アルゴリズム 11－3
（1989. 10. 24）

格子算法と乱数生成について

手塚 集
日本アイ・ビー・エム東京基礎研究所

ラティスの基底を縮約する方法は、線形合同法のランダム性のテストとして広く用いられているスペクトル検定に応用できる。本論文では、Tausworthe列の一般化として、GF[2,x]上の線形合同法を定義し、この方法により生成される系列のランダム性を検討する。Mahlerの定理に基づいて、この系列のk-distributionとGF[2,x]上のラティスの最小ベクトルとを関係づける定理を証明する。この定理の幾何学的解釈も付け加える。さらに、Lenstraの縮約基底法が、この定理により、ここで定義した系列のランダム性の解析に利用できることも示される。

Basis Reduction and Random Number Generation

Shu Tezuka

IBM Tokyo Research Laboratory

5-19, Sanbancho, Chiyodaku, Tokyo 102, Japan

ABSTRACT: A method for basis reduction in an integer lattice can be used for the spectral test, which is known as a theoretical test for investigating the k-distribution of linear congruential sequences. In this paper, we define an analogue of linear congruential sequences in $GF\{2,x\}$, and show that the so-called Tausworthe sequences are a subclass of this class of sequences. Based on Mahler's theory on the geometry of numbers in $GF\{p,x\}$, we derive a theorem that links the k-distribution of such sequences and the shortest vector in a lattice associated with the sequences, thereby leading to the consequence that the basis reduction method in $GF\{2,x\}$ proposed by Lenstra is applicable to the analysis of the randomness of these generators. In addition, the geometric interpretation of the lattice structure of these sequences is described.

1 Introduction

The linear congruential method is the most popular algorithm for random number generation in the field of computer simulations. The randomness of the sequences produced by this method can be analyzed by the so-called spectral test, which provides us with a measure defined as the length of the shortest vector in the dual lattice of the lattice spanned by the consecutive elements of a congruential sequence. This measure has proved to be powerful in examining the k-distribution of congruential sequences since Knuth [2] made a comprehensive study on this theory in his book, where an efficient approach due to Dieter for finding a shortest vector in an integer lattice is fully described, but unfortunately, it is known to be an exponential time algorithm.

Basis reduction of a lattice has many applications ranging from the geometry of numbers to cryptography. One of main problems closely related to this method is to find a nonzero shortest vector in a lattice. Recently, Lenstra, Lenstra, and Lovasz proposed a method for basis reduction, which runs in time polynomial for a fixed dimensions. However, this algorithm also suffer from the exponential time complexity depending on the dimension size. So in high dimensions, it becomes slow. Moreover, the problem of finding the shortest vector in integer lattice is believed to be NP-hard [1]. This fact is very critical in designing congruential generators with large period length for the applications in the area of large-scale computer simulation, since in such cases the designers of random number generators need to apply the spectral test of high dimensions(over 10 dimensions) to large period (over 2*60) congruential sequences, where the LLL algorithm fails to find a shortest vector in reasonable time.

On the other hand, Lenstra presented a polynomial time algorithm for finding a nonzero shortest vector of a lattice in a vector space over $GF\{p, x\}$, the field of Laurant series over GF(p). This fact leads us to consider the analogous version of the linear congruential method in $GF\{2, x\}$ for practical uses. The main result of this paper is a theorem that directly links the k-distribution of sequences generated by such analogous method and Lenstra's basis reduction method in $GF\{2, x\}$. The paper is organized as follows. Section 2 briefly overviews the conventional linear congruential generators. In Section 3, we define the linear congruential method in $GF\{2, x\}$ and show that Tausworthe generators are a special case of the above generators. Then we prove the main theorem by using the results on the uniform distribution of sequence of polynomials in $GF\{2, x\}$ and Mahler's theory on the geometry of numbers in $GF\{p, x\}$. We also present a geometric interpretation of the main theorem. Section 4 discusses the difference and similarity between this analogous version and the conventional linear congruential method.

2 Conventional linear congruential generators

Prior to introducing the definition of a new congruential method, in this section we summarize the conventional linear congruential generators.

$$\begin{aligned} X_i &= aX_{i-1} + c \pmod{M} \\ u_i &= X_i/M, \end{aligned}$$

where a, c, M are integers and X_i is a sequence of integers. The normalized sequence $u_i, i = 1, 2, ...,$ is a pseudorandom sequence in [0,1). Most common choice of parameters was that $a = 1 \pmod 4$, c=odd, and M = a power of two. However, it has been known that this choice is insufficient because of the nonrandomness of the lower bits of X_i. So, recently the choice is widely used that M is prime and a is a primitive root modulo M. One of most popular generators of this type is the so-called GGL, IBM random number subroutine, i.e. $M = 2^{31} - 1$, $a = 7^5$, and $c = 0$.

The spectral test is a theoretical test for examining the randomness of linear congruential sequences. The measure provided by this test is defined as follows: for k dimensions,

$$\nu_k = \min \sum_{i=1}^{k} s_i^2,$$

where the minimum is taken over all nonzero solutions of the equation

$$\sum_{i=1}^{k} a^i s_i = 0 \pmod M.$$

An intuitive interpretation of this measure is that ν_k^{-1} is the maximum distance of neighboring hyperplanes covering all lattice points generated by consecutive k terms of congruential sequences. In other words, ν_k is regarded as the nonzero shortest vector in the lattice spanned by the following vectors,

$$\begin{aligned} e_1 &= (M, 0, 0, ..., 0) \\ e_2 &= (-a, 1, 0, ..., 0) \\ &\vdots \quad \vdots \\ e_k &= (-a^{k-1}, 0, 0, ..., 1). \end{aligned}$$

For more detail, refer to [2]. In short words, for a given set of a, c and M the larger the value of ν_k, the more random the sequence is. Note that the value of c has no effect on the result of the spectral test, although the period length of the resulting sequence is influenced by the choice of c.

3 Linear congruential generators in $GF\{2, x\}$

3.1 Definition of linear congruential generators in $GF\{2, x\}$

Here we define an analogous version of linear congruential sequences in $GF\{2, x\}$. This generator is formulated as follows: let σ be a mapping from $GF\{2, x\}$ to the real field defined as

$$\sigma(\sum_{i=-\infty}^{m} a_i x^i) = \sum_{i=-\infty}^{m} a_i 2^i,$$

where a_i is in GF(2). Then a pseudorandom sequence $u_i, i = 1, 2, ...,$ in [0,1) is given as

$$\begin{aligned} f_i(x) &= g(x) f_{i-1}(x) + h(x) \pmod{M(x)}, \\ u_i &= \sigma(f_i(x)/M(x)), \end{aligned} \tag{1}$$

where $g(x), h(x), M(x)$ and $f_i(x)$ are polynomials in $GF\{2, x\}$. In practical situations, u_i is expressed by an approximate value with its leading bits as is the case of the congruential sequence.

Tausworthe sequences [6] have been known as one of other types of generators than linear congruential sequences ever since the mid of 60's. In what follows, we can show that this type of sequence is a special case of the above general class. Let $M(x)$ be a primitive polynomial, $g(x) = x^s \pmod{M(x)}$, with $0 \leq s < 2^p - 1$, and L is the word size. Then the sequence is given as

$$u_i = \sum_{j=1}^{L} a_{is+j} 2^{-j},$$

where a_i is a binary sequence generated by a linear recurrence relation whose characteristic polynomial is M(x). As easily seen, this is equivalent with the definition of Tausworthe sequences.

The following theorem assures the existence of the sequences with large periods defined in (1).

Theorem 1 *For $p > 2$, where p is the degree of $M(x)$, a sequence generated by (1) has the maximum possible period $2^p - 1$ if and only if $M(x)$ is irreducible and $g(x)$ is a primitive root modulo $M(x)$.*

(Proof)

In the case of $M(x)$ with $M(0) = 0$, the sequence has a period of at most 2^{p-1}, which is less than $2^p - 1$.
So assume that $M(0) \neq 0$. Let $\bar{f}_i(x) = f_i(x) - f_{i-1}(x)$. Then $\bar{f}_{i+1}(x) = g(x)\bar{f}_i(x) \pmod{M(x)}$. If $\bar{f}_i(x)$ has a period of $2^p - 1$, i.e., $M(x)$ is irreducible and $g(x)$ is primitive modulo $M(x)$, then $f_i(x)$ also has a period of $2^p - 1$.
If $M(x)$ is irreducible but $g(x)$ not primitive, then $f_i(x)$ has a period of at most double the order of $g(x)$ modulo $M(x)$, which is less than $2^p - 1$, since a possible factor of $2^p - 1$ is at least 3. If $M(x)$ is reducible, $f_i(x)$ has a period of at most double the order of $M(x)$, which is less than $2^p - 1$ when $p > 2$. Thus, the proof is complete.□

Unlike the conventional linear congruential method, these generators can not produce sequences of the maximum length 2^p for $p > 2$.

The implementation for fast generation of sequences defined by (1) is described as follows: The multiplication of g(x) and $u_i(x)$ is done by a shift operation and an exclusive-or operation. To reduce the number of operations, g(x) should be chosen as a polynomial with a few nonzero coefficients. In the following, we give an algorithm for the case of $g(x) = x^s, 0 < s \leq p-q$. Assume that M(x) is a primitive trinomial, i.e., $x^p+x^q+1, (p/2 > q)$. Note that each term of a sequence is expressed by its leading p bits in this algorithm.

(An algorithm for the generator defined in (1))

Step.0: A and B are p-bit words.
Step.1: B ⟵ q bits left shift of A
Step.2: B ⟵ A exclusive-or B
Step.3: B ⟵ $p - s$ bit right shift of B

Step.4: A $\longleftarrow$ s bit left shift of A
Step.5: A $\longleftarrow$ A exclusive-or B
Step.6: Output A

This idea is slightly modified from the original one due to Payne, who dealt with the case of $k = p$. The total numbers of shift operations and exclusive-or operations are three and two, respectively, thus the fast generation of sequences is realized.

3.2 A theorem on the k-distribution of the sequences

The next theorem links the k-distribution of the sequences defined above with the problem of finding the nonzero shortest vector, with respect to the maximum norm, of a lattice in the vector space over $GF\{2, x\}$. The definition of k-distribution is as follows:

Definition 1 *A sequence with period $2^p - 1$ is said to be k-distributed with d-bit resolution if every k-tuple of the leading d bits of each term of the sequence appears 2^{p-kd} times over the whole period except for one certain k-tuple appearing one time less.*

Let L_k be the lattice spanned by the k-tuple of consecutive elements of the sequence, and L_k^* be its dual. Then the respective bases for L_k and L_k^* are given as

$$\begin{array}{ll} e_1 = \frac{1}{M(x)}(1, g(x), g^2(x), ..., g^{k-1}(x)), & e_1^* = (M(x), 0, 0, ..., 0), \\ e_2 = (0, 1, 0, ..., 0), & e_2^* = (g(x), 1, 0, ..., 0), \\ \vdots & \vdots \\ e_k = (0, 0, 0, ..., 1), & e_k^* = (g(x)^{k-1}, 0, 0, ..., 1). \end{array}$$

Then we obtain the following theorem. The norm $|\alpha|$ of a vector $\alpha = (a_1, ..., a_k)$ is defined as $max\{deg(a_i); i = 1, ..., k\}$

Theorem 2 *A sequence with maximum possible period $2^p - 1$ defined by (1) is k-distributed with d-bit resolution if and only if the norm of the nonzero shortest vector in the lattice L_k^* is equal to or greater than d.*

(Proof)

From the theory of uniform distribution [3], a sequence defined in (1) of length $2^p - 1$ is k-distributed with d bit resolution if and only if, for any nonzero $(s_1(x), ..., s_k(x))$ with $deg(s_i) < d$,

$$\begin{aligned} \sum_{deg(n) < p} \Pi_{i=1}^{k} e(s_i(x)\frac{n(x)g^i(x)}{M(x)}) &= \sum_{deg(n) < p} e(n(x)\frac{\sum_{i=1}^{k} g^i(x)s_i(x)}{M(x)}) \\ &= 0. \end{aligned}$$

Here $e(\alpha)$ is the character of α in $GF\{2, x\}$ defined as

$$e(\alpha) = (-1)^{a_1},$$

where a_1 is the coefficient of x^{-1} in the expression for α. Let l be the norm of

a nonzero shortest vector of the lattice L_k^*. Then, from the definition of L_k^*, l is given as the norm of the nonzero solutions of

$$\sum_{i=1}^{k} g^i(x)s_i(x) = 0 \pmod{M(x)}.$$

This is equivalent to the following: for any nonzero $(s_1(x), ..., s_k(x))$ with $deg(s_i) < d \leq l$,

$$\sum_{i=1}^{k} g^i(x)s_i(x) \neq 0 \pmod{M(x)}.$$

This completes the proof.□

Although the above proof employed the result on the uniform distribution of sequences of polynomials, instead of it we can use the theorem on the Walsh-spectral test [7], which was developed for the analysis of the k-distribution of GFSR sequences, since the truncated version of the sequences defined in (1) constitutes a subclass of GFSR sequences.

Lenstra [4] presented a basis reduction algorithm in $GF\{2, x\}$ which runs in time polynomial in the size of data and the dimensions. Since this algorithm works with respect to the maximum norm of a vector over $GF\{2, x\}$, it can be applied to the investigation of the sequences defined in (1).

3.3 Geometric interpretation of Theorem 2

For simplicity, we consider the two-dimensional case. Let $S(l)$ be an equidissection of the two-dimensional unit space defined as

$$S(l) = \{J(l, i, j) | 0 \leq i, j < 2^l\},$$

where $J(l, i, j)$ is a subinterval $[i2^{-l}, (i+1)2^{-l}) \times [j2^{-l}, (j+1)2^{-l})$, for $0 \leq i, j < 2^l$. Let α_1,α_2 and β_1, β_2 be reduced bases corresponding to the successive minima of the primal lattice L_2 and of the dual lattice L_2^*, respectively. Since $|\alpha_1| \leq |\alpha_2|$, each cell of the equidissection $S(-|\alpha_2| - 1)$ contains $2^{p+2|\alpha_2|}$ quadrilaterals each consisting four lattice points P_1, P_2, P_3, P_4 specified as $P_2 = P_1 \oplus \alpha_1, P_3 = P_1 \oplus \alpha_2, P_4 = P_1 \oplus \alpha_1 \oplus \alpha_2$, where $\oplus$ is the bit-wise exclusive or operation of the corresponding coordinates. Furthermore, every cell of the equidissection $S(-|\alpha_2|)$ contains equal number of points, i.e., $2^{p+2|\alpha_2|}$ points.

Figure 1 shows the point set produced by the generator, $f_{i+1}(x) = x^8 f_i(x) \pmod{x^6 + x + 1}$, where the origin is added to the point set, and Figure 2 gives an example of the equidissection $S(2)$ of the unit space. As easily seen, each cell contains a quadrilateral consisting of four points in the point set, and each cell of the equidissection $S(3)$ contains one point.

Theorem 2 says that the point set is divided by the cells of the equidissection $S(|\beta_1|)$, where each cell contains $2^{p-2|\beta_1|}$ points, and, moreover, the point set can not be evenly distributed into smaller cells of the equidissections $S(k)$ for $k > |\beta_1|$. By Mahler's theorem [5] that $\beta_1\alpha_2 = 1$ (in general, $\beta_1\alpha_k = 1$ for k dimensions), we arrive at the interesting connection between the geometric idea of the 2-distribution and Theorem 2.

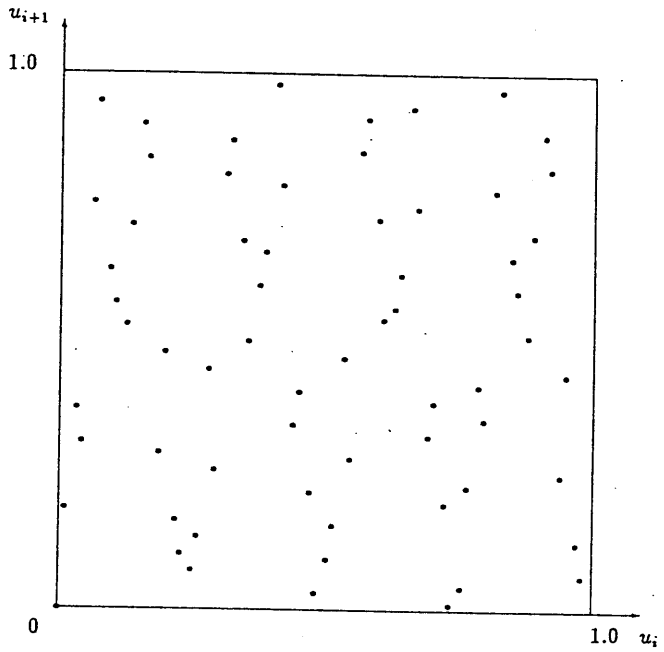

Figure 1: A set of two-dimensional points, $(u_i, u_{i+1}), i = 1, ..., 63$, produced by the generator $f_{i+1}(x) = x^8 f_i(x) \pmod{x^8 + x + 1}$.

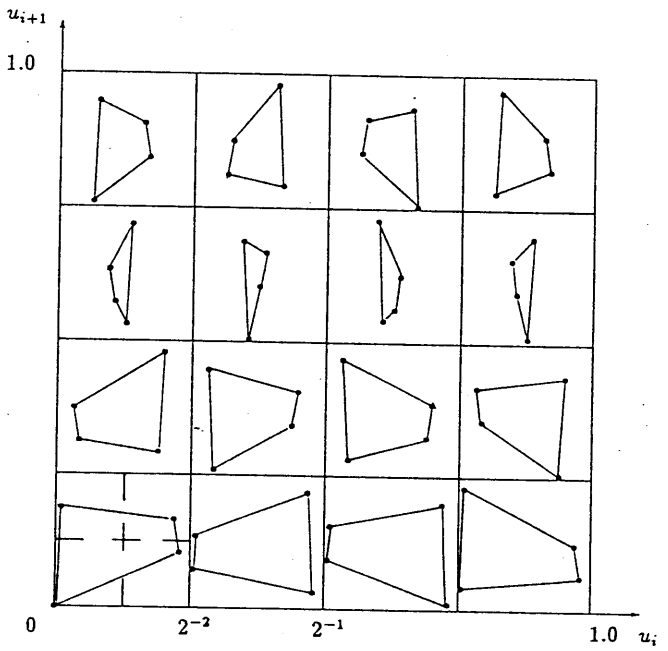

Figure 2: The dissection $S(2)$ of the same point set as Figure 1

4 Discussions

In this paper we have defined an analogue of the linear congruential method over $GF\{2, x\}$ for random number generation. The following are the major difference and similarity between this method and the conventional linear congruential method.

Similarity: In both cases the k-distribution of sequences is connected with the shortest vector in the lattice associated with the k consecutive elements of the sequences.

Difference: The shortest vector can be found in polynomial time in the case of a lattice in the vector space over $GF\{2, x\}$, whereas it is not the case for an integer lattice. Therefore, the generator defined in (1) with large period length can be employed for large-scale computer simulations for which the conventional linear congruential generators was not applicable due to the hardness to carry out the spectral test when the modulus and the dimension-size become large.

References

[1] R. Kannan, Algorithmic geometry of numbers, *Ann. Rev. Comput. Sci.*, vol. 2, (1987),231-267.

[2] D.E.Knuth, *The Art of Computer Programming: Vol. 2, Seminumerical Algorithms*, 2nd ed., Addison-Wesley, 1981.

[3] L. Kuipers and H. Niederreiter,*Uniform distribution of sequences* , New York, Wiley, 1974.

[4] A.K. Lenstra, Factoring multivariate polynomials over finite fields, *J. Comput. Syst. Sci.*, Vol. 30, (1985), 235-248.

[5] K. Mahler, An analogue to Minkowski's geometry of numbers in a field of series, *Ann. of Math.*, Vol. 42, (1941), 488-522.

[6] R.C. Tausworthe, Random numbers generated by linear recurrence modulo two, *Math. Comp.*, Vol. 19, (1965), 201-209.

[7] S. Tezuka, Walsh-spectral test for GFSR pseudorandom number generators, *Comm. ACM.*, Vol. 30, (1987), 731-735.