15. FORMAL LANGUAGE THEORY

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **38 (1992)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.07.2024**

if the limit exists. Then Veech showed that $\mu_\theta(I)$ exists for all $I \subseteq [0, 1)$ if and only if the partial quotients of θ are bounded.

For other connections with ergodic theory, see the papers of Stewart [286]; del Junco [154]; Dani [70, 72]; and Baggett and Merrill [14, 15].

14. PSEUDO-RANDOM NUMBER GENERATION

Lehmer [183] introduced the *linear congruential method* for pseudo-random number generation. Let X_0, m, a, c be given, and define

$$X_{k+1} = aX_k + c \pmod{m},$$

for $k \geqslant 0$. For this to be a good source of "random" numbers, we want the sequence X_k to be uniformly distributed, as well as the sequence of pairs (X_k, X_{k+1}), triples, etc.

A test for randomness called the *serial test* on pairs (X_k, X_{k+1}) amounts to the two-dimensional version of the discrepancy mentioned above in Section 12. This turns out to be essentially the function $\rho(\mathbf{g}, m)$ defined in Section 10. Thus linear congruential generators that pass the pairwise serial test arise from rationals a/m having small partial quotients in their continued fraction expansion. See the papers of Dieter [87, 88]; Niederreiter [219, 220, 222]; Knuth [170, Section 3.3.3]; and Borosh and Niederreiter [42].

15. FORMAL LANGUAGE THEORY

Let $w = w_0 w_1 w_2 \cdots$ be an infinite word over a finite alphabet. We say that the finite word $x = x_0 x_1 \cdots x_n$ is a *subword* of w if there exists $m \geqslant 0$ such that $w_{m+i} = x_i$, for $0 \leqslant i \leqslant n$. We say that w is *k-th power free* if x^k is never a subword of w, for all nonempty words x. Here is a classical example: let $s(n)$ denote the number of 1's in the binary expansion of n. Then the infinite *word of Thue-Morse*

$$t = t_0 t_1 t_2 \cdots = 0110100110010110 \cdots,$$

defined by $t_n = s(n) \bmod 2$, is cube-free.

Another way to define infinite words is as the fixed point of a homomorphism on a finite alphabet. For example, the Thue-Morse word t is a fixed point of φ, where $\varphi(0) = 01$ and $\varphi(1) = 10$.

A famous infinite word which has been extensively studied is the *Fibonacci word*

$$f = 101101011011010 \cdots ;$$

it is a fixed point of the homomorphism μ, where $\mu(1) = 10$ and $\mu(0) = 1$. For some of the properties of this word, see the survey of Berstel [28]. Karhumäki showed that f is fourth-power-free; see [155].

Now we define some special infinite words. Let $\theta \in [0, 1)$ and define the infinite word $w = w_1 w_2 w_3 \cdots$ as follows:

$$w_n = [(n+1)\theta] - [n\theta] .$$

If we set $\theta = (\sqrt{5} - 1)/2$, we get the Fibonacci word f. Recently, Mignosi [212] proved the following theorem: there exists a k such that w is k-th power-free, if and only if θ has bounded partial quotients. (One direction of Mignosi's theorem follows easily from two different descriptions of w in terms of the continued fraction expansion for θ; see Markoff [205]; Stolarsky [287]; and Fraenkel, Mushkin, and Tassa [107].)

16. Other Results

Let θ be an irrational number of constant type. Let p_n/q_n denote the n-th convergent to θ.

For n a positive integer, let $P(n)$ denote the largest prime factor of n. Then given $\varepsilon > 0$, there exists a constant $c = c(\theta; \varepsilon)$ such that the number of positive integers $n \leqslant x$ with

$$P(q_n) < c \log \log q_n$$

is at most εx. This is a result of Shorey [279].

Schmidt [269] showed that if $f_1, f_2, \ldots$ is a sequence of differentiable functions whose derivatives are continuous and vanish nowhere, then there are uncountably many numbers θ such that all the numbers $f_1(\theta), f_2(\theta), \ldots$ have bounded partial quotients. For related results, see Davenport [74, 75] and Cassels [51].

Other topics connected with real numbers with bounded partial quotients not discussed in this survey include transcendental number theory (see Baker [17]; Flicker [106]; Bundschuh [49]; Angell [11]), Fibonacci hashing on digital computers (see Knuth [169, pp. 510-512]), dynamical systems and global analysis (see Deligne [81]; Katznelson [156]; Herman [142, 143, 144, 145, 146]; Meyer [211]; de la Llave [193, 194]; MacKay [196, 197]; MacKay, Meiss, and