13. Connections with Ergodic Theory

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.05.2024**

For other results connecting discrepancy and the boundedness of the partial quotients, see the papers of Niederreiter [218] and Dupain and Sós [94, 95]. Also see Beck and Chen [25] and Richert [258].

We can also consider the so-called L^2 discrepancy, T_n, defined as follows: let

$$R_n(t) = \frac{S_n([0, t), \omega)}{n} - t$$

and put

$$T_n(\omega) = \left(\int_0^1 R_n^2(t)\,dt \right)^{1/2}.$$

It is possible to generalize the definitions of D_n and T_n to the multi-dimensional case, though we omit the details. By appealing to numbers with bounded partial quotients, Davenport [73] constructed sequences in two dimensions with low L^2 discrepancy. Also see Proinov [250, 251, 252].

Another measure connected with sequences is called *dispersion*. Let $\omega = (x_1, x_2, \ldots)$ and define the dispersion

$$d_n(\omega) = \sup_{x \in [0,1]} \min_{1 \leqslant k \leqslant n} |x - x_k|,$$

essentially half the distance between the most widely separated points of the sequence $x_1, x_2, \ldots, x_n$. (Compare with the function $\delta_\theta(n)$ in Section 11.)

Niederreiter [221] considered the dispersion of the sequence $\{n\theta\}$. He showed that if θ has bounded partial quotients, then $d_n(\omega) = O(1/n)$. He also gave a more detailed estimate, showing that $d_n(\omega)$ is approximately $K(\theta)/4n$. Also see Drobot [93] and Larcher [311].

13. Connections with Ergodic Theory

Let θ be irrational, $\omega = (\theta, 2\theta, \ldots)$ and $S_n(I, \omega)$ be defined as in the previous section. Veech [293] developed connections between S_n and ergodic theory. We mention one result that is number-theoretic in nature. Let $x_n = S_n(I, \omega) \bmod 2$, and define

$$\mu_\theta(I) = \lim_{n \to \infty} \frac{1}{n} \sum_{1 \leqslant k \leqslant n} x_k ,$$

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 $w = w_0w_1w_2 \cdots$ be an infinite word over a finite alphabet. We say that the finite word $x = x_0x_1 \cdots x_n$ 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*

$$t = t_0t_1t_2 \cdots = 0110100110010110 \cdots ,$$

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 $\varphi(1) = 10$.