Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 307 (2007) 3070–3075
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

# $p$-adic valuations and $k$-regular sequences

Jason P. Bell

*Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC, Canada V5A 1S6*

Received 6 October 2006; received in revised form 6 December 2006; accepted 13 March 2007
Available online 15 March 2007

**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.


*Keywords:* Automatic sequences; $k$-regular sequences; Valuations; Polynomials

## 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 $i \geqslant 0$ and $0 \leqslant j < k^i$. A sequence is $k$-automatic if and only if its $k$-kernel is finite. Using this definition of automaticity, Allouche and Shallit [1,3] 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 $i \geqslant 0$ and $0 \leqslant j < k^i$; 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.

*E-mail address:* jpb@math.sfu.ca.

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.03.009

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-archimedean valuation; namely,

- $v_p(ab) = v_p(a) + v_p(b)$ for $a, b \in \mathbb{Q}_p$;
- $v_p(a + b) \geqslant \min(v_p(a), v_p(b))$; 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 [1,3] 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 nonzero polynomial with rational coefficients 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 $\{\alpha_n | n \geqslant 0\}$. 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 $\mathbb{Z}_p$. $\square$

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]. $\square$

## 3. Proofs

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

**Notation 3.1.** *Given a statement $S$, we define*

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

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