An efficient algorithm for constructing low-discrepancy sequences over $\mathbb{F}_b$

Vesna Dimitrievska Ristovska

University "Ss Cyril and Methodius", FINKI,
16, Rugjer Boshkovikj str., 1000 Skopje, Macedonia,
vesna.dimitrievska.ristovska@finki.ukim.mk

Abstract. Binary Gray code is used elsewhere to propose a fast algorithm for construction of $\Lambda\Pi_\tau-$ sequences. In this paper, the binary Gray code is generalized in the case when the base b is an arbitrary prime number. This $b-$adic Gray code and direction matrices are used to propose a new efficient algorithm for construction of a special class of low-discrepancy sequences and nets, called digital $(t,s)-$ sequences and $(t,m,s)-$ nets in base b. Two computer programs are written. The first one generates generalized Gray code over the field $\mathbb{F}_b$. The results of the first program are used as input in the second program, which constructs $(t,s)-$ sequences and $(t,m,s)-$ nets in the base b. In this manner, this theoretical algorithm is practically realized. The generalization of Antonov and Saleev's approach is the main motivation of our theoretical and practical investigations.

Keywords: Low-discrepancy sequence, Sobol's sequence, (t,s)-sequence, (t,m,s)-net, $b-$adic Gray code, direction numbers, direction matrices

1 Motivation

This paper is based on two principles:

1. A generalization of the constructive approach of Antonov and Saleev ([1]), which produces classes of $(t,s)-$ sequences over the field $\mathbb{F}_2$ by using binary Gray code;
2. The results of our previous paper ([2]), where we constructed a class of digital $(t,s)-$ sequences and $(t,m,s)-$ nets over the field $\mathbb{F}_b$ with a prime base b.

The main progress of this paper is the possibility to use the $b-$adic Gray code to construct a class of $(t,s)-$ sequences and $(t,m,s)-$ nets over the field $\mathbb{F}_b$ with a prime base b.

2 Introduction

Let $s \geq 1$ be a fixed integer. The parameter s denotes the dimension in our investigation. Following Niederreiter ([6]), we will give a concept of a class of sequences with well distribution of their points in the unit $s-$dimensional cube $[0,1)^s$. So, let $b \geq 2$ be a fixed integer what is the base in which the considered sequences and nets are constructed. In the following, we give the definition of a $(t,m,s)-$net and a $(t,s)-$sequence.

Definition 1. *Let t and m $(0 \leq t \leq m)$ be given integers. A point set P consisting of b^m points in $[0,1)^s$ is called a $(t,m,s)-$net in base b, if every subinterval $J = \prod_{j=1}^{s} \left[\frac{a_j}{b^{d_j}}, \frac{a_j+1}{b^{d_j}}\right)$ has a volume b^{t-m} and contains exactly b^t points of P, where $d_j \geq 0$ and $0 \leq a_j < b^{d_j}$ are integers for $1 \leq j \leq s$.*

Definition 2. *Let $t \geq 0$ be a given integer. The sequence $(\mathbf{x}_n)_{n \geq 0}$ of points in $[0,1)^s$ is called a $(t,s)-$sequence in base b if for all $l \geq 0$ and $m \geq t$, the point set*

$$\{\mathbf{x}_{lb^m}, \ldots, \mathbf{x}_{(l+1)b^m-1}\}$$

is a $(t,m,s)-$net.

We denote that a $(t,m,s)-$net is extremely well distributed if the parameter t is small.

We will give some notations and statements about the linear homogeneous recurrence relations and primitive polynomials over the field $\mathbb{F}_b$.

Let $i \in \mathbb{Z}$, and $u_i \in \mathbb{F}_b$ for $0 \leq i \leq m-1$, $a_i \in \mathbb{F}_b$, $a_0 \neq 0$. A relation of the form

$$Lu_i = u_{i+m} + a_{m-1}u_{i+m-1} + \ldots + a_1u_{i+1} + a_0u_i \qquad (1)$$

is called linear homogeneous recurrence relation over $\mathbb{F}_b$ of order m with constant coefficients (LHRR). A solution of the equation

$$Lu_i = 0$$

is a sequence $\{u_i\} = \{\ldots u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots\}$ whose elements are from $\mathbb{F}_b$ and they satisfy previous equation for all integer i. The solutions of the equation $Lu_i = 0$ have cyclic character. It is easy to show that the solution $\{u_i\}$ is periodical with a period ω such that $\omega \leq b^m - 1$.

The relation Lu_i is called monocyclic if the equation $Lu_i = 0$ has only one solution with period $\omega = b^m - 1$.

For every LHRR (1), there exists a unique polynomial of degree m over $\mathbb{F}_b$ of the form

$$Lu_i \leftrightarrow P(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0, \qquad (2)$$

where for $i = 0, 1, \ldots m-1$, $a_i \in \mathbb{F}_b$.

An irreducible polynomial is a non-constant polynomial that cannot be factorized into the product of two non-constant polynomials. Lidl and Niederreiter in [7] give the following definitions and results: It is well known that to a monocyclic relation of the form (1) corresponds an irreducible polynomial. In other side, this condition is not sufficient. Zierler ([10]) proved that the condition "the polynomial (2) is primitive" is the necessary and sufficient condition for monocyclicality of relation (1). A polynomial is primitive if it is irreducible, a divisor of the binomial $x^\omega - 1$ (ω is the period of the corresponding monocyclic relation), and it is not a divisor of a binomial $x^q - 1$ of degree $q < \omega$.

Following Sobol' [9] and our paper[2] we will recall the theoretical bases of the construction of sequences of $b-$adic rational type, so-called $BR-$ sequences. So, the details are as follows: Let $\{V_j\}_{j\geq 1} = \{V_1, V_2, \dots, V_j, \dots, \}$ be an arbitrary sequence of $b-$adic rational numbers such that for $j \geq 1$ we have that $0 < V_j < 1$. The numbers of this sequence we will call direction numbers.

Definition 3. *A $BR-$ sequence $\{r(i)\}_{i\geq 0}$ which corresponds to the direction numbers $\{V_j\}_{j\geq 1}$ is defined as: if an arbitrary integer number i has the $b-$adic presentation*

$$i = e_m e_{m-1} \dots e_2 e_1,$$

then we replace

$$r(i) = e_1 V_1 * e_2 V_2 * \dots * e_m V_m,$$

*where * is the operation digit-by-digit summation modulo b and we have that* $e_j V_j = \underbrace{V_j * \dots * V_j}_{e_j - times}$.

We can represent the direction numbers V_j in the form of $b-$ adic fractions:

$$V_j = 0, v_{j1} v_{j2} \dots v_{ji} \dots, \tag{3}$$

where all $v_{ji} \in \mathbb{F}_b$. In this sense the setting of the sequence $\{V_s\}$ is equivalent to setting an infinite matrix (v_{ji}) with elements from the field $\mathbb{F}_b$, so let us signify

$$(v_{ji}) = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1i} & \dots \\ v_{21} & v_{22} & \dots & v_{2i} & \dots \\ \dots & \dots & \dots & \dots & \dots \\ v_{j1} & v_{j2} & \dots & v_{ji} & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix}.$$

This matrix is called direction matrix. By using results of the paper ([2]) the following statement holds:

Let Lu_i be an arbitrary monocyclic LHRR over the field $\mathbb{F}_b$ of order m. We generate the direction numbers $V_1, V_2, \dots, V_i, \dots$ as a solution of the equation

$$V_{i+m} * a_{m-1} V_{i+m-1} * \dots * a_1 V_{i+1} * a_0 V_i = b^{-m} V_i, \tag{4}$$

i.e., $LV_i = b^{-m} V_i$, obtained by replacing of symbol $+$ with operation $*$ in the relation Lu_i. The initial conditions $V_1, V_2, \dots, V_m$ of the equation (4) can be chosen in different manners, but for our purposes it is necessary to satisfy the next conditions: we assume that $v_{jj} \neq 0$ for all $j \geq 1$ in the $b-$adic presentation of the number V_j of the form (3) and $v_{ji} = 0$ for $i > j$. In this way the matrix

$$(v_{ji}) = \begin{bmatrix} v_{11} & 0 & \dots & 0 \\ v_{21} & v_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ v_{m1} & v_{m2} & \dots & v_{mm} \end{bmatrix}$$

is triangular and nonsingular. On the main diagonal there are nonzero numbers and all the entries above the main diagonal are zero.

In the next theorem given in [2], we show the possibility to use monocyclic LHRR as a tool to construct $(t, s)-$sequences.

Theorem 1. *Let b be a prime number and $L_1, L_2, \ldots, L_s$ be different monocyclic LHRR of orders $m_1, m_2, \ldots, m_s$ over $\mathbb{F}_b$. For $k = 1, 2, \ldots, s$, let $(P^{(k)}(i))_{i\geq 0}$ be the BR$-$ sequence which corresponds to the relation L_k. Then the sequence $(P(i))_{i\geq 0}$ of points of the form*

$$P(i) = (P^{(1)}(i), P^{(2)}(i), \ldots, P^{(s)}(i))$$

is a $(t, s)-$ sequence in base b with a parameter $t = \sum_{k=1}^{s}(m_k - 1)$.

3 Generalization of binary Gray code and other useful results

In the next formula we give the so-called $b-$adic Gray code in the case when b is an arbitrary prime number. For an arbitrary integer number i we define $b-$adic Gray code with

$$G(i) = i * (b - 1) \cdot [i/b], \tag{5}$$

where * is the operation digit-by-digit summation modulo b and $[\frac{i}{b}]$ means the integer part of the number $\dfrac{i}{b}$.

For the Gray code, it is essential to note the fact that Gray codewords $G(i)$ and $G(i-1)$ of two successive integers i and $i-1$, are different only in one digit, which position we will denote by l. Our investigations show that this difference is equal to 1 and the position l is the lowest nonzero position in the $b-$adic presentation of i.

On Table 1, we present Generalized Gray codes, for base $b = 7$, for some numbers n.

Let $Q_0, Q_1, \ldots$ be an arbitrary $s-$ dimensional $(t, s)-$ sequence in base b. Using (5), let us construct a new sequence $Q_0^{'}, Q_1^{'}, \ldots$ where $Q_i^{'} = Q_{G(i)}$. For an arbitrary integer i with the $b-$adic presentation $i = e_m e_{m-1} \ldots e_2 e_1$, we set

$$Q_i = e_1 V^{(1)} * \ldots * e_m V^{(m)},$$

where direction numbers $V^{(j)}, j = 1, 2, \ldots$ are defined in [2].

For an arbitrary $b-$adic digit $a \in \mathbb{F}_b$ we use the signification

$$\overline{a} = \begin{cases} 0, & a = 0 \\ b - a, & a \neq 0 \end{cases}$$

For an arbitrary integer i with the $b-$adic presentation $i = e_m e_{m-1} \ldots e_2 e_1$ we will use the notation

$$\overline{i} = \overline{e}_m \overline{e}_{m-1} \ldots \overline{e}_1.$$

Table 1. Generalized Gray code, base $b = 7$, for some numbers n

n$_{10}$	n_7	Gray code(n)	(Gray code(n))$_{10}$
51	102	162	93
52	103	163	94
53	104	164	95
54	105	165	96
55	106	166	97
56	110	106	55
57	111	100	49
58	112	101	50
59	113	102	51
60	114	103	52

From the previous analysis it is obvious that

$$Q_i^{'} * Q_{\overline{i-1}}^{'} = Q_{G(i)} * Q_{\overline{G(i-1)}} = V^{(l)},$$

where l is the lowest nonzero position in the $b-$adic presentation of i. It implies that

$$Q_i^{'} = Q_{i-1}^{'} * V^{(l)},$$

i.e., if the coordinates of the point $Q_i^{'}$ are $(q_{i,1}^{'}, \ldots, q_{i,s}^{'})$ then

$$q_{i,j}^{'} = q_{i-1,j}^{'} * V_j^{(l)}, i = 1, 2, \ldots, j = 1, 2, \ldots s, \tag{6}$$

with initial condition that $q_{0,j}^{'} = 0, j = 1, 2, \ldots s$.

4 Algorithm

According to (5), results in previous section and exposed algorithms in [2] and [3], in this paper we propose a new algorithm for construction of sequences in base b, where b is an arbitrary prime. The steps of the algorithm are:

1. **For an arbitrary integer i, find the $b-$adic presentation**

   $$i = e_m e_{m-1} \ldots e_2 e_1,$$

   and then compute number l as the lowest nonzero position in the previous formula.
2. **Compute direction vectors $V^{(l)}$ using algorithm in [2].**
3. **Compute coordinates of the new point $Q_i^{'}$ given by (6).**

In order to visualize the $(t, s)-$ sequences constructed by the proposed algorithm, a computer program is written. The output of this program is one s-dimensional $(t, m, s)-$ net, where b is an arbitrary prime.

5 Results from the software simulations and visualizations

In the following we present some results of this program for different dimensions s and different bases b, where N is the number of points of the net.

In Table 2, we present the times (in seconds) for generation of $(t, m, s)-$ net in base b, for the generalized Sobol's algorithm and for the new algorithm proposed here. It is obvious that the new proposed algorithm is faster than the our old generalized Sobol's algorithm.

On the next two figures there are visualized some obtained results by the new proposed algorithm.

Table 2. Comparison between the times (in seconds) for the generalized Sobol's algorithm and the new algorithm

Base b	Expon. ν	Number N	Dimension s	Generalized Sobol's alg.	New alg.
19	3	6,859	2	0.59	0.46
7	5	16,807	3	5.1	3.5
2	15	32,768	1	7.7	2.2
13	4	28,561	3	9.6	6.4
19	4	130,321	2	14.6	9.4
17	4	83,521	3	24.2	17.7
7	6	117,649	2	33.1	10.1
23	4	279,841	3	70.8	53.6

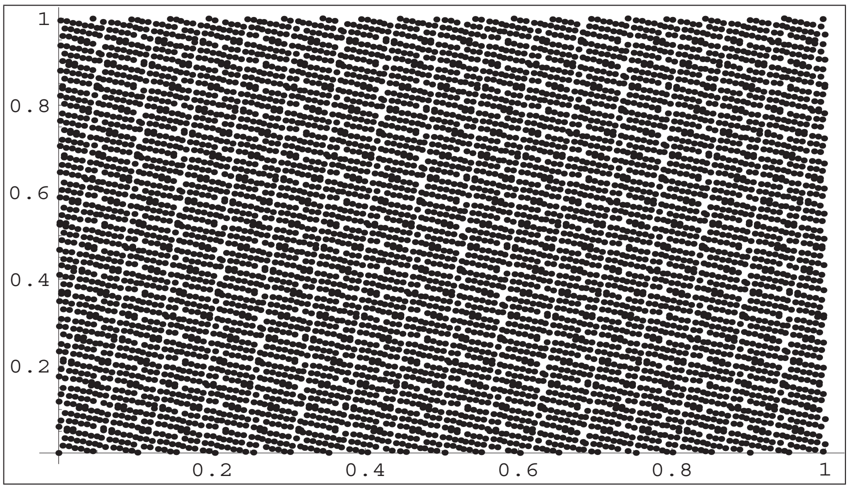

Fig. 1. Visualization: $s = 2$, $N = 6859$, $b = 19$

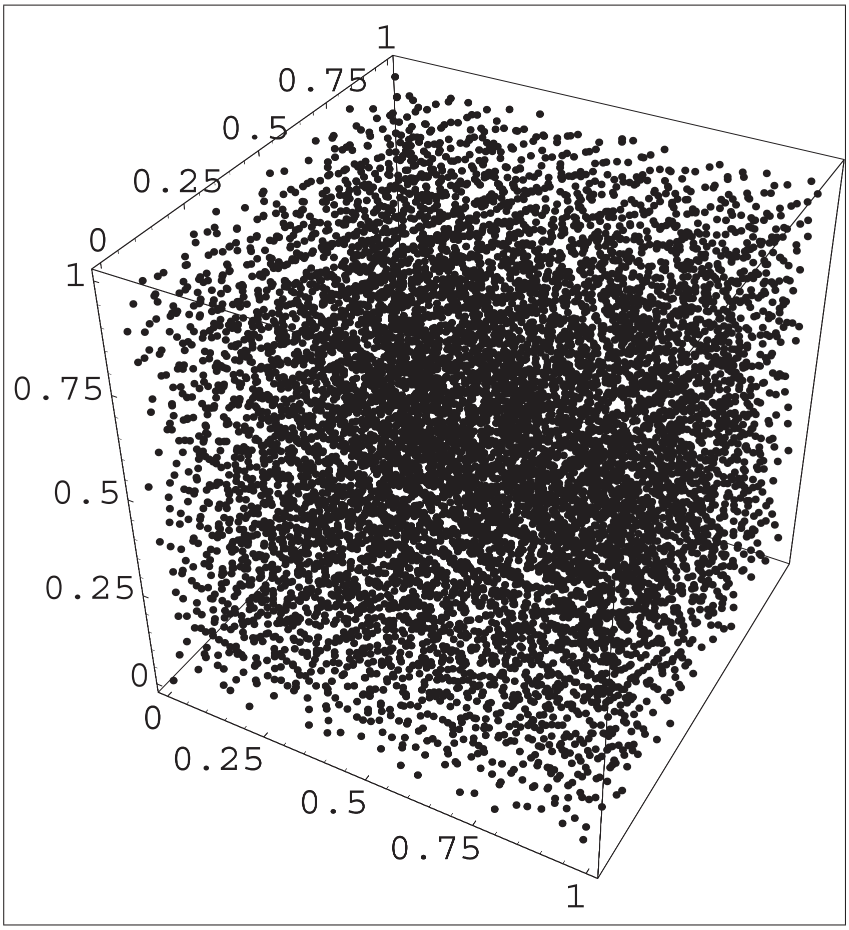

Fig. 2. Visualization: $s = 3$, $N = 16807$, $b = 7$

6 Conclusion

Obtained experimental results and their visualizations have verified our expectations that this new algorithm will produced well distrubuted $(t, s)-$ sequences over $\mathbb{F}_b$ for shorter time than our prevoius algorithm proposed in [3].

The next step will be to give mathematical proof for correctness of the proposed algorithm. We will stress the fact that this algorithm (for constructing of $(t, s)-$ sequences over $\mathbb{F}_b$), can be applied for construction of some classes of pseudo- random number generators.

References

1. Antonov, I.A., Saleev, V.M.: An economic method of computing $\Lambda\Pi_\tau-$ sequences, USSR Computational Mathematics and Mathematical Physics, 19 (1), 243–245 (1979) (in Russian),
2. Dimitrievska Ristovska, V., Grozdanov,V., Atanasov, A.: An effective algorithm for constructing of $(t, s)-$sequences over $\mathbb{F}_b$, Proceedings of the V Congress of CMM, Ohrid, (2014) (in print)
3. Dimitrievska Ristovska, V., Grozdanov,V.: Primitive polynomials as a tool in generation of $(t, s)-$ sequences, CIIT, Bitola, (2015) (in print)
4. Faure, H.:Discrépance de suites associées à un systeme de numeration (en dimension s), Acta Arithmetica, XLI, 337–351 (1982)
5. Faure, H. Variation on $(0, s)-$sequences, Journal of Complexity, 17, 741–753 (2001)
6. Kuipers,L., Niederreiter, H.: Uniform distribution of sequences, John Wiley & Sons, New York (1974)
7. Lidl, L., Niederreiter, H.: Introduction to finite fields and their applications, Cambridge University Press, New York, USA (1986)
8. Niederreiter, H. Random Number Generator and Quasi-Monte Carlo Methods, CBMS - NSF Series in Applied Mathematics, 63, SIAM, Philadelphia (1992)
9. Sobol, I.M.: Multidimensional Quadrature Formulas and Haar Functions, Nauka, Moscow (1969), (in Russian)
10. Zierler, N.: Linear recurring sequences, J. Soc. Industr. Appl. Math., 7 (1), 31–48 (1959)