DE GRUYTER
OPEN

uniform
distribution
theory

DOI: 10.1515/udt-2018–0006
Unif. Distrib. Theory **13** (2018), no.1, 109–129

# CONSTRUCTION OF UNIFORMLY DISTRIBUTED LINEAR RECURRING SEQUENCES MODULO POWERS OF 2

Tamás Herendi

ABSTRACT. The aim of the present paper is to provide the background to construct linear recurring sequences with uniform distribution modulo $2^s$. The theory is developed and an algorithm based on the achieved results is given. The constructed sequences may have arbitrary large period length depending only on the computational power of the used machines.

*Communicated by Katalin Gyarmati*

## 1. Introduction

Pseudo random numbers play an essential role in many applications. The traditional ones were simulations, Monte-Carlo methods [13] and coding, while recently cryptography is one of the main utilization area. Inside cryptography it is mainly used for key generation, in stream ciphers [11], asymmetric cryptosystems, zero-knowledge proofs, and in particular applications, such as authentication protocols [3], secure elections [5] and electronic exam schemes [6]. There is number of ways to produce sequences of pseudo random numbers see, e.g., [7], [9] and [2]. In [10] one can find a general construction for pseudo random numbers.

Depending on the application, there are several expectations for pseudo random number sequences. One of the most important requirements is the given or at least known distribution property. For general applications, the uniform distribution is the most acceptable. Another important attributes are low autocorrelation, wide range of the values for the sequence, fast computability, long

2010 Mathematics Subject Classification: 11B37, 11B50.
Keywords: uniform distribution, construction, long period, large numbers.
The publication is supported by the EFOP-3.6.1–16–2016–00022 project. The project is co-financed by the European Union and the European Social Fund.

period—or no periodicity at all, but this seems practically impossible—and unpredictability. To use linear recurring sequences as base objects for pseudo random number sequences is not a new idea (see, e.g., [7]), but in most of the cases, the obtained results has some insufficiency. In the following we provide the theoretical background for the construction of uniformly distributed linear recurring sequences. The presented design allows us to create sequences with rather (theoretically arbitrary) large period length —no difficulty to reach $2^{1000}$—basically without correlation between the members close to each other. (The distance can vary, but 1000 can be settled easily.) The numbers in the sequence can be not only 0 or 1, but arbitrary large and the computation of a new element requires only some addition. Unfortunately, the unpredictability of the forthcoming elements does not hold at all, because of the basic properties of linear recurring sequences.

At the end of the paper an example for construction of a sequence based on the presented theory is given.

We may summarize our results in the following

**Theorem.** *Let $Q \in \mathbb{Z}[x]$ be monic of degree $k$ such that its reduction modulo 2 is irreducible and let $P \in \mathbb{Z}[x]$ be monic satisfying*

$$P(x) \equiv (x^2 - 1)Q(x) \bmod 2.$$

*Let us define*

$$\begin{aligned} P_1(x) &= P(x), \\ P_2(x) &= P(x) - 2, \\ P_3(x) &= P(x) - 2x, \\ P_4(x) &= P(x) - 2x - 2 \end{aligned}$$

*and let $u^{(i)}$ be linear recurring sequences corresponding to $P_i$, such that the minimal period length of $u^{(i)}$ modulo 2 is $2\mathrm{ord}(Q)$, where $\mathrm{ord}(Q)$ is the order of $Q$ in $\mathbb{F}_2[x]$. Then at least one of the $u^{(i)}$'s is uniformly distributed modulo $2^s$ with period length $2^s\mathrm{ord}(Q)$ for any $s \in \mathbb{N}$.*

## 2. Definitions and preliminary results

**Definition 1.** Let $R$ be a Dedekind-domain and let $a_0, \ldots, a_{d-1} \in R$ and

$$u = \{u_n\}_{n=0}^{\infty}$$

be a sequence in $R$ satisfying the **recurrence relation**

$$u_{n+d} = a_{d-1}u_{n+d-1} + \cdots + a_0u_n \quad \text{for} \quad n = 0, 1, \ldots$$

Then $u$ is called a **linear recurring sequence** (for short **l.r.s.**) with **defining coefficients** $a_0, \dots, a_{d-1}$ and **initial values** $u_0, \dots, u_{d-1}$.

The integer $d$ is called the **order** of the recurrence and the polynomial

$$P(x) = x^d - a_{d-1}x^{d-1} - \cdots - a_0$$

is called a **characteristic polynomial** of $u$.

**Definition 2.** Let $u$ be an l.r.s. in the Dedekind-domain $R$, defined by the coefficients $a_0, \dots, a_{d-1}$ with initial values $u_0, \dots, u_{d-1}$. Then

$$\bar{u}_n(k) = (u_n, \dots, u_{n+k-2}, u_{n+k-1})^{tr}$$

denotes the $n$th $k$**-dimensional state vector** and

$$M(u) = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ a_0 & a_1 & \dots & a_{d-2} & a_{d-1} \end{pmatrix}$$

the **companion matrix** of $u$.

Since it causes no misunderstanding, we will omit the transpose sign from the state vector definitions.

**Remark 3.** With the above notations we have

$$\bar{u}_n(d) = M(u)^n \bar{u}_0(d).$$

**Definition 4.** Let $u$ be a sequence in the Dedekind-domain $R$ and let $I \subseteq R$ be an ideal. We say that $u$ is **periodic** modulo $I$ with **period length** $\varrho \in \mathbb{N}$, if there exists $\varrho_0 \in \mathbb{N}$, such that

$$u_{n+\varrho} \equiv u_n \bmod I \quad \text{for all} \quad n \geq \varrho_0.$$

The smallest $\varrho_0 = \varrho_{0,I}(u)$ and $\varrho = \varrho_I(u)$ with the previous property will be called the **preperiod** and **minimal period length** of $u$ modulo $I$, respectively.

If $\varrho_{0,I}(u) = 0$, then $u$ is said to be **purely periodic** modulo $I$.

**Remark 5.** Let $R$ be a Dedekind-domain, let $u$ be a linear recurring sequence in $R$ and let $I \subseteq R$ be an ideal with finite norm. A simple observation shows that $u$ is periodic modulo $I$.

**Definition 6.** Let $u$ be a sequence in the Dedekind-domain $R$ and let $I \subseteq R$ be an ideal with finite norm. We will say that $u$ is **uniformly distributed** (for short u.d.) modulo $I$ if

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \leq N | u_n \equiv a \bmod I\} = \frac{1}{\mathrm{Norm}(I)} \quad \text{for all } \ a \in R.$$

**Remark 7.** One can find criteria for the uniform distribution of linear recurring sequences of order $\leq 4$ over finite fields in [14] and [15].

Among other general results, criteria for the uniform distribution of linear recurring sequences of order $\leq 3$ over Dedekind-domains can be found in [17] and [16].

As a starting point we have to construct uniformly distributed recurring sequences over simpler structures. N i e d e r r e i t e r and S h i u e in [14] give a necessary condition on uniform distribution of linear recurring sequences over finite fields:

**Proposition 8.** *Let $\mathbb{F}$ be a finite field and let $u$ be an* l.r.s. over $\mathbb{F}$. If $u$ is uniformly distributed, the characteristic polynomial of $u$ has a multiple factor.

P r o o f. See, e.g., [14]. □

**Example 9.** Let us define the sequence $u$ by the following:

$$u_0 = 0, \quad u_1 = 1 \quad \text{and} \quad u_n = u_{n-2} \quad \text{for} \ \ n \geq 2.$$

Clearly, the sequence is uniformly distributed modulo 2. The characteristic polynomial of $u$ is

$$P(x) = x^2 - 1 \equiv (x+1)^2 \bmod 2.$$

**Example 10.** Define the sequence $u$ by the following:

$$u_0 = 0, \quad u_1 = 1 \quad \text{and} \quad u_n = u_{n-1} + u_{n-2} \quad \text{for} \quad n \geq 2.$$

The sequence $u$ is the well-known Fibonacci sequence. In [12] it is proven that $u$ is uniformly distributed modulo 5. Actually, even more proven there: $u$ is uniformly distributed modulo $m$ if and only if $m$ is a power of 5.

The characteristic polynomial of $u$ is

$$P(x) = x^2 - x - 1 \equiv (x+2)^2 \bmod 5.$$

Now, we turn to the known and the new results we use for finding linear recurring sequences with uniform distribution modulo some—in particular $2^k$–
–integer. The idea behind the construction is trying to find a linear recurring sequence with a characteristic polynomial having the property

$$P(x) \equiv (x+1)^2 Q(x) \bmod 2,$$

where $Q(x)$ is irreducible modulo 2 and has a particular degree. In this way we can find a linear recurring sequence with a large period length, which has some advantages for the later steps.

**Definition 11.** Let $\mathbb{F}$ be a finite field and $P \in \mathbb{F}[x]$ with the condition $P(0) \neq 0$. We will call $ord(P) = e$ the **order** of $P$, where $e$ is the smallest positive integer, such that $P(x) \mid x^e - 1$ over $\mathbb{F}[x]$.

**Remark 12.** The integer $e$ in the above definition always exists. See, e.g., in [8]

**Proposition 13.** *Let $\mathbb{F}$ be a finite field with $q$ elements and let $Q(x)$ be an irreducible polynomial of degree $k$ over $\mathbb{F}$. Then the order of $Q$ divides $q^k - 1$.*

Proof. See, e.g., Corollary 3.4 of [8]. □

**Proposition 14.** *Let $\mathbb{F}$ be a finite field of characteristic $p$, let $P \in \mathbb{F}[x]$ be a polynomial of positive degree with $P(0) \neq 0$ and let $P = aP_1^{b_1} \dots P_r^{b_r}$, where $a \in \mathbb{F}$ and $P_1, \dots, P_r$ are distinct monic irreducible polynomials.*

*If $e$ denotes the least common multiple of $\operatorname{ord}(P_1), \dots, \operatorname{ord}(P_r)$ and $t$ denotes the smallest integer, such that $p^t \geq \max\{b_1, \dots, b_r\}$, then $\operatorname{ord}(P) = ep^t$.*

Proof. See, e.g., Theorem 3.11 of [8]. □

We can use the above result to determine the order of polynomials in the required form.

**Corollary 15.** *Let $P(x), R(x) \in \mathbb{Z}[x]$ be such that*

$$P(x) \equiv (x+1)^2 Q(x) \bmod 2$$

*and*

$$R(x) \equiv (x+1) Q(x) \bmod 2,$$

*where $Q(x)$ is irreducible modulo 2.*

*Then for the orders of the polynomials over $\mathbb{F}_2$ we have*

$$\operatorname{ord}(P) = 2\operatorname{ord}(Q)$$

*and*

$$\operatorname{ord}(R) = \operatorname{ord}(Q).$$

**Definition 16.** Let $u$ be an l.r.s. of order $d$ over a Dedekind-domain $R$. We say that $u$ is an **impulse response sequence** if

$$u_0 = \dots = u_{d-2} = 0 \quad \text{and} \quad u_{d-1} = 1.$$

The following proposition shows the distinguished role of the impulse response sequence corresponding to a given recurrence relation.

**Proposition 17.** *Let $\mathbb{F}$ be a finite field and let $u$ be the impulse response sequence over $\mathbb{F}$ with characteristic polynomial $P(x)$. Then the minimal period length of $u$ is equal to $ord(P)$.*

Proof. See, e.g., Theorem 6.27. of [8]. □

**Definition 18.** Let $m > 1$ be an integer, let $u_n$ be a sequence of integers and let $u'_n \in \{0, \dots, m-1\}$ be such that

$$u'_n \equiv u_n \bmod m.$$

The sequence $u'$ is called the **reduced sequence** of $u$ mod $m$.

The following lemma assures the possibility to construct linear recurring sequences with large period lengths.

**Lemma 19.** *Let $Q(x) \in \mathbb{Z}[x]$ be monic of degree $k$ such that its reduction modulo 2 is irreducible in $\mathbb{F}_2[x]$. Let $u$ be the impulse response sequence corresponding to the characteristic polynomial $P(x) \equiv (x^2-1)Q(x) \bmod 2$. Then $u'$ — the reduced sequence of $u$ modulo 2 — has period length $2\varrho$ with some $\varrho$, such that $\varrho \mid 2^k - 1$.*

Proof. Let $\varrho = ord(Q)$. By Proposition 13, $\varrho \mid 2^k - 1$. The factorization of $P$ is $P \equiv (x+1)^2 Q(x) \bmod 2$, whence by Corollary 15,

$$\operatorname{ord}(P) = 2\operatorname{ord}(Q) = 2\varrho.$$

Hence by Proposition 17, the lemma follows. □

**Lemma 20.** *Let $Q(x) \in \mathbb{Z}[x]$, such that $2 \nmid Q(1)$ and let $u$ be an* l.r.s. of integers with characteristic polynomial

$$P(x) \equiv (x^2-1)Q(x) \bmod 2,$$

let $v$ be the sequence given by

$$v_n = u_n + 1 \qquad \text{for all } \ n \geq 0$$

and let $v'$ denote the modulo 2 reduced sequence of $v$. Then $v'$ modulo 2 satisfies the recurrence relation corresponding to $P$.

Proof. The polynomial $P$ is a characteristic polynomial of the sequence $w$ modulo 2, where $w_n = 1$ for all $n \geq 0$, whence by the additive property of linear recurring sequences, the lemma follows. □

**Remark 21.** The above lemma is proven in more general settings in Theorem 6.62 of [8].

**Definition 22.** Let $\mathbb{F}$ be a finite field with $q$ elements and let $u$ and $v$ be two linear recurring sequences of order $d$ with the same characteristic polynomial $P$. Suppose that $P(0) \neq 0$. We will say that $u$ and $v$ are **equivalent**, if there exists $N \in \mathbb{N}$, such that

$$u_n = v_{n+N} \quad \text{for all } \ n \in \mathbb{N}$$

or

$$u_{n+N} = v_n \quad \text{for all } \ n \in \mathbb{N}.$$

**Remark 23.** The following properties are easy to prove. Let $\mathbb{F}$ be a finite field with $q$ elements and let $P \in F[x]$ be a polynomial of degree $d$. Suppose that $P(0) \neq 0$. Then:

i) we have $q^d$ different linear recurring sequences having characteristic polynomial $P$, and they can be divided into equivalence classes by the above defined equivalence relation, such that

ii) in every equivalence class, the sequences have the same minimal period length

iii) the cardinality of the equivalence classes are equal to its elements' common minimal period length

iv) the sequences from the same equivalence classes have periods differing only in cyclic permutations.

**Lemma 24.** *Let $Q(x) \in \mathbb{Z}[x]$ be monic irreducible modulo 2 of degree $k$ and let*

$$P(x) \equiv (x+1)^2 Q(x) \bmod 2.$$

*Let $u$ be a sequence having characteristic polynomial $P$ and minimal period length modulo 2 equal to $\mathrm{ord}(P)$. Then $u$ is uniformly distributed modulo 2.*

P r o o f. Let denote by $L$ the set of different linear recurring sequences having characteristic polynomial $P$ modulo 2. We will consider two linear recurring sequences the same modulo 2 (notation: $w \equiv v \bmod 2$) if their reduced sequences are the same.

By (i) of Remark 23, $\#(L) = 2^{k+2}$.

We will use the fact that if $Q$ is a characteristic polynomial of an l.r.s., then $Q \cdot Q'$ is a characteristic polynomial of it, too, for all $Q'$ non-zero monic polynomials. We can partition $L = L_1 \cup L_2$, such that $\#(L_1) = \#(L_2) = 2^{k+1}$ by the following: an l.r.s. is in $L_1$ if it satisfies the recurrence relation corresponding to the characteristic polynomial $(x+1)Q(x) \bmod 2$ and it is in $L_2$, otherwise. The definition implies that $L_1$ is closed for the addition of sequences.

Let $e$ denote the impulse response sequence corresponding to the characteristic polynomial $P$, i.e., the sequence in $L$, satisfying the initial condition $e_0 = e_1 = \cdots$ $\cdots = e_k = 0$ and $e_{k+1} = 1$. Furthermore, let $\varphi : L \to L$ be the function defined by $\varphi(w) = w + e$. Clearly, $\varphi$ is injective, $\varphi^2 = Id$ and $w + \varphi(w) \equiv e \bmod 2$ for any $w \in L$. Since $e \notin L_1$ thus $w$ and $\varphi(w)$ cannot be in $L_1$ simultaneously. The cardinalities of $L_1$ and $L_2$ are equal, whence $\varphi(L_1) = L_2$, i.e., $\varphi$ is a bijection between $L_1$ and $L_2$.

Obviously, for any two sequences $v, w \in L$,

$$w + v \equiv \varphi(w) + \varphi(v) \bmod 2.$$

Further, if $w, v \in L_2$, then $\varphi(w), \varphi(v) \in L_1$, whence $w + v \in L_1$.

Let $v$ be an l.r.s. We will use the notation $\bar{v}_n = (v_n, \dots, v_{n+k+1})$ for the $k+2$ dimensional state vector of $v$.

Let $\varrho = \operatorname{ord}(Q)$. Then by Corollary 15, $\operatorname{ord}((x+1)Q) = \varrho$ and $\operatorname{ord}(P) = 2\varrho$.

By the definition of $u$ we know that $u \in L_2$, in other words,

$$\bar{u}_0 \equiv \bar{u}_{2\varrho} \bmod 2$$

and

$$\bar{u}_0 \not\equiv \bar{u}_{\varrho} \bmod 2.$$

Let $w \in L$ be the sequence for which

$$\bar{w}_0 \equiv \bar{u}_{\varrho} - \bar{u}_0 \bmod 2.$$

Clearly,

$$\bar{u}_{n+\varrho} \equiv \bar{u}_n + \bar{w}_n \bmod 2 \qquad \text{for all } \ n \in \mathbb{N}.$$

Let $v \in L$ be the sequence for which

$$\bar{v}_0 \equiv \bar{u}_1 \bmod 2.$$

Since $u, v \in L_2$, thus

$$u + v \in L_1 \quad \text{and} \quad \bar{u}_{\varrho} + \bar{v}_{\varrho} \equiv \bar{u}_0 + \bar{v}_0 \bmod 2,$$

i.e.,

$$\bar{u}_{\varrho} + \bar{u}_{\varrho+1} \equiv \bar{u}_0 + \bar{u}_1 \bmod 2.$$

This implies

$$\bar{u}_0 + \bar{w}_0 + \bar{u}_1 + \bar{w}_1 \equiv \bar{u}_0 + \bar{u}_1 \bmod 2,$$

i.e.,

$$\bar{w}_0 \equiv \bar{w}_1 \bmod 2.$$

Since $w \not\equiv 0 \bmod 2$, this yields

$$w_n \equiv 1 \bmod 2 \qquad \text{for all } \ n \in \mathbb{N}.$$

Consequently,

$$u_n \equiv u_{n+\varrho} + 1 \bmod 2 \qquad \text{for all } \ n \in \mathbb{N}. \tag{1}$$

However, this means that the number of 0s among the first $\varrho$ elements of the sequence is equal to the number of 1s among the second $\varrho$ elements of the sequence and vice versa. Then the number of 0s and 1s has to be the same in a period, which means that $u$ is uniformly distributed modulo 2. □

**Remark 25.** Although the statement of the lemma is proven in more general settings in [14], some details of the present proof are used later in the paper.

**Lemma 26.** *Let $u$ be a linear recurring sequence in $\mathbb{Z}$ with characteristic polynomial $P$, let $p$ be a prime, let $s > 0$ integer and let $\varrho_1$ and $\varrho_2$ the minimal period length of $u$ modulo $p^s$ and $p^{s+1}$ respectively. If $P$ is minimal characteristic polynomial of $u$ modulo $p$, then either $\varrho_2 = \varrho_1$ or $\varrho_2 = p\varrho_1$.*

P r o o f. The lemma is a particular case of Lemma 13 of [4]. With the given conditions on $P$, $T(u) = 1$. Here $T(u)$ denotes the smallest exponent, such that the sequence has fixed minimal order modulo $p^s$ for any $T(u) \leq s$. Since in our case $P$ is minimal characteristic polynomial modulo $p$, thus the minimal order of the sequence is $\deg(P)$ modulo $p^s$, for any $s$. □

**Remark 27.** Minimal characteristic polynomials expresses minimal degree.

The conditions of the lemma on $P$ are fulfilled, for instance, when $u$ is the impulse response sequence and $P(0) \not\equiv 0 \bmod p$.

## 3. Proof of the main result

**P r o o f o f t h e T h e o r e m**. Simplifying the proof, we suppose, that

$$\bar{u}_0^{(1)} = \bar{u}_0^{(2)} = \bar{u}_0^{(3)} = \bar{u}_0^{(4)},$$

where $\bar{u}_n$ is the state vector of $u_n$. In the proof we will use the notation $\varrho = \operatorname{ord}(Q)$ and $M_{(i)}$ for the companion matrix. Furthermore, in any case we will use upper or lower index $(i)$ with the different symbols corresponding to the proper sequence for $i = 1, 2, 3, 4$. For short, we will write $u = u^{(1)}$. For the convenient reference and better overview, we will enumerate the parts of the proof.

**(i)** Let us calculate

$$\bar{u}_{2\varrho+n} - \bar{u}_n = M^{2\varrho}\bar{u}_n - \bar{u}_n = (M^{2\varrho} - E)\bar{u}_n = (M^{\varrho} + E)(M^{\varrho} - E)\bar{u}_n\,, \qquad (2)$$

where $M$ is the companion matrix of $u$ and $E$ is the unit matrix of the same dimension. As we have seen in the proof of Lemma 24, by (1) we know, that

$$(M^{\varrho} - E)\bar{u}_n = \bar{1} + 2\bar{y}_n\,,$$

with some $\bar{y}_n$. Here $\bar{1}$ yields the $k+2$ dimensional $(1, 1, \ldots, 1)$ vector. One should remark, that the equation $\bar{y}_{n+1} = M\bar{y}_n$ not necessarily holds.

**(ii)** For the further calculations, examine first the behaviour of $M^{\varrho}\bar{1}$. Since the sequence $1, 1, 1\ldots$ satisfies the recurrence relation with characteristic polynomial $x-1$ and $x-1$ divides $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ modulo 2, thus $1, 1, 1\ldots$ also satisfies the recurrence relations with characteristic polynomials $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ modulo 2. Consequently,

$$M\bar{1} = \bar{1} + 2\bar{v} \quad \text{and} \quad M^{\varrho}\bar{1} = \bar{1} + 2\bar{z}, \quad \text{with some} \quad \bar{v} \quad \text{and} \quad \bar{z}.$$

Clearly, either $\bar{v} \equiv \bar{0} \bmod 2$ or $\bar{v} \equiv (0, 0, \ldots, 0, 1) \bmod 2$. We will use the notation $\bar{e} = (0, 0, \ldots, 0, 1) = \bar{u}_0$. In the first case, $\bar{z} \equiv \bar{0} \bmod 2$ should hold, too.

In the second case,

$$M^{\varrho+1}\bar{1} = M^{\varrho}(\bar{1}+2\bar{v}) = \bar{1}+2\bar{z}+2M^{\varrho}\bar{v} \equiv \bar{1}+2\bar{z}+2M^{\varrho}\bar{u}_0$$
$$= \bar{1}+2\bar{z}+2(\bar{1}+\bar{e}+2\bar{y}_0) \equiv \bar{1}+2(\bar{z}+\bar{1}+\bar{e}) \bmod 4.$$

From the other side,

$$M^{\varrho+1}\bar{1} = M(\bar{1}+2\bar{z}) = \bar{1}+2\bar{v}+2M\bar{z} \equiv \bar{1}+2\bar{e}+2M\bar{z} \bmod 4.$$

Hence,

$$\bar{1}+2(\bar{z}+\bar{1}+\bar{e}) \equiv \bar{1}+2\bar{e}+2M\bar{z} \bmod 4,$$

which is equivalent to

$$\bar{z}+\bar{1} \equiv M\bar{z} \bmod 2.$$

Let $\bar{z} = (z_1, z_2, \dots, z_{k+2})$. Then the above congruence means

$$\bar{z}+\bar{1} \equiv (z_2, \dots, z_{k+2}, z') \bmod 2 \ \text{ with some } \ z' \in \mathbb{Z}.$$

However, this yields

$$z_1 \equiv z_2 + 1 \bmod 2,$$
$$z_2 \equiv z_3 + 1 \bmod 2,$$
$$\dots$$
$$z_{k+1} \equiv z_{k+2} + 1 \bmod 2,$$

i.e., $\bar{z}$ is congruent to one of the alternating vectors beginning with $(0,1,0,1,\dots)$ or $(1,0,1,0,\dots)$ modulo 2.

**(iii)** We may write $M_{(i)}\bar{1} = \bar{1}+2\bar{v}^{(i)}$ corresponding to the different recurrence relations for $i = 1,2,3,4$. By the above, if $\bar{z}^{(1)} \equiv \bar{0} \bmod 2$, then $\bar{v}^{(1)} \equiv \bar{0} \bmod 2$. Hence by the properties of $P_1(x)$, $P_2(x)$, $P_3(x)$ and $P_4(x)$ we have

$$\bar{v}^{(2)} \equiv \bar{v}^{(3)} \equiv \bar{e} \bmod 2 \quad \text{and} \quad \bar{v}^{(4)} \equiv \bar{0} \bmod 2$$

which yield $\bar{z}^{(2)}$ and $\bar{z}^{(3)}$ are congruent to some of the vectors $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2 and $\bar{z}^{(4)} \equiv \bar{0} \bmod 2$. Similarly, if $\bar{z}^{(1)}$ is congruent to one of $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2, then $\bar{v}^{(1)} \equiv \bar{e} \bmod 2$, whence

$$\bar{v}^{(2)} \equiv \bar{v}^{(3)} \equiv \bar{0} \bmod 2 \quad \text{and} \quad \bar{v}^{(4)} \equiv \bar{e} \bmod 2,$$

i.e.,

$$\bar{z}^{(2)} \equiv \bar{z}^{(3)} \equiv \bar{0} \bmod 2$$

and $\bar{z}^{(4)}$ is congruent to one of $(0,1,0,1,\dots)$ and $(1,0,1,0,\dots)$ modulo 2.

**(iv)** Now, examine the behaviour of $M^{\varrho}\bar{y}_n$. Since $\bar{u}_0, \bar{u}_1, \dots, \bar{u}_{k+1}$ are independent, they form a basis in $\mathbb{F}_2^{k+2}$ and there exist $\alpha_0, \alpha_1, \dots, \alpha_{k+1} \in \mathbb{Z}$ such that

$$\bar{y}_n \equiv \alpha_0\bar{u}_0 + \alpha_1\bar{u}_1 + \dots + \alpha_{k+1}\bar{u}_{k+1} \bmod 2.$$

Hence, by (1)

$$\begin{aligned} M^\varrho \bar{y}_n &\equiv M^\varrho(\alpha_0\bar{u}_0 + \alpha_1\bar{u}_1 + \cdots + \alpha_{k+1}\bar{u}_{k+1}) \\ &\equiv M^\varrho\alpha_0\bar{u}_0 + M^\varrho\alpha_1\bar{u}_1 + \cdots + M^\varrho\alpha_{k+1}\bar{u}_{k+1} \\ &\equiv \alpha_0 M^\varrho\bar{u}_0 + \alpha_1 M^\varrho\bar{u}_1 + \cdots + \alpha_{k+1}M^\varrho\bar{u}_{k+1} \\ &\equiv \alpha_0(\bar{1} + \bar{u}_0) + \alpha_1(\bar{1} + \bar{u}_1) + \cdots + \alpha_{k+1}(\bar{1} + \bar{u}_{k+1}) \\ &\equiv (\alpha_0 + \alpha_1 + \cdots + \alpha_{k+1}) \cdot \bar{1} + \bar{y}_n \\ &\equiv \delta_n \cdot \bar{1} + \bar{y}_n \bmod 2, \quad \text{with some} \quad \delta_n \in \{0, 1\}. \end{aligned}$$

**(v)** Now, by (2) we can write

$$\begin{aligned} \bar{u}_{2\varrho+n} - \bar{u}_n &= (M^\varrho + E)(M^\varrho - E)\bar{u}_n \\ &= (M^\varrho + E)(\bar{1} + 2\bar{y}_n) \\ &= \bar{1} + 2\bar{z} + \bar{1} + 2M^\varrho\bar{y}_n + 2\bar{y}_n \\ &\equiv 2(\bar{1} + \bar{z}) + 2(\delta_n\bar{1} + \bar{y}_n) + 2\bar{y}_n \\ &\equiv 2(\bar{1} + \bar{z} + \delta_n\bar{1} + 2\bar{y}_n) \\ &\equiv 2(\bar{1} + \bar{z} + \delta_n\bar{1}) \bmod 4. \end{aligned} \tag{3}$$

Similarly,

$$\bar{u}_{2\varrho+n+1} - \bar{u}_{n+1} \equiv 2(\bar{1} + \bar{z} + \delta_{n+1}\bar{1}) \bmod 4.$$

Hence

$$\begin{aligned} 1 + z_2 + \delta_n &\equiv 1 + z_1 + \delta_{n+1} \bmod 2 \\ 1 + z_3 + \delta_n &\equiv 1 + z_2 + \delta_{n+1} \bmod 2 \\ &\cdots \\ 1 + z_{k+2} + \delta_n &\equiv 1 + z_{k+1} + \delta_{n+1} \bmod 2. \end{aligned}$$

This yields

$$\begin{aligned} &\text{if } \bar{z} \equiv (0, 0, \ldots, 0) \bmod 2, \text{ then } \delta_n = \delta_{n+1} \text{ and} \\ &\text{if } \bar{z} \text{ is congruent to one of } (0, 1, \ldots) \text{ or } (1, 0, \ldots), \text{ then } \delta_n = 1 - \delta_{n+1}. \end{aligned} \tag{4}$$

**(vi)** In the following we will prove that $\bar{z}^{(i)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(i)} = 0$ for at least one of the $i = 1, 2, 3, 4$. (If $\bar{z}^{(i)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(i)} = 0$, then $\delta_n^{(i)} = 0$ for all $n \in \mathbb{N}$.)

Suppose, that $\bar{z}^{(1)} \not\equiv \bar{0} \bmod 2$ or $\delta_0^{(1)} \neq 0$.

**(vi.a)** Clearly, $u_n^{(i)} \equiv u_n^{(j)} \bmod 2$ for any $i, j = 1, 2, 3, 4$. Define the sequences $r_n^{(i)}$ by

$$u_n^{(i)} = u_n^{(1)} + 2r_n^{(i)} \quad for \;\; i = 2, 3, 4$$

and denote $\hat{u}_n = (0, 0, \ldots, 0, u_n) \in \mathbb{Z}^{k+2}$.

Obviously, for the state vectors we have $\bar{r}_0^{(i)} = \bar{0}$ for $i = 2, 3, 4$.

By the definition of $M_{(i)}$,

$$\bar{u}^{(2)}_{n+1} = M_{(2)}\bar{u}^{(2)}_n = M_{(1)}\bar{u}^{(2)}_n + 2\hat{u}^{(2)}_n,$$
$$\bar{u}^{(3)}_{n+1} = M_{(3)}\bar{u}^{(3)}_n = M_{(1)}\bar{u}^{(3)}_n + 2\hat{u}^{(3)}_{n+1}$$

and

$$\bar{u}^{(4)}_{n+1} = M_{(4)}\bar{u}^{(4)}_n = M_{(1)}\bar{u}^{(4)}_n + 2\big(\hat{u}^{(4)}_n + \hat{u}^{(4)}_{n+1}\big) \quad \text{for all } n \geq 0.$$

Hence

$$\begin{aligned}
\bar{u}^{(1)}_{n+1} + 2\bar{r}^{(2)}_{n+1} &= \bar{u}^{(2)}_{n+1} \\
&= M_{(1)}\big(\bar{u}^{(1)}_n + 2\bar{r}^{(2)}_n\big) + 2\big(\hat{u}^{(1)}_n + 2\hat{r}^{(2)}_n\big) \\
&= \bar{u}^{(1)}_{n+1} + 2\big(M_{(1)}\bar{r}^{(2)}_n + \hat{u}^{(1)}_n + 2\hat{r}^{(2)}_n\big), \\
\bar{u}^{(1)}_{n+1} + 2\bar{r}^{(3)}_{n+1} &= \bar{u}^{(3)}_{n+1} \\
&= M_{(1)}(\bar{u}^{(1)}_n + 2\bar{r}^{(3)}_n) + 2\big(\hat{u}^{(1)}_{n+1} + 2\hat{r}^{(3)}_{n+1}\big) \\
&= \bar{u}^{(1)}_{n+1} + 2\big(M_{(1)}\bar{r}^{(3)}_n + \hat{u}^{(1)}_{n+1} + 2\hat{r}^{(3)}_{n+1}\big)
\end{aligned}$$

and

$$\begin{aligned}
\bar{u}^{(1)}_{n+1} + 2\bar{r}^{(4)}_{n+1} &= \bar{u}^{(4)}_{n+1} \\
&= M_{(1)}(\bar{u}^{(1)}_n + 2\bar{r}^{(4)}_n) + 2\left(\hat{u}^{(1)}_n + \hat{u}^{(1)}_{n+1} + 2\big(\hat{r}^{(4)}_n + \hat{r}^{(4)}_{n+1}\big)\right) \\
&= \bar{u}^{(1)}_{n+1} + 2\left(M_{(1)}\bar{r}^{(4)}_n + \hat{u}^{(1)}_n + \hat{u}^{(1)}_{n+1} + 2\big(\hat{r}^{(4)}_n + \hat{r}^{(4)}_{n+1}\big)\right).
\end{aligned}$$

Subtracting $\bar{u}^{(1)}_{n+1}$ and cancelling out 2, we obtain

$$\bar{r}^{(2)}_{n+1} = M_{(1)}\bar{r}^{(2)}_n + \hat{u}^{(1)}_n + 2\hat{r}^{(2)}_n,$$
$$\bar{r}^{(3)}_{n+1} = M_{(1)}\bar{r}^{(3)}_n + \hat{u}^{(1)}_{n+1} + 2\hat{r}^{(3)}_{n+1} \tag{5}$$

and

$$\bar{r}^{(4)}_{n+1} = M_{(1)}\bar{r}^{(4)}_n + \hat{u}^{(1)}_n + \hat{u}^{(1)}_{n+1} + 2\big(\hat{r}^{(4)}_n + \hat{r}^{(4)}_{n+1}\big) \quad \text{for all} \quad n \geq 0.$$

Further, we know $\bar{r}^{(i)}_0 = \bar{0}$ for $i = 2, 3, 4$.

**(vi.b)** One can prove

$$\bar{r}^{(2)}_{n+1} \equiv \bar{r}^{(3)}_n \bmod 2 \quad \text{for all } n \geq 0 \tag{6}$$

by the following:

Since $u_0 = 0$, thus $\hat{u}_0^{(1)} = \bar{0}$ and we have $\bar{r}_0^{(2)} = \bar{r}_0^{(3)} = \bar{0}$. Let $n = 0$, then by (5)

$$\bar{r}_1^{(2)} = M_{(1)}\bar{r}_0^{(2)} + \hat{u}_0^{(1)} + 2\hat{r}_0^{(2)} \equiv M_{(1)}\bar{0} + \hat{u}_0^{(1)} = \bar{0} + \hat{0} = \bar{r}_0^{(3)} \bmod 2.$$

Suppose that

$$\bar{r}_{n+1}^{(2)} \equiv \bar{r}_n^{(3)} \bmod 2 \quad \text{for some } \ n \geq 0.$$

Then again by (5)

$$\bar{r}_{n+2}^{(2)} = M_{(1)}\bar{r}_{n+1}^{(2)} + \hat{u}_{n+1}^{(1)} + 2\hat{r}_{n+1}^{(2)} \equiv M_{(1)}\bar{r}_n^{(3)} + \hat{u}_{n+1}^{(1)} \equiv \bar{r}_{n+1}^{(3)} \bmod 2.$$

Hence by induction, the claim follows.

Similarly, one can prove that

$$\bar{r}_n^{(4)} \equiv \bar{r}_n^{(2)} + \bar{r}_n^{(3)} \bmod 2 \quad \text{for all } \ n \geq 0. \tag{7}$$

**(vi.c)** By (3) we can write

$$\bar{u}_{2\varrho}^{(1)} + 2\bar{r}_{2\varrho}^{(i)} - \big(\bar{u}_0^{(1)} + 2\bar{r}_0^{(i)}\big) = \bar{u}_{2\varrho}^{(i)} - \bar{u}_0^{(i)} \equiv 2\big(\bar{1} + \bar{z}^{(i)} + \delta_0^{(i)}\bar{1}\big) \bmod 4$$

for all $i = 2, 3, 4$. Again by (3), using that $\bar{r}_0^{(i)} = \bar{0}$,

$$2\big(\bar{1} + \bar{z}^{(1)} + \delta_0^{(1)}\bar{1}\big) + 2\bar{r}_{2\varrho}^{(i)} \equiv 2\big(\bar{1} + \bar{z}^{(i)} + \delta_0^{(i)}\bar{1}\big) \bmod 4,$$

which is equivalent to

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2\varrho}^{(i)} \equiv \bar{z}^{(i)} + \delta_0^{(i)}\bar{1} \bmod 2 \tag{8}$$

for all $i = 2, 3, 4$.

**(vi.d)** At the beginning of part (vi) we assumed that $\bar{z}^{(1)} \not\equiv \bar{0} \bmod 2$ or $\delta_0^{(1)} \neq 0$. Suppose first that $\bar{z}^{(1)} \not\equiv \bar{0} \bmod 2$. By part (iii) of the proof, we have then $\bar{z}^{(i)} \equiv \bar{0} \bmod 2$ for $i = 2, 3$. Assume further that $\delta_0^{(2)} \neq 0$ (i.e., $\delta_0^{(2)} = 1$).

By (8)

$$\bar{r}_{2\varrho}^{(i)} \equiv \bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \delta_0^{(i)}\bar{1} \bmod 2 \quad \text{for } \ i = 2, 3.$$

Since by part (ii) $\bar{z}^{(1)}$ is congruent to one of $(0, 1, 0, 1, \dots)$ and $(1, 0, 1, 0, \dots)$ modulo 2, thus $\bar{r}_{2\varrho}^{(2)}$ and $\bar{r}_{2\varrho}^{(3)}$ are also congruent to some of the vectors $(0, 1, 0, 1, \dots)$ and $(1, 0, 1, 0, \dots)$ modulo 2. However, by (6) if

$$\bar{r}_{2\varrho}^{(2)} \equiv (0, 1, 0, 1, \dots) \bmod 2,$$

then

$$\bar{r}_{2\varrho}^{(3)} \equiv (1, 0, 1, 0, \dots) \bmod 2,$$

and vice versa. Hence, by (8)

$$\delta_0^{(3)}\bar{1} \equiv \bar{r}_{2\varrho}^{(2)} + \bar{r}_{2\varrho}^{(3)} + \delta_0^{(2)}\bar{1} \equiv \bar{1} + \bar{1} \equiv \bar{0} \bmod 2,$$

that is both condition $\bar{z}^{(3)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(3)} = 0$ are fulfilled.

Suppose now that $\bar{z}^{(1)} \equiv \bar{0} \bmod 2$. Then, by part (iii) of the proof, we have $\bar{z}^{(4)} \equiv \bar{0} \bmod 2$. Since we assumed at the beginning of this part that $\bar{z}^{(1)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(1)} = 0$ do not hold simultaneously, we have $\delta_0^{(1)} = 1$. By (8) we can write

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2^\varrho}^{(4)} \equiv \bar{z}^{(4)} + \delta_0^{(4)}\bar{1} \bmod 2.$$

By (7)

$$\bar{z}^{(1)} + \delta_0^{(1)}\bar{1} + \bar{r}_{2^\varrho}^{(2)} + \bar{r}_{2^\varrho}^{(3)} \equiv \bar{z}^{(4)} + \delta_0^{(4)}\bar{1} \bmod 2.$$

Similarly, as above we can prove that

$$\bar{r}_{2^\varrho}^{(2)} + \bar{r}_{2^\varrho}^{(3)} \equiv \bar{1} \bmod 2,$$

whence substituting the proper values for $\bar{z}^{(1)}$, $\bar{z}^{(4)}$ and $\delta_0^{(1)}$ we obtain

$$\bar{1} + \bar{1} \equiv \delta_0^{(4)}\bar{1} \bmod 2.$$

However, this yields $\bar{z}^{(4)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(4)} = 0$.

With this we could prove the claim of part (vi). We should remark here, that the careful reading of the proof gives a stronger result, namely that $\bar{z}^{(i)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(i)} = 0$ hold simultaneously for exactly one $i \in \{1, 2, 3, 4\}$.

**(vii)** The above ensures us, that there exists an $i$, such that $\bar{z}^{(i)} \equiv \bar{0} \bmod 2$ and $\delta_0^{(i)} = 0$. In the following, without loss of generality, we may suppose $i = 1$.

In this part of the proof we will prove that

$$u_{2^s\varrho+n} \equiv u_n + 2^s \bmod 2^{s+1} \quad \text{for all} \quad s = 1, 2, \dots \text{ and } n = 0, 1, \dots \tag{9}$$

**(vii.a)** By the definition of $M$ we know that

$$M^{2\varrho}\bar{y} \equiv \bar{y} \bmod 2 \qquad \text{for all } \bar{y} \in \mathbb{Z}^{k+2}.$$

Suppose that for a fixed $s$

$$M^{2^s\varrho}\bar{y} \equiv \bar{y} \bmod 2^s \qquad \text{for all } \bar{y} \in \mathbb{Z}^{k+2}$$

holds. Then

$$\begin{aligned} M^{2^{s+1}\varrho}\bar{y} - \bar{y} &= (M^{2^{s+1}\varrho} - E)\bar{y} \\ &= (M^{2^s\varrho} + E)(M^{2^s\varrho} - E)\bar{y} \\ &\equiv (M^{2^s\varrho} + E)2^s\bar{x} \\ &\equiv M^{2^s\varrho}2^s\bar{x} + 2^s\bar{x} \\ &\equiv 2^{s+1}\bar{x} \\ &\equiv \bar{0} \bmod 2^{s+1} \quad \text{with some} \bar{x} \in \mathbb{Z}^{k+2} \quad \text{for any } \bar{y} \in \mathbb{Z}^{k+2}. \end{aligned}$$

By induction

$$M^{2^s\varrho}\bar{y} \equiv \bar{y} \bmod 2^s \quad \text{for any } \bar{y} \in \mathbb{Z}^{k+2} \quad \text{and} \quad s = 1, 2, \dots \tag{10}$$

**(vii.b)** Now we prove a similar, but somewhat stronger result than (10), assuming $\bar{y} = \bar{1}$. Recall that in our case $\bar{z} \equiv \bar{0} \bmod 2$, whence

$$M^{2\varrho}\bar{1} \equiv \bar{1} \bmod 4.$$

Suppose that for a fixed $s$

$$M^{2^s\varrho}\bar{1} \equiv \bar{1} \bmod 2^{s+1}.$$

Then by (10)

$$\begin{aligned} M^{2^{s+1}\varrho}\bar{1} &= M^{2^s\varrho}M^{2^s\varrho}\bar{1} \\ &\equiv M^{2^s\varrho}(\bar{1} + 2^{s+1}\bar{y}_n) \\ &\equiv M^{2^s\varrho}\bar{1} + M^{2^s\varrho}2^{s+1}\bar{y}_n \\ &\equiv \bar{1} + 2^{s+1}\bar{y}_n + 2^{s+1}\bar{y}_n \\ &\equiv \bar{1} \bmod 2^{s+2} \qquad \text{with some } \bar{y}_n \in \mathbb{Z}^{k+2}. \end{aligned}$$

By induction

$$M^{2^s\varrho}\bar{1} \equiv \bar{1} \bmod 2^{s+1} \qquad \text{for all } s = 1, 2, \ldots \tag{11}$$

**(vii.c)** Finally, we finish the proof of (9), assuming $\bar{z} \equiv \bar{0} \bmod 2$ and $\delta_n = 1$. Hence by (4) $\delta_0 = \delta_n$. By (3)

$$\bar{u}_{2\varrho+n} - \bar{u}_n \equiv 2(\bar{1} + \bar{z} + \delta_n\bar{1}) \equiv 2 \cdot \bar{1} \bmod 4.$$

This means that

$$u_{2\varrho+n} \equiv u_n + 2 \bmod 4 \qquad \text{for all } n \in \mathbb{N}.$$

Suppose, that $s$ is fixed and

$$u_{2^s\varrho+n} \equiv u_n + 2^s \bmod 2^{s+1} \qquad \text{for all } \ n = 0, 1, \ldots$$

Then by (10) and (11)

$$\begin{aligned} \bar{u}_{2^{s+1}\varrho+n} - \bar{u}_n &= M^{2^{s+1}\varrho}\bar{u}_n - \bar{u}_n \\ &= (M^{2^{s+1}\varrho} - E)\bar{u}_n \\ &= (M^{2^s\varrho} + E)(M^{2^s\varrho} - E)\bar{u}_n \\ &= (M^{2^s\varrho} + E)(2^s \cdot \bar{1} + 2^{s+1}\bar{y}_n) \\ &= M^{2^s\varrho}2^s \cdot \bar{1} + 2^s \cdot \bar{1} + M^{2^s\varrho}2^{s+1}\bar{y}_n + 2^{s+1}\bar{y}_n \\ &\equiv 2 \cdot 2^s \cdot \bar{1} + 2 \cdot 2^{s+1}\bar{y}_n \\ &\equiv 2^{s+1} \cdot \bar{1} \bmod 2^{s+2}, \quad \text{with some } \ \bar{y}_n \in \mathbb{Z}^{k+2}, \end{aligned}$$

which by induction proves (9).

**(viii)** By Lemma 24, $u_n$ is uniformly distributed modulo 2 with period length $2\varrho$.

Suppose that $u_n$ is uniformly distributed modulo $2^s$ with period length $2^s\varrho$. This yields

$$\#\{n \mid u_n \equiv i \bmod 2^s\,,\ 0 \le n < 2^s\varrho\} = \varrho \qquad \text{for all } 0 \le i < 2^s.$$

Obviously,

$$\begin{aligned}\#\{n \mid u_n \equiv i \bmod 2^s,\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} \qquad \text{for all } 0 \le i < 2^s.\end{aligned}$$

Furthermore, by (9)

$$\begin{aligned}\#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\}\end{aligned}$$

and symmetrically

$$\begin{aligned}\#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\} \quad \text{for all } 0 \le i < 2^s.\end{aligned}$$

Hence, using (2)

$$\begin{aligned}\#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n <2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i \bmod 2^{s+1}\,,\ 0 \le n < 2^s\varrho\} + \\ \#\{n \mid u_n \equiv i \bmod 2^{s+1}\,,\ 2^s\varrho \le n < 2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 2^s\varrho \le n < 2^{s+1}\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} = \\ \#\{n \mid u_n \equiv i+2^s \bmod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} \\ \text{for all } 0 \le i < 2^s.\end{aligned}$$

However,

$$\begin{aligned}\#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} + \\ \#\{n \mid u_n \equiv i + 2^s \bmod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} = \\ \#\{n \mid u_n \equiv i \bmod 2^s,\ 0 \le n < 2^{s+1}\varrho\} = \\ 2 \cdot \#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n < 2^s\varrho\} = 2 \cdot \varrho \\ \text{for all } 0 \le i < 2^s,\end{aligned}$$

whence

$$\#\{n \mid u_n \equiv i \bmod 2^{s+1},\ 0 \le n < 2^{s+1}\varrho\} = \varrho \qquad \text{for all } 0 \le i < 2^{s+1}.$$

By (vii)

$$u_{2^s\varrho+n} \not\equiv u_n \bmod 2^{s+1},$$

thus $2^s\varrho$ is not a period length of $u$ modulo $2^{s+1}$, but then by Lemma 26 the minimal period length of $u$ modulo $2^{s+1}$ is

$$2 \cdot 2^s\varrho = 2^{s+1}\varrho.$$

Consequently, $u$ is uniformly distributed modulo $2^{s+1}$.

By induction, this leads to the result, $u$ is uniformly distributed modulo $2^s$ for all $s = 1, 2, \dots$ and the period length of $u$ modulo $2^s$ is $2^s\varrho = 2^s\mathrm{ord}(Q)$. □

**Remark 28.** Experience shows that among the sequences $u^{(i)}$ there is only one, which is uniformly distributed.

## 4. Algorithm and example

**Algorithm 29.** Now we have everything together for the construction of a modulo $2^s$ uniformly distributed linear recurring sequence with large period length.

**Step 1.** Choose a suitable integer $k$ and find a monic polynomial $Q(x) \in \mathbb{Z}[x]$ of degree $k$, which reduction modulo 2 is irreducible in $\mathbb{F}_2[x]$.

**Step 2.** Calculate the monic polynomials $P(x) = p_{k+2}x^{k+2} + p_{k+1}x^{k+1} + \cdots + p_0$ and $P'(x)$ such that

$$P(x) \equiv (x^2 - 1)Q(x) \bmod 2$$

and $p_0, \dots, p_{k+1} \in \{0, -1\}$ and

$$P'(x) \equiv (x - 1)Q(x) \bmod 2$$

with similar condition on its coefficients. Determine

$$P_1(x) = P(x), \quad P_2(x) = P_1(x) - 2, \quad P_3(x) = P_1(x) - 2x$$

and

$$P_4(x) = P_1(x) - 2x - 2.$$

**Step 3.** Calculate the companion matrices $M_{(i)}$ corresponding to the characteristic polynomials $P_i(x)$. Check $M_{(i)}\bar{1} \equiv \bar{1} \bmod 4$. Keep the two matrices which satisfy the congruence and denote them by $M_1$ and $M_2$.

**Step 4.** Compute $\varrho = \mathrm{ord}(Q)$ modulo 2 and $M_1^{2\varrho}$ modulo 4. If $M_1^{2\varrho} \not\equiv E \bmod 4$, then set $M = M_1$ else $M = M_2$.

**Step 5.** Choose initial values of the sequence. This can be done by the following: assuming, we want to have $s$ bits long random numbers, choose random $u_0, u_1, \ldots, u_k \in [0, 2^s - 1]$. Set these values as initial values of the linear recurring sequence with characteristic polynomial $P'(x)$. Compute the next element of the sequence $u'_{k+1}$. Find a random number $u_{k+1} \in [0, 2^s - 1]$ satisfying $u_{k+1} \not\equiv u'_{k+1} \bmod 2$. The set $u_0, u_1, \ldots, u_k, u_{k+1}$ are suitable initial values for the sequence.

**Remark 30.** If $k$ is such that $2^k - 1$ is a prime (Mersenne prime), then by Proposition 13, $\operatorname{ord}(Q) = 2^k - 1$, i.e., maximal as a function of $k$.

If we choose $P$ such that its coefficient are 0 and $-1$, except the leading coefficient which is 1, then the computation of the elements of the recurring sequence is very fast, since there are no need for multiplication, only addition. Further, because of the inner representation of the numbers in computers, also the reduction modulo $2^s$ can be easily performed. (By a simple logical bit operation.)

Since we can obtain not only single digits, choosing $s$ to be suitably large, we may have a very effective method for constructing pseudo random sequences of large numbers. (In the case we have to compose large numbers from sequence of pseudo random bits, it is more difficult to prove uniform distribution, if we can do it at all.)

The sequence of numbers with $s$ binary digit can be regarded as a sequence of $s$ dimensional 0-1 vectors.

**Example 31.** In a small example we demonstrate the use of Algorithm 29. In particular, we will follow the consideration of Remark 30.

**Step 1.** Let $k = 3$ and choose a random polynomial of degree 3, which is irreducible modulo 2, say $Q(x) = x^3 + x^2 + 1$.

**Step 2.** We put

$$P(x) = x^5 - x^4 - x^3 - 1 \equiv (x^3 + x^2 + 1)(x^2 - 1) \bmod 2$$

and

$$P'(x) = x^4 - x^2 - x - 1 \equiv (x^3 + x^2 + 1)(x - 1) \bmod 2.$$

Thus we have:

$$\begin{aligned} P_1(x) &= x^5 - x^4 - x^3 - 1, \\ P_2(x) &= x^5 - x^4 - x^3 - 3, \\ P_3(x) &= x^5 - x^4 - x^3 - 2x - 1, \\ P_4(x) &= x^5 - x^4 - x^3 - 2x - 3. \end{aligned}$$

**Step 3.** Following the steps of the algorithm, we compute the companion matrices, corresponding to the proper recurrence relations:

$$M_{(1)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}, \qquad M_{(2)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 1 & 1 \end{pmatrix},$$

$$M_{(3)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 1 \end{pmatrix}, \qquad M_{(4)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 3 & 2 & 0 & 1 & 1 \end{pmatrix}.$$

Computing $M_{(1)}\bar{1}$, we obtain

$$M_{(1)}\bar{1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 3 \end{pmatrix} \not\equiv \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \bmod 4.$$

By **(iii)** of the proof of the Theorem, we can set $M_1 = M_{(2)}$ and $M_2 = M_{(3)}$.

**Step 4.** By Remark 30, $\varrho = 2^3 - 1 = 7$. We can use fast exponentiation for the calculation of $M_1^{14}$ and we get

$$M_1^{14} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \bmod 4,$$

whence

$$M = M_2 = M_{(3)} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 1 \end{pmatrix}.$$

**Step 5.** Suppose, that we want to construct a sequence of bytes. Then $s = 8$. We can choose random values for the first 4 elements, say

$$u_0 = 113, \quad u_1 = 5, \quad u_2 = 209 \quad \text{and} \quad u_3 = 198.$$

Satisfying the recurrence relation defined by $P'(x)$, the next value of the sequence is

$$u'_4 = 113 + 5 + 209 \equiv 1 \bmod 2.$$

Hence $u_4$ can be any number divisible by 2, say 66.

Thus we have constructed a linear recurring sequence, with recurrence relation

$$u_{n+5} = u_{n+4} + u_{n+3} + 2u_{n+1} + u_n$$

and initial values

$$u_0 = 113, \quad u_1 = 5, \quad u_2 = 209, \quad u_3 = 198 \quad \text{and} \quad u_4 = 66.$$

Reducing the sequence modulo 256, by the Theorem, we obtain a pseudo random byte sequence, which has period length

$$7 \cdot 256 = 1792.$$

There are the first few values of the sequence:

$$\begin{array}{cccccccc} 113\,, & 5\,, & 209\,, & 198\,, & 66\,, & 131\,, & 108\,, & 76\,, \\ 2\,, & 150\,, & 243\,, & 141\,, & 208\,, & 139\,, & 215\,, & 111. \end{array}$$

**Example 32.** In [1] Brent and Zimmermann describes the framework of a mod2 irreducible trinomial searching project. After the discovery of the new Mersenne prime $2^{74207281}-1$ by GIMPS on January 7, 2016, they started a search for primitive trinomials of degree 74207281 over $\mathbb{F}_2$. By the beginning of May they could prove that there are only 3 irreducible trinomials of degree 74207281 over $\mathbb{F}_2$, which means they are the only primitive ones. These trinomials are:

$$x^{74207281} + x^{9156813} + 1,$$

$$x^{74207281} + x^{9999621} + 1$$

and

$$x^{74207281} + x^{30684570} + 1.$$

Based on their results, you can find an example of a sequence with the period length $2^{74207345}$ at:

`https://arato.inf.unideb.hu/herendi.tamas/UDLRS/ExampleSequence.htm`.

## REFERENCES


[1] BRENT, R. P.—ZIMMERMANN, P.: *The great trinomial hunt*, Notices of the American Mathematical Society **58** (2011), 233–239.

[2] FOLLÁTH, J.: *Construction of Pseudorandom Binary Sequences Using Additive Characters Over* $GF(2^k)$, Periodica Mathematica Hungarica **57** (2008), 73–81.

[3] FOLLÁTH, J.—HUSZTI, A.—PETHŐ, A.: *DESignIn Asymmetric Authentication System*, Proceedings of ICAI'07 7th International Conference on Applied Informatics **1** (2007), 53–61.

[4] HERENDI, T.: *Uniform distribution of linear recurring sequences modulo prime powers*, Finite Fields and Applications **10** (2004), 1–23.

[5] HUSZTI, A.: *A Secure Electronic Voting Scheme*, Periodica Polytechnica Electrical Engineering **51** (2007), 141–146.

[6] HUSZTI, A.—PETHŐ, A.: *A Secure Electronic Exam System*, Publicationes Mathematicae Debrecen **77** (2010), 299–312.

[7] KNUTH, D. E.: *The Art of Computer Programming*. Vol. 2. Addison-Wesley, 1973.

[8] LIDL, R.—NIEDERREITER, H.: *Introduction to finite fields and their applications*. Cambridge University Press, 1986.

[9] MATSUMOTO, M.—NISHIMURA, T.: *Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator*, ACM Trans. on Modeling and Computer Simulation **8** (1998), 3–30.

[10] MAUDUIT, C.—SÁRKÖZY, A.: *On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol*, Acta Arith. **82** (1997), 365–377.

[11] MENEZES, A.—VAN OORSCHOT, P.—VANSTONE, S.: *Handbook of Applied Cryptography*. CRC Press, Boca Raton new York London Tokyo, 1996.

[12] NIEDERREITER, H.: *Distribution of Fibonacci numbers* $\mod 5^k$, Fibonacci Quart. **10** (1972), 373–374.

[13] ——— *Pseudo-random Number Generation and Quasi-Monte Carlo Methods*. Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania, 1992.

[14] NIEDERREITER, H.—SHIUE, J.: *Equidistribution of linear recurring sequences in finite fields*, Indag. Math. **39** (1977), 397–405.

[15] ——— *Equidistribution of linear recurring sequences in finite fields. II*, Acta Arith. **38** (1980), 197–207.

[16] TURNWALD, G.: *Gleichverteilung von linearen rekursiven Folgen*, Sitzungber., Abt. II, Oesterr. Akad. Wiss., Math.-Naturwiss. **193** (1985), 201–245.

[17] ——— *Uniform distribution of second-order linear recurring sequences*, Proc. Amer. Math. Soc. **96** (1986), 189–198.


Received September 12, 2016
Accepted November 21, 2017

**Tamás Herendi**
*Faculty of Informatics*
*University of Debrecen*
*Kassai str. 26*
*4028 Debrecen*
*HUNGARY*
*E-mail*: herendi.tamas@inf.unideb.hu