14. PSEUDO-RANDOM NUMBER GENERATION

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **05.06.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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 $\varphi(1) = 10$.