The b-adic Diaphony as a Tool to Study Pseudo-randomness of Nets

Ivan Lirkov[1] and Stanislava Stoilova[2]

[1] Institute of Information and Communication Technologies
Bulgarian Academy of Sciences
Acad. G. Bonchev, bl. 25A, 1113 Sofia, Bulgaria
ivan@parallel.bas.bg
[2] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Acad. G. Bonchev, bl. 8, 1113 Sofia, Bulgaria
stoilova@math.bas.bg

Abstract. We consider the b-adic diaphony as a tool to measure the uniform distribution of sequences, as well as to investigate pseudo-random properties of sequences. The study of pseudo-random properties of uniformly distributed nets is extremely important for quasi-Monte Carlo integration. It is known that the error of the quasi-Monte Carlo integration depends on the distribution of the points of the net. On the other hand, the b-adic diaphony gives information about the points distribution of the net.

Several particular constructions of sequences (x_i) are considered. The b-adic diaphony of the two dimensional nets $\{y_i = (x_i, x_{i+1})\}$ is calculated numerically. The numerical results show that if the two dimensional net $\{y_i\}$ is uniformly distributed and the sequence (x_i) has good pseudo-random properties, then the value of the b-adic diaphony decreases with the increase of the number of the points. The analysis of the results shows a direct relation between pseudo-randomness of the points of the constructed sequences and nets and the b-adic diaphony as well as the discrepancy.

1 Introduction

The quasi-Monte Carlo methods can be described in simple words as a deterministic version of the Monte Carlo methods. The difference lies in the replacement of the random points by well-distributed deterministic nodes. One way to introduce the randomization into the quasi-Monte Carlo method is randomizing the deterministic integration nodes used in the method, e.g. [9,10,2]. In this way we can combine the faster convergence rates of the quasi-Monte Carlo methods and the possibility to estimate the error of the Monte Carlo methods. In this context, the study of pseudo-random properties of the deterministic sequences is inescapable. The approach to examine the pseudo-randomness of the deterministic sequences is to estimate the measures of distribution of the points of these sequences.

I. Dimov, S. Dimova, and N. Kolkovska (Eds.): NMA 2010, LNCS 6046, pp. 68–76, 2011.

Many authors study pseudo-random properties of the sequences by using the bounds of the discrepancy [3,4,5,11,12,13,14,1]. We consider the relationship between the pseudo-randomness and the $b-$adic diaphony.

We will recall some known notions. Let $\xi = (\mathbf{x}_j)_{j\geq 1}$ be a sequence in $[0,1)^s$. For arbitrary integer M and $J = [\boldsymbol{\alpha}, \boldsymbol{\beta}) \subseteq [0,1)^s$ $A_M(\xi; J)$ is the number of belonging to J points of ξ. We denote the Lebesgue measure on J with $\mu(J) = \prod_{i=1}^{s}(\beta_i - \alpha_i)$.

Definition 1. *The sequence $\xi = (\mathbf{x}_j)_{j\geq 1}$ is uniformly distributed mod 1 in $[0,1)^s$ if for every $J = [\boldsymbol{\alpha}, \boldsymbol{\beta}) \subseteq [0,1)^s$ the equality*

$$\lim_{M\to\infty} \frac{A_M(\xi; J)}{M} = \mu(J)$$

is hold, see [15].

The last equality shows when a sequence of points in $[0,1)^s$ is uniformly distributed but it does not allow to compare the distributions of two sequences. For that purpose measures of the distribution of the sequences are used. Such measures are the discrepancy [8] and the diaphony [6].

Definition 2. *Let $M \geq 1$ be an arbitrary fixed integer and $\xi_M = \{\mathbf{x}_0, \dots \mathbf{x}_{M-1}\}$ is a net of real numbers in $[0,1)^s$. The quantity*

$$D(\xi_M) = \sup_{J\subseteq[0,1)^s} \left| \frac{A(\xi_M; J)}{M} - \mu(J) \right|$$

is called a discrepancy of the given net.

Let $b \geq 2$ be a fixed integer and b denotes the base of the number system everywhere in this paper. Also, let an arbitrary $x \in [0,1)$ have a $b-$adic representation $x = \sum_{l=0}^{\infty} x_l b^{-1-l}$, where for $l \geq 0$, $x_l \in \{0, 1. \dots, b-1\}$ and for infinitely many values of l, $x_l \neq b-1$. The integer part of $b-$adic logarithm of x is $\lfloor \log_b x \rfloor = -g$, if $x_l = 0$ for $l < g$ and $x_g \neq 0$. We denote the operation $x \dot{-} y = \sum_{l=0}^{\infty} [(x_l - y_l)(\mod b)] b^{-1-l}$ and for vectors $\mathbf{x}, \mathbf{y} \in [0,1)^s$ we note $\mathbf{x} \dot{-} \mathbf{y} = (x_1 \dot{-} y_1, x_2 \dot{-} y_2, \dots, x_s \dot{-} y_s)$, where $\mathbf{x} = (x_1, x_2, \dots, x_s), \mathbf{y} = (y_1, y_2, \dots, y_s)$.

We define the functions $\gamma : [0,1) \to \mathbb{R}$ and $\Gamma : [0,1)^s \to \mathbb{R}$ as

$$\gamma(x) = \begin{cases} b+1-(b+1)b^{1+\lfloor \log_b x \rfloor}, & \text{if } x \in (0,1) \\ b+1, & \text{if } x = 0 \end{cases}$$

and

$$\Gamma(\mathbf{x}) = -1 + \prod_{d=1}^{s} \gamma(x_d), \qquad \mathbf{x} = (x_1, x_2, \dots, x_s).$$

Definition 3. *The $b-$adic diaphony $F_M(\xi)$ of the first M elements of the sequence $\xi = (\mathbf{x}_i)_{i\geq 0}$ in $[0,1)^s$ is defined as*

$$F_M(\xi) = \left(\frac{1}{(b+1)^s - 1} \frac{1}{M^2} \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} \Gamma(\mathbf{x}_i \dot{-} \mathbf{x}_j) \right)^{\frac{1}{2}},$$

where the coordinates of all points of the sequence ξ are $b-$adic rational.

Let $i = \sum_{l=0}^{\infty} i_l b^l$ be the $b-$adic representation of the non-negative integer i. Then the i-th element of the Van der Corput sequence is defined as

$$\zeta_b(i) = \sum_{l=0}^{\infty} i_l b^{-l-1}.$$

Let us introduce $f_M \equiv a_2 y_i^2 + a_1 y_i + a_0 (\mod M)$, where $M \geq 2$ is an integer and a_2, a_1, a_0 are three integer parameters. The number M is called modulus. Let $y_0 \in [0, M)$ be initial starting point. The sequence of pseudo-random numbers $\left\{x_i = \frac{y_i}{M}\right\}$ is produced by quadratic congruential generator

$$y_{i+1} = f_M(y_i), \quad y_i \in [0, M), \quad i = 0, 1, \ldots, M-1. \tag{1}$$

The quadratic congruential generator (1) is introduced by Knuth [7]. He also proved that the sequence y_i is purely periodic with maximum possible period length M if and only if:

$(a_0, M) = 1$;
$p|a_2$ for every prime $p|M,\ p > 2$;
$a_1 \equiv 1 (\mod p)$ for every prime $p|M,\ p > 2$;
If $9|M$, then either $9|a_2$ or $a_1 \equiv 1 (\mod 9)$ and $a_2 a_0 \equiv 6 (\mod 9)$;
If $4|M$, then $2|a_2$ and $a_2 \equiv a_1 - 1 (\mod 4)$;
If $2|M$, then $a_2 \equiv a_1 - 1 (\mod 2)$.

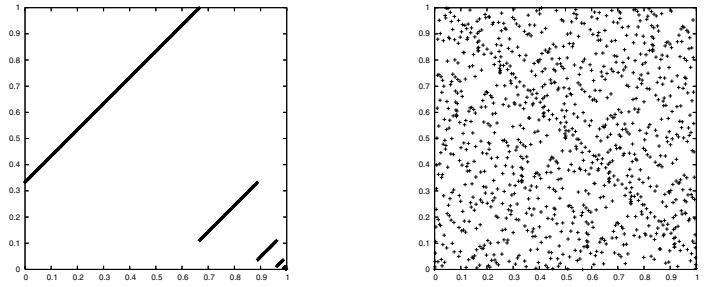
Some authors researched pseudo-randomness of $x_i, i = 0, 1, \ldots, M-1$ under the discrepancy D_M of the two-dimensional net

$$(x_i, x_{i+1}) = \left(\frac{y_i}{M}, \frac{y_{i+1}}{M}\right), i = 0, 1, \ldots, M-1.$$

J. Eichenauer-Herrmann and H. Niederreiter [4,5] proved bounds of the discrepancy D_M of the two-dimensional net produced by quadratic congruential generator which are $D_M = \mathcal{O}\left(\frac{(\log M)^2}{\sqrt{M}}\right)$. Using the geometric approach O. Blažeková and O. Strauch [1] obtained order $\mathcal{O}\left(\frac{(\log M)^{3/2}}{\sqrt{M}}\right)$ of the star-discrepancy D_M^* of the same net. From the uniform distribution theory [8] it is well known that the discrepancy and the star discrepancy are always of the same order of magnitude, they differ at most by 2^s, where s is the dimension. Obviously, the order obtained in [1] is better than the previously proved estimates in [4,5].

2 The $b-$adic Diaphony and Pseudo-randomness

The study of the pseudo-random property of the sequence $x_i, i = 0, 1, \ldots$ is associated with an estimation of the distribution of the two-dimensional net (x_i, x_{i+1}). Until now, the discrepancy is used to estimate the distribution of



Van der Corput sequence quadratic generator

Fig. 1. The distribution of points of sequences (2) and (3), $M = 1024$, $b = 3$

the nets. Here we use the $b-$adic diaphony for the study of the distribution of the two-dimensional net (x_i, x_{i+1}) and the pseudo-randomness of the sequence $x_i, i = 0, 1, \ldots$.

2.1 Pseudo-randomness of the Van der Corput Sequence Using the $b-$adic Diaphony

We consider the net

$$(\zeta_b(i), \zeta_b(i+1)), \quad i = 0, 1, \ldots, M-1. \tag{2}$$

This net is not uniformly distributed, because the points of the net lie on the lines $y = x + \frac{1}{b^{j+1}} + \frac{1}{b^j} - 1, j = 0, 1, 2, \ldots$ (see Fig. 1).

The bad distribution of the two-dimensional net (2), based on the Van der Corput sequence is seen from the values of the $b-$adic diaphony in Table 1.

2.2 Pseudo-randomness of a Quadratic Generator Using the $b-$adic Diaphony

We consider the quadratic congruential generator (1) and obtain the sequence $x_i = \frac{y_i}{M}$ of quadratic congruential pseudo-random numbers. To investigate

Table 1. The diaphony F_M of the Van der Corput sequence, $b = 3$

$M = b^\nu, 3 \le \nu \le 10$		$M = 2^\mu, 4 \le \mu \le 16$			
M	F_M	M	F_M	M	F_M
27	0.374992	16	0.387033	4096	0.372105
81	0.37243	32	0.376644	8192	0.372104
243	0.372141	64	0.373283	16384	0.372104
729	0.372108	128	0.372489	32768	0.372104
2187	0.372105	256	0.372197	65536	0.372104
6561	0.372104	512	0.372126		
19683	0.372104	1024	0.372112		
59049	0.372104	2048	0.372106		

Table 2. The diaphony F_M of the quadratic generator $b = 3$

$3x^2 + x + 2 (\text{mod } M)$ $M = b^\nu, 3 \leq \nu \leq 10$		$6x^2 + 3x + 1 (\text{mod } M)$ $M = 2^\mu, 4 \leq \mu \leq 16$			
M	F_M	M	F_M	M	F_M
27	0.214727	16	0.187028	4096	0.0125823
81	0.10644	32	0.150217	8192	0.00912462
243	0.0592701	64	0.105382	16384	0.00630444
729	0.0348591	128	0.0760402	32768	0.00436687
2187	0.0165547	256	0.0544161	65536	0.00314525
6561	0.0119346	512	0.0362376		
19683	0.0072553	1024	0.0242248		
59049	0.00361669	2048	0.0171268		

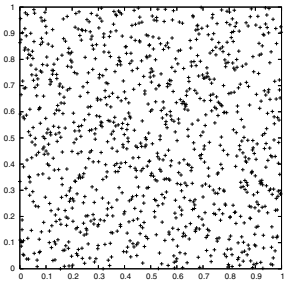


Fig. 2. The distribution of points of the combination of quadratic generator with Van der Corput sequence with $M = 1024$, $b = 3$, $f_M(i) \equiv 6i^2 + 3i + 1 (\text{mod } M)$

pseudo-random property of the sequence x_i, we calculate the $b-$adic diaphony of the net

$$(x_i, x_{i+1}), i = 0, 1, \ldots, M - 1 \tag{3}$$

for two concrete quadratic generators in the case when $M = b^\nu$ and $M = 2^\mu$ and Table 2 shows the results.

2.3 Pseudo-random Property of the Combination of the Van der Corput Sequence with a Quadratic Generator

O. Strauch proposed to combine the Van der Corput sequence with a quadratic generator. In such way, the obtained net has a better pseudo-random property than original sequences.

To improve the distribution of the two-dimensional net we combine the Van der Corput sequence $\zeta_b(i)$ with the quadratic generator $y_{i+1} = f_M(y_i)$. In this way we obtain the net

$$(\zeta_b(y_i), \zeta_b(y_{i+1})), i = 0, 1, \ldots, M - 1. \tag{4}$$

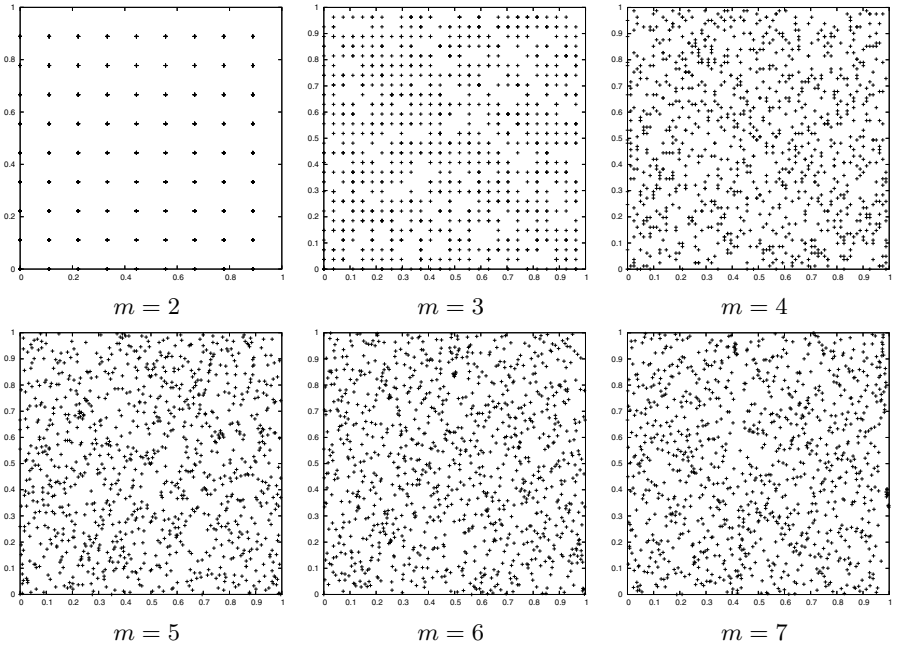


Fig. 3. The distribution of the combination of quadratic generator with Van der Corput sequence with $M = 1024$

Table 3. The diaphony F_M of the net (6) of the combination of quadratic generator $f_M(i) \equiv 6i^2 + 3i + 1 (\mathrm{mod}\ M)$ with Van der Corput sequence, $b = 3$, $M = 2^\mu$, $4 \le \mu \le 16, 3 \le \nu \le 9$, and $m \le \nu$

M	F_M							
	m=2	m=3	m=4	m=5	m=6	m=7	m=8	m=9
16	0.19484	0.20886						
32	0.14907	0.1374	0.17695					
64	0.11024	0.09258	0.09042					
128	0.10049	0.06829	0.0731	0.07685				
256	0.08596	0.05764	0.04742	0.04808	0.05253			
512	0.07979	0.03917	0.03482	0.03402	0.03164			
1024	0.07538	0.03483	0.0256	0.02179	0.02098	0.03035		
2048	0.07313	0.0298	0.02051	0.01555	0.01698	0.01398		
4096	0.07217	0.02667	0.01602	0.01264	0.01263	0.01061	0.01293	
8192	0.07154	0.02542	0.01174	0.01009	0.00927	0.00878	0.00862	0.01095
16384	0.07118	0.02441	0.01042	0.00657	0.00639	0.00577	0.00602	0.00702
32768	0.07109	0.02385	0.00900	0.00517	0.00511	0.00458	0.00403	0.00416
65536	0.07102	0.02364	0.00841	0.00423	0.00347	0.00295	0.00305	0.00286

If the quadratic generator produced purely full period of the length M, then the net (4) has the same points as $(\zeta_b(i), \zeta_b(f_M(i))), i = 0, 1, \ldots, M-1$. The distribution of the obtained net is seen at Fig. 2.

Table 4. The diaphony F_M of the net (6) of the combination of quadratic generator $f_M(i) \equiv 3i^2+i+2 (\mathrm{mod}\ M)$ with Van der Corput sequence, $b = 3, M = b^\nu, 3 \leq \nu \leq 10$, and $m \leq \nu$

M	F_M							
	m=2	m=3	m=4	m=5	m=6	m=7	m=8	m=9
27	0.23612	0.37499						
81	0.20728	0.21735	0.37243					
243	0.11450	0.18947	0.21512	0.37214				
729	0.08438	0.08945	0.18739	0.21487	0.37211			
2187	0.07770	0.04994	0.08626	0.18715	0.21484	0.37211		
6561	0.07182	0.03851	0.04458	0.08590	0.18713	0.21484	0.37210	
19683	0.07173	0.02585	0.03139	0.04395	0.08585	0.18713	0.21484	0.37210
59049	0.07118	0.02562	0.01334	0.03050	0.04388	0.08585	0.18713	0.21483

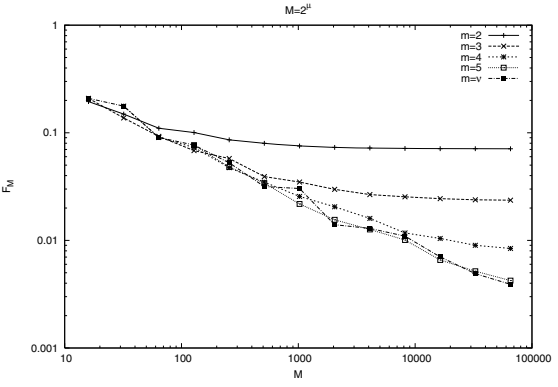


Fig. 4. The diaphony F_M of the combination of quadratic generator with Van der Corput sequence, $M = 2^\mu$

2.4 Simplification

For $x \in [0,1)$ with the $b-$adic expression $x = 0.x_1x_2 \ldots x_{m-1}x_mx_{m+1} \ldots$ let $\zeta^*_{b^m}(x)$ be defined as $\zeta^*_{b^m}(x) = 0.x_mx_{m-1} \ldots x_2x_1$. O. Strauch proposed the net

$$\zeta^*_{b^m}\left(\frac{y_i}{M}\right), i = 0, 1, \ldots, M-1. \tag{5}$$

For pseudo-randomness of (5) we study the $b-$adic diaphony F_M of the two-dimensional net

$$\left(\zeta^*_{b^m}\left(\frac{y_i}{M}\right), \zeta^*_{b^m}\left(\frac{y_{i+1}}{M}\right)\right), i = 0, 1, \ldots, M-1.$$

If $f_M(i)$ has a purely full period, then the net has the same points as

$$\left(\zeta^*_{b^m}\left(\frac{i}{M}\right), \zeta^*_{b^m}\left(\frac{f_M(i)}{M}\right)\right), i = 0, 1, \ldots, M-1 \tag{6}$$

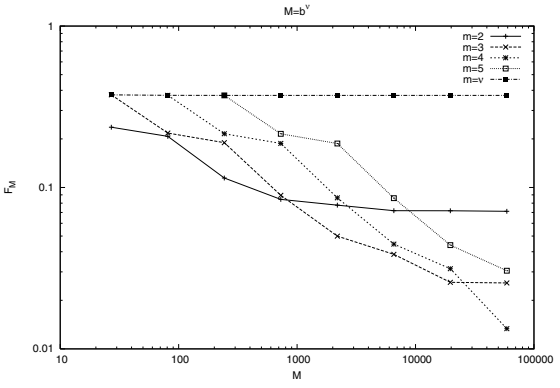


Fig. 5. The diaphony F_M of the combination of quadratic generator with Van der Corput sequence, $M = b^\nu$

and the same $b-$adic diaphony. The distribution of the points of the net (6) for six values of the number m is shown in Fig. 3.

Tables 3 and 4 as well as Fig. 4 and 5 show the computed $b-$adic diaphony of the nets using two quadratic generators with functions $f_M(i) \equiv 6i^2 + 3i + 1 (\mathrm{mod}\ M), M = 2^\mu$ and $f_M(i) \equiv 3i^2 + i + 2 (\mathrm{mod}\ M), M = 3^\nu$.

Conclusion and Future Work

The obtained results show that the $b-$adic diaphony is a good tool to study pseudo-randomness of sequences and nets. The calculations for the $b-$adic diaphony of the net (2) confirm the fact that the Van der Corput sequence is a deterministic and does not have pseudo-random properties. Last figures illustrate that the $b-$adic diaphony of the net (6) decreases with the increasing of the number of the points. This shows that the net (6) is uniformly distributed and therefore the sequence (5) has good pseudo-randomness. Hence, the $b-$adic diaphony can be used to research the pseudo-randomness of the sequences and nets. Furthermore, the $b-$adic diaphony of the nets (4) and (6) as well as of the sequence (5) can be theoretically estimated. In the future we plan to find such theoretical bounds.

Acknowledgments. We would like to thank Professor Oto Strauch for the wonderful ideas about the combination of the Van der Corput sequence with quadratic generator and the simplification of this combination. The study of pseudo-randomness of the proposed by Prof. Oto Strauch sequences is very interesting and useful for us. The authors thank to Professor Ivan Dimov for very useful remarks during the work on the paper. This work is supported by the project Bg-Sk-207, Bulgarian NSF.

References

1. Blaželková, O., Strauch, O.: Pseudo-randomness of quadratic generators. Uniform Distribution Theory 2(2), 105–120 (2007)
2. Dimov, I., Atanassov, E.: Exact Error Estimates and Optimal Randomized Algorithms for Integration. In: Boyanov, T., Dimova, S., Georgiev, K., Nikolov, G. (eds.) NMA 2006. LNCS, vol. 4310, pp. 131–139. Springer, Heidelberg (2007)
3. Drmota, M., Tichy, R.F.: Sequences, Discrepancies and Applications. LNM, vol. 1651. Springer, Heidelberg (1997)
4. Eichenauer-Herrmann, J., Niederreiter, H.: On the discrepancy of quadratic congruential pseudorandom numbers. J. Comput. Appl. Math. 34(2), 243–249 (1991)
5. Eichenauer-Herrmann, J., Niederreiter, H.: An improved upper bound for the discrepancy of quadratic congruential pseudorandom numbers. Acta Arithmetica 69(2), 193–198 (1995)
6. Grozdanov, V., Stoilova, S.: The $b-$adic diaphony. Rendiconti di Matematica 22, 203–221 (2002)
7. Knuth, D.E.: Seminumerical algorithms, 2nd edn. The art of computer programming, vol. 2. Addison Wesley, Reading (1981)
8. Kuipers, L., Niederreiter, H.: Uniform distribution of sequences. John Wiley, New York (1974)
9. L'Ecuyer, P., Lemieux, C.: Recent Advances in Randomized Quasi-Monte Carlo Methods. In: Dror, M., L'Ecuyer, P., Szidarovszki, F. (eds.) Modeling Uncertainty: An Examination of Stochastic Theory, Methods, and Applications, pp. 419–474. Kluwer Academic Publishers, Dordrecht (2002)
10. Lemieux, C., L'Ecuyer, P.: Randomized Polynomial Lattice Rules for Multivariate Integration and Simulation. SIAM Journal on Scientific Computing 24(5), 1768–1789 (2003)
11. Niederreiter, H.: Random number generation and quasi-Monte Carlo methods. In: CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63. SIAM, Philadelphia (1992)
12. Niederreiter, H., Shparlinski, I.E.: On the distribution of inversive congruential pseudorandom numbers in parts of the period. Mathematics of Computation 70(236), 1569–1574 (2000)
13. Niederreiter, H., Shparlinski, I.E.: Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arithmetica XCII(1), 89–98 (2000)
14. Strauch, O., Porubský, Š.: Distribution of Sequences: A Sampler, Peter Lang, Frankfurt am Main (2005)
15. Weil, H.: Über die Gleichverteilung von Zahlen mod. Eins. Math. Ann. 77, 313–352 (1916)