p-Adic valuations and k-regular sequences

Jason P. Bell
Department of Mathematics
Simon Fraser University
8888 University Drive
Burnaby, B.C., Canada
V5A 1S6
jpb@math.sfu.ca

Abstract

A sequence is said to be *k-automatic* if the n^{th} term of this sequence is generated by a finite state machine with n in base k as input. Regular sequences were first defined by Allouche and Shallit as a generalization of automatic sequences. Given a prime p and a polynomial $f(x) \in \mathbb{Q}_p[x]$, we consider the sequence $\{v_p(f(n))\}_{n=0}^{\infty}$, where v_p is the p-adic valuation. We show that this sequence is p-regular if and only if $f(x)$ factors into a product of polynomials, one of which has no roots in $\mathbb{Z}_p$, the other which factors into linear polynomials over $\mathbb{Q}$. This answers a question of Allouche and Shallit.

1 Introduction

A sequence is said to be *k-automatic* if the n^{th} term of this sequence is generated by a finite state machine with n in base k as input. These sequences have found applications to many different areas of mathematics [3]. Another way of defining automaticity comes from looking at the *k-kernel* of a sequence. The k-kernel of a sequence $\{f(n)\}_{n=0}^{\infty}$ is defined to be the collection of sequences of the form $\{f(k^i n + j)\}_{n=0}^{\infty}$ where $i \geq 0$ and $0 \leq j < k^i$. A sequence is k-automatic if and only if its k-kernel is finite. Using this definition of automaticity, Allouche and Shallit [2], [3] generalized the notion of automaticity.

Given a sequence $\{f(n)\}_{n=0}^{\infty}$ taking values in some abelian group, we create a $\mathbb{Z}$-module $M(\{f(n)\}; k)$ which is defined to be the $\mathbb{Z}$-module generated by all sequences $\{f(k^i n + j)\}_{n=0}^{\infty}$, where $i \geq 0$ and $0 \leq j < k^i$; that is,

$$M(\{f(n)\}; k) \ := \ \sum_{i=0}^{\infty} \sum_{j=0}^{k^i - 1} \mathbb{Z}\{f(k^i n + j)\}. \tag{1.1}$$

Definition 1.1 *A sequence is* k-regular *if* $M(\{f(n)\}; k)$ *is finitely generated as a* $\mathbb{Z}$*-module.*

Since the k-kernel of a sequence $\{f(n)\}$ spans $M(\{f(n)\}; k)$ as a $\mathbb{Z}$-module, we see that an automatic sequence is necessarily regular.

Given a prime number p, we have a p-adic *valuation* v_p with the property that for any integer n, $n = p^{v_p(n)}m$ for some divisor m of n with m relatively prime to p. In addition to this, the valuation satisfies the standard properties of a non-archimedian valuation; namely,

- $v_p(ab) = v_p(a) + v_p(b)$ for $a, b \in \mathbb{Q}_p$;
- $v_p(a + b) \geq \min(v_p(a), v_p(b))$; and
- $v_p(x) = \infty$ if and only if $x = 0$.

This valuation gives rise to an absolute value, denoted by $|\cdot|_p$, on $\mathbb{Q}_p$. It is defined by

$$|x|_p \ := \ p^{-v_p(x)}. \tag{1.2}$$

We are interested in sequences of the form $v_p(f(n))$, where $f(n)$ is a polynomial with rational coefficients and which has no natural number roots. The reason we avoid considering polynomials which have natural number roots is because $v_p(0) = \infty$ and we only consider sequences with integer values. Allouche and Shallit [2], [3] ask when such a sequence is p-regular. We give necessary and sufficient conditions for this to occur. Our main result is the following theorem.

Theorem 1.2 *Let* $f(x)$ *be a polynomial and let* p *be a prime number. Then* $v_p(f(n))$ *is a* p*-regular sequence if and only if* $f(x)$ *factors into a product of two polynomials, one of which splits over* $\mathbb{Q}$ *and the other of which has no roots in* $\mathbb{Z}_p$*.*

2 A well-known remark

We begin with a well-known result. We nevertheless include the proof for the sake of completeness.

Lemma 2.1 *Let* $f(x) \in \mathbb{Z}_p[x]$*. Then* $f(x)$ *has a root in* $\mathbb{Z}_p$ *if and only if* $f(x)$ *has a solution mod* $p^n\mathbb{Z}_p$ *for all* n*.*

Proof. If $f(x)$ has a root in $\mathbb{Z}_p$, then it is clear that it has a root mod $p^n\mathbb{Z}_p$ for all n. Conversely, suppose that it has a root $\alpha_n \in \mathbb{Z}_p$ mod $p^n\mathbb{Z}_p$ for all n. Then $f(\alpha_n) \in p^n\mathbb{Z}_p$. Consider the set $\{\alpha_n \mid n \geq 0\}$. This is an infinite subset of $\mathbb{Z}_p$, a compact set. By the Bolzano-Weierstrass theorem, it must have a limit point $\alpha \in \mathbb{Z}_p$. By continuity $f(\alpha) = 0$, and so $f(x)$ has a root in $\mathbb{Z}_p$. ∎

We note that Hensel's lemma is an effective tool for testing whether or not a polynomial has a root in $\mathbb{Z}_p$.

Theorem 2.2 *(Hensel's lemma) Let $f(x) \in \mathbb{Z}_p[x]$. Suppose that $|f(a)|_p < |f'(a)|_p^2$ for some $a \in \mathbb{Z}_p$. Then $f(x)$ has a root in $\mathbb{Z}_p$.*

Proof. See Theorem 7.3 of Eisenbud [4]. ∎

3 Proofs

We now introduce some notation which will simplify the proofs in the this section.

Notation 3.1 *Given a statement S, we define*

$$\chi(S) \;=\; \begin{cases} 0 & \text{if } S \text{ is false;} \\ 1 & \text{if } S \text{ is true.} \end{cases}$$

Proposition 3.2 *Let $\theta \in \mathbb{Z}_p \setminus \mathbb{Q}$. Then the sequence $\{v_p(n-\theta)\}$ is not p-regular.*

Proof. Suppose that this sequence is p-regular. Then the $\mathbb{Z}$-module

$$M \;:=\; \sum_{i=0}^{\infty} \sum_{j=0}^{p^i-1} \mathbb{Z}\{v_p(p^i n + j - \theta)\}$$

is finitely generated. Write $\theta = \sum_{i=0}^{\infty} a_i p^i$, with $0 \leq a_i < p$ for all $i \geq 0$. Define

$$\theta_j \;=\; a_0 + a_1 p + \cdots + a_{j-1} p^{j-1}.$$

Observe that $0 \leq \theta_j < p^j$ for all $j \geq 1$. Consider the sequence

$$\{v_p(p^j n + \theta_j - \theta)\}_{n=0}^{\infty}.$$

Since $\theta - \theta_j = \sum_{i \geq j} a_i p^i$, we have

$$\begin{aligned} v_p(p^j n + \theta_j - \theta) &= v_p(p^j n - a_j p^j - a_{j+1} p^{j+1} - \cdots) \\ &= j + v_p(n - a_j - a_{j+1} p - \cdots) \\ &= j + \sum_{i=0}^{\infty} \chi(n \equiv a_j + \cdots + a_{j+i} p^i \bmod p^{i+1}). \end{aligned}$$

Define

$$G(n; (b_0, b_1, \ldots)) = \sum_{i=0}^{\infty} \chi(n \equiv b_0 + \cdots + b_i p^i).$$

Let M' be the $\mathbb{Z}$-submodule of M generated by $\{v_p(p^i n + \theta_i - \theta)\}$ for $i \geq 0$ along with the constant sequence $(1, 1, \ldots)$. By assumption M is Noetherian and so M' is finitely generated. It follows that there exists some $j > 0$ such that M' is generated by

$$\{(1, 1, \ldots)\} \cup \{\{v_p(p^i n + \theta_i - \theta)\} \mid 1 \leq i < j\}.$$

Consequently, there exist integers $c_1, \ldots, c_{j-1}$ such that

$$G(n; (a_j, a_{j+1}, \ldots)) = c_0(1, 1, \ldots) + \sum_{i=1}^{j-1} c_i G(n; (a_i, a_{i+1}, \ldots)). \tag{3.3}$$

We claim that there exists some $k < j$ such that $a_{i+k} = a_{i+j}$ for all $i \geq 0$. To see this, suppose that this is not the case. Then there exists some natural number s such that

$$a_j + a_{j+1} p + \cdots + a_{j+s} p^s \neq a_k + a_{k+1} p + \cdots + a_{k+s} p^s \qquad \text{for } 0 \leq k < j.$$

It follows that there exist constants $e_1, \ldots, e_{j-1}$ such that

$$G(a_j + \cdots + a_{j+t} p^t; (a_i, a_{i+1}, \ldots)) = e_i \qquad \text{for } t \geq s.$$

Equation (3.3) then gives that

$$G(a_j + \cdots + a_{j+t} p^t; (a_j, a_{j+1}, \ldots)) = c_0 + c_1 e_1 + \cdots c_{j-1} e_{j-1}$$

for all $t \geq s$. But $G(a_j + \cdots + a_{j+t} p^t; (a_j, a_{j+1}, \ldots)) \geq t$ and so we get a contradiction. It follows that there exists some $k < j$ such that $a_{i+k} = a_{i+j}$.

Let $d = j - k$. Then there exists some natural number N such that $a_{d+i} = a_i$ for all $i > N$. Hence

$$\begin{aligned}
\theta &= \sum_{i=0}^{\infty} a_i p^i \\
&= \sum_{i=0}^{N} a_i p^i + \sum_{i=1}^{d} a_{N+i}(p^{N+i} + p^{N+i+d} + p^{N+i+2d} + \cdots) \\
&= \sum_{i=0}^{N} a_i p^i + \sum_{i=1}^{d} a_{N+i} p^{N+i}/(1 - p^d) \\
&\in \mathbb{Q},
\end{aligned}$$

which is again a contradiction. ∎

Lemma 3.3 *Let $h(x) \in \mathbb{Z}_p[x]$ be a polynomial with no roots in $\mathbb{Z}_p$. Then the sequence $\{h(n)\}$ is periodic.*

Proof. Since $h(x)$ has no roots mod p^m for some $m > 1$, there exists some $m \geq 2$ such that $|h(n)|_p > p^{-m}$ for all integers n. By Taylor's theorem

$$h(n + p^m) = h(n) + p^m h'(n) + p^{2m} h''(n)/2! + \cdots + p^{md} h^{(d)}(n)/d!,$$

where d is the degree of $h(x)$. Notice that for $2 \leq j \leq d$,

$$\begin{aligned}
v_p(p^{jm} h^{(j)}(n)/j!) &= jm + v_p(h^{(j)}(n)) - v_p(j!) \\
&\geq jm - v_p(j!) \\
&= jm - \lfloor j/p \rfloor - \lfloor j/p^2 \rfloor - \cdots \\
&\geq jm - j/p - j/p^2 - \cdots \\
&= jm - j/(p-1) \\
&\geq j(m-1) \\
&\geq 2(m-1) \\
&\geq m.
\end{aligned}$$

Since $v_p(p^m h'(n)) \geq m$, we see by the non-archimedian property that

$$|p^m h'(n) + p^{2m} h''(n)/2! + \cdots p^{md} h^{(d)}(n)/d!|_p \leq p^{-m},$$

while $v_p(h(n)) < m$. Thus the non-archimedian property gives $v_p(h(n + p^m)) = v_p(h(n))$ for all $n \geq 0$ and so we obtain the desired result. ∎

Lemma 3.4 *Let $g(x) \in \mathbb{Q}_p[x]$ be a polynomial which splits over $\mathbb{Q}$ and has no natural number roots. Then $\{v_p(g(n))\}$ is p-regular.*

Proof. There exists some constant C and rational numbers $\alpha_1, \ldots, \alpha_d$ such that

$$v_p(g(n)) \;=\; C + v_p(n-\alpha_1) + \cdots + v_p(n-\alpha_d) \qquad \text{for } n \geq 0.$$

Since a sum of p-regular sequences is p-regular, it suffices to prove this lemma in the case that $g(x) = x - \alpha$, where $\alpha \in \mathbb{Q} \setminus \mathbb{N}$. If $v_p(\alpha) < 0$, there is nothing to prove, so we may assume that $\alpha \in \mathbb{Z}_p$. Write

$$\alpha \;=\; \sum_{i=0}^{\infty} a_i p^i$$

where $0 \leq a_i < p$ for $i \geq 0$. Notice that for $0 \leq j < p^i$,

$$v_p(p^i n + j - \alpha) \;=\; v_p(j - \alpha)$$

for all $n \geq 0$ unless $j = a_0 + \cdots + a_{i-1}p^{i-1}$. If $j = a_0 + \cdots + a_{i-1}p^i$, then

$$v_p(p^i n + j - \alpha) \;=\; i + G(n; (a_i, a_{i+1}, \ldots)).$$

By assumption, $\alpha \in \mathbb{Q}$ and so there exist d, N such that $a_i = a_{i+d}$ for $i > N$. It follows that for any j, there exists some $i \leq N + d$ such that $G(n; (a_j, a_{j+1}, \ldots)) = G(n; (a_i, a_{i+1}, \ldots))$. Thus the $\mathbb{Z}$-module generated by the sequences $\{v_p(p^i n + j - \alpha)\}$ is a submodule of the finitely generated module generated by

$$\{(1, 1, \ldots)\} \cup \{G(n; (a_i, a_{i+1}, \ldots)) \mid i \leq N + d\}.$$

Hence the $\mathbb{Z}$-module is Noetherian. The result follows. ∎

Theorem 3.5 *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with no natural number roots. Then the sequence $\{v_p(f(n)\}_{n=0}^{\infty}$ is p-regular if and only if $f(x) = g(x)h(x)$ for some polynomials $g(x)$ and $h(x)$ in which $h(x)$ has no roots in $\mathbb{Z}_p$ and $g(x)$ splits over $\mathbb{Q}$.*

Proof. Suppose that $f(x)$ has no such factorization. Then $f(x)$ has a root θ in $\mathbb{Z}_p$ which is not rational. Then $f(x) = (x-\theta)^d g(x)$, where $g(\theta) \neq 0$. Let $m = v_p(g(\theta))$. Write

$$\theta \;=\; a_0 + a_1 p + a_2 p^2 + \cdots$$

and let

$$\theta_j \;:=\; a_0 + \cdots + a_{j-1} p^{j-1}.$$

Since $g(\theta) \neq 0$ and $\theta_j \to \theta$ as $d \to \infty$, there is some N such that

$$|g(\theta) - g(\theta_j)|_p \;<\; p^m \qquad \text{for } j > N.$$

Consequently, $v_p(g(\theta_j)) = m$ for all $j > N$. Thus

$$v_p(f(p^j n + \theta_j)) \;=\; d v_p(p^j n + \theta_j - \theta) + m \qquad \text{for } j > N.$$

Pick $k > N$ and let $\tau = p^{-k}(\theta - \theta_k)$. Then $\tau \in \mathbb{Z}_p \setminus \mathbb{Q}$. Now

$$v_p(f(p^k n + \theta_k)) \;=\; d v_p(p^k n - p^k \tau) + m \;=\; (dk + m) + v_p(n - \tau).$$

By Proposition 3.2 we have that the sequence $\{v_p(n-\tau)\}$ is not p-regular and consequently $\{v_p(f(p^k n + \theta_k)\}$ is not p-regular; it follows that $\{v_p(f(n))\}$ is not a p-regular sequence.

Conversely, suppose that $f(x) = g(x)h(x)$ where $g(x)$ splits over $\mathbb{Q}$ and $h(x)$ has no roots in $\mathbb{Z}_p$. Then $v_p(f(n)) = v_p(g(n)) + v_p(h(n))$. By Lemma 3.3 we have that $\{v_p(h(n))\}$ is periodic and hence it is p-automatic. By Lemma 3.4, the sequence $\{v_p(g(n))\}$ is p-regular. Thus $v_p(f(n))$ is p-regular since it is a sum of p-regular sequences. ∎

Corollary 3.6 *Let $f(x) \in \mathbb{Z}[x]$ which has no natural number roots. Then $\{v_p(f(n))\}$ is p-automatic if and only if $f(x)$ factors into $g(x)h(x)$ where $h(x)$ has no roots mod p^n for sufficiently large n and $g(x)$ splits over $\mathbb{Q}$.*

Proof. Straightforward. ∎

We remark that if a polynomial $f(x)$ is in $\mathbb{Q}[x]$, then it can be expressed as $g(x)/m$ for some positive integer m and some polynomial $g(x) \in \mathbb{Z}[x]$. Then $v_p(f(n)) = v_p(g(n)) - v_p(m)$. Since the constant sequence $\{v_p(m)\}$ is p-regular, the sequence $\{v_p(f(n))\}$ is p-regular if and only if $\{v_p(g(n))\}$ is

p-regular. Consequently it is no loss of generality to restrict our attention to polynomials with integer coefficients.

We note that Allouche and Shallit [1] motivate looking at the sequence of p-adic valutations of polynomial values by pointing out that, for example, the sequence $\{v_5(n^2+1)\}$ is intimately connected to the 5-adic expansion of $\sqrt{-1}$. Of course, if we found some increasing sequence of numbers $n_1, n_2, \ldots$ satisfying $v_5(n_j^2+1) \to \infty$ with $n_j \equiv 2 \bmod 5$ for all j, then this by Hensel's lemma this sequence must converge to some element $\mathbf{u} \in \mathbb{Z}_5$ with $\mathbf{u}^2+1=0$. We see, however, that since x^2+1 splits over $\mathbb{Z}_5$ and has no rational roots, the sequence $\{v_5(n^2+1)\}$ is not 5-regular. Consequently, regular sequences do not give any insight into understanding the 5-adic expansion of $\sqrt{-1}$ in this instance.

4 Acknowledgments

I thank Jean-Paul Allouche and Jeffrey Shallit for many helpful conversations.

References

[1] J.-P. Allouche and J. Shallit. The ring of k-regular sequences, II. *Theoret. Comput. Sci.* **307** (2003), 3–29.

[2] J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoret. Comput. Sci.* **98** (1992), 163–197.

[3] J.-P. Allouche, J. Shallit. *Automatic sequences. Theory, applications, generalizations.* Cambridge University Press, Cambridge, 2003.

[4] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.