x^i$, and $c\in\mathbb{Z}_2$ and compute

$$f\left(n+c2^k\right)=\sum_{i=0}^d a_i\sum_{j=0}^i\binom{i}{j}c^j 2^{jk}n^{i-j} \tag{8.94}$$

$$=\sum_{i=0}^d a_i\sum_{j=0}^5\binom{i}{j}c^j 2^{jk}n^{i-j}+\sum_{i=6}^d a_i\sum_{j=6}^i\binom{i}{j}c^j 2^{jk}n^{i-j} \tag{8.95}$$

$$=\sum_{i=0}^5 c^i 2^{ik}\frac{f^{(i)}(n)}{i!}+2^{k+5}2^{5k-5}\sum_{i=6}^d a_i\sum_{j=6}^i\binom{i}{j}c^j 2^{(j-6)k}n^{i-j} \tag{8.96}$$

$$\equiv\sum_{i=0}^5 c^i 2^{ik}\frac{f^{(i)}(n)}{i!} \mod 2^{k+5} \tag{8.97}$$

where $f^{(i)}$ denotes the i-th derivative of f. Thus,

$$\mathrm{D}(\mathrm{F}_2)[f(n+c2^k)][k,k+4] \tag{8.98}$$

$$=\mathrm{D}(\mathrm{F}_2)\left[\sum_{i=0}^5 c^i 2^{ik}\frac{f^{(i)}(n)}{i!}\right][k,k+4] \tag{8.99}$$

$$=\mathrm{D}(\mathrm{F}_2)\left[\frac{f(n)-f(n)\%2^k}{2^k}+cf'(n)+\left(k\leq 4\ ?\ \sum_{i=2}^5 c^i 2^{(i-1)k}\frac{f^{(i)}(n)}{i!}:0\right)\right][\overline{4}]. \tag{8.100}$$

Consequently, (2) can be rewritten as

$$\begin{aligned}(8.101)\qquad & \varphi_{f,k+2}(n_{000}) + \varphi_{f,k+2}(n_{010}) + \varphi_{f,k+3}(n_{000}) + \varphi_{f,k+3}(n_{010}) + \\ & \quad \varphi_{f,k+3}(n_{001}) + \varphi_{f,k+3}(n_{011}) \equiv \\ & 0 \mod 2 \Leftrightarrow \\ (8.102)\qquad & \mathrm{D}(\mathrm{F}_2)\left[f(n+0\cdot 2^k)\right][k+2] + \mathrm{D}(\mathrm{F}_2)\left[f(n+2\cdot 2^k)\right][k+2] + \\ & \quad \mathrm{D}(\mathrm{F}_2)\left[f(n+0\cdot 2^k)\right][k+3] + \mathrm{D}(\mathrm{F}_2)\left[f(n+2\cdot 2^k)\right][k+3] + \\ & \quad \mathrm{D}(\mathrm{F}_2)\left[f(n+4\cdot 2^k)\right][k+3] + \mathrm{D}(\mathrm{F}_2)\left[f(n+6\cdot 2^k)\right][k+3] \equiv \\ & 0 \mod 2 \Leftrightarrow \\ (8.103)\qquad & \mathrm{D}(\mathrm{F}_2)[u_0][2] + \mathrm{D}(\mathrm{F}_2)[u_0+2u_1][2] + \\ & \quad \mathrm{D}(\mathrm{F}_2)[u_0][3] + \mathrm{D}(\mathrm{F}_2)[u_0+2u_1+(k=1\ ?\ 8u_2:0)][3] + \\ & \quad \mathrm{D}(\mathrm{F}_2)[u_0+4u_1][3] + \mathrm{D}(\mathrm{F}_2)[u_0+6u_1+(k=1\ ?\ 8u_2:0)][3] \equiv \\ & 0 \mod 2\end{aligned}$$

where $u_0 := \big((f(n) - f(n)\%2^k)/2^k\big)\,\%2^4 \in \underline{2}^4$, $u_1 := f'(n)\%2^4 \in \underline{2}^4 \cap (2\mathbb{Z}+1)$ (if $f'(n) \in 2\mathbb{Z}_2$ then $f(n+2^k) \equiv f(n) + 2^{k+1}f'(n)/2 \equiv f(n) \mod 2^{k+1}$ but $n + 2^k \not\equiv n \mod 2^{k+1}$ which contradicts the assumption that f is a 2-permutation polynomial), and $u_2 = (f''(n)/2)\,\%2^4 \in \underline{2}^4$. It can easily be verified that Eqn. (8.103) holds for all $k \in \{1,2,3,4\}$, $u_0, u_2 \in \underline{2}^4$, and $u_1 \in \underline{2}^4 \cap (2\mathbb{Z}+1)$ which completes the proof of (2).

The proofs of (3) and (4) can be done in an analogous fashion using again Eqn. (8.100). The relations we need to verify in order to prove (3) are

$$\begin{aligned}(8.104)\qquad & \mathrm{D}(\mathrm{F}_2)[u_0][1] + \mathrm{D}(\mathrm{F}_2)[u_0][2] + \mathrm{D}(\mathrm{F}_2)[u_0+2u_1+(k=1\ ?\ 8u_2:0)][3] + \\ & \quad \mathrm{D}(\mathrm{F}_2)[u_0+6u_1+(k=1\ ?\ 8u_2:0)][3] \equiv \\ & 0 \mod 2\end{aligned}$$

for all $k \in \{1,2,3,4\}$, $u_0, u_2 \in \underline{2}^4$, and $u_1 \in \underline{2}^4 \cap (2\mathbb{Z}+1)$. To prove (4) we need to show that

$$\begin{aligned}(8.105)\qquad & (\mathrm{D}(\mathrm{F}_2)[u_0][1] + \mathrm{D}(\mathrm{F}_2)[u_0+2u_1][2] + \mathrm{D}(\mathrm{F}_2)[u_0][3] \in \{0,3\}\ ?\ 0:1) \equiv \\ & \mathrm{D}(\mathrm{F}_2)[u_0][0] + \mathrm{D}(\mathrm{F}_2)[u_0+u_1+(k=1\ ?\ 2u_2:0)][1] + \mathrm{D}(\mathrm{F}_2)[u_0][2] + \\ & \quad \mathrm{D}(\mathrm{F}_2)[u_0+2u_1+(k=1\ ?\ 8u_2:0)][3] + \mathrm{D}(\mathrm{F}_2)[u_0][4] + \mathrm{D}(\mathrm{F}_2)[u_0+4u_1][4] \mod 2\end{aligned}$$

for all $k \in \{1,2,3,4\}$, $u_0, u_2 \in \underline{2}^5$, and $u_1 \in \underline{2}^5 \cap (2\mathbb{Z}+1)$.

With the relations (1) – (4) at our disposal we are now able to prove the original statement of the theorem. It turns out that the isomorphism classes of subtrees of the tree of cycles $\mathcal{G}(\pi)$ of some 2-adic permutation π which satisfies the relations given in (1) – (4) are exactly those indicated by black boxes in Figure 6. Specifically, we will show,

$$\begin{aligned}(8.106)\quad S'_{2,4} \supseteq S''_{2,4} \ :=\ \big\{&\text{isomorphism class of } T \mid \pi \in \overline{\mathcal{P}}_2 \text{ such that } \pi \text{ satisfies (1)} \\ &T \text{ full 4-layer rooted subtree of } (\mathcal{G}(\pi), c(\pi))\big\} \\ (8.107)\quad T'_{2,4} \supseteq T''_{2,4} \ :=\ \big\{&\text{isomorphism class of } T \mid \pi \in \overline{\mathcal{P}}_2 \text{ such that } \pi \text{ satisfies (1)} \\ &T \text{ full 4-layer rooted subtree of } (\mathcal{G}(\pi), c(\pi)) \\ &|\sigma| > 1 \text{ for root } (\ell, \sigma) \text{ of } T\big\} \\ (8.108)\quad U'_{2,4} \supseteq U''_{2,4} \ :=\ \big\{&\text{isomorphism class of } T \mid f \in \overline{\mathcal{P}}_2 \text{ such that } f \text{ satisfies (2), (3)} \\ &T \text{ full 4-layer rooted subtree of } (\mathcal{G}(f), c(f))\big\} \\ (8.109)\quad V'_{2,4} \supseteq V''_{2,4} \ :=\ \big\{&\text{isomorphism class of } T \mid f \in \overline{\mathcal{P}}_2 \text{ such that } f \text{ satisfies (2), (3), (4)} \\ &T \text{ full 4-layer rooted subtree of } (\mathcal{G}(f), c(f)) \\ &|\sigma| > 1 \text{ for root } (\ell, \sigma) \text{ of } T\big\}\end{aligned}$$

where $S'_{2,4}$, $T'_{2,4}$, $U'_{2,4}$, and $V'_{2,4}$ are the sets of those 71, 50, 83, and 7 isomorphism classes of 4-layer rooted trees with out-degrees in $\{1,2\}$ which are claimed to form the sets $S_{2,4}$, $T_{2,4}$, $U_{2,4}$, and $V_{2,4}$ respectively in Figure 6. Note that we already proved $S'_{2,4} \subseteq S_{2,4}$, $T'_{2,4} \subseteq T_{2,4}$, $U'_{2,4} \subseteq U_{2,4}$, $V'_{2,4} \subseteq V_{2,4}$ (by listing examples) and $S_{2,4} \subseteq S''_{2,4}$, $T_{2,4} \subseteq T''_{2,4}$, $U_{2,4} \subseteq U''_{2,4}$, $V_{2,4} \subseteq V''_{2,4}$ (by showing (1) – (4)).

We demonstrate the idea of proof by showing that tree 4-52 from Figure 6 does not belong to $S''_{2,4}$. All other trees can be dealt with in an analogous fashion. Figure 7 shows a possible realization of tree 4-52 and it is indicated in the caption that $k = 4$ and $n \in \{2, 8\}$ violate relation (1). In the following we will argue that any such possible realization of tree 4-52 necessarily violates relation (1) and thus the isomorphism class of the tree cannot be contained in $S''_{2,4}$. We start by defining the auxiliary function

$$\begin{aligned} \overline{\varphi}_{\pi,k}(n) : \mathbb{Z}_2 &\to \{0,1\} \\ n &\mapsto \big(\varphi_{\mathrm{id}_{\mathbb{Z}_2},k}(n) + \varphi_{\pi,k}(n)\big)\,\%2 \end{aligned} \tag{8.110}$$

for all 2-adic permutations π and all $k \in \mathbb{N}_0$, where $\mathrm{id}_{\mathbb{Z}_2}$ is the identity function on $\mathbb{Z}_2$. Then,

$$\overline{\varphi}_{\pi,k}(n) = (\mathrm{D}((x, x-1))[n][k] = \mathrm{D}((x, x-1))[\pi(n)][k]\ ?\ 0 : 1) \tag{8.111}$$

for all $n \in \mathbb{Z}_2$, i.e. $\overline{\varphi}_{\pi,k}(n) = 0$ if the k-th binary digits of n and $\pi(n)$ coincide, and $\overline{\varphi}_{\pi,k}(n) = 1$ otherwise. Furthermore,

$$\overline{\varphi}_{\pi,k}(n) = \overline{\varphi}_{\pi,k}(n + 2^k) \tag{8.112}$$

and if $\pi = \pi_{\mathrm{F,G}}$ for some $\mathbb{Z}_2$-polynomial 2-adic systems F and G then,

$$\begin{aligned} &\overline{\varphi}_{\pi,k+1}(n_0) + \overline{\varphi}_{\pi,k+1}(n_1) + \\ &\quad \overline{\varphi}_{\pi,k+2}(n_{00}) + \overline{\varphi}_{\pi,k+2}(n_{01}) + \\ &\quad \overline{\varphi}_{\pi,k+3}(n_{100}) + \overline{\varphi}_{\pi,k+3}(n_{110}) + \overline{\varphi}_{\pi,k+3}(n_{101}) + \overline{\varphi}_{\pi,k+3}(n_{111}) \\ &\equiv 0 \mod 2 \end{aligned} \tag{8.113}$$

$$\begin{aligned} &\overline{\varphi}_{\pi,k+1}(n_0) + \overline{\varphi}_{\pi,k+1}(n_1) + \\ &\quad \overline{\varphi}_{\pi,k+2}(n_{10}) + \overline{\varphi}_{\pi,k+2}(n_{11}) + \\ &\quad \overline{\varphi}_{\pi,k+3}(n_{000}) + \overline{\varphi}_{\pi,k+3}(n_{010}) + \overline{\varphi}_{\pi,k+3}(n_{001}) + \overline{\varphi}_{\pi,k+3}(n_{011}) \\ &\equiv 0 \mod 2 \end{aligned} \tag{8.114}$$

for all $k \in \mathbb{N}_0$ and $n \in \mathbb{Z}_2$ by (1). Consequently,

$$\begin{aligned} &\sum_{i=0}^{\ell-1} \Big(\overline{\varphi}_{\pi,k+1}(n[i]_0) + \overline{\varphi}_{\pi,k+1}(n[i]_1) + \\ &\quad \overline{\varphi}_{\pi,k+2}(n[i]_{d[i]0}) + \overline{\varphi}_{\pi,k+2}(n[i]_{d[i]1}) + \\ &\quad \overline{\varphi}_{\pi,k+3}(n[i]_{e[i]00}) + \overline{\varphi}_{\pi,k+3}(n[i]_{e[i]10}) + \overline{\varphi}_{\pi,k+3}(n[i]_{e[i]01}) + \overline{\varphi}_{\pi,k+3}(n[i]_{e[i]11}) \Big) \\ &\equiv 0 \mod 2 \end{aligned} \tag{8.115}$$

for all $\ell \in \mathbb{N}$, $n \in \mathbf{S}(\mathrm{bnd}_{2^k}, \mathrm{len}_\ell)$, and $d, e \in \mathbf{S}(\mathrm{bnd}_{\{0,1\}}, \mathrm{len}_\ell)$ with $e = 1 - d$.

Using Eqn. (8.115) we will now show that tree 4-52 from Figure 6 does not belong to $S''_{2,4}$. For this purpose let $\pi \in \overline{\mathcal{P}}_2$ and $k \in \mathbb{N}_0$ such that $(\mathcal{G}(\pi), c(\pi))$ contains a subtree T which is isomorphic to tree 4-52. Note that in the example given in Figure 7 we have $k = 4$ and $\sigma_0 = (0, 2, 8, 10)$ (to improve readability we omit the square brackets indicating equivalence classes). Let $v_1, \ldots, v_{15}$ denote the remaining vertices of T, ordered in a way that is compatible (regarding graph isomorphy) with the ordering given in Figure 7, and let $\sigma_0, \ldots, \sigma_{15}$ denote the corresponding cycles. If we set $\ell := |\sigma_0|$, then $|\sigma_1| = |\sigma_2| = |\sigma_4| = |\sigma_5| = \ell$, $|\sigma_3| = |\sigma_6| = |\sigma_7| = |\sigma_8| = |\sigma_9| = |\sigma_{12}| = |\sigma_{13}| = |\sigma_{14}| = |\sigma_{15}| = 2\ell$, and $|\sigma_{10}| = |\sigma_{11}| = 4\ell$ by Corollary 3.24. Furthermore, by the defining properties of p-adic permutations (cf. Eqn. (3.93), Eqn. (3.94), and Theorem 3.22) we get the following structural properties of the tables representing the binary expansions of the cycles corresponding to the vertices of T (cf. Figure 7):

- The block below the first row of every child vertex (gray and dark gray parts) is either a copy of the whole table of its parent vertex (if it has a sibling) or two such copies next to each other (if it is an only child).
- The first rows (light gray parts) of two siblings are ones' complements of each other and the first row of an only child has two parts of equal lengths which are ones' complements of each other.
- On top of every "parent block" the first row of every child vertex v which has a sibling has an even number $c(v)$ of entries which differ from the respective following entries (cyclically) and the first row of every only child has an odd number of such entries (in Figure 7 the numbers $c(v)$ are given next to the respective vertex). If $v = (k, \sigma)$, $c(v) = \sum_{i=0}^{l-1} \overline{\varphi}_{\pi,k-1}(\sigma[i])$ by Eqn. (8.111).

Let $n \in \mathbf{S}(\mathrm{bnd}_{2^k}, \mathrm{len}_\ell)$ such that $\sigma_0 = [([n[0]], \ldots, [n[\ell-1]])]_{\sim_\sigma}$ (n is one of the sequences $(0,2,8,10)$, $(2,8,10,0)$, $(8,10,0,2)$, $(10,0,2,8)$ in the example given in Figure 7). Furthermore, let $d \in \mathbf{S}(\mathrm{bnd}_{\{0,1\}}, \mathrm{len}_\ell)$ be the corresponding top row of v_1 (i.e. $(0,1,0,1)$, $(1,0,1,0)$, $(0,1,0,1)$, or $(1,0,1,0)$ in the example given in Figure 7) and set $e := 1 - d$. Since v_3 is an only child and v_4, v_6, v_{12}, and v_{14} all have siblings, $c(v_3) + c(v_4) + c(v_6) + c(v_{12}) + c(v_{14})$ is odd. But by definition of n, d, and e, this sum is equal to the sum given in Eqn. (8.115) which is even if π satisfies (1). Consequently, tree 4-52 cannot belong to $S''_{2,4}$ as claimed.

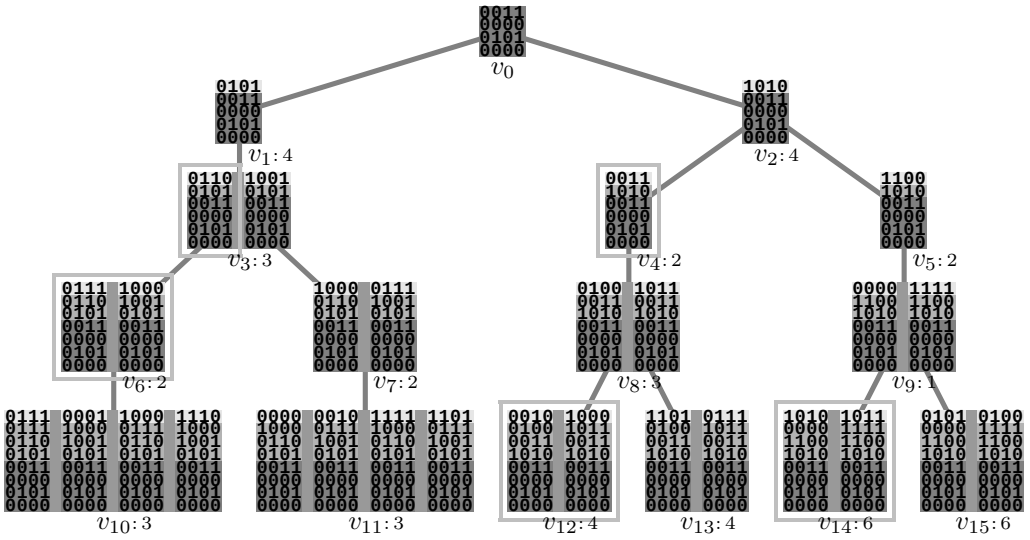

FIGURE 7. A possible scenario for obtaining tree 4-52 from Figure 6. The vertices $v_0, \ldots, v_{15}$ correspond to the cycles $\sigma_0 = (0,2,8,10)$ of π_4, $\sigma_1 = (0,18,8,26)$, $\sigma_2 = (16,2,24,10)$ of π_5, $\sigma_3 = (0,50,40,26,32,18,8,58)$, $\sigma_4 = (16,2,56,42)$, $\sigma_5 = (48,34,24,10)$ of π_6, $\sigma_6 = (0,114,104,90,96,18,8,58)$, $\sigma_7 = (64,50,40,26,32,82,72,122)$, $\sigma_8 = (16,66,56,42,80,2,120,106)$, $\sigma_9 = (48,34,24,10,112,98,88,74)$ of π_7, and $\sigma_{10} = (0,242,232,218,96,18,8,186,128,114,104,90,224,146,136,58)$, $\sigma_{11} = (64,50,40,26,32,82,200,122,192,178,168,154,160,210,72,250)$, $\sigma_{12} = (16,66,184,42,208,2,120,106)$, $\sigma_{13} = (144,194,56,170,80,130,248,234)$, $\sigma_{14} = (176,34,152,10,240,98,216,202)$, $\sigma_{15} = (48,162,24,138,112,226,88,74)$ of π_8, written in base 2 with most significant digits being in the top rows. The tree violates $\varphi_{\pi,k+2}(n_{000}) + \varphi_{\pi,k+2}(n_{010}) + \varphi_{\pi,k+3}(n_{100}) + \varphi_{\pi,k+3}(n_{110}) + \varphi_{\pi,k+3}(n_{101}) + \varphi_{\pi,k+3}(n_{111}) \equiv \varphi_{\pi,k+1}(n_{000}) + \varphi_{\pi,k+1}(n_{100}) \mod 2$ (relation (1)) for $k = 4$ and $n \in \{2,8\}$ ($1+0+0+0+1+0 \not\equiv 1+0 \mod 2$ and $0+0+1+1+0+0 \not\equiv 1+0 \mod 2$) and can thus not be realized as a subtree of $(\mathcal{G}(\pi_{\mathrm{F,G}}), c(\pi_{\mathrm{F,G}}))$ for any $\mathrm{F}, \mathrm{G} \in \overline{\mathcal{F}}_2(\mathrm{poly}_{\mathbb{Z}_2})$.

□

Theorem 8.5 finally allows us to prove that there is a p-permutation polynomial f which cannot be written as $f = \pi_{\mathrm{F,G}}$ where F and G are $\mathbb{Z}_p$-polynomial p-adic systems as the following example shows.

Example 8.6. Let $f(x) = 2x^3+x+2 \in \mathbb{Z}_2[x]$. Then f is a 2-permutation polynomial by Lemma 8.1 and $(\mathcal{G}(f), c(f))$ contains a subtree which is isomorphic to tree 4-15 from Figure 6. Thus $f \neq \pi_{\mathrm{F,G}}$ for all $\mathbb{Z}_2$-polynomial 2-adic systems F and G by Theorem 8.5.

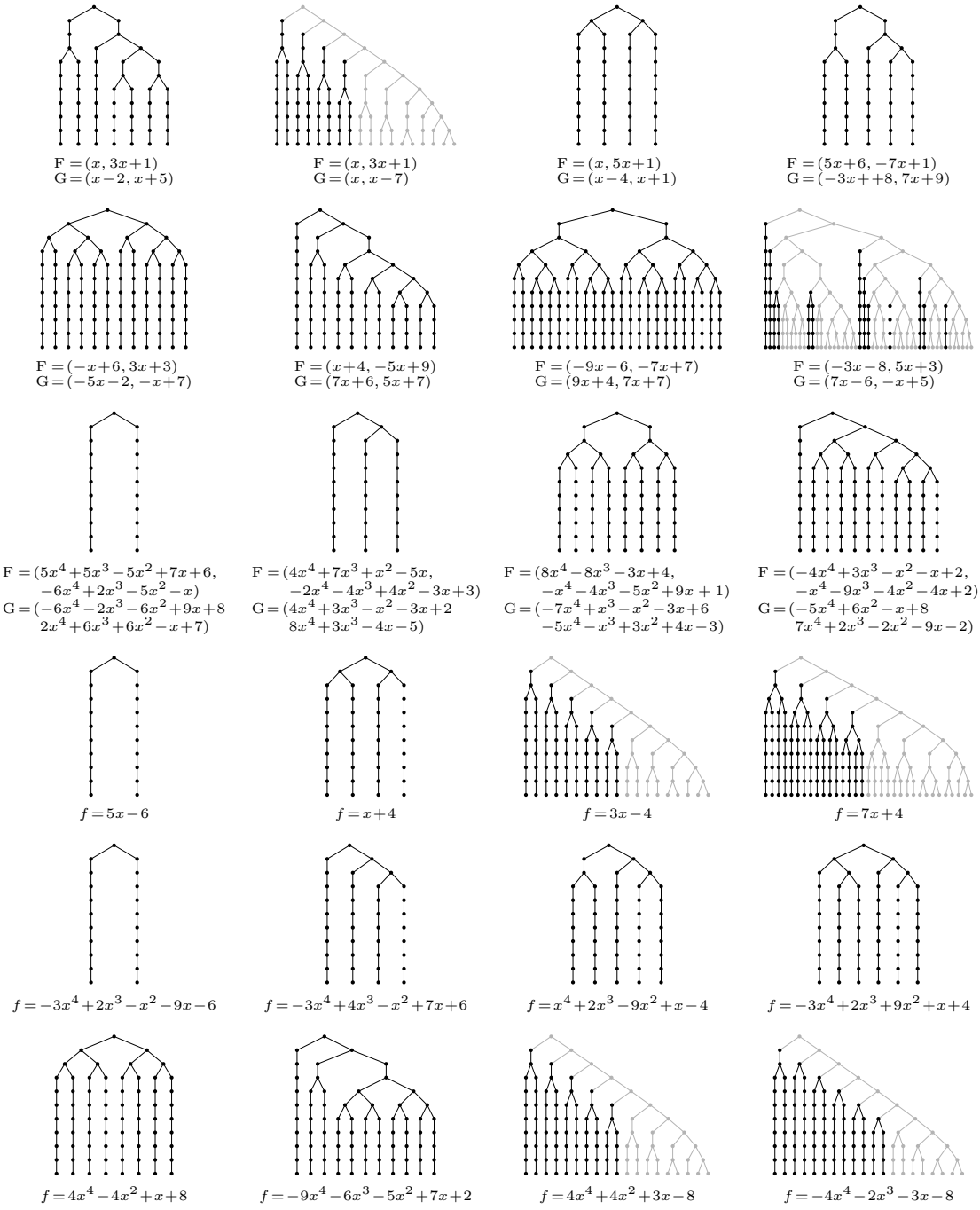

FIGURE 8. Several examples of 2-cycle trees of the form $\mathcal{G}(\pi_{\mathrm{F,G}})$, respectively $\mathcal{G}(f)$. Infinite subtrees rooted in black vertices are completely characterized due to Corollary 8.7.

In certain situations the following corollary of Theorem 8.5 allows for the characterization of the complete (infinite) tree $(\mathcal{G}(\pi_{\mathrm{F,G}}), c(\pi_{\mathrm{F,G}}))$ where F and G are $\mathbb{Z}_2$-polynomial 2-adic systems, respectively $(\mathcal{G}(f), c(f))$ where f is a 2-permutation polynomial.

Corollary 8.7 (No "Y" property)**.** *Let* $\mathrm{F}, \mathrm{G} \in \overline{\mathcal{F}}_2(\mathrm{poly}_{\mathbb{Z}_2})$*, f a 2-permutation polynomial, and* $\pi = \pi_{\mathrm{F,G}}$ *or* $\pi = f$*. Furthermore, let* $\ell \in \mathbb{N}$ *and* $(v_1, \ldots, v_\ell)$ *be a (directed) path in* $\mathcal{G}(\pi)$ *with* $\deg_o(v_i) = 1$ *(out-degree) for all* $i \in [\![1, \ell - 1]\!]$ *and* $deg_o(v_\ell) = 2$ *(i.e. the graph induced by the vertices* $v_1, \ldots, v_\ell$ *and the two children of* v_ℓ *looks like the letter "Y"). Then,* $\ell \leq 3$*.*

Proof. Follows directly from the absence of black boxes underneath tree 4-2 in Figure 6. □

Informally, the previous corollary states that if a branch of a 2-cycle tree defined by $\mathbb{Z}_2$-polynomial 2-adic systems or by 2-permutation polynomials doesn't split for 3 consecutive times, it will never split. Thus, several of the trees shown in Figure 8 are completely characterized and others are characterized at least in (infinite) parts.

9. Open questions and problems

To provide a possible roadmap for future investigations of p-adic systems in many different directions we give a list, by no means exhaustive, of potentially interesting questions and problems below. Whenever we refer to "classes of p-adic systems" (or, analogously, "classes of p-digit tables with block property" or "classes of p-adic permutations", cf. Section 3), we intend this to be understood as any meaningful collection of p-adic systems that is described in this article or that will be found during future investigations of p-adic systems. Examples of such classes are

- the class $\overline{\mathcal{F}}_p(\mathrm{poly}_{A,D})$ of A-polynomial p-adic systems with degree in D with some natural choices for A and D, such as $A = \mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q} \cap \mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p, \ldots$ and $D = \{d\}, \overline{d}, \mathbb{N}, \ldots$
- p-adic systems defined by rational functions or power series, again with possible restrictions to the occurring coefficients and degrees
- p-adic systems of the form $\mathrm{F_D}$ (cf. Theorem 3.12) where D belongs to some class of p-digit tables with block property, such as p-digit tables defined by sequences like the Thue-Morse sequence (p. 18)
- p-adic systems of the form ${\Pi_{\mathrm{G}}}^{-1}(f)$ where G is a fixed p-adic system or itself ranging over some class of p-adic systems and f belongs to some class of p-adic permutations, such as
  - p-permutation polynomials with possible restrictions to the occurring coefficients and degrees
  - p-adic permutations of the form $\pi_{\mathrm{F,G}}$ with F and G again belonging to some classes of p-adic systems
  - finite products $\mathrm{F}_1 \circ_{\mathrm{G}} \ldots \circ_{\mathrm{G}} \mathrm{F}_\ell$ of p-adic systems from a certain class (cf. Theorem 3.19 et seq.) with a fixed or bounded number ℓ of operands
  - the closure under $\circ_{\mathrm{G}}$ of any union of previously mentioned classes of p-adic permutations
- any of the above, with bounds on p (fixed value, range, only primes, etc.) or restrictions imposed by demanding additional properties, such as being contractive, expansive, of mixed type, avoiding, periodic, ultimately periodic, or aperiodic on some given set, etc.

With these examples of classes of p-adic systems at hand we are ready to provide the announced list of open questions and problems.

1) Investigate p-adic systems from the perspective of them being number systems. For a p-adic system F let $S \star_{\mathrm{F}} T := \psi_{\mathrm{F}}\left(\psi_{\mathrm{F}}^{-1}(S) \star \psi_{\mathrm{F}}^{-1}(T)\right)$ for all $S, T \in \mathbf{S}(\mathrm{bnd}_{\underline{p}}, \neg\mathrm{fin})$ and any operation $\star \in \{+, -, \cdot\}$. If $\mathrm{F} = \mathrm{F}_p$, there are efficient algorithms for the computation of $S \star_{\mathrm{F}} T$. Are there other choices for F for which useful algorithms can be found? Furthermore, if $\mathrm{F} = \mathrm{F}_p$ there is no known efficient algorithm for the computation of a prime factor of some $n \in \mathbb{N}$ from its F-digit expansion $\psi_{\mathrm{F}}(n)$. Are there other choices for F for which efficient algorithms can be found?

2) Prove Conjecture 4.18 on the characterization of all (weakly) (p, r)-suitable rational functions (cf. also Theorem 4.16 which proves a special case of the conjecture). More generally, characterize all (weakly) (p, r)-suitable analytic functions. Generalize Theorem 5.12 and characterize all (p, r)-avoiding polynomial functions in $\mathbb{Q}_p[x]$, all (p, r)-avoiding rational functions, or

even all (p,r)-avoiding analytic functions.

3) Example 4.2 demonstrates that the weak block property for p-fibred functions does not permit a necessary and sufficient characterization that only considers the functions $\mathrm{F}[0],\ldots,\mathrm{F}[p-1]$ independently from one another. Furthermore, Example 4.3 shows that there is a p-digit table with weak block property that is the p-digit table of a p-fibred function but cannot be realized as the p-digit table of a p-fibred function, whose entries are weakly (p,r)-suitable functions. Is there a predicate P on the set of functions on $\mathbb{Z}_p$ other than being weakly (p,r)-suitable which satisfies that a p-digit table that is the p-digit table of a p-fibred function has the weak block property if and only if it can be realized as the p-digit table of a p-fibred function whose entries satisfy the predicate P?

4) For every p-adic permutation π and every p-adic system G there is a unique p-adic system F such that $\pi=\pi_{\mathrm{F,G}}$ (cf. Theorem 3.18). If π belongs to a certain subclass of p-adic permutations, are there particularly "nice" choices for F and G? As examples consider the 2-adic permutations

$$f(x)=10x^2-3x+4 \tag{9.1}$$

$$g(x)=-2x^2+7x-6 \tag{9.2}$$

from the class of 2-permutation polynomials. If we set (cf. Example 5.5)

$$\mathrm{F}_1 := \left(\frac{\sqrt{200x^2-60x-71}+3}{10},\frac{\sqrt{200x^2-60x-91}+3}{10}\right) \tag{9.3}$$

$$\mathrm{F}_2 := \left(\frac{\sqrt{200x^2-60x+90-161}+3}{10},\frac{\sqrt{3(200x^2-60x+90)-161}+3}{10}\right) \tag{9.4}$$

$$\mathrm{F}_3 := \left(\frac{\sqrt{8x^2-28x+25}+7}{2},\frac{\sqrt{8x^2-28x+29}+7}{2}\right) \tag{9.5}$$

$$\mathrm{F}_4 := \left(\frac{\sqrt{8x^2-28x+22+3}+7}{2},\frac{\sqrt{3(8x^2-28x+22)+3}+7}{2}\right) \tag{9.6}$$

$$\mathrm{G}_1 := (x,x) \tag{9.7}$$

$$\mathrm{G}_2 := (x,3x+1), \tag{9.8}$$

then $f=\pi_{\mathrm{F}_1,\mathrm{G}_1}=\pi_{\mathrm{F}_2,\mathrm{G}_2}$ and $g=\pi_{\mathrm{F}_3,\mathrm{G}_1}=\pi_{\mathrm{F}_4,\mathrm{G}_2}$. Under which conditions can F and G be chosen to be both polynomial or from some other fixed class of p-adic systems?

5) Study the relation between p-adic systems and known sequences which have the (p,k)-block property such as the (slightly modified) Thue-Morse sequence (cf. p. 18).

6) Investigate the group structure of $\left(\overline{\mathcal{F}}_p,\circ_{\mathrm{G}}\right)$, respectively $\left(\overline{\mathcal{P}}_p,\circ\right)$. What do the subgroups gained from forming the closure of any of the classes of p-adic systems under $\circ_{\mathrm{G}}$ look like? Are any of the classes of p-adic systems already closed under $\circ_{\mathrm{G}}$? If F_1 and F_2 are p-adic systems, what is the relation between the sets of periodic, ultimately periodic, or aperiodic points of F_1, F_2, and their product $\mathrm{F}_1\circ_{\mathrm{G}}\mathrm{F}_2$? Can $\mathrm{F}_C=(x,3x+1)$ be written as the product of other (possibly polynomial) 2-adic systems whose sets of ultimately periodic points are known? More generally, can specific p-adic systems or even all p-adic systems from a certain class be written as the product of "nice" p-adic systems (e.g. whose sets of periodic, ultimately periodic, or aperiodic points are known, which are contractive, expansive, avoiding, etc.)?

7) Hensel's Lemma can be used to show that certain real or complex numbers that are defined by polynomial equations (such as $\sqrt{2}$ or i) have counterparts within $\mathbb{Z}_p$ for some $2\leq p\in\mathbb{N}$. Do the generalizations of Hensel's Lemma (Theorem 5.2 and Theorem 5.11) have similar applications, possibly with respect to other classes of functions?

8) Further investigate trees of cycles. What are the possible finite subtrees of trees of cycles of classes of p-adic permutations other than those covered by Theorem 8.5 (especially for $p\geq 3$ and $k\geq 4$ there)? Is it possible to characterize all trees of cycles of p-adic permutations of the form $\pi_{\mathrm{F,G}}$, where F and G are $\mathbb{Z}_p$-polynomial p-adic systems, or $\pi=f$ for some p-permutation

polynomial $f \in \mathbb{Z}_p[x]$ by extending the results of Theorem 8.5 (cf. Figure 9 below)? If π_1 and π_2 are p-adic permutations, what can be said about the relation between the trees of cycles $(\mathcal{G}(\pi_1), c(\pi_1))$, $(\mathcal{G}(\pi_2), c(\pi_2))$, and $(\mathcal{G}(\pi_1 \circ \pi_2), c(\pi_1 \circ \pi_2))$? "Having identical trees of cycles" defines an equivalence relation on the set of all p-adic systems. Theorem 8.4 gives an explicit construction of at least one p-adic permutation from a given equivalence class (given by its shared tree of cycles). Find a full characterization of all p-adic permutations in a given equivalence class. Does every equivalence class contain elements of a specific class of p-adic systems and can they too be characterized? What can be said about the relation between trees of cycles $(\mathcal{G}(\pi_{\mathrm{F,G}}), c(\pi_{\mathrm{F,G}}))$ and the sets of periodic, ultimately periodic, and aperiodic points of F and G? Conjecture 7.9 states that $\mathrm{F}_2 = (x, x-1)$ and $\mathrm{F}_C = (x, 3x+1)$ have identical sets of ultimately periodic points $(\mathbb{Q} \cap \mathbb{Z}_2)$, but F_2 and $\mathrm{F} = (x, 5x+1)$ do not (cf. also the "In particular" of Theorem 7.14). Can trees of cycles shed some light on why this is the case (cf. the first three trees in the first row of Figure 8)?

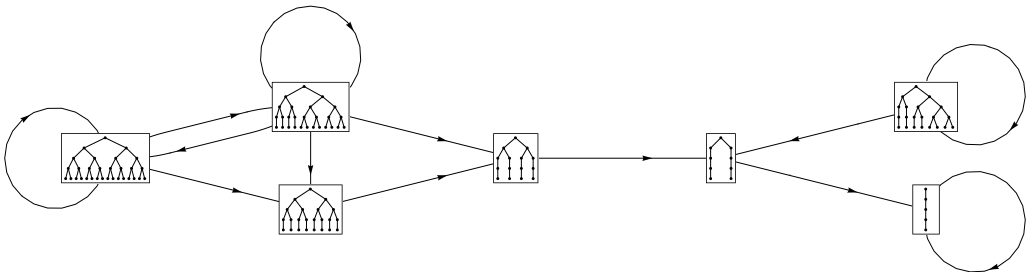

FIGURE 9. The seven elements of $V_{2,4}$ of Theorem 8.5. A directed edge from tree S to tree T indicates that S can be extended by T by one layer. It can be seen that tree 4-1 (on the bottom right) is a terminal object of the graph which is essentially the statement of Corollary 8.7 on trees of cycles of 2-permutation polynomials (no "Y" property). By studying $V_{2,k}$ for $k \geq 4$ more terminal objects may be found allowing for a full characterization of all trees of cycles $(\mathcal{G}(\pi), c(\pi))$ where $\pi = f$ for some 2-permutation polynomial f. The corresponding tree representing the extensibility of the 50-element set $T_{2,4}$ has also only one terminal object (tree 4-1 again, which is also part of the statement of Corollary 8.7). Here too it may be possible to find other terminal objects by analyzing $T_{2,k}$ for larger k.

9) Prove conjectures 7.7 – 7.12 or at least achieve first non-trivial results on the question of ultimate periodicity of linear-polynomial p-adic systems of mixed type, such as proving

- $\mathrm{D}((x^2 + x, x))[n]$ aperiodic for some concrete $n \in \mathbb{Z}$
- $\mathrm{D}((x^{1000000p} + x)^{p-1} \cdot ((p-1)x))[n]$ aperiodic for some concrete $2 \leq p \in \mathbb{N}$ and $n \in \mathbb{Z}$
- $\mathrm{D}((1000001x, x))[n]$ aperiodic for some concrete $n \in \mathbb{Z}$
- $\mathrm{D}(((p^{1000000p} + 1)x)^{p-1} \cdot ((p-1)x))[n]$ aperiodic for some concrete $2 \leq p \in \mathbb{N}$ and $n \in \mathbb{Z}$
- $\mathrm{D}((1/(p+1)x, (p-1)x) \cdot (x)^{p-2})[n]$ aperiodic for some concrete $2 \leq p \in \mathbb{N}$ and $n \in \mathbb{Z}$
- $\text{uper-on}_{\mathbb{Q} \cap \mathbb{Z}_p}(((p+1)x) \cdot (x)^{p-1})$ for some concrete $2 \leq p \in \mathbb{N}$
- $\text{uper-on}_{\mathbb{Q} \cap \mathbb{Z}_p}((1/3x, 3x))$
- $\text{uper-on}_{\mathbb{Q} \cap \mathbb{Z}_2}((1/(p-1)x) \cdot ((p-1)x)^{p-1})$ for some concrete $3 \leq p \in \mathbb{N}$

(cf. also Corollary 7.21, Figure 4, and the subsequent list of examples of p-adic systems). Is $\mathrm{D}((21/5x, 5/7x + 1))[27]$ ultimately periodic or aperiodic? If it is aperiodic, try to formulate the correct version of the condition $B \in \mathbb{Z}$ in Conjecture 7.10 (cf. the discussion of the issue between Conjecture 7.10 and Conjecture 7.11). Show $[\mathbb{Q} \cap \mathbb{Z}_p \not\subseteq \mathrm{UPerP}](\mathrm{F})$ for every polynomial p-adic system F which is not also $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial (cf. Theorem 7.13 and the subsequent comment).

10) Prove Conjecture 7.15 and Conjecture 7.17 for $p \geq 3$: the constant coefficients and the order of the linear coefficients of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems are irrelevant for the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$. Considering the condition $|B| < p^p$ in Conjecture 7.9, prove for $p \geq 2$ that the signs of the linear coefficients of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems are

irrelevant for the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$. Do other classes of p-adic systems (especially $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems of larger degrees) have similar symmetries which also fix the sets of periodic, ultimately periodic, or aperiodic points?

11) What can be said about the sets PerP(F), UPerP(F), and APerP(F) for a p-adic system F from a specific class? Do these sets have any structure, symmetries, invariants, etc.? The second generalization of Hensel's Lemma (Theorem 5.11) reveals structural properties of the set PerP(F) if F is an avoiding $\mathbb{Z}_p$-polynomial p-adic system, as the example following Theorem 5.12 shows: if $\mathrm{F} = (7x^3 - 4x^2 + x - 6, 3x^7 - x + 1, 5x^4 + 4x - 1)$, then the set of periodic points of F is equal to the set of all fixed points of arbitrary compositions of the polynomial functions F[0]/3, F[1]/3, and F[2]/3. PerP(F) can be interpreted as a "generalized zero set" defined by three polynomials in $\mathbb{Q}_3[x]$.

12) Study any of the sets PerP(A), UPerP(A), APerP(A), PerP-Gen(A), UPerP-Gen(A), or APerP-Gen(A) for any class A of p-adic systems (cf. the subsection "Generalizations" of Section 7). Do these sets have any structure, symmetries, invariants, etc.? Theorem 7.14 and Theorem 7.16 provide first results in this direction: for F from the class A of $(\mathbb{Q} \cap \mathbb{Z}_2)$-linear-polynomial 2-adic systems , UPerP(F) is invariant under the change of constant coefficients or the change of the order of linear coefficients. What is

$$\text{UPerP-Gen}(\{\mathrm{F}\}) \cap \overline{\mathcal{F}}_p(\text{poly}_{\mathbb{Q}\cap\mathbb{Z}_p}), \tag{9.9}$$

i.e. for which $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems G does one get UPerP(F) = UPerP(G), where $\mathrm{F} = (x, 5x+1)$, $\mathrm{F} = (5x, 5x+1)$, $\mathrm{F} = (x, x^2+x)$, $\mathrm{F} = (x^2+x, x^2+x)$, or F is some other concrete $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic system? This can be seen as the inverse problem of the previous question 11): for a fixed "generalized zero set" $Z \subseteq \mathbb{Z}_p$, what can be said about the p-adic systems from a certain class whose sets of periodic points are equal to the given Z? Is there a generalized Galois theory in this setting?

13) If F is a $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic system, then $[\text{UPerP} \subseteq \mathbb{Q} \cap \mathbb{Z}_p](\mathrm{F})$ by the "In particular" part of Corollary 7.3 (cf. also Conjecture 7.10 on when we have $[\text{UPerP} = \mathbb{Q} \cap \mathbb{Z}_p](\mathrm{F})$). Find any such F and a p-adic integer n whose F-digit expansion is aperiodic and equal to any known sequence in $\mathbf{S}(\mathrm{bnd}_{\underline{p}}, \neg\mathrm{fin})$ (like the real base p expansion of some irrational number or the Thue-Morse sequence). Specifically, what is $\pi_{(x,3x+1),(x,x-1)}(\sqrt{17})$ (cf. Example 5.5)?

14) For every $2 \leq p \in \mathbb{N}$, every countable subset A of $\mathbb{Z}_p$ and every finite $\underline{p}$-bounded sequence S there is a p-adic system F such that the periodic part of the F-digit expansion of every n in A is cyclically equivalent to S (cf. the definition of $\sim_\sigma$ on p. 21). In order to find such an F, pick any countable subset B of $\mathbb{Z}_p$ which is dense in $\mathbb{Z}_p$ and construct a p-digit table D by fixing an ultimately periodic D-digit expansion with period S (or an aperiodic D-digit expansion if S is empty) for the elements of $A \cup B$ one at a time, in a way that is compatible (regarding the block property) with what has already been fixed. After D has been constructed, let $\mathrm{E} \in \overline{\mathcal{D}}_p$ be its unique extension by Lemma 3.15 and let $\mathrm{F} := \mathrm{F_E}$ be the p-adic system corresponding to E according to Theorem 3.12. For specific choices for A and S, are there "nice" p-adic systems F with the described property? As an example consider the non-standard ternary (cf. [54, 27]) system $\mathrm{F} = (x, x+1, x-1)$ which has the property that all integers (i.e. $A = \mathbb{Z}$) have an ultimately periodic F-digit expansion with period (0) (i.e. $S = (0)$). This can be proven by verifying that the F-sequences of all integers n with $|n| \leq 2$ are ultimately periodic with period (0) (cf. the definition of M in the proof of Theorem 7.19 and the "In particular" part of Lemma 6.2 (1)). The "niceness" of F in this case is of course given by the fact that F is $\mathbb{Z}$-linear-polynomial. Is there a "nice" (from a specific class, closed on the integers, etc.) p-adic system F which has the property that all rational numbers (i.e. $A = \mathbb{Q} \cap \mathbb{Z}_p$) have an ultimately periodic F-digit expansion with period (0)?

15) If F and G are concrete p-adic system systems and f is a concrete p-permutation polynomial, plotting any of the permutations π_k of $\underline{p^k}$ (we identify $\mathbb{Z}_p/p^k\mathbb{Z}_p$ and $\underline{p^k}$) for $\pi := \pi_{\mathrm{F,G}}$ or $\pi = f$ often reveals intriguing patterns, as Figure 10 shows. Study such permutations with regard to randomness and discrepancy (see [16] for an introduction to discrepancy theory and notions of randomness).

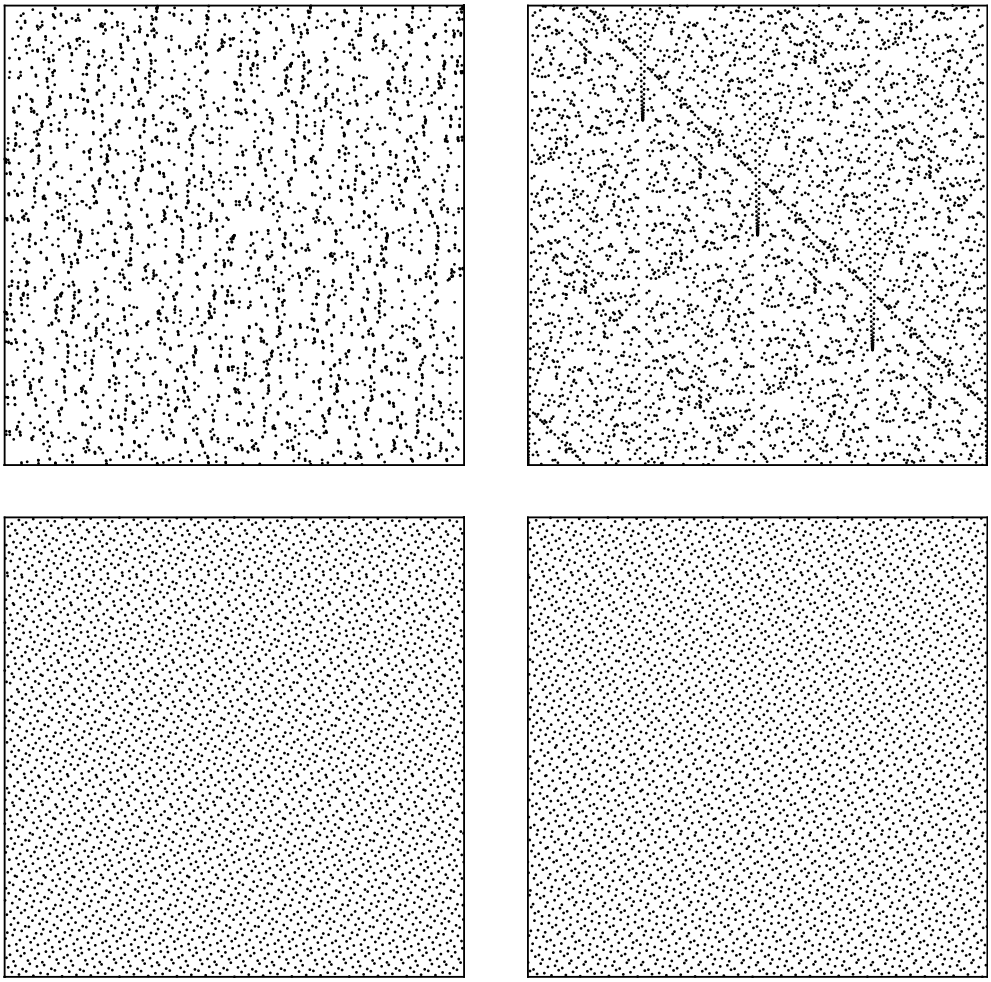

FIGURE 10. The permutation $\pi_{12} : \underline{2^{12}} \to \underline{2^{12}}$ for $\pi = \pi_{(x,3x+1),(x,x-1)}$ (top left) and $\pi = 2x^2 + 3x + 2$ (top right). The respective images in the bottom row show the permutations $\mathrm{inv} \circ \pi_{12} : \underline{2^{12}} \to \underline{2^{12}}$ where $\mathrm{inv} : \underline{2^{12}} \to \underline{2^{12}}$ inverts the 12 digits of the binary expansion of its input (e.g. $\mathrm{inv}(318) = 1992$).

ACKNOWLEDGMENT

The author is supported by the FWF stand-alone project P 30205-NBL "Arithmetic Dynamical Systems, Polynomials, and Polytopes" (`http://marioweitzer.com/fwf_adspp`).

REFERENCES

[1] S. AKIYAMA, T. BORBÉLY, H. BRUNOTTE, A. PETHŐ, AND J. M. THUSWALDNER, *Generalized radix representations and dynamical systems. I*, Acta Math. Hungar., 108 (2005), pp. 207–238.

[2] S. AKIYAMA, H. BRUNOTTE, A. PETHŐ, AND J. M. THUSWALDNER, *Generalized radix representations and dynamical systems. II*, Acta Arith., 121 (2006), pp. 21–61.

[3] ———, *Generalized radix representations and dynamical systems. III*, Osaka J. Math., 45 (2008), pp. 347–374.

[4] ———, *Generalized radix representations and dynamical systems. IV*, Indag. Math. (N.S.), 19 (2008), pp. 333–348.

[5] J. M. AMIGÓ, *Accelerated Collatz Dynamics*, Report de recerca, Centre de Recerca Matemática, Barcelona, 2000.

[6] ———, *Representing the integers with powers of* 2 *and* 3, Acta Inform., 43 (2006), pp. 293–306.

[7] G. BARAT, V. BERTHÉ, P. LIARDET, AND J. M. THUSWALDNER, *Dynamical directions in numeration*, Ann. Inst. Fourier, 56 (2006), pp. 1987–2092.

[8] E. G. BELAGA AND M. MIGNOTTE, *Embedding the* $3x+1$ *conjecture in a* $3x+d$ *context*, Exp. Math., 7 (1998), pp. 145–151.

[9] A. Bertrand-Mathis, *Comment écrire les nombres entiers dans une base qui n'est pas entière*, Acta Math. Hungar., 54 (1989), pp. 237–241.
[10] F. Blanchard, *β-expansions and symbolic dynamics*, Theoret. Comput. Sci., 65 (1989), pp. 131–141.
[11] C. Böhm and G. Sontacchi, *On the existence of cycles of given length in integer sequences like $x_{n+1} = x_n/2$ if x_n even, and $x_{n+1} = 3x_n + 1$ otherwise*, Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur., 8/64 (1978), pp. 260–264.
[12] H. Brunotte, P. Kirschenhofer, and J. M. Thuswaldner, *Shift radix systems for Gaussian integers and Pethő's Loudspeaker*, Publ. Math. Debrecen, 79 (2011), pp. 341–356.
[13] M. Chamberland, *An update on the $3x + 1$ problem*, Butl. Soc. Catalana Mat., 22 (2003), pp. 1–27.
[14] V. Dimitrov, L. Imbert, and K. M. Pradeep, *The double-base number system and its application to elliptic curve cryptography*, in Mathematics of Computation, 2008, pp. 1075–1104.
[15] V. S. Dimitrov, G. A. Jullien, and W. C. Miller, *Theory and applications of the double-base number system*, IEEETC, 48 (1999), pp. 1098–1106.
[16] M. Drmota and R. F. Tichy, *Sequences, Discrepancies and Applications*, Lecture Notes in Mathematics, Springer, Heidelberg, 1997.
[17] C. Frougny, *Number representation and finite automata*, in Topics in symbolic dynamics and applications (Temuco, 1997), vol. 279 of London Math. Soc. Lecture Note Ser., Cambridge University Press, 2000, pp. 207–228.
[18] C. Frougny and B. Solomyak, *Finite beta-expansions*, Ergodic Theory Dynam. Systems, 12 (1992), pp. 713–723.
[19] W. J. Gilbert, *Radix representations of quadratic fields*, J. Math. Anal. Appl., 83 (1981), pp. 264–274.
[20] F. Gouvêa, *p-adic Numbers: An Introduction*, Universitext, Springer, Berlin, 1997.
[21] K. Hensel, *Neue Grundlagen der Arithmetik*, J. Reine Angew. Math., 127 (1904), pp. 51–84.
[22] I. Kátai and B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged), 42 (1980), pp. 1–2.
[23] ———, *Canonical number systems in imaginary quadratic fields*, Acta Math. Hungar., 37 (1981), pp. 159–164.
[24] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged), 37 (1975), pp. 255–260.
[25] S. Katok, *p-adic Analysis Compared with Real*, Student mathematical library, American Mathematical Society, Orlando, 2007.
[26] G. Keller and F. R. Olsen, *Counting polynomial functions* (mod p^n), Duke Math. J., 35 (1968), pp. 835–838.
[27] R. Kenyon, *Open problems*. `http://www.math.brown.edu/~rkenyon/openprobs/index.html`. Accessed: November 12, 2019.
[28] P. Kirschenhofer and J. M. Thuswaldner, *Shift radix systems - A survey*, RIMS Kôkyûroku Bessatsu, B46 (2014), pp. 1–59.
[29] D. E. Knuth, *A imaginary number system*, Commun. ACM, 3 (1960), pp. 245–247.
[30] ———, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Addison Wesley, Boston, 3rd ed., 1998.
[31] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Hungar., 37 (1981), pp. 405–407.
[32] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged), 55 (1991), pp. 287–299.
[33] J. C. Lagarias, *The $3x + 1$ problem and its generalizations*, Amer. Math. Monthly, 92 (1985), pp. 3–23.
[34] ———, *The $3x + 1$ problem: An annotated bibliography (1963–1999)*, 2003.
[35] ———, *The $3x + 1$ problem: An annotated bibliography, II (2000–2009)*, 2006.
[36] ———, *The Ultimate Challenge: The $3x + 1$ Problem*, American Mathematical Society, Providence, 2010.
[37] R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly, 95 (1988), pp. 243–246.
[38] ———, *When does a polynomial over a finite field permute the elements of the field? II*, Amer. Math. Monthly, 100 (1993), pp. 71–74.
[39] M. Lothaire, *Algebraic combinatorics on words*, vol. 90 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2002.
[40] K. Mahler, *p-adic numbers and their functions*, Cambridge University Press, Cambridge, 2nd ed., 1981.
[41] W. Parry, *On the β-expansions of real numbers*, Acta Math. Hungar., 11 (1960), pp. 401–416.
[42] W. Penney, *A "binary" system for complex numbers*, J. ACM, 12 (1965), pp. 247–248.
[43] A. Pethő, P. Varga, and M. Weitzer, *On shift radix systems over imaginary quadratic Euclidean domains*, Acta Cybernet., 22 (2015), pp. 485–498.
[44] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, in Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 31–43.
[45] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Hungar., 8 (1957), pp. 477–493.
[46] E. Roosendaal, *On the $3x + 1$ problem*. `http://www.ericr.nl/wondrous`. Accessed: November 12, 2019.
[47] F. Schweiger, *Ergodic theory of fibred systems and metric number theory*, Oxford science publications, Clarendon Press, Oxford, 1995.

[48] B. G. Seifert, *On the arithmetic of cycles for the Collatz-Hasse ("Syracuse") conjectures*, Discrete Math., 68 (1988), pp. 293–398.
[49] C. Shallue, *Permutation polynomials of finite fields*, honours thesis, Monash University, Melbourne, 2015.
[50] N. Sidorov, *Arithmetic dynamics*, in Topics in dynamics and ergodic theory, vol. 310 of Lond. Math. Soc. Lect. Note Ser., Cambridge, 2003, Cambridge University Press, pp. 145–189.
[51] T. O. Silva, *Computational verification of the* $3x+1$ *conjecture*. `http://sweet.ua.pt/tos/3x+1.html`. Accessed: November 12, 2019.
[52] R. Steiner, *On the "*$qx+1$ *problem", q odd*, Fibonacci Quart., 19 (1981), pp. 285–288.
[53] ———, *On the "*$qx+1$ *problem", q odd II*, Fibonacci Quart., 19 (1981), pp. 293–296.
[54] C. Van de Woestijne, *Noncanonical number systems in the integers*, J. Number Theory, 128 (2008), pp. 2914–2938.
[55] M. Weitzer, *Characterization algorithms for shift radix systems with finiteness property*, Int. J. Number Theory, 11 (2015), pp. 211–232.
[56] ———, *On the characterization of Pethő's Loudspeaker*, Publ. Math. Debrecen, 87 (2015).
[57] ———, *Shift radix systems and their generalizations*, PhD thesis, University of Leoben, Leoben, 2015.
[58] G. Wirsching, *The Dynamical System Generated by the* $3n+1$ *Function*, Springer, Heidelberg, 1998.
[59] E. Yurova, *On ergodicity of p-adic dynamical systems for arbitrary prime p*, P-Adic Numbers Ultrametric Anal. Appl., 5 (2013), pp. 239–241.
[60] E. Yurova Axelsson and A. Khrennikov, *Generalization of Hensels lemma, finding the roots of p-adic Lipschitz functions*, J. Number Theory, 158 (2016), pp. 217–233.

Appendix

p-adic pseudo-valuations. For $2 \leq p \in \mathbb{N}$ let

$$\nu_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}\,. \tag{A.1}$$
$$x \mapsto \begin{cases} \max\left\{k \in \mathbb{N}_0 \mid x/p^k \in \mathbb{Z}_p\right\} & \text{if } x \in \mathbb{Z}_p \setminus \{0\} \\ -\min\left\{k \in \mathbb{N} \mid xp^k \in \mathbb{Z}_p\right\} & \text{if } x \in \mathbb{Q}_p \setminus \mathbb{Z}_p \\ \infty & \text{if } x = 0 \end{cases}$$

If p is a prime then ν_p is the p-adic valuation. If p is not a prime then ν_p is not a valuation as the multiplicative property $\nu_p(ab) = \nu_p(a) + \nu(b)$ is violated in general (not only due to the existence of zero divisors but even if p is a prime power: $\nu_4(2 \cdot 2) = 1 \neq 0 = \nu_4(2) + \nu_4(2)$). It is well-known that if $q_1, \ldots, q_s \in \mathbb{P}$ are the distinct prime factors of $2 \leq p \in \mathbb{N}$ then $\mathbb{Q}_p$ and $\mathbb{Q}_{q_1} \times \cdots \times \mathbb{Q}_{q_s}$ are isomorphic with an isomorphism given by

$$\varphi_p : \mathbb{Q}_p \to \mathbb{Q}_{q_1} \times \cdots \times \mathbb{Q}_{q_s}. \tag{A.2}$$
$$\sum_{k=j}^{\infty} a_k p^k \mapsto \left(\sum_{k=j}^{\infty} a_k (p/q_1)^k q_1^k, \ldots, \sum_{k=j}^{\infty} a_k (p/q_s)^k q_s^k\right) = \left(\sum_{k=j_1}^{\infty} a_k^{(1)} q_1^k, \ldots, \sum_{k=j_s}^{\infty} a_k^{(s)} q_s^k\right)$$

We thus may extend the q-adic valuation ν_q to $\mathbb{Q}_p$ for every $q \in \{q_1, \ldots, q_s\}$ by

$$\nu_q : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}\,. \tag{A.3}$$
$$\sum_{k=j}^{\infty} a_k p^k \mapsto \nu_q\left(\sum_{k=j}^{\infty} a_k (p/q)^k q^k\right)$$

ν_p and $\nu_{q_1}, \ldots, \nu_{q_s}$ satisfy the following properties ($x, y \in \mathbb{Q}_p$, $k \in \mathbb{Z}$):

- $\nu_p(x) = \inf\left\{\lfloor \nu_q(x)/\nu_q(p) \rfloor \mid q \in \{q_1, \ldots, q_s\}\right\}$
- $x = 0 \Leftrightarrow \nu_p(x) = \infty \Leftrightarrow \forall\, q \in \{q_1, \ldots, q_s\} : \nu_q(x) = \infty$
- $x \in p^k\mathbb{Z}_p \Leftrightarrow \nu_p(x) \geq k \Leftrightarrow \forall\, q \in \{q_1, \ldots, q_s\} : \nu_q(x) \geq \nu_q(p)k$
- $\forall\, q \in \{q_1, \ldots, q_s\} : \nu_q(xy) = \nu_q(x) + \nu_q(y)$
- $\forall\, q \in \{q_1, \ldots, q_s\} : \nu_q(x+y) \geq \inf\{\nu_q(x), \nu_q(y)\}$
- $\forall\, q \in \{q_1, \ldots, q_s\} : \nu_q(x) \neq \nu_q(y) \vee \nu_q(x) = \infty \vee \nu_q(y) = \infty \Rightarrow \nu_q(x+y) = \inf\{\nu_q(x), \nu_q(y)\}$.

List of theorems.

Lemma 3.1 (p. 9): Every p-fibred function has a unique canonical form. $\sim_p$ is an equivalence relation on $\mathcal{F}_p$ and the canonical forms constitute a complete set of representatives.

Lemma 3.2 (p. 9): A sufficient condition for the weak block property and a necessary and sufficient condition for the block property of closed p-fibred functions when interpreted as ordinary functions.

Example 3.3 (p. 10): The sufficient condition for the weak block property in Lemma 3.2 neither is necessary.

Theorem 3.4 (p. 11): Characterization of all p-fibred functions which define a given p-digit table D in terms of the sets $\mathrm{D}(n)$, $n \in \mathrm{dom}(\mathrm{D})$.

Lemma 3.5 (p. 11): If D is a p-digit table of length k which has the block property at k, then every given sequence of length k with entries in $\underline{p}$ can be found exactly once among the initial parts of length k of the D-digit expansions of any CRS modulo p^k.

Lemma 3.6 (p. 12): If a p-digit table whose domain contains a CRS modulo p^ℓ has the block property at ℓ and the weak block property at $k \leq \ell$, then it also has the block property at k.

Theorem 3.7 (p. 12): An analysis of the structure of the sets $\mathrm{D}(n)$ for a p-digit table D under the assumption of various (weak) block properties.

Corollary 3.8 (p. 14): Simplifying the computation of F-digit expansions for a closed p-fibred function F which has various (weak) block properties.

Lemma 3.9 (p. 15): If D is an infinite p-digit table with block property, then the function mapping an element of the domain of D to its D-digit expansion is injective.

Corollary 3.10 (p. 15): For a p-adic system F the lengths of the initial and periodic parts of the F-sequence and the F-digit expansion of some p-adic integer coincide.

Lemma 3.11 (p. 16): If D is an infinite p-digit table with domain $\mathbb{Z}_p$ and block property, then the function mapping an element of $\mathbb{Z}_p$ to its D-digit expansion is bijective (infinite version of Lemma 3.5 and specialization of Lemma 3.9). In particular, the sets $\mathrm{D}(n)$ are singletons.

Theorem 3.12 (p. 16): For every infinite p-digit table with domain $\mathbb{Z}_p$ and block property D there is a unique p-fibred function F in canonical form whose F-digit table coincides with D.

Example 3.13 (p. 16): An example of a p-digit table with domain $\mathbb{Z}_p$ and weak block property which cannot be expressed as the F-digit table of any p-fibred function F.

Lemma 3.14 (p. 17): If two p-digit tables with weak block property and equal domain coincide on some subset of their shared domain that is dense in $\mathbb{Z}_p$, then the two p-digit tables coincide as a whole.

Lemma 3.15 (p. 17): Explicit construction of the unique p-digit table E with domain $\mathbb{Z}_p$ and weak block property which extends a given p-digit table D with weak block property, whose domain contains a subset which is dense in $\mathbb{Z}_p$.

Corollary 3.16 (p. 17): If a p-fibred function G with weak block property extends to all of $\mathbb{Z}_p$ another p-fibred function F whose domain is dense in $\mathbb{Z}_p$, it does so in accordance with the unique extension of the corresponding p-digit tables as given in Lemma 3.15.

Lemma 3.17 (p. 19): Basic properties of permutations of $\mathbb{Z}_p$ of the form $\pi_{\mathrm{F,G}}$ if F and G are p-adic systems.

Theorem 3.18 (p. 20): For every p-adic permutation π and every p-adic system G there is a unique (up to $\sim_p$) p-adic system F so that $\pi = \pi_{\mathrm{F,G}}$.

Theorem 3.19 (p. 20): The set of all p-adic permutations forms a subgroup of the set of all permutations of $\mathbb{Z}_p$ with respect to composition.

Lemma 3.20 (p. 20): Basic properties of the isomorphism Π_{G} which transports the group structure on the set of p-adic permutations to the set of p-adic systems and an explicit formula for the resulting group operation on p-adic systems.

Example 3.21 (p. 21): An example illustrating the group operation on p-adic systems analyzed in Lemma 3.20.

Theorem 3.22 (p. 21): If π is a p-adic permutation, then every cycle S of π_k splits into up to p cycles of π_{k+1} which are congruent to S modulo p^k (entry-wise, cyclically) and every cycle of π_{k+1} is a "child" of some cycle of π_k in this way.

Corollary 3.23 (p. 22): If π is a p-adic permutation, then the prime factors of the lengths of all cycles of π_k are contained in $\overline{p}$.

Corollary 3.24 (p. 22): Basic properties of the edge labeled graph $(\mathcal{G}(\pi), c(\pi))$ defined by a p-adic permutation π.

Theorem 4.1 (p. 24): A sufficient condition for the weak block property and a necessary and sufficient condition for the block property of a closed p-fibred function F in terms of weak (p,r)-suitability and (p,r)-suitability of the functions $\mathrm{F}[r]$, $r \in \underline{p}$.

Example 4.2 (p. 24): The weak block property of a closed p-fibred function F neither does (like the block property) permit a necessary and sufficient characterization that only considers the functions $\mathrm{F}[0], \ldots, \mathrm{F}[p-1]$ independently from one another.

Example 4.3 (p. 24): An example of a p-digit table with weak block property which is the p-digit table of a p-fibred function but cannot be realized as the p-digit table of a p-fibred function whose entries are weakly (p,r)-suitable functions.

Corollary 4.4 (p. 25): A stronger version of statement (3) of Corollary 3.8, which loosens the condition that F must have the block property at k to the weak block property S at k.

Lemma 4.5 (p. 26): Basic properties of (p,r)-suitable functions.

Corollary 4.6 (p. 26): A p-adic system F is surjective and p-to-one (as a function on $\mathbb{Z}_p$) and its restriction $\mathrm{F}|_{r+p\mathbb{Z}_p}$, $r \in \underline{p}$, is surjective and one-to-one.

Theorem 4.7 (p. 26): If g is a weakly (p,r)-suitable function at $\overline{k}$ satisfying $\gcd(p, g(n)\%p) = 1$ for all n in its domain, then the product fg is (weakly) (p,r)-suitable at $\overline{k}$ if and only if f is (weakly) (p,r)-suitable at $\overline{k}$.

Theorem 4.8 (p. 28): Characterization of (weakly) (p,r)-suitable polynomial functions in $\mathbb{Z}_p[x]$.

Lemma 4.9 (p. 30): Characterization of (p,r)-integral polynomial functions in $\mathbb{Q}_p[x]$.

Theorem 4.10 (p. 30): Characterization of (weakly) (p,r)-suitable polynomial functions in $\mathbb{Q}_p[x]$.

Corollary 4.11 (p. 36): Every $\mathbb{Z}_p$-polynomial p-fibred function has the weak property S and it has the block property if and only if it has the block property at k for any $k \geq 2$.

Corollary 4.12 (p. 36): For every polynomial p-fibred function F a $K \in \mathbb{N}_0$ is constructed such that F has the weak property S if and only if it has the weak property S at $\overline{K+1}$ and F has the block property if and only if it has the block property at $\overline{K+3}$.

Corollary 4.13 (p. 37): The p-digit table of the extension of a p-fibred function F with domain $\mathbb{Z}$ defined by polynomial functions in $\mathbb{Z}[x]$ obtained by extending the domain from $\mathbb{Z}$ to $\mathbb{Z}_p$ coincides with the unique extension of the p-digit table of F as given by Lemma 3.15.

Lemma 4.14 (p. 37): Construction of a polynomial $g \in \underline{p^k}[x]$ with degree less than k which coincides modulo p^k on $r + p\mathbb{Z}_p$ with a given polynomial $f \in \mathbb{Z}_p[x]$.

Theorem 4.15 (p. 38): Construction of a $\underline{p^k}$-polynomial p-fibred function G with degree in $\underline{k}$ satisfying $\mathrm{D}(\mathrm{F})[\![\underline{k}]\!] = \mathrm{D}(\mathrm{G})[\![\underline{k}]\!]$ for a given $\mathbb{Z}_p$-polynomial p-fibred function F.

Theorem 4.16 (p. 38): Characterization of (weakly) (p,r)-suitable rational functions $f = g/h$ with $g, h \in \mathbb{Z}_p[x]$ and $\gcd(p, h(r)\%p) = 1$ for all $n \in r + p\mathbb{Z}_p$.

Corollary 4.17 (p. 39): Every p-fibred function defined by rational functions of the kind treated in Theorem 4.16 has the weak property S and it has the block property if and only if it has the block property at k for any $k \geq 2$.

Conjecture 4.18 (p. 39): Conjecture on the characterization of (weakly) (p,r)-suitable rational functions $f = g/h$ with $g, h \in \mathbb{Z}_p[x]$ but without the condition $\gcd(p, h(r)\%p) = 1$ for all

$n \in r + p\mathbb{Z}_p$.

Lemma 5.1 (p. 40): Hensel's Lemma: a polynomial $f \in \mathbb{Z}_p[x]$ has a unique root in $r + p\mathbb{Z}_p$ if $f(r)\%p = 0$ and $f'(r)\%p \neq 0$.

Theorem 5.2 (p. 40): Generalization of Hensel's Lemma: a general function $f \in \mathbb{Z}_p[x]$ has a unique root in $r + p\mathbb{Z}_p$ if $f(r + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$ and f is (p, r)-suitable.

Lemma 5.3 (p. 40): The sum of a function which is weakly (p, r)-suitable at k and a linear polynomial is weakly (p, r)-suitable at k, and the sum of a function which is (p, r)-suitable at $\overline{k}$ and a linear polynomial whose linear coefficient is in $p\mathbb{Z}_p$ is (p, r)-suitable at $\overline{k}$.

Example 5.4 (p. 41): Lemma 5.3 cannot be generalized by loosening the condition "(p, r)-suitable at $\overline{k}$" by requiring "(p, r)-suitable at k" instead.

Example 5.5 (p. 41): Examples of applications of Hensel's Lemma to prove that certain real or complex numbers defined by polynomial equations have counterparts within $\mathbb{Z}_p$.

Theorem 5.6 (p. 42): Stronger version of Theorem 5.2: A general function $f \in \mathbb{Z}_p[x]$ which maps $r+p\mathbb{Z}_p$ to $p\mathbb{Z}_p$ is (p, r)-suitable if and only if f has a unique root a in $r+p\mathbb{Z}_p$ and $\gcd(p, g(r)\%p) = 1$, where $g \in \mathbb{Z}_p[x]$ so that $f(x) = (x - a)g(x)$.

Example 5.7 (p. 42): Even if p is prime the condition $\gcd(p, g(r)\%p) = 1$ in Theorem 5.6 cannot be dropped.

Lemma 5.8 (p. 43): Relation between the application of a p-fibred rational function R and the corresponding p-fibred function $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p \cap \mathrm{dom}(\mathrm{R})})$.

Lemma 5.9 (p. 44): Relation between the application of a p-fibred rational function R and the corresponding p-fibred function $\mathrm{F} := \mathrm{int}(\mathrm{R}|_{\mathbb{Z}_p})$ under the condition that R is avoiding.

Example 5.10 (p. 45): The assumptions of Lemma 5.9 cannot be loosened, even if the entries of R are polynomials.

Theorem 5.11 (p. 45): Generalization of Hensel's Lemma: under natural technical conditions, the function R_D has a unique fixed point in $\mathbb{Z}_p$ for every avoiding p-fibred rational function R and every sequence of digits D.

Theorem 5.12 (p. 46): Characterization of (p, r)-avoiding polynomial functions in $\mathbb{Z}_p[x]$.

Lemma 6.1 (p. 49): Characterization of when two p-adic systems F and G are periodic, ultimately periodic, or aperiodic on the same sets using $\pi_{\mathrm{F,G}}$.

Lemma 6.2 (p. 49): Consequences of a p-fibred function being contractive or expansive for periodic and ultimately periodic digit expansions.

Theorem 6.3 (p. 50): $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems where each polynomial is either of degree 2 or higher or has a linear coefficient greater than p in absolute value, are expansive, and $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems that are contractive are linear-polynomial.

Lemma 7.1 (p. 51): Analysis of (weak) (p, r)-suitability and (p, r)-avoidance of linear polynomials.

Theorem 7.2 (p. 51): Explicit formula for $\mathrm{R}_D(n)$ if R is a linear-polynomial p-fibred rational function.

Corollary 7.3 (p. 52): Explicit formula for the unique p-adic integer having a given ultimately periodic F-digit expansion for a given linear-polynomial p-adic system F.

Corollary 7.4 (p. 53): Explicit formula for the unique element of $\underline{p^{|D|}}$ having a given initial F-digit expansion for a given linear-polynomial p-adic system F.

Corollary 7.5 (p. 54): Explicit construction of all linear-polynomial p-adic systems F for which a given p-adic integer n has a given ultimately periodic digit expansion D.

Corollary 7.6 (p. 55): Explicit construction of all pairs (F, n) of linear-polynomial p-adic systems and p-adic integers for which a given ultimately periodic digit expansion D coincides with the F-digit expansion of n.

Conjecture 7.7 (p. 59): The original Collatz conjecture.

Conjecture 7.8 (p. 59): Generalization of the Collatz conjecture: F_C is ultimately periodic on $\mathbb{Q} \cap \mathbb{Z}_2$ and ultimately periodic orbits of natural numbers end up at 1.

Conjecture 7.9 (p. 59): Variant of the the Collatz conjecture for $\mathbb{Z}$-linear-polynomial p-adic systems.

Conjecture 7.10 (p. 60): Variant of the the Collatz conjecture for $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems.

Conjecture 7.11 (p. 62): Variant of the the Collatz conjecture for $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems.

Conjecture 7.12 (p. 62): Variant of the the Collatz conjecture for polynomial p-adic systems.

Theorem 7.13 (p. 63): Conjecture 7.11 (1) and Conjecture 7.12 (1) are equivalent.

Theorem 7.14 (p. 63): Explicit formula for $\pi_{\mathrm{F},\mathrm{G}}(n)$ if F and G are linear-polynomial 2-adic systems with matching linear coefficients, which implies that the constant coefficients of $(\mathbb{Q} \cap \mathbb{Z}_2)$-linear-polynomial 2-adic systems have no influence on the question of whether all rational numbers have ultimately periodic digit expansions.

Conjecture 7.15 (p. 66): Conjecture that the constant coefficients of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems have no influence on the question of whether all rational numbers have ultimately periodic digit expansions.

Theorem 7.16 (p. 67): Explicit formula for $\pi_{\mathrm{F},\sigma,\mathrm{G}}(n)$ if F and G are linear-polynomial 2-adic systems with swapped linear coefficients, which implies that the order of the linear coefficients of $(\mathbb{Q} \cap \mathbb{Z}_2)$-linear-polynomial 2-adic systems has no influence on the question of whether all rational numbers have ultimately periodic digit expansions.

Conjecture 7.17 (p. 68): Conjecture that the order of the linear coefficients of $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems has no influence on the question of whether all rational numbers have ultimately periodic digit expansions.

Example 7.18 (p. 68): Application of the formulas for $\pi_{\mathrm{F},\mathrm{G}}(n)$ and $\pi_{\mathrm{F},\sigma,\mathrm{G}}(n)$ given in Theorem 7.14 and Theorem 7.16.

Theorem 7.19 (p. 68): Characterization of contractive, expansive, and mixed type $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems.

Corollary 7.20 (p. 70): Answer to the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$ for contractive $\mathbb{Z}$-linear-polynomial- and for expansive $(\mathbb{Q} \cap \mathbb{Z}_p)$-linear-polynomial p-adic systems.

Corollary 7.21 (p. 70): Summary of results on the question of ultimate periodicity on $\mathbb{Q} \cap \mathbb{Z}_p$ for $(\mathbb{Q} \cap \mathbb{Z}_p)$-polynomial p-adic systems.

Lemma 8.1 (p. 73): Characterization of p-permutation polynomials.

Theorem 8.2 (p. 73): A polynomial $f \in \mathbb{Z}_p[x]$ is a p-permutation polynomial if and only if it is a p-adic permutation.

Example 8.3 (p. 73): There are p-adic permutations defined by $\mathbb{Z}$-linear-polynomial p-adic systems which are neither p-permutation polynomials.

Theorem 8.4 (p. 73): Every p-cycle tree can be realized as the tree of cycles of some p-adic permutation.

Theorem 8.5 (p. 77): Characterization of the sets of all isomorphism classes of trees with up to 4 layers which may occur as subtrees of trees of cycles of 2-adic permutations defined by $\mathbb{Z}_2$-polynomial 2-adic systems or by 2-permutation polynomials.

Example 8.6 (p. 88): There are p-permutation polynomials which are neither p-adic permutations defined by $\mathbb{Z}_p$-polynomial p-adic systems.

Corollary 8.7 (p. 89): No "Y" property: the trees of cycles of 2-adic permutations defined by $\mathbb{Z}_2$-polynomial 2-adic systems or by 2-permutation polynomials do not contain "Y"-shaped subtrees.

List of symbols in order of first appearance.

$A(\mathcal{P})$	elements of A satisfying predicates in $\mathcal{P}$	5
$[\![a,b]\!]$	integer interval $\{n \in \mathbb{Z} \mid a \leq n \leq b\}$	5
$\underline{a}$	integer interval $[\![0, a-1]\!]$	5
$\overline{a}$	integer interval $[\![0, a]\!]$	5
$\mathbf{S}$	class of sequences	6
$\lvert S\rvert$	length/size of S	6
$S[A]$	subsequence of S, indices in A	6
$S[i,j]$	subsequence of S, indices in $[\![i,j]\!]$	6
$\mathrm{len}_A(S)$	S has length in A	6
$\mathrm{fin}(S)$	S is finite	6
$\mathrm{emp}(S)$	S is empty	6
$\mathrm{bnd}_A(S)$	S is A-bounded	6
$\mathrm{pre}_T(S)$	S has prefix T	6
$\mathrm{suf}_T(S)$	S has suffix T	6
$S \cdot T$	product/concatenation of S and T	6
S^n	n-th power of S	6
S^∞	infinite periodic sequence with period S	6
$\mathcal{I}(S)$	initial part of S	6
$\mathcal{P}(S)$	periodic part of S	6
$\mathrm{per}(S)$	S is (purely) periodic	6
$\mathrm{uper}(S)$	S is ultimately periodic	6
$\mathrm{aper}(S)$	S is aperiodic	6
$f(S)$	entry-wise application of f to S	6
$\mathcal{S}$	class of sequence tables	6
dom(S)	domain of S	6
$\lvert$S$\rvert$	length/size of S	6
S$[n]$	n-th row of S/S-sequence of n	6
S$\lvert_A$	restriction of S to A	6
S$[\![A]\!]$	subtable of S, indices in A	6
S$[\![i,j]\!]$	subtable of S, indices in $[\![i,j]\!]$	6
S $\cdot$ T	product/concatenation of S and T	6
S^n	n-th power of S	6
S$^\infty$	infinite periodic table with period S	6
f(S)	entry-wise application of f to S	6
dom_A(S)	S has domain A	6
len_A(S)	S has length in A	6
fin(S)	S is finite	6
emp(S)	S is empty	6
bnd_A(S)	S is A-bounded	6
$\mathcal{D}_p$	set of p-digit tables	7
D$[n]$	D-digit expansion of n	7
D$[n][k]$	k-th digit of n with respect to D	7
w-block$_K$(D)	D has the weak block property at K	7
w-block(D)	D has the weak block property	7
block$_K$(D)	D has the block property at K	7
block(D)	D has the block property	7
$\mathcal{F}_p$	set of p-fibred functions	7
dom(F)	domain of F	7
F(n)	application of F to n	7
%	modulo function	7
F$\lvert_A$	restriction of F to A	7

$\mathrm{F} \sim_p \mathrm{G}$	equivalence of F and G	7
canf(F)	F is in canonical form	8
w-canf(F)	F is in weak canonical form	8
$\mathrm{dom}_A(\mathrm{F})$	F has domain A	8
$\mathrm{bnd}_A(\mathrm{F})$	F is A-bounded	8
closed(F)	F is closed	8
S(F)	F-sequence table	8
D(F)	F-digit table	8
S(F)[n]	F-sequence of n	8
D(F)[n]	F-digit expansion of n	8
D(F)[n][k]	k-th digit of n with respect to F	8
$\text{w-block}_K(\mathrm{F})$	F has the weak block property at K	8
w-block(F)	F has the weak block property	8
$\mathrm{block}_K(\mathrm{F})$	F has the block property at K	8
block(F)	F has the block property	8
$\overline{\mathcal{F}}_p$	set of p-adic systems	8
F_C	Collatz transformation	8
F_2	binary transformation	8
$(P(x)\ ?\ f(x) : g(x))$	conditional function	8
$\overline{\mathcal{Z}}_p$	set of functions with p-block property	10
$\overline{\mathcal{D}}_p$	set of p-digit tables with block property	11
$\mathrm{D}(n)$	application of D to n	11
$\mathcal{P}(A)$	powerset of n	11
$R(n)$	application of R to n	11
F_D	unique p-adic system defined by given p-digit table D	16
$\text{w-block}_{p,k}(S)$	S has the weak (p,k)-block property	18
$\mathrm{block}_{p,k}(S)$	S has the (p,k)-block property	18
$\psi_\mathrm{F}(n)$	F-digit expansion of n	18
$\pi_{\mathrm{F},\mathrm{G}}(n)$	number whose G-digit expansion equals the F-digit expansion of n	18
F_p	p-ary transformation	18
$\overline{\mathcal{P}}_p$	set of p-adic permutations	19
π_k	π modulo p^k	19
Π_G	group isomorphism between $\overline{\mathcal{F}}_p/_{\sim_p}$ and $\overline{\mathcal{P}}_p$ with respect to G	20
$\circ_\mathrm{G}$	group operation on $\overline{\mathcal{F}}_p$ transported by Π_G	20
$\sigma(S,s)$	cyclic shift of S by s steps	21
$\Sigma(\pi)$	set of cycles of π	21
$S \sim_\sigma T$	cyclical equivalence of S and T	21
$\lvert[S]_{\sim_\sigma}\rvert$	length/size of $[S]_{\sim_\sigma}$	21
$\mathcal{V}(\pi)$	set of vertices of tree of cycles of π	22
$\mathcal{E}(\pi)$	set of edges of tree of cycles of π	22
$\mathcal{G}(\pi)$	tree of cycles of π	22
$c(\pi)$	edge labeling of tree of cycles of π	22
$\text{w-suit}_{p,r,K}(f)$	f is weakly (p,r)-suitable at K	23
$\text{w-suit}_{p,r}(f)$	f is weakly (p,r)-suitable	23
$\mathrm{suit}_{p,r,K}(f)$	f is (p,r)-suitable at K	23
$\mathrm{suit}_{p,r}(f)$	f is (p,r)-suitable	23
$\text{w-block-F}_K(\mathrm{D})$	D has the weak block property F at K	25
w-block-F(D)	D has the weak block property F	25
$\text{w-block-S}_K(\mathrm{D})$	D has the weak block property S at K	25
w-block-S(D)	D has the weak block property S	25
$\text{w-block-F}_K(\mathrm{F})$	F has the weak block property F at K	25
w-block-F(F)	F has the weak block property F	25
$\text{w-block-S}_K(\mathrm{F})$	F has the weak block property S at K	25

w-block-S(F)	F has the weak block property S	25
integral$_{p,r}(f)$	f is (p,r)-integral	30
poly$_{A,D}$(F)	F is A-polynomial with degree in D	36
poly$_A$(F)	F is A-polynomial	36
poly(F)	F is polynomial	36
lin-poly$_A$(F)	F is A-linear-polynomial	36
lin-poly(F)	F is linear-polynomial	36
$\mathcal{R}_p$	set of p-fibred rational functions	42
dom(R)	domain of R	42
R$\vert_A$	restriction of R to A	42
dom$_A$(R)	R has domain A	42
bnd$_A$(R)	R is A-bounded	42
closed(R)	R is closed	42
integral(R)	R is integral	42
R$_D(x)$	application of R$_D$ to x	42
S$_D$(R)	R-sequence table with respect to D	42
S$_D$(R)(n)	R-sequence of n with respect to D	42
poly$_{A,D}$(R)	R is A-polynomial with degree in D	43
poly$_A$(R)	R is A-polynomial	43
poly(R)	R is polynomial	43
lin-poly$_A$(R)	R is A-linear-polynomial	43
lin-poly(R)	R is linear-polynomial	43
int(R)	p-fibred function corresponding to R	43
avoid$_{p,r}(f)$	f is (p,r)-avoiding	44
avoid(R)	R is avoiding	44
avoid(F)	F is avoiding	44
PerP(F)	set of periodic points of F	48
UPerP(F)	set of ultimately periodic points of F	48
APerP(F)	set of aperiodic points of F	48
$[E]$(F)	F satisfies E	48
per-on$_A$(F)	F is periodic on A	48
uper-on$_A$(F)	F is ultimately periodic on A	48
aper-on$_A$(F)	F is aperiodic on A	48
contr(F)	F is contractive	49
exp(F)	F is expansive	49
mix(F)	F is of mixed type	49
d-contr(F)	F contracts denominators	49
d-exp(F)	F expands denominators	49
d-mix(F)	F mixes denominators	49
$A_{\mathrm{F}}(D)$	constant coefficient of $p^{\lvert D\rvert}\mathrm{R}_D(x) \in \mathbb{Z}_p[x]$	51
$B_{\mathrm{F}}(D)$	linear coefficient of $p^{\lvert D\rvert}\mathrm{R}_D(x) \in \mathbb{Z}_p[x]$	51
$\pi_{\mathrm{F},\sigma,\mathrm{G}}(n)$	variant of $\pi_{\mathrm{F},\mathrm{G}}(n)$ involving swapping of digits as specified by σ	66
PerP(A)	union of sets of periodic points of F for all F $\in A$	72
UPerP(A)	union of sets of ultimately periodic points of F for all F $\in A$	72
APerP(A)	union of sets of aperiodic points of F for all F $\in A$	72
f_k	f modulo k	73
$\psi_{\mathrm{F},k}$	ψ_{F} modulo k	76

Institute of Analysis and Number Theory, Graz University of Technology, Steyrergasse 30/II, 8010 Graz, AUSTRIA

E-mail address: weitzer@math.tugraz.at