On subwords in the base-q expansion of polynomial and exponential functions

Hajime Kaneko, Thomas Stoll

ON SUBWORDS IN THE BASE-q EXPANSION OF POLYNOMIAL AND EXPONENTIAL FUNCTIONS

Hajime Kaneko[1]
Institute of Mathematics, University of Tsukuba, 1-1-1, Tennodai, Tsukuba, Ibaraki, 305-8571, JAPAN; Research Core for Mathematical Sciences, University of Tsukuba, 1-1-1, Tennodai, Tsukuba, Ibaraki, 305-8571, JAPAN
kanekoha@math.tsukuba.ac.jp

Thomas Stoll[2]
Universit de Lorraine, CNRS, IECL, F-54000 Nancy, France
thomas.stoll@univ-lorraine.fr

Abstract

Let w be any word over the alphabet $\{0,1,\ldots,q-1\}$, and denote by f either a polynomial of degree $d \geq 1$ or $f : n \mapsto m^n$ for a fixed m. Furthermore, denote by $e_q(w; f(n))$ the number of occurrences of w as a subword in the base-q expansion of $f(n)$. We show that

$$\limsup_{n\to\infty} \frac{e_q(w; f(n))}{\log n} \geq \frac{\gamma(w)}{\ell(w)\log q},$$

where $\ell(w)$ is the length of w and $\gamma(w) \geq 1$ is a constant depending on a property of circular shifts of w. This generalizes work by the second author as well as is related to a generalization of Lagarias of a problem of Erdős.

1 Introduction

Let $q \geq 2$ be an integer and w a non-empty finite word over the alphabet $\mathcal{A}_q := \{0,1,\ldots,q-1\}$. We denote by $\ell(w)$ the length of w which is the number of symbols (or letters) in w. For any integer $n \geq 1$, consider the finite base-q expansion of n,

$$n = \sum_{i=0}^{M} n_i q^i,$$

where $M = M(n) = \lfloor \log_q n \rfloor$ denotes the position of the most significant digit. We write

$$(n)_q = n_M n_{M-1} \cdots n_0$$

[1]The first author is supported by JSPS KAKENHI Grant Number 15K17505.
[2]The second author acknowledges the support of the bilateral project ANR-FWF (France-Austria) called MUDERA (Multiplicativity, Determinism, and Randomness), ANR-14-CE34-0009.

as a shorthand notation and regard this as a word over $\mathcal{A}_q$. For convenience, put $(0)_q := 0$. In this paper, we are concerned with the quantity $e_q(w;n)$ which denotes the number of (possibly overlapping) occurrences of the word w in the finite base-q expansion of n. For example, for $q = 10$, $w = 202$ and $n = 20202$ we have $e_{10}(202; 20202) = 2$. Note that

$$e_q(w;n) \le \frac{\log n}{\log q} + 1. \tag{1}$$

The aim in this paper is to study the quantity $e_q(w;n)$ for thin subsequences of the integers. In what follows, we denote by w^k the k-th concatenation power of a word w; if $k = 0$, then w^k will denote the empty word. For instance, for the word $w = 20$ and $k = 3$ we have $w^k = 202020$.

The investigation on the number of occurrences of subwords in digital expansions along special subsequences of integers has undergone some fundamental progress in recent times. A classical point of view, dating back to the work of Gelfond [4], is to study the distribution in residue classes. The related sequences are automatic sequences such as, for example, the Thue–Morse sequence or the Rudin–Shapiro sequence. We refer the reader to [2, 5, 10, 11, 12] for an up-to-date list of the related work.

A second and different problem is to investigate the number of occurrences of digital blocks in these rarefied sequences. We will consider this problem along polynomial and exponential subsequences in the present paper. We will show that for any fixed w there are terms in these rarefied sequences whose base-q expansion contains *not too few* occurrences of w as subwords. For that purpose we will establish lower bounds on the maximal order of magnitude of the associated counting function.

We denote the set of nonnegative integers (resp. positive integers) by $\mathbb{N}$ (resp. $\mathbb{Z}^+$) and use the standard Landau resp. Vinogradov notation $f = O(g)$ resp. $f \ll g$ to indicate that $|f| \le C|g|$ for some absolute constant $C > 0$. As common, we denote a possible dependence on the parameters in the index of the symbols.

For a better understanding of the flavour of our results, let us first give two examples in the case of a polynomial rarification.

First, consider $w' = 0^l$ (l fixed) which is the l-th concatenation power of the single letter 0 and let $f(X) \in \mathbb{Z}[X]$ be any arbitrary but fixed polynomial of degree $d \ge 1$ with $f(\mathbb{N}) \subset \mathbb{N}$. Since by (1),

$$e_q(w; f(n)) \le \frac{\log f(n)}{\log q} + 1$$

for all non-empty words w and sufficiently large n, we have

$$\limsup_{n\to\infty} \frac{e_q(w'; f(n))}{\log n} \le \frac{d}{\log q}. \tag{2}$$

On the other hand, by choosing a positive integer a such that the coefficients of

$f(X+a)$ are all positive, we have

$$\limsup_{n\to\infty} \frac{e_q(w';f(n))}{\log n} \geq \limsup_{L\to\infty} \frac{e_q(w';f(q^L+a))}{\log(q^L+a)} \geq \frac{d}{\log q}. \tag{3}$$

This is due to fact that in the base-q expansion of $f(q^L+a)$ the d blocks of 0's between consecutive powers of q are each of length $L+O_{q,f}(1)$ as $L\to\infty$. The two inequalities (2) and (3) lead to

$$\limsup_{n\to\infty} \frac{e_q(w';f(n))}{\log n} = \frac{d}{\log q}. \tag{4}$$

As a second example, on the other end of the spectrum, let $w''=(q-1)^l$ be the l-th concatenation power of the single letter $q-1$. Theorem 1 in [12] states that there exists $N_0(q,f,l)>1$ such that for all $N\geq N_0(q,f,l)$ there is an n with $e_q(w'';f(n))=N$. From the method of the proof, it follows that

$$\limsup_{n\to\infty} \frac{e_q(w'';f(n))}{\log n} \geq \frac{1}{\log q}. \tag{5}$$

In fact, in the proof the author generates *one* block of consecutive $q-1$'s, hence also losing the factor d with respect to the previous result.

Our first result gives a result for general w in the spirit of (5) and deals with a question posed in [12].

Theorem 1. *Let $q\geq 2$ be a positive integer and let w be a finite word in the alphabet $\mathcal{A}_q=\{0,1,\ldots,q-1\}$ with length $\ell(w)\geq 1$. Let $f(X)\in\mathbb{Z}[X]$ be a polynomial of degree $d\geq 1$ with $f(\mathbb{N})\subset\mathbb{N}$. Then*

$$\limsup_{n\to\infty} \frac{e_q(w;f(n))}{\log n} \geq \frac{\gamma(w)}{\ell(w)\log q},$$

where $\gamma(w)=\gamma'(w)-1$ and $\gamma'(w)\geq 2$ is the number of circular shift occurrences of w in w^2.

Note that $1\leq\gamma(w)\leq\ell(w)$ for all non-empty words w. For example, $\gamma(2020)=2$, $\gamma(0^l)=\gamma((q-1)^l)=l$. Unfortunately, our method of proof does not allow to get the degree d as a multiplicative factor in the lower bound (compare with (3)).

We conjecture that (4) holds true for any w, however, this seems to be a very difficult question.

Conjecture 1. *Let $f(X)\in\mathbb{Z}[X]$ be a polynomial of degree $d\geq 1$ with $f(\mathbb{N})\subset\mathbb{N}$. Let w be a word in the alphabet $\mathcal{A}_q=\{0,1,\ldots,q-1\}$ with length $\ell(w)\geq 1$ and denote by $e_q(w;f(n))$ the number of (possibly overlapping) occurrences of the word w in the finite base-q expansion of $f(n)$. Then*

$$\limsup_{n\to\infty} \frac{e_q(w;f(n))}{\log n} = \frac{d}{\log q}.$$

Our second result concerns exponential functions. A famous (still open) problem by Erdős says that for all sufficiently large n the ternary expansion of 2^n always contains the digit 2. We refer to the article of Lagarias [8] and to [3] for recent and related results. Lagarias [8, Conjecture 1.12] generalized Erdős' conjecture: For all multiplicatively independent positive integers m and q the base-q expansion of the integers m^n, $n = 1, 2 \dots$ contain any given word w in its base-q expansion for all sufficiently large $n \geq n_0(w)$. While Theorem 2 does not provide an answer to this conjecture it gives a quantitative lower bound along a subsequence of integers and therefore (up to a constant factor) the correct maximal order of magnitude.

Theorem 2. *Let $p \geq 2$ be a prime number and let w be a finite word in the alphabet $\mathcal{A}_p = \{0, 1, \dots, p-1\}$ with length $\ell(w) \geq 1$. Let $f(x) = m^x$ for an integer $m \geq 2$, m not a power of p. Then*

$$\limsup_{n \to \infty} \frac{e_p(w; m^n)}{\log n} \geq \frac{\gamma(w)}{\ell(w) \log p},$$

where $\gamma(w) = \gamma'(w) - 1$ and $\gamma'(w) \geq 2$ is the number of circular shift occurrences of w in w^2.

In Section 2 we provide a proof of Theorem 1 and Section 3 is devoted to a proof of Theorem 2. Both proofs are based on Hensel's lifting lemma. For a prime number p we use $\mathbb{Z}_p$ for the ring of p-adic integers and $\mathbb{Q}_p$ for the field of p-adic numbers; we denote by $v_p(u)$ the p-adic order of $u \in \mathbb{Z}_p$.

2 Proof of Theorem 1

In what follows, we suppose that $w \neq 0^l$ since we have a better result by (4) in the case of a block consisting of 0's only. We start with an important auxiliary result.

Lemma 1. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \geq 1$ with $f(\mathbb{N}) \subset \mathbb{N}$. Denote by a_0 a nonnegative integer satisfying $f'(a_0) \neq 0$. Let w be a word in the alphabet $\mathcal{A}_q = \{0, 1, \dots, q-1\}$ that we write*

$$w = 0^k w_{k+1} \cdots w_l, \qquad k+1 \leq l$$

with $w_{k+1} \neq 0$, where all of the w_i, $i = k+1, \dots, l$, are of length 1 (letters). For any positive integers c and L let L' be the length of the word $w^L 0^c (f(a_0))_q$. Then there exists $c = c(q, f) > 0$ only depending on q and f, such that for any positive integer L there is a nonnegative integer $N < q^{L'}$ with

$$(f(N))_q = v w_{k+1} \cdots w_l w^{L-1} 0^c (f(a_0))_q,$$

where v is some finite (or the empty) word over $\mathcal{A}_q = \{0, 1, \dots, q-1\}$.

Proof. Let $q := p_1^{e_1} \cdots p_t^{e_t}$, where $p_1, \ldots, p_t$ are distinct prime factors of q and $e_1, \ldots, e_t$ are positive integers. Let $b_{q,L}$ be a nonnegative integer whose base-q expansion is denoted as

$$(b_{q,L})_q = w_{k+1} \cdots w_l w^{L-1} 0^c (f(a_0))_q,$$

for some c that we will determine later.

Let L' be the length of the word $w^L 0^c (f(a_0))_q$. For any $i = 1, \ldots, t$, consider the p_i-adic order of an integer m by $v_{p_i}(m)$. If c is sufficiently large depending only on q and $f(X)$, then we see for any $i = 1, \ldots, t$ that

$$v_{p_i}(f(a_0) - b_{q,L}) > 2v_{p_i}(f'(a_0))$$

by $f'(a_0) \neq 0$. Putting

$$g(X) := f(X) - b_{q,L},$$

we get

$$v_{p_i}(g(a_0)) > 2v_{p_i}(f'(a_0)) = 2v_{p_i}(g'(a_0)).$$

By Hensel's lifting lemma [9] there exists a p_i-adic integer $\xi_i \in \mathbb{Z}_{p_i}$ such that $f(\xi_i) = b_{q,L}$. Thus, for any $i = 1, \ldots, t$, there exists an integer $N_i \leq p_i^{L' e_i}$ such that

$$f(N_i) \equiv b_{q,L} \pmod{p_i^{L' e_i}}.$$

By the Chinese remainder theorem, there is an integer N with

$$0 \leq N < p_1^{L' e_1} \cdots p_t^{L' e_t} = q^{L'} \tag{6}$$

and

$$N \equiv N_i \pmod{p_i^{L' e_i}}$$

for any $i = 1, \ldots, t$. Consequently, we obtain

$$f(N) \equiv b_{q,L} \pmod{q^{L'}},$$

which implies the lemma. □

Note that the statement of the lemma also implies an upper bound on the length of the prefix v.

We are now ready to prove Theorem 1.

Proof of Theorem 1. In what follows, we use the integer N constructed in the proof of Lemma 1 (note that $N < q^{L'}$, see (6)). For any positive integer L, we see by Lemma 1 that

$$e_q(w; f(N)) \geq \gamma(w)(L - 2). \tag{7}$$

By (6) and the definition of L', we get

$$N < q^{L'} \leq q^{lL + c'}, \tag{8}$$

where $c' = c'(q, f)$ is a constant depending only on q and $f(X)$. Thus, we obtain from (7) and (8) that

$$\frac{1}{l \log q} - \frac{c'}{l \log N} \leq \frac{L}{\log N} \leq \frac{2}{\log N} + \frac{e_q(w; f(N))}{\gamma(w) \log N}.$$

Noting that N tends to infinity as L tends to infinity (by $w \neq 0^l$), we deduce the theorem by the inequality above. This concludes the proof of Theorem 1. □

3 Proof of Theorem 2

For the proof of Theorem 2, we first introduce a generalization of Hensel's lemma and define the notation which we use throughout this section. Let p be a prime number. For any positive integer m_1 with $m_1 \equiv 1 \pmod{p}$, we set $m_1 = 1 + ap^e$, where a, e are positive integers with $p \nmid a$. Put $g(u) := (1+ap^e)^u$ for any $u \in \mathbb{Z}_p$. Let again $v_p(u)$ be the p-adic order of $u \in \mathbb{Z}_p$. It is known that for any $u, u' \in \mathbb{Z}_p$ with $v_p(u - u') \geq N$ and $N \in \mathbb{N}$, we have

$$v_p\big(g(u) - g(u')\big) \geq N + 1 \tag{9}$$

(see [7, Chapter 2, p.26]).

Let F be a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$ and let u be a fixed element of $\mathbb{Z}_p$. We call F differentiable modulo p^s at u with order N, where $s \in \mathbb{Z}^+$ and $N \in \mathbb{N}$, if there exists $\partial_s F(u) \in \mathbb{Q}_p$ satisfying, for any integer $k > N$ and $h \in \mathbb{Z}_p$,

$$F(u + p^k h) \equiv F(u) + p^k h \partial_s F(u) \pmod{p^{k+s}}. \tag{10}$$

Note that if we add a constant term to F, then both the differentiability of F and the value $\partial_s F(u)$ are not changed.

In the following proposition we generalize the second statement of Corollary 2.6 in [1]. This is needed in order to consider the case where the derivative is not a p-adic unit. We investigated this concept for general continuous functions that are not necessarily differentiable in [6].

Proposition 1. *Let F be a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Let j, n, s, N be nonnegative integers with $j + N < n$ and $j < s$ and let $u \in \mathbb{Z}_p$. Assume that*

$$v_p\big(F(u)\big) \geq n. \tag{11}$$

Moreover, suppose for any $x \in \mathbb{Z}_p$ with $x \equiv u \pmod{p^{n-j}}$ that F is differentiable modulo p^s at x with order N and that

$$v_p\big(\partial_s F(x)\big) = j. \tag{12}$$

Then there exists a $\xi \in \mathbb{Z}_p$ satisfying

$$F(\xi) = 0$$

and

$$\xi \equiv u \pmod{p^{n-j}}.$$

Proof. We construct $\xi \in \mathbb{Z}_p$ satisfying the conditions of Proposition 1, using the Newton method. It suffices to show that there exists a $u_1 \in \mathbb{Z}_p$ satisfying

$$v_p\big(F(u_1)\big) \geq n+1 \tag{13}$$

and

$$u_1 \equiv u \pmod{p^{n-j}}. \tag{14}$$

In fact, u_1 will then satisfy (11), the assumption on the differentiability, and (12) with new nonnegative integers $j_1 = j$, $n_1 = n+1$, $s_1 = s$, and $N_1 = N$ because if $x \in \mathbb{Z}_p$ satisfies $x \equiv u_1 \pmod{p^{n_1-j_1}}$, then $x \equiv u \pmod{p^{n-j}}$.

Let i be an integer with $0 \leq i \leq p-1$. Noting that $n-j > N$ and $n-j+s \geq n+1$, we see by (10) that

$$F\left(u + p^{n-j}\cdot i\right) \equiv F(u) + p^{n-j}\cdot i\partial_s F(u) \pmod{p^{n+1}}.$$

Using

$$v_p\left(p^{n-j}\partial_s F(u)\right) = n \leq v_p\big(F(u)\big),$$

we find i satisfying

$$F(u + p^{n-j}\cdot i) \equiv 0 \pmod{p^{n+1}}.$$

Putting $u_1 := u + p^{n-j}\cdot i$, we obtain (13) and (14). □

We now prove the differentiability of the function $g(u) = (1+ap^e)^u$, where a and e are positive integers with $p \nmid a$.

Proposition 2. *Let $g(u) = (1+ap^e)^u$, where a, e are positive integers with $p \nmid a$.*

1. *Suppose that $e \geq 2$ or $p \geq 3$. Then, for any $u \in \mathbb{Z}_p$, we have that g is differentiable modulo p^{e+1} at u with order 0. Moreover,*

$$\partial_{e+1} g(u) = ap^e.$$

2. *Assume that $e = 1$ and $p = 2$. Let $1 + a'\cdot 2^t := (1+2a)^2$, where a' and t are integers with $2 \nmid a'$ and $t \geq 3$. Then g is differentiable modulo 2^t at u with order 0. Moreover,*

$$\partial_t g(u) = a'2^{t-1}.$$

For the proof of Proposition 2, we need the following auxiliary result.

Lemma 2. *Assume that $e \geq 2$ or $p \geq 3$. Let k be a nonnegative integer and $h \in \mathbb{Z}_p$. Then we have*

$$(1+ap^e)^{hp^k} \equiv 1 + ahp^{k+e} \pmod{p^{k+e+1}}. \tag{15}$$

Proof. We may assume that h is a nonnegative integer because $\mathbb{N}$ is dense in $\mathbb{Z}_p$. Moreover, it suffices to show (15) in the case where h is not divisible by p. In fact, assume that (15) holds for any $h \in \mathbb{N}$ not divisible by p. Then, for any nonnegative integer $h = h'p^s$, where $s = v_p(h) \geq 1$, we see

$$(1+ap^e)^{hp^k} = (1+ap^e)^{h'p^{k+s}} \equiv 1 \equiv 1 + ahp^{k+e} \pmod{p^{k+e+1}},$$

which implies (15).

First, we show (15) in in the case of $h = 1$, namely,

$$(1+ap^e)^{p^k} \equiv 1 + ap^{k+e} \pmod{p^{k+e+1}}. \tag{16}$$

If $k = 0$, then (16) is trivial. If $k \geq 1$, then the inductive hypothesis implies that

$$(1+ap^e)^{p^{k-1}} = 1 + ap^{e+k-1} + cp^{e+k}$$

for some integer c, and so

$$(1+ap^e)^{p^k} = (1 + ap^{e+k-1} + cp^{e+k})^p \equiv (1+ap^{e+k-1})^p \pmod{p^{k+e+1}}.$$

Since

$$(1+ap^{e+k-1})^p = 1 + ap^{e+k} + \sum_{j=2}^{p} \binom{p}{j} (ap^{e+k-1})^j,$$

we deduce (16), using

$$e + k < p(e+k-1)$$

by $k \geq 1$, and $e \geq 2$ or $p \geq 3$.

Finally, if $h \geq 0$ is a general integer not divisible by p, then (15) follows from (16) by considering the binomial expansion of $(1+ap^{k+e})^h$. □

Proof of Proposition 2. Let k be any positive integer and $u, h \in \mathbb{Z}_p$. First, we assume that $e \geq 2$ or $p \geq 3$. Using Lemma 2, we get

$$\begin{aligned} g(u+hp^k) &= g(u)(1+ap^e)^{hp^k} \\ &\equiv g(u)(1+ahp^{e+k}) \pmod{p^{k+e+1}} \\ &\equiv g(u) + hp^k \cdot ap^e \pmod{p^{k+e+1}} \end{aligned}$$

by $g(u) \equiv 1 \pmod{p}$, which implies the first statement.

Next, suppose that $e = 1$ and $p = 2$. In the same way as above, using Lemma 2 again, we see by $k - 1 \geq 0$ that

$$\begin{aligned} g(u + 2^k \cdot h) &= g(u)(1 + a' \cdot 2^t)^{h \cdot 2^{k-1}} \\ &\equiv g(u) + (h \cdot 2^k) \cdot (a' \cdot 2^{t-1}) \pmod{2^{k+t}}, \end{aligned}$$

which implies the second statement. □

We are now ready to give a proof of Theorem 2.

Proof of Theorem 2. We may assume that m and p are coprime. In fact, if m is not coprime to p, then putting $m =: m'p^s$, where $s = v_p(m)$ and $m' \geq 2$, we have

$$e_p(w; m^n) \geq e_p(w; m'^n).$$

Put $m^{p-1} =: 1 + ap^e$ and $g(u) := (1 + ap^e)^u$, where a and e are positive integers with $p \nmid a$ and $u \in \mathbb{Z}_p$. If $p = 2$ and $e = 1$, then we define a' and t as in Proposition 2.

For any finite word $v = v_{d-1}v_{d-2}\cdots v_0$ on the alphabet $\mathcal{A}_p$, we put

$$\varphi_p(v) := \sum_{i=0}^{d-1} v_i p^i.$$

Moreover, for any positive integer L, let

$$\varphi_p(w^L 0^c 1) =: b_{p,L},$$

for some c that we will determine later.

Put $F(u) := g(u) - b_{p,L}$ for $u \in \mathbb{Z}_p$. We apply Proposition 1 with $u = 0, N = 0$,

$$j = \begin{cases} e & \text{if } e \geq 2 \text{ or } p \geq 3, \\ t - 1 & \text{if } e = 1 \text{ and } p = 2, \end{cases}$$

$s = j + 1$, $n = j + 1$ and put $c := n - 1$. Then we see

$$v_p\big(F(0)\big) = v_p(1 - b_{p,L}) \geq n,$$

which implies (11). Moreover, the assumption on the differentiability and (12) in Proposition 1 are satisfied by Proposition 2.

Thus, Proposition 1 implies that there exists $\xi \in \mathbb{Z}_p$ satisfying $g(\xi) = b_{p,L}$. Let L' be the length of the word $w^L 0^c 1$. Then we have

$$L' = lL + c + 1.$$

Let N be an integer with

$$p^{L'} \leq N < 2p^{L'}$$

and

$$N \equiv \xi \pmod{p^{L'}}.$$

Using (9), we get

$$m^{(p-1)N} = g(N) \equiv g(\xi) = b_{p,L} \pmod{p^{L'}} \tag{17}$$

Putting $N' = (p-1)N$, we obtain by (17) and $m^{N'} > p^{L'}$ that

$$e_p(w; m^{N'}) \geq \gamma(w)(L - 1) \tag{18}$$

and that

$$\begin{aligned} \log N' &\leq \log\big(2(p-1)\big) + L' \log p \\ &= \log\big(2(p-1)\big) + (c+1)\log p + lL \log p. \end{aligned} \tag{19}$$

Combining (18) and (19), we deduce Theorem 2 by letting L tend to infinity. □

Acknowledgement

We would like to thank the reviewers for helpful remarks that helped to improve the presentation of our results.

References

[1] E. Y. Axelsson and A. Khrennikov, Generalization of Hensel's lemma: Finding the roots of p-adic Lipschitz functions, *J. Number Theory* **158** (2016), 217-233.

[2] M. Drmota, C. Mauduit and J. Rivat, The Thue–Morse sequence along squares is normal, submitted, available at `http://www.dmg.tuwien.ac.at/drmota/`.

[3] T. Dupuy and D. Weirich, Bits of 3^n in binary, Wieferich primes and a conjecture of Erdős, *J. Number Theory* **158** (2016), 268-280.

[4] A. O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1967/1968), 259-265.

[5] G. Hanna, Sur les occurrences des mots dans les nombres premiers, *Acta Arith.* **178** (2017), no. 1, 15-42.

[6] H. Kaneko and T. Stoll, Hensel's lemma for general continuous functions, submitted, `arXiv:1707.01445`.

[7] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd edition, Graduate Texts in Mathematics 58, Springer Verlag 1984.

[8] J. Lagarias, Ternary expansions of powers of 2, *J. Lond. Math. Soc. (2)* **79** (2009), no. 3, 562-588.

[9] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing Company, 1970.

[10] C. Mauduit and J. Rivat, Prime numbers along Rudin-Shapiro sequences, *J. Eur. Math. Soc. (JEMS)* **17** (2015), no. 10, 2595-2642.

[11] C. Müllner, Automatic sequences fulfill the Sarnak conjecture, *Duke Math. J.* **166** (2017), no. 17, 3219-3290. .

[12] T. Stoll, On digital blocks of polynomial values and extractions in the Rudin–Shapiro sequence, *RAIRO Theor. Inform. Appl.* **50** (2016), no. 1, 93-99.