RECENT ADVANCES IN THE THEORY OF NONLINEAR PSEUDORANDOM NUMBER GENERATORS

by

AYÇA ÇEŞMELİOĞLU

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

Spring 2002

RECENT ADVANCES IN THE THEORY OF NONLINEAR PSEUDORANDOM NUMBER GENERATORS

APPROVED BY

Prof. Dr. Alev TOPUZOĞLU .....
(Thesis Supervisor)

Assist. Prof. Cem GÜNERİ .....

Assist. Prof. Berrin YANIKOĞLU .....

DATE OF APPROVAL: September 18th, 2002

Anneme, babama

ve

biricik kızkardeşime...

Acknowledgments

I would like to express my gratitude and deepest regards to my supervisor Prof.Dr. Alev Topuzoğlu for her motivation, guidance and encouragement throughout this thesis.

I also would like to thank Damla-Emrah Acar, Dilek Akyalçın, Tuğba Demirci, Beril Çiftçi, Sibel Koyuncu and Narcisa Poturak for their friendship and endless support.

RECENT ADVANCES IN THE THEORY OF PSEUDORANDOM NUMBERS

Abstract

The classical linear congruential method for generating uniform pseudorandom numbers has some deficiencies that can render them useless for some simulation problems. This fact motivated the design and the analysis of nonlinear congruential methods for the generation of pseudorandom numbers.

In this thesis, we aim to review the recent developments in the study of nonlinear congruential pseudorandom generators. Our exposition concentrates on inversive generators. We also describe the so-called power generator and the quadratic exponential generator which are particularly interesting for cryptographic applications. We give results on the period length and theoretical analysis of these generators. The emphasis is on the lattice structure, discrepancy and linear complexity of the generated sequences.

Keywords: Discrepancy, inversive congruential generator, lattice test, linear complexity profile, linear complexity, power generator, period length, pseudorandom number generator

Özet

Düzgün dağılan sözde rastgele sayı üretmede genellikle doğrusal kongruans tipi üreteçler kullanılır. Ancak, bu üreteçlerin bazı özellikleri simülasyon problemlerinde hatalı sonuçlara yol açabilmektedir. Bu nedenle, doğrusal olmayan kongruans tipi üreteçler önem kazanmıştır.

Bu tezin amacı, doğrusal olmayan kongruans tipi üreteçlere ilişkin son gelişmeleri sunmaktır. Bu çalışmada, özellikle tersinme üreteci üzerinde durulmuş ayrıca kriptografik uygulamaları açısından ilginç olan üstsel üreteçler de incelenmiş ve bu üreteçler yoluyla elde edilen dizilerin period uzunluğu, örgü yapısı, sapma özellikleri ve doğrusal karmaşıklığı üzerindeki güncel sonuçlar verilmiştir.

Anahtar kelimeler: Doğrusal karmaşıklık, doğrusal karmaşıklık profili, period uzunluğu, sapma, sözde rastgele sayı üreteci, tersinme üreteci, üstsel üreteç

TABLE OF CONTENTS

RECENT ADVANCES IN THE THEORY OF NONLINEAR PSEUDORANDOM NUMBER GENERATORS

by

AYÇA ÇEŞMELİOĞLU

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

Spring 2002

RECENT ADVANCES IN THE THEORY OF NONLINEAR PSEUDORANDOM NUMBER GENERATORS

APPROVED BY

Prof. Dr. Alev TOPUZOĞLU .....
(Thesis Supervisor)

Assist. Prof. Cem GÜNERİ .....

Assist. Prof. Berrin YANIKOĞLU .....

DATE OF APPROVAL: September 18th, 2002

Anneme, babama

ve

biricik kızkardeşime...

Acknowledgments

I would like to express my gratitude and deepest regards to my supervisor Prof.Dr. Alev Topuzoğlu for her motivation, guidance and encouragement throughout this thesis.

I also would like to thank Damla-Emrah Acar, Dilek Akyalçın, Tuğba Demirci, Beril Çiftçi, Sibel Koyuncu and Narcisa Poturak for their friendship and endless support.

RECENT ADVANCES IN THE THEORY OF PSEUDORANDOM NUMBERS

Abstract

The classical linear congruential method for generating uniform pseudorandom numbers has some deficiencies that can render them useless for some simulation problems. This fact motivated the design and the analysis of nonlinear congruential methods for the generation of pseudorandom numbers.

In this thesis, we aim to review the recent developments in the study of nonlinear congruential pseudorandom generators. Our exposition concentrates on inversive generators. We also describe the so-called power generator and the quadratic exponential generator which are particularly interesting for cryptographic applications. We give results on the period length and theoretical analysis of these generators. The emphasis is on the lattice structure, discrepancy and linear complexity of the generated sequences.

Keywords: Discrepancy, inversive congruential generator, lattice test, linear complexity profile, linear complexity, power generator, period length, pseudorandom number generator

Özet

Düzgün dağılan sözde rastgele sayı üretmede genellikle doğrusal kongruans tipi üreteçler kullanılır. Ancak, bu üreteçlerin bazı özellikleri simülasyon problemlerinde hatalı sonuçlara yol açabilmektedir. Bu nedenle, doğrusal olmayan kongruans tipi üreteçler önem kazanmıştır.

Bu tezin amacı, doğrusal olmayan kongruans tipi üreteçlere ilişkin son gelişmeleri sunmaktır. Bu çalışmada, özellikle tersinme üreteci üzerinde durulmuş ayrıca kriptografik uygulamaları açısından ilginç olan üstsel üreteçler de incelenmiş ve bu üreteçler yoluyla elde edilen dizilerin period uzunluğu, örgü yapısı, sapma özellikleri ve doğrusal karmaşıklığı üzerindeki güncel sonuçlar verilmiştir.

Anahtar kelimeler: Doğrusal karmaşıklık, doğrusal karmaşıklık profili, period uzunluğu, sapma, sözde rastgele sayı üreteci, tersinme üreteci, üstsel üreteç

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Numbers that are "chosen at random" are needed in many different areas; their use is crucial in stochastic simulations, computer programming and cryptography. In practice, random numbers are generated by deterministic algorithms and hence are not really "random" so we actually work with the so-called "pseudorandom" numbers. Throughout this thesis we will concentrate on uniform pseudorandom numbers (abbreviated PRN). In fact, no formal definition of a sequence of uniform PRN can be given, we only have certain characteristics in mind when we talk about such a sequence:

- the sequence is generated by a deterministic algorithm;
- the sequence should be uniformly distributed on the unit interval $[0, 1)$;
- it should pass relevant statistical and theoretical tests for randomness.

Reader is referred to the books Knuth [16] and Niederreiter [25] for further discussion on "randomness" of generated sequences.

Definition 1.0.1 *Let* $(x_n)_{n\geq 0}$ *be a sequence in the unit interval* $[0, 1)$. $(x_n)_{n\geq 0}$ *is said to be* uniformly distributed *on the unit interval if*

$$\lim_{N\to\infty} \frac{A_N(x)}{N} = x \quad \text{for all } x \in [0, 1)$$

where $A_N(x)$ *is the* counting function *which denotes the cardinality of the set* $\{x_n | 1 \leq n \leq N,\ x_n \in [0, x)\}$.

Definition 1.0.2 *Let* S *be an arbitrary nonempty set and* $(s_n)_{n\geq 0}$ *be a sequence of elements of* S*. If there exist integers* $r > 0$ *and* $n_0 \geq 0$ *such that* $s_{n+r} = s_n$ *for all* $n \geq n_0$*, then the sequence is called* periodic *and* r *is called a* period *of the sequence. The smallest number among the possible periods of the sequence is called the* period length *of the sequence, denoted by* $per(y_n)$ *. If* $(s_n)_{n\geq 0}$ *is periodic with period length* r*, then the least nonnegative integer* n_0 *such that* $s_{n+r} = s_n$ *for all* $n \geq n_0$ *is called the* preperiod*. We call* $(s_n)_{n\geq 0}$ purely periodic *if* $n_0 = 0$.

All standard methods of generating uniform PRNs are based on congruences and they all yield periodic sequences.

The desired properties of sequences of PRNs can be summarized as follows:

- long period length
- good statistical properties
- little intrinsic structure (such as lattice structure)
- reasonably fast generation

The classical method for the generation of uniform PRN is the *linear congruential method*. Choose a large integer M called the modulus and generate a sequence $(x_n)_{n\geq 0}$ of integers in $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$ by the recursion

$$x_{n+1} = ax_n + b \pmod{M} \quad \text{for } n = 0, 1, \ldots$$

with initial value x_0 and $a, b \in \mathbb{Z}_M$ where we assume that $gcd(a, M) = 1$ to get a purely periodic sequence. The linear congruential PRNs in $[0, 1]$ are obtained by the normalization

$$y_n = \frac{x_n}{M}, \quad \text{for } n = 0, 1, \ldots$$

We always have $per(y_n) \leq M$. The conditions on $a, b \in \mathbb{Z}_M$ such that $per(y_n) = M$ is given in Knuth [16, section 3.2]. Linear congruential generators are fast and easy to implement. Theoretical results on the structural and statistical properties of linear congruential generators indicate that these generators show a reasonable behavior if a judicious choice of parameters is made. But, to guarantee acceptable properties, a considerable amount of computational effort is needed. Because of the simple nature of the underlying linear recursion, the generator has an unfavorable lattice structure which can not be overcome by any choice of parameters. This lattice structure can render the generator useless for many simulations that require random irregularities. We will give the definition of the lattice of a generator in chapter 3.

To overcome these deficiencies of the linear congruential method, nonlinear methods for uniform PRN generation have been introduced. The first nonlinear congruential method is the *quadratic congruential generator*

$$x_{n+1} \equiv ax_n^2 + bx_n + c \pmod{m}$$

which has been introduced by Knuth [16] and studied in J.Eichenauer, J.Lehn [10], J.Eichenauer-Herrmann [3–5] and J.Eichenauer-Herrmann, H.Niederreiter [7]. In J.Eichenauer-Herrmann and E.Herrmann [6] another polynomial generator, namely, the *cubic generator* is studied.

An overview of the general nonlinear congruential generators are given in [25, section 8.1].

Let M be a large modulus. A sequence $x_0, x_1, \ldots$ of elements in $\mathbb{Z}_M$ is given by the recursion

$$x_{n+1} = f(x_n) \pmod{M} \quad \text{for } n = 0, 1, \ldots$$

with initial value x_0 where f is a fixed integer-valued function on $\mathbb{Z}_M$. We obtain the PRNs $y_0, y_1, \ldots$ in $[0, 1)$ by normalization

$$y_n = \frac{x_n}{M} \quad \text{for } n = 0, 1, \ldots$$

If the function f can not be represented by a linear polynomial modulo M, then we arrive at a nonlinear generator.

In the course of this thesis, we are going to deal with nonlinear congruential generators with a stress on the inversive congruential generator which employs the operation of multiplicative inversion modulo M .

1.1. Preliminaries

Let $\mathbb{F}_q$ be a finite field with q elements. In this section, we introduce the notation and the terminology and give the results which will be used in the subsequent chapters. We refer the reader to the classical book of Lidl and Niederreiter [17] for proofs and related results.

For every finite field $\mathbb{F}_q$, we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements in $\mathbb{F}_q$. $\mathbb{F}_q^*$ is a cyclic group with $q-1$ elements.

Definition 1.1.3 *A generator of the cyclic group $\mathbb{F}_q^*$ is called a* primitive element *of $\mathbb{F}_q$.*

In $\mathbb{F}_q$ there are $\varphi(q-1)$ primitive elements, where φ is the Euler's function.

Definition 1.1.4 *A polynomial $f \in \mathbb{F}_q[x]$ of degree $m \geq 1$ is called a* primitive polynomial *over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^m}$.*

Definition 1.1.5 *Let k be a positive integer and $a_0, a_1, \ldots, a_{k-1}$ be given elements of a finite field $\mathbb{F}_q$. A sequence $s_0, s_1, \ldots$ of elements of $\mathbb{F}_q$ satisfying the relation*

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n-k-2} + \cdots + a_0 s_n + a \tag{1.1}$$

for $n = 0, 1, \ldots$ is called a kth-order linear recurring sequence *in $\mathbb{F}_q$*

The terms $s_0, s_1, \ldots, s_{k-1}$ which determines the rest of the sequence uniquely are called *initial values*. The relation in (1.1) is called a linear recurrence relation of

order k. If $a = 0$ then (1.1) is called *homogeneous linear recurrence relation in* $\mathbb{F}_q$, otherwise we call it as *inhomogeneous*.

Definition 1.1.6 *Let* $s_0, s_1, \ldots$ *be a* kth-order homogeneous linear recurring sequence *in* $\mathbb{F}_q$ *satisfying the relation in (1.1) for* $n = 0, 1, \ldots$ *where* $a_j \in \mathbb{F}_q$ *for* $0 \leq j \leq k-1$. *The* characteristic polynomial *of the linear recurring sequence is defined as*

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0 \in \mathbb{F}_q[x] \tag{1.2}$$

A linear recurring sequence satisfies many linear recurring relations. For example, if the sequence s_n is periodic with period p, then for $n = 0, 1, \ldots$, $s_{n+p} = s_n$, $s_{n+2p} = s_n$ and so on. The following theorem gives us a relation between the different linear recurring relations satisfied by a given linear recurring sequence.

Theorem 1.1.1 *Let* $s_0, s_1, \ldots$ *be a homogeneous linear recurring sequence in* $\mathbb{F}_q$ *Then there exists a uniquely determined monic polynomial* $m(x) \in \mathbb{F}_q[x]$ *having the following property: a monic polynomial* $f(x) \in \mathbb{F}_q[x]$ *of positive degree is a characteristic polynomial of the given sequence if and only if* $m(x)|f(x)$.

The uniquely determined polynomial $m(x)$ of the above theorem is called the *minimal polynomial* of the sequence $s_0, s_1, \ldots$. In fact minimal polynomial is the characteristic polynomial of the linear recurrence relation of *least possible order* satisfied by the given sequence.

Definition 1.1.7 *Let* $s_0, s_1, \ldots$ *be a* kth-order homogeneous linear recurring sequence *in* $\mathbb{F}_q$ *which is given by (1.1). The* reciprocal characteristic polynomial *is defined as*

$$f^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \cdots - a_0x^k \in \mathbb{F}_q[x]\ . \tag{1.3}$$

The reciprocal characteristic polynomial and the characteristic polynomial are related by $f^*(x) = x^k f(\frac{1}{x})$.

Definition 1.1.8 *Let* $s_0, s_1, \ldots$ *be an arbitrary sequence of elements of* $\mathbb{F}_q$. *The*

generating function *of this sequence is defined as*

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{n=0}^{\infty} s_n x^n \tag{1.4}$$

Theorem 1.1.2 *Let* $s_0, s_1, \ldots$ *be a* kth-order homogeneous linear recurring sequence *in* $\mathbb{F}_q$ *which is given by (1.1). Let* $f^*(x)$ *be its reciprocal characteristic polynomial and* $G(x)$ *be its generating function. Then the identity*

$$G(x) = \frac{g(x)}{f^*(x)}$$

holds with

$$g(x) = -\sum_{j=0}^{k-1} \sum_{i=0}^{j} a_{i+k-j} s_i x^j \in \mathbb{F}_q[x]$$

where we set $a_k = -1$.

For the terms of a linear recurring sequence, an explicit formula is given in Lidl-Niederreiter [18] as follows: let $s_0, s_1, \ldots$ be a *kth-order homogeneous linear recurring sequence* in $\mathbb{F}_q$ which is defined as (1.1) with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$ as in (1.2) and the reciprocal characteristic polynomial as in (1.3). Let e_0 be the multiplicity of 0 as a root of $f(x)$, and let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the distinct nonzero roots of $f(x)$ with multiplicities $e_1, e_2, \ldots, e_m$, respectively.

Then, for the reciprocal characteristic polynomial we get

$$f^*(x) = x^k f(\frac{1}{x}) = \prod_{i=1}^{m} (1 - \alpha_i x)^{e_i} \ .$$

Since we have $deg(f^*) = k - e_0$, by theorem 1.1.2

$$G(x) = \frac{g(x)}{f^*(x)} = \sum_{n=0}^{e_0 - 1} t_n x^n + \frac{b(x)}{f^*(x)}$$

with $t_n \in \mathbb{F}_q$ and $deg(b) < k - e_0$. Partial fraction decomposition gives

$$\frac{b(x)}{f^*(x)} = \sum_{i=1}^{m} \sum_{j=0}^{e_i - 1} \frac{\beta_{ij}}{(1 - \alpha_i x)^{j+1}}$$

where the β_{ij} belong to the splitting field of $f(x)$ over $\mathbb{F}_q$.

$$\frac{1}{(1 - \alpha_i x)^{j+1}} = \sum_{n=0}^{\infty} \binom{n+j}{j} \alpha_i^n x^n$$

and hence

$$G(x) = \sum_{n=0}^{\infty} s_n x_n = \sum_{n=0}^{e_0-1} t_n x^n + \sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=0}^{e_i-1} \binom{n+j}{j} \beta_{ij} \right) x_n$$

Then, comparing the coefficients, we get

$$s_n = t_n + \sum_{i=1}^{m} \sum_{j=0}^{e_i-1} \binom{n+j}{j} \beta_{ij} \alpha_i^n \tag{1.5}$$

for $n = 0, 1, \ldots$ where $t_n = 0$ for $n \geq e_0$ and β_{ij} belong to the splitting field of $f(x)$.

Theorem 1.1.3 *Let $s_0, s_1, \ldots,$ be a sequence in $\mathbb{F}_q$ satisfying a k-th order homogeneous linear recurrence relation with characteristic polynomial $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is the minimal polynomial of the sequence if and only if the state vectors $\mathbf{s_0}, \mathbf{s_1}, \ldots, \mathbf{s_{k-1}}$ are linearly independent over $\mathbb{F}_q$, where $\mathbf{s_n} = (s_n, s_{n+1}, \ldots, s_{n+k-1})$, $n = 0, \ldots, k-1$.*

Definition 1.1.9 *A polynomial $f \in \mathbb{F}_q[x]$ is called a* permutation polynomial *if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.*

Lemma 1.1.4 *If $d \geq 1$ is a divisor of $q-1$, then there is no permutation polynomial of $\mathbb{F}_q$ of degree d.*

Lemma 1.1.5 *Let $a_0, a_1, \ldots, a_{q-1}$ be elements of $\mathbb{F}_q$. Then the following conditions are equivalent:*

- *$a_0, a_1, \ldots, a_{q-1}$ are distinct*
- $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } t = 0, 1, \ldots, q-1 \\ -1 & \text{for } t = q-1 \end{cases}$

Let G be a finite abelian group of order $|G|$ with identity element 1_G . A *character* χ of G is a *homomorhism* from G into the multiplicative group U of complex numbers of absolute value 1. In other words χ is a mapping from G onto U satisfying $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. Note that $\chi(1_G) = 1$. Among the characters of G, there is the *trivial character* which is defined by $\chi_0(g) = 1$ for all $g \in G$, all other characters of G are nontrivial.

Remark 1.1.1 *For a nontrivial character of the finite abelian group G, we have*

$$\sum_{g\in G}\chi(g)=0\ .$$

We use the term, *additive character* for the characters of the additive group of $\mathbb{F}_q$ and the term *multiplicative character* for the characters of the multiplicative group $\mathbb{F}_q^*$.

Now, we define certain exponential sums and give the upper bounds on them which will be used in the subsequent chapters.

Definition 1.1.10 *Let ψ be a multiplicative and χ be an additive character of $\mathbb{F}_q$. Then the* Gaussian sum *is defined by*

$$G(\psi,\chi)=\sum_{c\in\mathbb{F}_q^*}\psi(c)\chi(c)$$

Theorem 1.1.6 *Let ψ be a multiplicative and χ be an additive character of $\mathbb{F}_q$. Then the Gaussian sum $G(\psi,\chi)$ satisfies*

$$G(\psi,\chi)=\begin{cases} q-1 & \text{for } \psi=\psi_0, \quad \chi=\chi_0\\ -1 & \text{for } \psi=\psi_0, \quad \chi\neq\chi_0\\ 0 & \text{for } \psi\neq\psi_0, \quad \chi=\chi_0 \end{cases}$$

If $\psi\neq\psi_0$ and $\chi\neq\chi_0$ then

$$|G(\psi,\chi)|=q^{1/2}\ .$$

If λ is a multiplicative character of $\mathbb{F}_q$, then λ is defined for all nonzero elements of $\mathbb{F}_q$. But we can extend the definition of λ by setting $\lambda(0)=1$ if λ is the trivial character and $\lambda(0)=0$ if λ is a nontrivial character. Then we have

$$\sum_{c\in\mathbb{F}_q}\lambda(c)=\begin{cases} q & \text{if} \quad \lambda \text{ is trivial,}\\ 0 & \text{if} \quad \lambda \text{ is nontrivial.} \end{cases}$$

Definition 1.1.11 *Let $\lambda_1,\ldots,\lambda_k$ be k multiplicative characters of $\mathbb{F}_q$. Then the sum*

$$J(\lambda_1,\ldots,\lambda_k)=\sum\lambda_1(c_1)\ldots\lambda_k(c_k)$$

with the summation extended over all k-tuples $(c_1,\ldots,c_k)$ of elements of $\mathbb{F}_q$ satisfying $c_1+\cdots+c_k=1$, is called a Jacobi sum *in $\mathbb{F}_q$.*

If $k = 1$ then $J(\lambda_1) = \lambda_1(1) = 1$ for any multiplicative character of $\mathbb{F}_q$.

Theorem 1.1.7 *Let $\lambda_1, \ldots, \lambda_k$ be nontrivial multiplicative characters of $\mathbb{F}_q$. Then*

$$|J(\lambda_1, \ldots, \lambda_k)| = q^{\frac{k-1}{2}}$$

Definition 1.1.12 *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let $a, b \in \mathbb{F}_q$. Then the sum*

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1})$$

is called a Kloosterman sum.

Theorem 1.1.8 *If χ is a nontrivial additive character of $\mathbb{F}_q$ and $a, b \in \mathbb{F}_q$ are not both zero, then the Kloosterman sum $K(\chi; a, b)$ satisfies*

$$|K(\chi; a, b)| \leq 2q^{1/2} .$$

CHAPTER 2

PERIOD LENGTH

2.1. The Period Length of Inversive Congruential Generators

The widely used method of PRN generation, linear congruential method, has been investigated extensively and the research uncovered many deficiencies of this method. To overcome these deficiencies new methods of PRN generation have been designed and analysed. In this chapter we will mainly deal with the inversive congruential generator with modulus M which is defined as follows:

Let M be a large, fixed integer. For fixed elements $a, b \in \mathbb{Z}_M$ where $gcd(a, M) = 1$ and an initial value $x_0 \in \mathbb{Z}_M$, we define *inversive congruential generator modulo M* by

$$x_{n+1} = \begin{cases} b & \text{if } x_n = 0 \\ ax_n^{-1} + b & \text{if } x_n \neq 0 \end{cases} \tag{2.1}$$

where x_n^{-1} is the multiplicative inverse of x_n modulo M. We will consider the case where the modulus M is a prime $p \geq 5$ and the case $M = 2^e$ where $e \geq 3$ respectively and establish the criteria for these generators to have maximal period

length. The case $M = p^n$ where p is an odd prime and $n \geq 2$ was studied by Eichenauer-Herrmann,Topuzoğlu in [8].

2.1.1. The Period Length of Inversive Congruential Generators with Prime Modulus

The finiteness of $\mathbb{F}_p$ guarantees that the sequence $(x_n)_{n\geq 0}$ defined in (2.1) is purely periodic with period length being at most p. Our aim in this section is to determine the conditions which guarantee the maximal period length for the inversive generator. It turns out that the study of the polynomial $f(x) = x^2 - bx - a$ is crucial in obtaining these conditions. We first note that $f(x) = x^2 - bx - a$ needs to be irreducible over $\mathbb{F}_q$ in order to obtain the maximal period. When $f(x) = x^2 - bx - a$ has a root $c \in \mathbb{F}_q$ then $x_k = c$ for some $k \in \mathbb{Z}$ implies that $x_n = c$ for all $n \geq k$. We assume therefore that $f(x)$ is irreducible. Then $f(x)$ factors completely in $F_{p^2}[x]$ and $f(x) = (x - \alpha)(x - \beta)$ for $\alpha, \beta \in F_{p^2}$ such that $\alpha, \beta \notin \mathbb{F}_p$. Choose the initial value $x_0 = b$. Define $A_0, A_1, ...$ of elements of $\mathbb{F}_p$ by $A_0 = 1, A_1 = b$ and $A_{n+1} \equiv aA_{n-1} + bA_n \pmod{p}$ for all $n \geq 1$. Now, we can characterize x_n by using A_n as follows:

$$x_n = \begin{cases} \frac{A_{n+1}}{A_n} & \text{if } A_n \neq 0 \\ b & \text{if } A_n = 0 \end{cases} \tag{2.2}$$

From the definition it follows that A_n is a second order homogeneous linear recurring sequence with $f(x) = x^2 - bx - a$ as its characteristic polynomial. $f(x)$ is irreducible over $\mathbb{F}_p$ but it splits in F_{p^2} and it has two distinct roots $\alpha, \beta \in F_{p^2}$. Therefore $A_n = \gamma_1\alpha^n + \gamma_2\beta^n$ for $n = 0, 1, ...$ where $\gamma_1, \gamma_2 \in F_{p^2}$ are uniquely determined by the initial values of the sequence.

$A_0 = 1$ implies that $\gamma_1 = 1 - \gamma_2$.

$A_1 = b$ implies $\gamma_2 = \frac{b-\alpha}{\beta-\alpha}$ and $\gamma_1 = \frac{\beta-b}{\beta-\alpha}$.

From $f(x) = (x-\alpha)(x-\beta) = x^2 - bx - a$, we get $b = \alpha + \beta$. Therefore $\gamma_2 = \frac{\beta}{\beta-\alpha}$ and $\gamma_1 = \frac{\alpha}{\alpha-\beta}$ and we finally get

$$A_n = \frac{\alpha}{\alpha-\beta}\alpha^n + \frac{\beta}{\beta-\alpha}\beta^n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha-\beta} \tag{2.3}$$

for all $n \geq 0$.

Lemma 2.1.1 *Let $f(x)$ be irreducible in $\mathbb{F}_p[x]$. Let $\alpha, \beta \in F_{p^2}$ be the roots of $f(x)$. If N is the order of the element $\frac{\beta}{\alpha}$ in the multiplicative group of F_{p^2}, then the period length of the sequence $\{x_n\}$ generated by the inversive congruential method is $N-1$ with $x_0 = b$.*

Proof: If the order of $\frac{\beta}{\alpha}$ is N, then for all $1 \leq n < N$, $\beta^n \neq \alpha^n$ but $\beta^N = \alpha^N$. So $A_n \neq 0$ for all $0 \leq n < N-1$ while $A_{N-1} = 0$. Since $A_{N-1} = 0$, we get $x_{N-1} = b$ by definition and $N-1$ is the smallest such index. Therefore the period length of the sequence $(x_n)_{n\geq 0}$ with $x_0 = b$ is $N-1$.

□

Definition 2.1.1 *$f(x) = x^2 - bx - a$ will be called an* inversive maximal period polynomial*(or an IMP polynomial) if the period length of the corresponding inversive cogruential sequence equals p.*

Theorem 2.1.2 *$f(x) = (x-\alpha)(x-\beta)$ is an IMP polynomial if and only if the order of $\frac{\beta}{\alpha}$ in the multiplicative group of F_{p^2} is $p+1$.*

Proof:

Suppose that $f(x)$ is an IMP polynomial. Then the sequence obtained from $f(x)$ has period length p. From the remarks at the beginning of the section, $f(x)$ is irreducible over $\mathbb{F}_p$. Since $(x_n)_{n\geq 0}$ is assumed to have period length p, finiteness of $\mathbb{F}_p$ guarantees that $b \in \mathbb{F}_p$ occurs in the sequence. Without loss of generality we can assume that the initial value is b, i.e, $x_0 = b$. Therefore $x_p = x_0 = b$.

From equation (2.2), $x_p = \frac{A_{p+1}}{A_p}$ and $x_{p-1} = 0$ which implies $A_p = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha-\beta} = 0$ and $\alpha^{p+1} - \beta^{p+1} = 0$. Then $(\frac{\beta}{\alpha})^{p+1} = 1$ and $p+1$ is the least such integer, hence the order of $\frac{\beta}{\alpha} \in F_{p^2}$ is $p+1$.

Conversely, assume that the order of $\frac{\beta}{\alpha}$ in the multiplicative group of F_{p^2} is $p+1$. Then $f(x)$ is irreducible over $\mathbb{F}_p$ otherwise the roots α, β of $f(x)$ would be in $\mathbb{F}_p$ and the order of $\frac{\beta}{\alpha}$ would divide $p-1$.Therefore, by Lemma 2.1.1 we can conclude that the period length of the sequence $(x_n)_{n\geq 0}$ generated by equation (2.1) with initial value $x_0 = b$ has period length p. In fact with any initial value this sequence will have period length p .

□

Corollary 2.1.3 *Let σ be any generator of the multiplicative group of $\mathbb{F}(p^2)$, and $\alpha = \sigma^t$, for $0 \leq t \leq p^2 - 1$ be a root of $f(x) = x^2 - bx - a$. Then $f(x)$ is an IMP polynomial if and only if $gcd(t, p+1) = 1$. In particular, any primitive quadratic polynomial over $\mathbb{F}_p$ is an IMP polynomial.*

Proof:

Assume that $f(x)$ is irreducible over $\mathbb{F}_p$. If $\alpha = \sigma^t$ is a root of $f(x)$ then the other root of $f(x)$, $\beta = \alpha^p = \sigma^{tp}$.

Assume that $f(x)$ is an IMP polynomial. Then the order of $\frac{\beta}{\alpha} = \alpha^{p-1} = \sigma^{t(p-1)}$ is $p+1$. Suppose that $gcd(t, p+1) \neq 1$, then there exists $k \in Z^+$ such that $t = rk$ and $p+1 = sk$ for some $r, s \in \mathbb{Z}$. So,

$$(\frac{\beta}{\alpha})^s = (\sigma^{t(p-1)})^s = \sigma^{rk(p-1)s} = \sigma^{r(p^2-1)} = 1$$

The order of $\frac{\beta}{\alpha}$ is $p+1$ hence $gcd(t, p+1) = 1$.

Conversely, assume that $gcd(t, p+1) = 1$ but $f(x)$ is not an IMP polynomial. By Theorem 1, $f(x)$ is an IMP polynomial if and only if the order of $\frac{\beta}{\alpha} = p+1$. Hence $\frac{\beta}{\alpha} \neq p+1$ but at the same time,

$$(\frac{\beta}{\alpha})^{p+1} = (\alpha^{p-1})^{p+1} = \alpha^{p^2-1} = 1 \ .$$

Therefore the order of $\frac{\beta}{\alpha}$ is less than $p+1$. Suppose that the order of $\frac{\beta}{\alpha}$ is $k < p+1$. Then

$$(\frac{\beta}{\alpha})^k = (\alpha^{p-1})^k = (\sigma^{t(p-1)})^k = 1$$

Since σ is a primitive element of F_{p^2}, $p^2-1|t(p-1)k$, i.e, $p+1|tk$. $gcd(t, p+1) = 1$ implies $p+1|k$ which is a contradiction $(k < p+1)$.

If $t = 1$ then α is a primitive element of F_{p^2} and $f(x)$ becomes a primitive quadratic polynomial over $\mathbb{F}_p$. Since $gcd(1, p+1) = 1$, $f(x)$ is an IMP polynomial.

□

The above corollary shows that the set of IMP polynomials over $\mathbb{F}_p$ contains all primitive quadratic polynomials. We can obtain polynomials over $\mathbb{F}_p$ satisfying the condition of Corollary 2.1.3 in the following way:

Suppose that $g(x) \in \mathbb{F}_p[x]$ is a primitive quadratic polynomial and $\sigma \in F_{p^2}$ be any root of it. Let $t \in \mathbb{Z}$ such that $0 \leq t < p^2 - 1$,then the minimal polynomial of σ^t satisfies the required condition.

Corollary 2.1.4 *Let $T = \frac{p+1}{2}$ and let $m(x)$ be the minimal polynomial of $\frac{\beta}{\alpha}$ over $\mathbb{F}_p$ where α, β are the roots of the polynomial $f(x) = x^2 - bx - a \in \mathbb{F}_p[x]$. If $f(x)$ is an IMP polynomial, then $gcd(m(x), x^T + 1) \neq 1$.*

Proof:

Suppose that $f(x)$ is an IMP polynomial. Then the order of $\frac{\beta}{\alpha}$ is $p+1$. Therefore $(\frac{\beta}{\alpha})^T = -1$ and $\frac{\beta}{\alpha}$ is a root of $x^T + 1$. Furthermore $\frac{\beta}{\alpha}$ is a root of $m(x)$ so $gcd(m(x), x^T + 1) \neq 1$.

□

Let us remark here that $gcd(m(x), x^T + 1) \neq 1$ does not imply that $f(x)$ is an IMP polynomial.

Example 2.1.1 *In $\mathbb{F}_{11}$, $T = 6$ and $x^2 + 1$ divides both $x^6 + 1$ and $x^4 - 1$. $x^2 + 1$ is irreducible in $\mathbb{F}_{11}$ and since $x^2 + 1$ divides $x^4 - 1$, the order of the roots $\frac{\beta}{\alpha}$ and $\left(\frac{\beta}{\alpha}\right)^p = \frac{\alpha}{\beta}$ of $x^2 + 1$ is 4 and hence $f(x) = (x - \alpha)(x - \beta)$ is not an IMP.*

Theorem 2.1.5 *Let $f(x) = x^2 - bx - a$ be an IMP polynomial. Let a_1, b_1 be elements of $\mathbb{F}_p$ such that $\frac{b_1^2}{a_1} = \frac{b^2}{a}$ and $b_1^2 + 4a_1$ is a quadratic non-residue mod p. Then $g(x) = x^2 - b_1 x - a_1$ is also an IMP ploynomial.*

Proof:

If $\alpha, \beta \in F_{p^2}$ are the roots of $f(x)$ and $m(x)$ is the minimal polynomial of $\frac{\beta}{\alpha}$ over $\mathbb{F}_p$, then $m(x)$ is irreducible over $\mathbb{F}_p$ and

$$\begin{aligned} m(x) &= \left(x - \frac{\beta}{\alpha}\right)\left(x - (\frac{\beta}{\alpha})^p\right) \\ &= x^2 - \left(\frac{\beta}{\alpha} + (\frac{\beta}{\alpha})^p\right)x + (\frac{\beta}{\alpha})^{p+1} \\ &= x^2 - \left(\frac{\beta}{\alpha} + (\frac{\beta}{\alpha})^p\right)x + 1 \end{aligned}$$

the last step follows from the fact that $f(x)$ is an IMP polynomial. For the roots α and β of $f(x)$ we have $\beta^p = \alpha$ and $\alpha^p = \beta$, hence

$$\frac{\beta}{\alpha} + (\frac{\beta}{\alpha})^p = \frac{\beta}{\alpha} + \frac{\alpha}{\beta} = -\frac{b^2}{a} - 2$$

Let $g(x) = x^2 - b_1 x - a_1$. Since $b_1^2 + 4a_1$ is a quadratic non-residue mod p, $g(x)$ does not have a root in $\mathbb{F}_p$ and therefore $g(x)$ is irreducible over $\mathbb{F}_p$. Let δ, γ be the roots of $g(x)$ in F_{p^2}. Then

$$\begin{aligned} g(x) &= x^2 - b_1 x - a_1 = (x - \delta)(x - \gamma) \\ &= x^2 - (\delta + \gamma)x + \delta\gamma \end{aligned}$$

with $\gamma \cdot \delta = -a_1$ and $\delta + \gamma = b_1$. Now, we find the minimal polynomial $m_1(x)$ of $\frac{\delta}{\gamma}$;

$$\begin{aligned} m_1(x) &= (x - \frac{\delta}{\gamma})(x - (\frac{\delta}{\gamma})^p) = x^2 - (\frac{\delta}{\gamma} + \frac{\gamma}{\delta})x + (\frac{\delta}{\gamma})^{p+1} \\ &= x^2 - (-\frac{b_1^2}{a_1} - 2)x + 1 \\ &= x^2 - (-\frac{b^2}{a} - 2)x + 1 = m(x) \end{aligned}$$

Therefore the minimal polynomial of $\frac{\beta}{\alpha}$ and the minimal polynomial of $\frac{\delta}{\gamma}$ are the same and this means

$$(\frac{\delta}{\gamma})^p = \frac{\beta}{\alpha}$$

Now, it must be shown that the order of $\frac{\delta}{\gamma}$ is $p+1$. Suppose that $(\frac{\delta}{\gamma})^k = 1$ for some $k \in \mathbb{Z}$ with $k < p+1$. Then $(\frac{\beta}{\gamma})^{pk} = 1$ and this means $p+1|pk$. But $gcd(p, p+1) = 1$ which implies $p+1|k$, a contradiction. Therefore the order of $\frac{\delta}{\gamma}$ is $p+1$ and g(x) is an IMP polynomial.

□

Example 2.1.2 *Here, we have an example of a non-primitive IMP polynomial. In* $\mathbb{F}_7$*, let* $m(x) = x^2 - Ax + 1$ *and* $f(x) = x^2 - bx - a$ *where* $A = -\frac{b^2}{a} - 2 = 3, -3$. $x^T + 1 = x^4 + 1$

$$x^4 + 1 = m(x)(x^2 + Ax + 1)$$

$x^4 + 1|x^8 - 1$ *so* $m(x)|x^8 - 1$ *and this means that the roots of* $m(x)$ *are also roots of* $x^8 - 1$. $m(x)$ *does not divide* $x^k - 1$ *for* $k < 8$ *and therefore the order of both roots of* $m(x)$ *is* 8. *Then, By Theorem 1,* $f(x)$ *is an IMP.Now, let* $a_1 = b_1 = 1$*, then* $\frac{b_1^2}{a_1}+2 = 3$ *and* $b_1^2+4a_1 = 5$ *is a quadratic non-residue mod* 7. *Hence,* $f_1(x) = x^2-x-1$ *is an IMP polynomial over* $\mathbb{F}_7$ *but the roots* δ *and* δ^7 *of* $f_1(x) = x^2 - x - 1$ *in* F_{7^2} *has order 16. Therefore* $f_1(x)$ *is not a primitive polynomial.*

2.1.2. The Period Length of Inversive Congruential Generators with Power of 2 Modulus

The period length of the inversive congruential generators with power of 2 modulus was first studied by Eichenauer,Lehn,Topuzoğlu [11]. In this section we will consider this case.

$$x_{n+1} = ax_n^{-1} + b \pmod{2^e}, \quad x_{n+1} \in \mathbb{Z}_{2^e}, \ n \geq 0 \tag{2.4}$$

where $e \geq 3$ and $a, b, x_0 \in \mathbb{Z}_{2^e} = \{0, 1, \ldots, 2^e - 1\}$ with $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, and $x_0 \equiv 1 \pmod 2$. With these assumptions, $x_n \equiv 1 \pmod 2$ for all $n \geq 0$ and therefore $x_n^{-1} \in \mathbb{Z}_{2^e}$ is well-defined and the generator (2.4) is purely periodic. Here, the necessary and sufficient conditions are derived for this generator to have maximal period length 2^{e-1}.

Lemma 2.1.6 *Consider the matrix*

$$A = \begin{pmatrix} 0 & 1 \\ 4\alpha + 1 & 4\beta + 2 \end{pmatrix} \tag{2.5}$$

for some fixed non-negative integers α, β. Then

$$A^{2^{f-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^f(\alpha + \beta) + 1 \\ 2^f(\alpha + \beta + 1) + 1 \end{pmatrix} \pmod{2^{f+1}} \tag{2.6}$$

for every $f \geq 3$.

Proof:

First, we want to show that

$$A^{2^{f-1}} = \begin{pmatrix} \gamma_f \cdot 2^{f+1} + \alpha \cdot 2^f + 2^{f-1} + 1 & \delta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} \\ \epsilon_f \cdot 2^{f+1} + \beta \cdot 2^f + 32^{f-1} & \eta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} + 1 \end{pmatrix}$$

for some nonnegative integers $\gamma_f, \delta_f, \epsilon_f, \eta_f$.

The proof is by induction on f. By a short calculation,

$$A^2 = \begin{pmatrix} 4\alpha + 1 & 4\beta + 2 \\ 16\alpha\beta + 8\alpha + 4\beta + 2 & 16\beta^2 + 16\beta + 4\alpha + 5 \end{pmatrix}$$

then

$$A^4 = A^{2^{3-1}} = \begin{pmatrix} 16\gamma_3 + 8\alpha + 5 & 16\delta_3 + 8\beta + 12 \\ 16\epsilon_3 + 8\beta + 12 & 16\eta_3 + 8\alpha + 13 \end{pmatrix}$$

for some nonnegative integers $\gamma_3, \delta_3, \epsilon_3, \eta_3$ where,

$$\gamma_3 = \alpha^2 + 4\alpha\beta^2 + \beta^2 + 4\alpha\beta + \beta + \alpha$$

$$\delta_3 = 2\alpha\beta + 4\beta^3 + 6\beta^2 + \alpha + 3\beta$$

$$\epsilon_3 = \alpha^2\beta + 3\alpha^2 + 16\alpha\beta + 4\alpha + 16\alpha\beta^3 + 24\alpha\beta^2 + 4\beta^3 + 6\beta^2 + 3\beta$$

$$\eta_3 = 12\alpha\beta^2 + 12\alpha\beta + 3\alpha + 25\beta^2 + 11\beta + \alpha^2 + 16\beta^4 + 32\beta^3 + 24\beta^3 + 1$$

Hence the above equality is true for $f = 3$. Now suppose that

$$A^{2^{f-1}} = \begin{pmatrix} \gamma_f \cdot 2^{f+1} + \alpha \cdot 2^f + 2^{f-1} + 1 & \delta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} \\ \epsilon_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} & \eta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} + 1 \end{pmatrix}$$

for some $f \geq 3$

Then

$$A^{2^f} = A^{2^{f-1}} \cdot A^2 = \begin{pmatrix} \gamma_f \cdot 2^{f+1} + \alpha \cdot 2^f + 2^{f-1} + 1 & \delta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} \\ \epsilon_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} & \eta_f \cdot 2^{f+1} + \beta \cdot 2^f + 3 \cdot 2^{f-1} + 1 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 2^2\alpha + 1 & 2^2\beta + 2 \\ 2^4\alpha\beta + 2^3\alpha + 2^2\beta + 2 & 2^4\beta^2 + 2^4\beta + 2^2\alpha + 5 \end{pmatrix}$$

$$= \begin{pmatrix} \gamma_{f+1} \cdot 2^{f+2} + \alpha \cdot 2^{f+1} + 2^f + 1 & \delta_{f+1} \cdot 2^{f+2} + \beta \cdot 2^{f+1} + 3 \cdot 2^f \\ \epsilon_{f+1} \cdot 2^{f+2} + \beta \cdot 2^{f+1} + 3 \cdot 2^f & \eta_{f+1} \cdot 2^{f+2} + \beta \cdot 2^{f+1} + 3 \cdot 2^f + 1 \end{pmatrix}$$

for some nonnegative integers $\gamma_{f+1}, \delta_{f+1}, \epsilon_{f+1}, \eta_{f+1}$. Therefore we have proved the equality for $A^{2^{f-1}}$ and after this step the proof of the lemma is trivial.

□

Theorem 2.1.7 *The nonlinear generator* (2.4) *has maximal period length* 2^{e-1} *if and only if*

$$a \equiv 1 \pmod 4 \text{ and } b \equiv 2 \pmod 4 \tag{2.7}$$

Proof:

By definition of the generator in (2.4) we have $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$ and $x_0 \equiv 1 \pmod 2$. These assumptions show that the sequence (x_n) is a subset of

the multiplicative group $\mathbb{Z}_{2^e}^*$. Therefore the period length of the generator in (2.4) is at most $\phi(2^e) = 2^{e-1}$. Without loss of generality we assume that $x_0 = 1$ in what follows.

First, suppose that the generator in (2.4) is maximal period length 2^{e-1} for some $e \geq 3$. If $e = 2$ then the maximal period length is $\phi(4) = 2$ and $x_2 \equiv x_0 \equiv 1 \pmod 4$. When $e = 3$, the period length is 4 and $x_4 \equiv 1 \pmod 8$, $x_2 \not\equiv 1 \pmod 8$. Therefore $x_2 \equiv 5 \pmod 8$. For $x \in \mathbb{Z}_{2^3}^*$, $x^{-1} \equiv x \pmod 8$ and $a \in \{1, 3, 5, 7\}$, $b \in \{0, 2, 4, 6\}$. Hence, it follows that

$$x_2 \equiv a x_1^{-1} + b$$

$$x_2 \equiv a(a+b)^{-1} + b \equiv a(a+b) + b \equiv (a+1)b + 1 \pmod 8 \tag{2.8}$$

Therefore, $(a+1)b \equiv 4 \pmod 8$, i.e, $(a+1)b \equiv 0 \pmod 4$. Now there are 3 cases:

1. $b \equiv 0 \pmod 4$
2. $a \equiv 3 \pmod 4$
3. $b \equiv 2 \pmod 4$ and $a \equiv 1 \pmod 4$

Case 1 implies that $b \equiv 0 \pmod 8$ or $b \equiv 4 \pmod 8$. First one leads to the contradiction that $(a+1)b \equiv 0 \pmod 8$ and second one implies $a \equiv 0 \pmod 8$, which is not true. From case 2, it follows that $a \equiv 3 \pmod 8$ or $a \equiv 7 \pmod 8$. First one implies that $b \equiv 1 \pmod 8$ which is impossible and second one leads to the contradiction that $(a+1)b \equiv 0 \pmod 8$. Therefore, case 3 true.

Conversely, suppose that $b \equiv 2 \pmod 4$ and $a \equiv 1 \pmod 4$. For $e = 3$, (2.7) and (2.8) imply that the period length of the generator is 4. Now, we assume that the generator (2.4) has period length 2^{f-1} modulo 2^f for every integer with $3 \leq f \leq e-1$. Note that, $x_n \not\equiv 1 \pmod{2^{f+1}}$ for $n \in \mathbb{Z}_{2^f} \setminus \{0, 2^{f-1}\}$, otherwise, $x_n \equiv 1 \pmod{2^f}$ for $n \in \mathbb{Z}_{2^f} \setminus \{0, 2^{f-1}\}$, which contradicts our assumption. Therefore, we only need to show that $x_{2^{f-1}} \equiv 2^f + 1 \pmod{2^{f+1}}$.

Define a new sequence (y_n) by

$$y_n \equiv by_{n-1} + ay_{n-2} \pmod{2^e} \tag{2.9}$$

$y_n \in \mathbb{Z}_{2^e}$, $n \geq 2$ with $y_0 = y_1 = 1$. $a + b \equiv 1 \pmod 2$ it follows that $y_n \equiv 1 \pmod 2$ for $n \geq 0$ by induction on n. Consider

$$y_{n+1} \equiv ay_{n-1} + by_n \pmod{2^e}$$

Multiply both sides by y_n^{-1}, then

$$y_{n+1}y_n^{-1} \equiv a(y_n y_{n+1}^{-1})^{-1} + b \pmod{2^e}$$

By keeping in mind that $x_0 = y_0 = y_1$ and looking at the generator in (2.4), it is easily seen that

$$x_n \equiv y_{n+1}y_n^{-1} \pmod{2^e}, n \geq 0 \tag{2.10}$$

$a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$ implies that there are integers α, β such that $a = 4\alpha + 1$ and $b = 4\beta + 2$. So, (2.9) yields

$$\begin{aligned}
\begin{pmatrix} y_n \\ y_{n+1} \end{pmatrix} &\equiv \begin{pmatrix} y_n \\ ay_{n-1} + by_n \end{pmatrix} \equiv A \cdot \begin{pmatrix} y_{n-1} \\ y_n \end{pmatrix} \\
&\equiv A^2 \begin{pmatrix} y_{n-2} \\ y_{n-1} \end{pmatrix} \equiv \cdots \equiv A^n \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\
&\equiv A^n \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\end{aligned}$$

where the matrix A is defined as in (2.5). Therefore the lemma yields

$$\begin{pmatrix} y_{2^{f-1}} \\ y_{2^{f-1}+1} \end{pmatrix} \equiv A^{2^{f-1}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^f(\alpha+\beta)+1 \\ 2^f(\alpha+\beta+1)+1 \end{pmatrix} \pmod{2^{f+1}}$$

Since

$$y_{2^{f-1}}^2 \equiv 2^{2f}(\alpha+\beta)^2 + 2^{f+1}(\alpha+\beta) + 1 \equiv 1 \pmod{2^{f+1}}$$

$$y_{2^{f-1}}^{-1} \equiv y_{2^{f-1}} \pmod{2^{f+1}}$$

equation (2.10) gives us

$$x_{2^{f-1}} \equiv y_{2^{f-1}} y_{2^{f-1}+1} \equiv (2^f(\alpha+\beta)+1)(2^f(\alpha+\beta+1)+1)$$

□

2.2. The Period Length of the Power Generator

Let $e \geq 2$, $m \geq 1$ and ϑ be integers such that $gcd(\vartheta, m) = 1$. Then the *power generator* is defined as

$$u_n \equiv u_{n-1}^e \pmod{m}, \qquad 0 \leq u_n \leq m-1,\ n = 1, 2, \ldots \tag{2.11}$$

with initial value $u_0 = \vartheta$. When $gcd(e, \phi(m)) = 1$ where $\phi(m)$ is the Euler's phi function function, this generator is known as the *RSA generator* and in the case $e = 2$, it is called as the *Blum- Blum- Shub generator*.

We define the *Carmicheal function*, $\lambda(n)$ as the largest possible order of elements of the unit group in the residue ring modulo n, for $n \geq 1$. In other words, for a prime power p^k,

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1)\ , & if\ p \geq 3\ or\ k \leq 2 \\ 2^{k-2}\ , & if\ p = 2\ and\ k \geq 3 \end{cases}$$

and for $n = p_1^{k_1} \ldots p_r^{k_r}$,

$$\lambda(n) = lcm(\lambda(p_1^{k_1}), \ldots, \lambda(p_r^{k_r}))$$

If $gcd(e, \lambda(m)) = 1$, then e is a unit in the residue ring modulo $\lambda(m)$ and $e^{\lambda(\lambda(m))} \equiv 1 \pmod{\lambda(m)}$ by the definition of the Carmicheal function. So, there

exists $\alpha \in \mathbb{Z}$ such that $e^{\lambda(\lambda(m))} = \alpha\lambda(m) + 1$. At the same time, $gcd(\upsilon, m) = 1$ implies that ϑ is a unit in the residue ring modulo m and $\vartheta^{\lambda(m)} \equiv 1 \pmod{m}$. Hence

$$\vartheta^{e^{\lambda(\lambda(m))}} = \vartheta^{\alpha\lambda(m)+1} \equiv \vartheta \pmod{m}$$

i.e,

$$u_{\lambda(\lambda(m))} = u_0 .$$

This shows us that the sequence generated by (2.11) is purely periodic.

For integers g and $M \geq 2$ with $gcd(g, M) = 1$ denote by $ord_M g$ the multiplicative order of g modulo M . Let t be the smallest integer such that $u_t \equiv \vartheta^{e^t} \equiv \vartheta \pmod{m}$. Then $e^t \equiv 1 \pmod{ord_m \vartheta}$ and the smallest t satisfying this condition is $t = ord_s e$ where $s = ord_m \vartheta$. Hence the period length of the sequence is $t = ord_s e$ and $\lambda(\lambda(m))$ is the largest possible period.

The following result which was proved in Friedlander, Pomerance and Shparlinski [13], gives the lower bound on the period length of the sequence $(u_n)_{n\geq 0}$ generated by (2.11) with $m = pl$ when the primes p, l, the initial value ϑ with $gcd(\vartheta, m) = 1$ and the exponent $e \geq 2$ are chosen randomly.

Theorem 2.2.8 *For Q sufficiently large, for any $\Delta \geq 6(\log\log Q)^3$, and for all pairs prime pairs (p, l) , $1 < p < l \leq Q$, except at most $Q^2 \exp(-0,1(\Delta \log \Delta)^{1/3})$ of them, the following statement holds. For all pairs (ϑ, e) with*

$$1 \leq \vartheta \leq m - 1, \quad 1 \leq e \leq \lambda(m), \quad gcd(\vartheta, m) = gcd(e, \lambda(m)) = 1,$$

where $m = pl$, except at most $m\lambda(m)\exp(-0,2\Delta)$ of them, the period t of the sequence (u_n) given by (2.11) satisfies

$$t \geq Q^2 \exp(-\Delta)$$

With the below theorem given in [13], we have the lower bound of the period of Blum-Blum-Shub generator, that is, the case where the exponent is $e = 2$. Here, p, l, ϑ are arbitrary.

Theorem 2.2.9 *Given $\epsilon > 0$, there exist positive constants c, γ such that for Q sufficiently large, there are more than $cQ^2/(\log Q)^4$ prime pairs (p, l), $p < l \leq Q$ such that for all integers ϑ with*

$$1 \leq \vartheta \leq m - 1 \ \ and \ \ gcd(\vartheta, m) = 1 \ ,$$

where $m = pl$, except at most $m^{1-\gamma}$ of them, the period t of the sequence (u_n) given by (2.11) with $e = 2$ satisfies

$$t \geq cQ^{1-\epsilon} \ .$$

CHAPTER 3

ANALYSIS OF PSEUDORANDOM SEQUENCES

The outcome of a stochastic simulation depends on the quality of the PRNs. The sequences generated by the classical linear congruential method show a coarse lattice structure which causes undesirable regularities that can make the generated PRNs useless for simulations that requires random irregularities and the problem can not be overcome by any choice of the parameters. This fact was first pointed out in Marsaglia's famous paper "Random numbers fall mainly in the planes" [19], which provided the motivation for the study of nonlinear methods for the generation of PRNs. In this chapter we are going to deal with the distribution properties of nonlinear PRN generators.

3.1. Lattice Test

In this section we will consider recursive congruential generators of the form

$$x_{n+1} \equiv g(x_n)\ ,\ x_{n+1} \in \mathbb{F}_q\ ,\ n \geq 0 \tag{3.1}$$

where the modulus $q = p^k\ , k \geq 1$, is a power of a prime p, $x_0 \in \mathbb{F}_q$, and $f : \mathbb{F}_q \to \mathbb{F}_q$ denotes a function such that the generator in (3.1) has maximal period

length, i.e, $\{x_0, x_1, \ldots, x_{q-1}\} = \mathbb{F}_q$. Eichenauer, Grothe and Lehn studied nonlinear generators in (3.1) and established results on the performance of these generators under the lattice test in [9]. Later, in [22], Niederreiter presented a quicker approach to their results and made some improvements by using linear recurring sequences and permutation polynomials . He also improved the results on the performance of the inversive congruential generator under the lattice test which were given in [9] .We will mainly follow his treatment.

3.1.1. Nonlinear congruential generators and the lattice test

In order to avoid trivial cases, we assume that $p \geq 5$ and that the generator (3.1) is not additive, hence there exists no $\alpha \in \mathbb{F}_p^*$ such that

$$f(x) \equiv x + \alpha \pmod{p} \quad , x \in \mathbb{F}_p \tag{3.2}$$

Define the difference operator Δ^k on a sequence (y_n), $n = 0, 1, ...$ of elements of a field F as:

$$\Delta^0 y_n = y_n, \quad \Delta^k y_n = \Delta^{k-1} y_{n+1} - \Delta^{k-1} y_n$$

for $k \geq 1$.

Lemma 3.1.1

$$\Delta^k y_n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$$

Proof: The proof is by induction on k. When $k = 0$, $\Delta^0 y_n = y_n$ by definition and $\sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$ becomes y_n. So, the basis step is complete. Now, assume that

$$\Delta^k y_n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$$

for some $k \geq 0$. We want to show that

$$\Delta^{k+1} y_n = \sum_{j=0}^{k+1} (-1)^{k+1-j} \binom{k+1}{j} y_{n+j}$$

.

$$\Delta^{k+1} y_n = \Delta^k y_{n+1} \; - \; \Delta^k y_n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+1+j} - \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$$

Replace j by $j-1$ in the first sum, hence we get

$$\sum_{j=1}^{k+1} (-1)^{k-j+1} \binom{k}{j-1} y_{n+j} \; - \; \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$$

Taking out $j = k+1$ term from the first sum and $j = 0$ term from the second sum yields

$$= (-1)^0 \binom{k}{k} y_{n+k+1} \; + \; \sum_{j=1}^{k} (-1)^{k-j+1} \left(\binom{k}{j-1} + \binom{k}{j} \right) y_{n+j} - (-1)^k \binom{k}{0} y_n$$

since $\binom{k}{k} = \binom{k+1}{k+1}$ and $\binom{k}{0} = \binom{k+1}{0}$

$$= (-1)^0 \binom{k+1}{k+1} y_{n+k+1} \; + \; \sum_{j=1}^{k} (-1)^{k-j+1} \left(\binom{k+1}{j} \right) y_{n+j} \; + \; (-1)^{k+1} \binom{k+1}{0} y_n$$

hence we get the desired equality

$$\Delta^{k+1} y_n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}$$

.

□

Remark 3.1.1 *Let $h(x) \in F[x]$ with $deg(h) < k$. Then*

$$\Delta^k h(n) = 0 \tag{3.3}$$

Since we assumed that the generator in (3.1) yields a sequence of period p, we can write $x_{n+p} = x_n$ for $n \geq 0$. Now, (x_n) can be viewed as a linear recurring

sequence with characteristic polynomial $x^p - 1 = (x-1)^p$. The minimal polynomial of (x_n) which is a divisor of $(x-1)^p$ by Theorem 1.1.1, is of the form $(x-1)^t$ with $1 \leq t \leq p$. $t \neq 0$ since (x_n) is not the zero sequence.

From (1.5), it follows that

$$x_n = \sum_{j=0}^{s} \binom{n+j}{j} a_j = g(n) \quad for \quad all \quad n \geq 0 \tag{3.4}$$

where $s = t-1$, $a_j \in \mathbb{F}_p$ and $g \in \mathbb{F}_p[x]$ with $deg(g) \leq s$. If $deg(g) < s$ then

$$\Delta^s g(n) = \Delta^s x_n = \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} x_{n+j} = 0$$

and hence $(x-1)^s$ with $s = t-1$ is a characteristic polynomial of (x_n), which is a contradiction to the definition of the minimal polynomial. Therefore $deg(g) = s$.

Lemma 3.1.2 *We always have* $1 \leq s \leq p-2$ *and if* $s > 1$*, then* s *does not divide* $p-1$*. In the non-additive case,* $s \geq 3$*.*

Proof:

Since $\{g(0), g(1), ..., g(p-1)\} = \mathbb{F}_p$, g is a permutation polynomial of $\mathbb{F}_p$. This implies that $s \neq 0$. If $s > 1$, then by lemma 1.1.4, s does not divide $p-1$. Therefore, $1 \leq t \leq p$ implies $1 \leq s \leq p-2$. The generator is called additive if $x_{n+1} = x_n + \alpha$ for all $n \geq 0$ with $x_0 \in \mathbb{F}_p$ where $\alpha \in \mathbb{F}_p^*$. This means Δx_n is a constant which is α here. In the non-additive case, $s \neq 1$ otherwise the generator is additive, $s \neq 2$ either, since $p \geq 5$ and s can not divide $p-1$ by the same reason as above. Thus, $s \geq 3$ in the non-additive case.

□

Now, let

$$\nu_i^d = (x_i, x_{i+1}, \ldots, x_{i+d-1})^T \in \mathbb{F}_p^d, \ i \geq 0 \tag{3.5}$$

denote the vectors of $d \geq 2$ consecutive PRNs and let

$$\omega_i^d = \nu_i^d - \nu_0^d \in \mathbb{F}_p^d \ \ i \geq 0 \tag{3.6}$$

be the corresponding difference vectors.

Let

$$\mathbf{u_i} = (0, x_{i+1} - x_i, x_{i+2} - x_i, \ldots, x_{i+p-1})^T,\ \mathbf{u_i} \in \mathbb{F}_p^p,\ i \geq 0 \tag{3.7}$$

be a sequence of difference vectors of p consecutive PRNs and denote by

$$G^d = (\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{d-1}})^T = (\omega_0^d, \omega_1^d, \ldots, \omega_{p-1}^d) \in \mathbb{F}_p^{d \times p} \tag{3.8}$$

the $d \times p$ matrix whose rows are the vectors $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{d-1}}$.

Lemma 3.1.3

$$\sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \mathbf{u_{k+j}} = \mathbf{0}$$

for all $k \geq 0$ *where* $\mathbf{u_n}$ *is defined as in* (3.7).

Proof:

For any $h \geq 0$,

$$\begin{aligned}
\sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} (x_{k+j+h} - x_{k+j}) &= \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \sum_{n=k}^{k+h-1} (x_{j+n+1} - x_{j+n}) \\
&= \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \sum_{n=k}^{k+h-1} \Delta x_{j+n} \\
&= \sum_{n=k}^{k+h-1} \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \Delta_{j+n} x \\
&= \sum_{n=k}^{k+h-1} \Delta^s (\Delta x_n) = \sum_{n=k}^{k+h-1} \Delta^{s+1} x_n \\
&= \Delta^{s+1} g(n) = 0
\end{aligned}$$

where the last step follows from the fact that $deg(g) = s$.

□

Lemma 3.1.4 *Let* G^d *be the* $d \times p$ *matrix over* $\mathbb{F}_p$ *which was defined in* (3.8). *Then* $rank(G^d) = d$ *for* $d \leq s$ *and* $rank(G^d) = s$ *for* $d > s$.

Proof:

For $k = 0$, Lemma 2 shows us that $\mathbf{u_s}$ is a linear combination of $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{s-1}}$ which implies that $rank(G^{(s+1)}) \leq s$. From the definition of the matrix G^d (3.8), we can see that the columns of the matrix are the vectors $\omega_0^{s+1}, \omega_1^{s+1}, \ldots, \omega_{p-1}^{s+1}$. The congruential sequence (x_n) in (3.1) has a minimal polynomial of degree $t = s + 1$, hence by theorem 1.1.3, the vectors $\nu_0^{s+1}, \nu_1^{s+1}, \ldots, \nu_s^{s+1}$ are linearly independent. Therefore the vectors $\omega_1^{s+1}, \omega_2^{s+1}, \ldots, \omega_s^{s+1}$ are linearly independent which yields $rank(G^{s+1}) \geq s$ (Note that $\omega_0^{s+1} = \mathbf{0}$). Thus, $rank(G^{s+1}) = s$ and the rows of the matrix, $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{s-1}}$ are linearly independent. Hence, for any $d \leq s$, $rank(G^d) = d$ since the rows of the matrix, $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{d-1}}$ are linearly independent. From lemma 3.1.3 we see that, for any $d > s$, $\mathbf{u_d}$ is a linear combination of $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{s-1}}$. Therefore $rank(G^d) = s$ for any $d > s$.

□

Let

$$V^d = \{v \in \mathbb{F}_p^d | v = \sum_{i=0}^{d-1} z_i \omega_i^d \pmod{p}; z_1, ..., z_{p-1} \in \mathbb{F}_p\} \tag{3.9}$$

The set V^d is called as the *d-lattice* of the generator (3.1) spanned by the vectors $\omega_0^d, \omega_1^d, \ldots, \omega_{p-1}^d$ in $\mathbb{F}_p^d$. Marsaglia proposed the following lattice test that can be applied to generators of the form (3.1). The generator passes the lattice test for fixed $d \geq 2$ if $V^d = \mathbb{F}_p^d$ and it fails the d-lattice test if $V^d \neq \mathbb{F}_p^d$.

There is a connection between the d-lattice V^d and the matrix G^d. The following lemma [9] establishes this relation.

Lemma 3.1.5 *The generator* (3.1) *passes d-dimensional lattice test for fixed* $d \geq 2$ *if and only if its d-matrix has rank d.*

Proof:

First, note that V^d is the column space of G^d. Then the proof follows from the fact that the condition $rank(G^d) = d$ is equivalent to $V^d = \mathbb{F}_p^d$.

□

Lemma 3.1.6 *The generator* (3.1) *passes the d-dimensional lattice test for any* $d \leq s$ *and it fails the test for any* $d > s$.

Proof: Proof follows from lemma (3.1.5) and lemma (3.1.4)

□

The performance of the special nonlinear generator

$$x_{n+1} = \begin{cases} b & \text{if } x_n = 0 \\ ax_n^{-1} + b & \text{if } x_n \neq 0 \end{cases} \tag{3.10}$$

where $a, b \in \mathbb{F}_p$ and $n \geq 0$ was considered in [9]. We choose a, b such that (x_n) has period p and $\{x_0, x_1, ..., x_{p-1} = \mathbb{F}_p\}$. The conditions on a, b under which (x_n) has maximal period p is studied in chapter 2.

Theorem 3.1.7 *The generator in* (3.10) *passes the d-dimensional lattice test for all* $d \leq \frac{p+1}{2}$

Proof: It suffices to show that $s \geq \frac{p+1}{2}$. Let $z_n = x_n x_{n+1} - bx_n - a$. Then z_n is zero for $p-1$ of the values $z_0, z_1, ..., z_{p-1}$. Hence $p - 1 \leq 2s$, i.e, $s \geq \frac{p-1}{2}$. But $s = \frac{p-1}{2}$ is impossible since s does not divide $p-1$. Therefore s is an integer implies $s \geq \frac{p-1}{2} + 1 = \frac{p+1}{2}$.

□

Now, consider the sequence (x_n) of elements of $\mathbb{F}_q$,with period q and $\{x_0, x_1, ..., x_{q-1}\}$ $= \mathbb{F}_q$ where $q \geq 3$ is an arbitrary prime power . We can develop a theory for this case analogous to the prime modulus case.

(x_n) can be viewed as a linear recurring sequence since $x_{n+q} = x_n$ for all $n \geq 0$. A characteristic polynomial of this sequence is $x^q - 1 = (x-1)^q$. Hence its minimal polynomial is of the form $(x-1)^t$ with $1 \leq t \leq q$. Again, by (1.5), we have the representation,

$$x_n = \sum_{j=0}^{s} \binom{n+j}{j} a_j \tag{3.11}$$

for all $n \geq 0$,where $s = t - 1$ and $a_j \in \mathbb{F}_q$. (x_n) is additive if Δx_n is constant.

Theorem 3.1.8 *$1 \leq s \leq q-2$ and in the non-additive case $s \geq 3$ for $q \geq 5$.*

Proof: If $s = 0$ then by (3.11) $x_n = a_0$ for all $n \geq 0$, so (x_n) is a constant sequence which is a contradiction. Suppose $s = q-1$. Then the minimal polynomial of (x_n) has degree $t = s+1 = q$ and by theorem 1.1.3

$$\mathbf{x_n} = (x_n, x_{n+1}, ..., x_{n+q-1}) \;\; 0 \leq n \leq q-1$$

are linearly independent. Each component of

$$\sum_{n=0}^{q-1} \mathbf{x_n} = \sum_{n=0}^{q-1} (x_n, x_{n+1}, ..., x_{n+q-1})$$

is equal to

$$\sum_{k=0}^{q-1} x_{n+j+k} = \sum_{c \in \mathbb{F}_q} c = 0$$

for all $0 \leq j \leq q-1$ by lemma (1.1.5) since $q \geq 3$. Therefore $\sum_{n=0}^{q-1} \mathbf{x_n} = \mathbf{0}$ which is a contradiction. So, $1 \leq s \leq q-2$.

If $q \geq 5$ is prime in the non-additive case, then $s \geq 3$ by Lemma 3.1.2. If $q = p^e$ where $p \geq 3$ is a prime, $e \geq 2$ and $s \leq 2$, then

$$x_n = \sum_{j=0}^{s} \binom{n+j}{j} a_j$$

yields $x_p = x_0$ for $s = 1$ and $s = 2$ which is a contradiction to the assumption that the period length of (x_n) is q. If $q = 2^e$ such that $e \geq 3$ and $s \leq 2$, then $x_4 = x_0$ which is a contradiction.

□

Remark 3.1.2 $\binom{n}{m} = 0$ *for* $m < 0$.

Lemma 3.1.9 $\sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \mathbf{u_{k+j}} = 0$ *for all* $k \geq 0$ *where*

$$\mathbf{u_n} = (0, x_{n+1} - x_n, x_{n+2}, ..., x_{n+q-1} - x_n) \in \mathbb{F}_q^q$$

Proof:

$$\sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}\mathbf{u_{k+j}} = \sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}(0, x_{k+j+1}-x_{k+j}, \ldots, x_{k+j+q-1}-x_{k+j})$$

Now we will show that each component of the above vector is 0. Let $h \geq 0$. Then

$$\sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}(x_{k+j+h}-x_{k+j}) = \sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}\sum_{n=k}^{k+h-1}\Delta x_{j+n}$$

Proceeding as in the proof of Lemma 3.1.3 we get

$$\begin{aligned} &= \sum_{n=k}^{k+h-1}\Delta^{s+1}(x_n) = \sum_{n=k}^{k+h-1}\Delta^{s+1}\sum_{j=0}^{s}\binom{n+j}{j}a_j \\ &= \sum_{j=0}^{s}a_j\sum_{n=k}^{k+h-1}\Delta^{s+1}\binom{n+j}{j} \end{aligned}$$

Now, we want to show that

$$\Delta^r\binom{n+j}{j} = \binom{n+j}{j-r} \tag{3.12}$$

by induction on r.

When $j = 0$

$$\Delta^0\binom{n+j}{j} = \binom{n+j}{j} = \binom{n+j}{j-0}$$

Suppose that

$$\Delta^r\binom{n+j}{j} = \binom{n+j}{j-r}$$

for some $r \geq 0$.Then

$$\begin{aligned} \Delta^{r+1}\binom{n+j}{j} &= \Delta^r\binom{n+1+j}{j} - \Delta^r\binom{n+j}{j} \\ &= \binom{n+1+j}{j-r} - \binom{n+j}{j-r} \\ &= \binom{n+j}{j-r-1} \end{aligned}$$

Hence,

$$\Delta^{s+1}\binom{n+j}{j} = \binom{n+j}{j-s-1} = 0$$

for $0 \leq j \leq s$ by the previous remark. Therefore

$$\sum_{j=0}^{s}(-1)^{s-j}\binom{s}{j}(x_{k+j+h} - x_{k+j}) = \sum_{j=0}^{s} a_j \sum_{n=k}^{k+h-1} \Delta^{s+1}\binom{n+j}{j} = 0$$

for each $0 \leq h \leq q-1$. So the result follows.

□

Theorem 3.1.10 *Let G^d be the $d \times q$ matrix over $\mathbb{F}_q$ whose rows $\mathbf{u_0}, \mathbf{u_1}, \ldots, \mathbf{u_{d-1}}$ are as given in* Lemma 3.1.9. *Then $rank(G^d) = d$ for $d \leq s$ and $rank(G^d) = s$ for $d > s$.*

Proof: This theorem is a generalization of lemma 3.1.4 and it can be proved in the same way. But here lemma 3.1.9 is used instead of Lemma 3.1.3.

□

Let (x_n) be a sequence of elements in $\mathbb{F}_q$ generated by (3.10)with period length q and $\{x_0, ..., x_{q-1}\} = \mathbb{F}_q$.

Theorem 3.1.11 *The sequence (x_n) defined as in* (3.10) *in $\mathbb{F}_q$ passes the d-dimensional lattice test for all $d \leq \frac{q+1}{2}$ if $q \geq 4$.*

Proof: The special sequence (x_n) generated by inversive congruential generator with modulo q passes the d-dimensional lattice test for $d \leq s$. So, it suffices to show that $s \geq \frac{q}{2}$. Let $z_n = x_n x_{n+1} - bx_n - a$, $n \geq 0$.

$$\Delta^{2s+1} z_n = \Delta^{2s+1}(x_n x_{n+1} - bx_n - a)$$

By, induction on r, it can be shown that

$$\Delta^r z_n = \Delta^r(x_n x_{n+1}) - b\Delta^r x_n$$

for $r \geq 0$. Hence,

$$\Delta^{2s+1} z_n = \Delta^{2s+1}(x_n x_{n+1}) - b\Delta^{2s+1} x_n = \Delta^{2s+1}(x_n x_{n+1}) \ ,$$

since

$$\Delta^{2s+1} x_n = \sum_{j=0}^{s} a_j \Delta^{2s+1} \binom{n+j}{j} = \sum_{j=0}^{s} a_j \binom{n+j}{j-2s-1} = 0$$

by remark 3.1.2. Therefore, (3.3) implies,

$$\Delta^{2s+1} z_n = \sum_{j,k=0}^{s} a_j a_k \Delta^{2s+1} \binom{n+j}{j} \binom{n+1+k}{k} = 0$$

since $\binom{n+j}{j}\binom{n+1+k}{k}$ can be viewed as a polynomial in n with degree $j+k \leq 2s$. Now, by lemma 3.1.1, we can write

$$\sum_{j=0}^{2s+1} (-1)^{2s+1-j} \binom{2s+1}{j} z_{n+j} = 0 \tag{3.13}$$

for all $n \geq 0$. When $x_n \neq 0$

$$z_n = x_n x_{n+1} - b x_n - a = 0$$

and when $x_n = 0$

$$z_n = -a \ .$$

Therefore, among any q consecutive terms of the sequence (z_n), $q-1$ of them are zero and only one of them is different from zero. Suppose, we had $2s+1 \leq q-1$ and choose n such that $z_n \neq 0$, then $z_{n+j} = 0$ for $1 \leq j \leq 2s+1$. If q is even then $1 \leq j \leq 2s+1$ and $s \in \mathbb{Z}$ yields $s \geq \frac{q}{2}$. Now, suppose that $q \geq 5$ is odd.

$$\Delta^{s} x_n = \sum_{j=0}^{s} a_j \Delta^{s} \binom{n+j}{j} = \sum_{j=0}^{s} a_j \binom{n+j}{j-s} = a_s$$

$a_s \neq 0$ since $(x-1)^{s+1}$ is the minimal polynomial of (x_n) .

$$\sum_{n=0}^{q-1} x_n^2 = \sum_{j,k=0}^{s} a_j a_k \sum_{n=0}^{q-1} \binom{n+j}{j}\binom{n+k}{k} \tag{3.14}$$

Fix $j,k \geq 0$ and let $\upsilon_n = \binom{n+j}{j}\binom{n+k}{k}$ $n \geq 0$. We consider υ_n as a sequence of elements in $\mathbb{F}_p$. Then $\Delta^{j+k} = \binom{j+k}{j}$ and $\Delta^{j+k+1} = 0$ for all $n \geq 0$ since υ_n can be viewed as a polynomial in n of degree $j+k$. By comparing the results above and (1.5),(3.12) we get,

$$\upsilon_n = \sum_{h=0}^{j+k} \binom{n+h}{h} b_h$$

for all $n \geq 0$ with $b_h \in \mathbb{F}_p$ and $b_{j+k} = \binom{j+k}{j}$. Therefore

$$\sum_{n=0}^{q-1} \binom{n+j}{j}\binom{n+k}{k} = \sum_{h=0}^{j+k} b_h \sum_{n=0}^{q-1} \binom{n+h}{h}$$

$$= \sum_{h=0}^{j+k} b_h \sum_{r=h}^{h+q-1} \binom{r}{h} = \sum_{h=0}^{j+k} b_h \binom{q+h}{h+1} \tag{3.15}$$

Let $e(r,m)$ be the largest exponent such that $p^{e(r,m)}$ divides $\binom{r}{m}$ where $r \geq m \geq 0$. Then by lemma 6.39 in [17],

$$\begin{aligned} e(r,m) &= E_p(r) - E_p(r-m) - E_p(m) \\ &= \frac{r - s(m) - (r-m) + s(r-m) - m + s(m)}{p-1} \\ &= \frac{s(m) + s(r-m) - s(r)}{p-1} \end{aligned}$$

where $s(n)$ is the sum of digits in the representation of n to the base p. $e(q+h, h+1) > 0$ for $0 \leq h < q-1$, hence $\binom{q+h}{h+1} = 0$ in $\mathbb{F}_p$ for $0 \leq h < q-1$ and the sum

$$\sum_{n=0}^{q-1} x_n^2 = \sum_{j,k=0}^{s} a_j a_k \sum_{h=0}^{j+k} b_h \binom{q+h}{h+1} = 0$$

for $0 \leq j+k < q-1$.

If we had $s = \frac{q-1}{2}$, then for $j = k = s$, $j + k = q - 1$ and for $h = j + k = q - 1$ the term $\binom{q+h}{h+1} \neq 0$ and

$$\sum_{n=0}^{q-1} x_n^2 = a_s^2 \sum_{n=0}^{q-1} \binom{n+s}{s}^2 = a_s^2 \binom{q-1}{\frac{q-1}{2}} \binom{2q-1}{q}$$

$e(q-1, \frac{q-1}{2}) = 0 = e(2q-1, q)$, hence $\sum_{n=0}^{q-1} x_n^2 \neq 0$. But, lemma 1.1.5 and $\{x_0, x_1, \ldots, x_{q-1}\} = \mathbb{F}_q$ implies

$$\sum_{n=0}^{q-1} x_n^2 = 0$$

which is a contradiction. So $s > \frac{q-1}{2}$, i.e, $s \geq \frac{q+1}{2}$.

□

Now, we characterize the generators (3.1) with prime modulus p and maximal period length which passes the d-dimensional lattice test for all $d \leq p-2$ by following the treatment of [12].

Theorem 3.1.12 *A nonlinear generator passes d-dimensional lattice test exactly for all dimensions*

$$d \leq max\{k \leq p-2 | \sum_{n \in \mathbb{F}_p} n^{p-1-k} x_n \not\equiv 0 \pmod{p}\}$$

Proof: Let g be the permutation polynomial over $\mathbb{F}_p$ defined by $g(n) = x_n$ where $n \in \mathbb{F}_p$. Then g can be written as

$$g(t) = \sum_{n \in \mathbb{F}_p} (1 - (t-n)^{p-1}) x_n$$

$$= \sum_{n \in \mathbb{F}_p} x_n - \sum_{n \in \mathbb{F}_p} \left(\sum_{k=0}^{p-1} (-1)^{p-1-k} \binom{p-1}{k} n^{p-1-k} t^j \right) x_n$$

By Lemma (1.1.5), $\sum_{n \in \mathbb{F}_p} x_n = 0$, hence the sum becomes

$$= \sum_{k=0}^{p-1} \left((-1)^{k+1} \binom{p-1}{k} \sum_{n \in \mathbb{F}_p} n^{p-1-k} x_n \right) t^k$$

By the same lemma, the term for $k = p-1$ is zero, therefore we get

$$g(t) = \sum_{k=0}^{p-2} \left((-1)^{k+1} \binom{p-1}{k} \sum_{n \in \mathbb{F}_p} n^{p-1-k} x_n \right) t^k$$

Hence

$$max\{k \leq p-2 | \sum_{n \in \mathbb{F}_p} n^{p-1-k} x_n \not\equiv 0 \pmod{p}\}$$

represents the degree of g. By Lemma 3.1.6 the generator passes the d-dimensional lattice test for all

$$d \leq max\{k \leq p-2 | \sum_{n \in \mathbb{F}_p} n^{p-1-k} x_n \not\equiv 0 \pmod{p}\}$$

□

Corollary 3.1.13 *A nonlinear congruential generator passes d-dimensional lattice test for all dimensions $d \leq p-2$ if and only if*

$$\sum_{n \in \mathbb{F}_p} n x_n \not\equiv 0 \pmod{p}$$

Now, we give an example of a generator which behaves optimally under d-dimensional lattice test although it is in fact an extremely bad generator. This demonstrates the weakness of the test and indicates that it should be applied in addition to other criteria for selecting good PRN generators.

Example 3.1.3 *The nonlinear generator which generates the sequence $(x_n)_{n \geq 0}$ with*

$$\{x_0, x_1, ..., x_{p-1}\} = \{0, 1, ..., p-3, p-2, p-1\}$$

passes d-dimensional lattice test for all dimensions $d \leq p-2$.

Proof:

$$\sum_{n\in\mathbb{F}_p} nx_n = \sum_{n=1}^{p-3} n^2 + 2(p-1)(p-2) \equiv -1 \pmod{p}$$

Therefore the generator passes d-dimensional lattice test for all $d \leq p-2$. But this generator shows extremely bad behaviour with respect to standard statistical tests for the randomness of uniform PRNs.

□

The inversive congruential generators with prime modulus do not show the lattice structure of the widely used linear congruential generator and they posses even a stronger property: any hyperplane in d-space contains at most d points generated generated by the inversive method. This was shown by Eichenauer-Herrmann in [2].

Let $p \geq 3$ be a prime number and denote by $\mathbb{Z}_{p,1} = \{1, 2, \ldots, p-1\}$ the set of positive integers less than p. For integers $a, b \in \mathbb{Z}_{p,1}$, an inversive congruential sequence $(x_n)_{n\geq 0}$ is obtained by the recursion

$$x_{n+1} \equiv \begin{cases} b & \text{if } x_n = 0 \\ ax_n^{-1} + b \pmod{p} & \text{if } x_n \neq 0 \end{cases} \tag{3.16}$$

$n \geq 0$ and $x_n \in \mathbb{Z}_{p,1}$. Suppose that the sequence defined has maximal period p.

Let $2 \leq d < p$ be an integer and define

$$V_d = \{(x_n, \ldots, x_{n+d-1}) \in \mathbb{Z}_p^d |\ x_n, \ldots, x_{n+d-2} \neq 0\ , 0 \leq n > p\}$$

the set of d-tuples of consecutive PRNs generated by the inversive congruential method, the d-tuples with zeros in the first $d-1$ coordinates are omitted. Let $\alpha_0, \ldots, \alpha_d \in \mathbb{Z}_p$ be arbitrary elements with $(\alpha_0, \ldots, \alpha_d) \neq (0, \ldots, 0)$. Then the set

$$H = \{(z_1, \ldots, z_d) \in \mathbb{Z}_p^d\ |\alpha_1 z_1 + \cdots + \alpha_d z_d \equiv \alpha_0\}$$

is a *hyperplane* in $\mathbb{Z}_p^d$.

To prove the main theorem we need auxiliary results. Let $\mathbb{Z}_{p,0} = \mathbb{Z}_p$. A function $f_1 : \mathbb{Z}_{p,1} \longrightarrow \mathbb{Z}_p$ is given by

$$f_1(x) \equiv ax^{-1} + b \pmod{p} .$$

For $2 \leq k < p$, the sets $\mathbb{Z}_{p,k}$ and the functions $f_k : \mathbb{Z}_{p,k} \to \mathbb{Z}_p$ are defined recursively by

$$\mathbb{Z}_{p,k} = \{x \in \mathbb{Z}_{p-1,k} |\ f_{k-1}(x) \not\equiv 0\}$$

and

$$f_k(x) = f_1(f_{k-1}(x))$$

Let $\pi_0 : \mathbb{Z}_p \to \mathbb{Z}_p$ be defined as $\pi_0(x) = x$ and for $1 \leq k < p$ define $\pi_k : \mathbb{Z}_{p,k} \to \mathbb{Z}_p$ by

$$\pi_k(x) \equiv x \prod_{j=1}^{k} f_j(x) \pmod{p}$$

A linear congruential sequence $(\tau_n)_{n\geq 0}$ in $\mathbb{Z}_p$ is given by $\tau_0 = 0$, $\tau_1 = 1$ and

$$\tau_n \equiv b\tau_{n-1} + a\tau_{n-2} \pmod{p} \ \ n \geq 2$$

and for $0 \leq k < p$, linear functions $\ell_k : \mathbb{Z}_p \to \mathbb{Z}_p$ are defined by

$$\ell_(x) \equiv \tau_{k+1}x + \tau_k a \pmod{p}$$

Lemma 3.1.14 *The function π_k is the restriction of the linear function ℓ_k to the set $\mathbb{Z}_{p,k}$ for $0 \leq k < p$, i.e, $\pi_k(x) = \ell_k(x)$ for $x \in \mathbb{Z}_{p,k}$*

Proof: The proof is by induction on k. For $k = 0$, $\pi_0(x) = x$ and $\ell_0(x) = \tau_1 x + \tau_0 a = x$. Hence their values are the same. Suppose that $\pi_k(x) = \ell_k(x)$ for some integer k

with $0 \leq k < p-1$ where $x \in \mathbb{Z}_{p,k}$. Then

$$\begin{aligned}
\pi_{k+1}(x) &\equiv x\prod_{j=1}^{k+1} f_j(x) \equiv x f_{k+1}(x) f_k(x) \dots f_2(x) f_1(x) \equiv x\pi_k(f_1(x)) \\
&\equiv \ell_k(f_1(x)) \equiv x(\tau_{k+1} f_1(x) + \tau_k a) \\
&\equiv x(\tau_{k+1}(ax^{-1} + b) + \tau_k a) \equiv \tau_{k+1} a + (\tau_{k+1} b + \tau_k a)x \\
&\equiv \ell_{k+1}(x)
\end{aligned}$$

for $x \in \mathbb{Z}_{p,k+1}$ since,

$$\begin{aligned}
f_{n+1}(x) &= f_1(f_n(x)) = \dots = f_1(f_1(\dots f_1(f_1(x))) \\
&= f_1(f_{n-1}(f_1(x))) = f_n(f_1(x))
\end{aligned}$$

for every $n \geq 1$.

□

$\tau_1, \tau_2, \dots, \tau_p \neq 0$, therefore $\xi_k \in \mathbb{Z}_p$ with $\xi_k \equiv -\tau_{k+1}^{-1}\tau_k a \pmod p$ is the unique zero of the linear function ℓ_k for $0 \leq k < p$.

Lemma 3.1.15 *The zeros $\xi_0, \dots, \xi_{p-1}$ of the linear functions $\ell_0, \dots, \ell_{p-1}$ are pairwise different, i.e, $\{\ell_0, \dots, \ell_{p-1}\} = \mathbb{Z}_p$*

Proof: Define elements $y_k \in \mathbb{Z}_p$ by $y_k \equiv \tau_{k+1}\tau_k^{-1} \pmod p$ for $1 \leq k \leq p$. Then

$$\begin{aligned}
y_{k+1} &\equiv \tau_{k+2}\tau_{k+1}^{-1} \equiv (b\tau_{k+1} + a\tau_k)\tau_{k+1}^{-1} \\
&\equiv b + a\tau_k\tau_{k+1}^{-1} \equiv a y_k^{-1} + b \pmod p
\end{aligned}$$

for $1 \leq k < p$.

$y_1 \equiv b \pmod p$ where $b \in \mathbb{Z}_{p,1}$ and the parameters a, b in the above equality are the same with the generator in (3.16) which has maximal period. This means $\{y_1, \dots, y_p\} = \{x_0, \dots, x_{p-1}\} = \mathbb{Z}_p$ but not necessarily in the same order, since the first elements may be different. Now,

$$\xi_k \equiv -\tau_{k+1}^{-1}\tau_k a \equiv b - y_k \pmod p$$

for $0 \leq k < p$, implies that $\xi_0, \ldots, \xi_{p-1}$ are pairwise different since $y_1, \ldots, y_p$ are pairwise different.

□

Let $\alpha_0, \alpha_1, \ldots, \alpha_d \in \mathbb{Z}_p$ such that $(\alpha_0, \alpha_1, \ldots, \alpha_d) \neq (0, 0, \ldots, 0)$ and let $P_d : \mathbb{Z}_p \to \mathbb{Z}_p$ be a polynomial defined by

$$P_d(x) \equiv (\alpha_1 x - \alpha_0) \prod_{j=0}^{d-2} \ell_j(x) + \sum_{k=2}^{d} \alpha_k \ell_{k-1}(x) \prod_{\substack{j=0 \\ j \neq k-2}}^{d-2} \ell_j(x) \pmod{p}$$

Lemma 3.1.16 *The polynomial has at most d zeros.*

Proof: First of all we should show that the polynomial above is not identically zero. Suppose that $P_d(x) = 0$ for all $x \in \mathbb{Z}_p$. Now consider $P_d(\xi_i)$. By our assumption $P_d(\xi_i) = 0$ but also for $0 \leq i \leq d-2$

$$P_d(\xi_i) \equiv \alpha_{i+2} \ell_{i+1}(\xi_i) \prod_{\substack{j=0 \\ j \neq i}}^{d-2} \ell_j(x) \pmod{p}$$

since ξ_i is the zero of the $\ell_i(x)$ and for only $k = i+2$, $P_d(\xi_i)$ has nonzero summands. Therefore our assumption and lemma 3.1.15 implies that $\alpha_{i+2} = 0$ for $0 \leq i \leq d-2$ and hence

$$P_d(x) \equiv (\alpha_1 x - \alpha_0) \prod_{j=0}^{d-2} \ell_j(x) \pmod{p}$$

for $x \in \mathbb{Z}_p$. From our assumption, it follows that $P_d(\xi_{d-1}) = P_d(\xi_d) = 0$ and lemma 3.1.15 implies that $\alpha_0 = \alpha_1 = 0$. But this contradicts $(\alpha_0, \alpha_1, \ldots, \alpha_d) \neq (0, 0, \ldots, 0)$ and shows that the polynomial $P_d(x)$ is not identically zero. Since the degree of $P_d(x)$ is at most d, it can have at most d zeros.

□

Now, we can prove the main theorem in [2]

Theorem 3.1.17 *Any hyperplane H in $\mathbb{Z}_p^d$ contains at most d points of the set V_d.*

Proof: $x \in \mathbb{Z}_{p,d-1}$ implies $x \neq 0$ and $f_k(x) \neq 0$ for $1 \leq k \leq d-2$. Furthermore, x together with $f_k(x)$ for $1 \leq k \leq d-1$ defines d consecutive elements of the sequence in (3.16) since $f_k(x) = f_1(f_{k-1}(x))$. Hence we can write the set V_d as

$$V_d = \{(x, f_1(x), \ldots, f_{d-1}(x)) \in \mathbb{Z}_p^d \mid x \in \mathbb{Z}_{p,d-1}\}$$

Therefore

$$\#\,(H \cap V_d) = \#\,\{x \in \mathbb{Z}_{p,d-1} \mid \alpha_1 x + \alpha_2 f_1(x) + \cdots + \alpha_d f_{d-1}(x) \equiv \alpha_0 \pmod p\}$$

$$= \#\{x \in \mathbb{Z}_{p,d-1} \mid (\alpha_1 x + \alpha_2 f_1(x) + \cdots + \alpha_d f_{d-1}(x)) \prod_{j=0}^{d-2} \pi_j(x) \equiv \alpha_0 \prod_{j=0}^{d-2} \pi_j(x) \pmod p\}$$

$$= \#\{x \in \mathbb{Z}_{p,d-1} \mid (\alpha_1 x - \alpha_0) \prod^{d-2} \pi_j(x) + \sum_{k=2}^{d} \alpha_k f_{k-1}(x) \pi_{k-2}(x) \prod_{\substack{j=0 \\ j \neq k-2}}^{d-2} \pi_j(x) \equiv 0 \pmod p\}$$

$$= \#\{x \in \mathbb{Z}_{p,d-1} \mid (\alpha_1 x - \alpha_0) \prod^{d-2} \pi_j(x) + \sum_{k=2}^{d} \alpha_k \pi_{k-1}(x) \prod_{\substack{j=0 \\ j \neq k-2}}^{d-2} \pi_j(x) \equiv 0 \pmod p\}$$

for any hyperplane H in $\mathbb{Z}_p^d$. By lemma 3.1.14 $\pi_j(x) = \ell_j(x)$ for $0 \leq j \leq d-1$, since $x \in \mathbb{Z}_{p,d-1}$. So, the elements in $\mathbb{Z}_{p,d-1}$ that satisfies the last statement are just the zeros of the polynomial $P_d(x)$ and by lemma 3.1.16, the number of zeros can not exceed d. Therefore $\#(H \cap V_D) \leq d$.

□

This result shows that inversive congruential generators do not fall on the planes in contrast to the linear congruential method. Hence, they are suitable for simulation problems which require random irregularities.

3.2. Estimates For The Discrepancy Of The Inversive Congruential Generators

3.2.1. Upper Bounds

In this section, the statistical independence properties of the PRNs with prime modulus generated by (3.16) will be studied. A reliable theoretical test for the statistical independence is the *serial test* which employs the *discrepancy* of tuples of successive PRNs. For a given dimension $k \geq 2$ and arbitrary N points $\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}} \in [0,1)^k$ the *discrepancy* is defined by

$$D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}) = \sup_J |F_N(J) - V(J)|$$

where the supremum is taken over all subintervals J of $[0,1)^k$, $F_N(J)$ is N^{-1} times the number of terms among $\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}}$ in J and $V(J)$ is the volume of J. If $x_0, x_1, \ldots,$ is a sequence of uniform PRNs in $[0,1)$ which is purely periodic with period τ, then we consider the points

$$\mathbf{x_n} = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in [0,1)^k$$

for $n = 0, 1, \ldots, \tau - 1$ and we write $D_\tau(k) = D_\tau(\mathbf{x_0}, \mathbf{x_1}, \ldots, \mathbf{x_{\tau-1}})$ for their discrepancy. The PRNs x_n pass the k-dimensional series test over the full period if $D_\tau(k)$ is reasonably small.

Consider the generator in (3.16) with prime modulus $p \geq 5$. Suppose that $a, b \in \mathbb{F}_p$ are chosen such that $f(x) = x^2 - bx - a$ is a primitive polynomial. Then the period length of the sequence is p.

We will derive an upper bound for the discrepancy $D_p(k)$ by using the results in Niederreiter [23]. Let $y_n = \frac{x_n}{p}$, then we get a sequence of uniform PRNs $y_0, y_1, \ldots$.

Let $m \geq 2$ and $k \geq 1$ be integers and let $C_k(m)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-m/2 < h_j \leq m/2$ for 1 $leqj \leq k$. We put

$$r(h,m) = \begin{cases} 1 & for\ h\ =\ 0 \\ m \sin \frac{\pi |h|}{m} & for\ h \in C_1(m) \end{cases}$$

and for $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(m)$ we define

$$r(\mathbf{h}, m) = \prod_{j=1}^{k} r(h_j, m)$$

For $t \in \mathbb{R}$, we write $e(t) = e^{2\pi i t}$. Let $\mathbf{x} \cdot \mathbf{y}$ denote the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbb{R}^k$.

Lemma 3.2.18 *Let $m \geq 2$ be an integer and let $\mathbf{x_0}, \mathbf{x_1}, \ldots, \mathbf{x_{N-1}} \in \mathbb{Z}^k$ with $k \geq 2$ be the lattice points, all of whose coordinates are in $[0, m)$. Then the discrepancy of the points $\mathbf{t_n} = m^{-1}\mathbf{x_n}$ for $0 \leq n \leq N-1$ satisfies*

$$D_N(\mathbf{t_0}, \ldots, \mathbf{t_{N-1}}) \leq \frac{k}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_k(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) \right|$$

Lemma 3.2.19 *For any integer $m \geq 2$, we have*

$$\sum_{h \in C_1(m)} \frac{1}{r(h,m)} < \frac{2}{\pi} \log m + \frac{2}{5}$$

Let χ be the canonical additive character of $\mathbb{F}_p$ defined by $\chi(n) = e(n/p)$ for $n \in \mathbb{F}_p$.

Lemma 3.2.20 *For polynomials $Q, R \in \mathbb{F}_p[x]$ with $1 \leq deg(R) < deg(Q) < p$ we have*

$$\left| \sum_{\substack{n\in\mathbb{F}_p \\ R(n)\neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| \leq \left(r-2+\sum_{i=1}^{r} m_i\right) p^{1/2}$$

where r is the number of distinct poles of Q/R in the algebraic closure $\overline{\mathbb{F}_P}$ (including the point at infinity) and $m_1, \ldots, m_r$ are the multiplicities of the poles.

The proofs of the above lemmas can be found in [20, section 2] .

Theorem 3.2.21 *For PRNs derived from inversive generator and for $2 \leq k < p$ we have*

$$D_p^{(k)} < 2p^{-1/2}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{2k-7}{5}\right)+2p^{-1/2}+$$

$$+\frac{1}{p}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{12k-7}{5}\right)$$

Proof: Define $\psi : \mathbb{F}_p \to \mathbb{F}_p$ by $\psi(n) = an^{-1} + b$ for $n \in \mathbb{F}_p$ and let ψ^j be the jth iterate of ψ and $\psi^0(n) = n$. Then

$$\begin{aligned}&\{(x_n, x_{n+1}, \ldots, x_{n+k-1}) : 0 \leq n \leq p-1\}\\ &= \{(\psi^0(x_n), \psi^1(x_n), \ldots, \psi^{k-1}(x_n)) : 0 \leq n \leq p-1\}\end{aligned}$$

and by lemma 3.2.18

$$D_p^{(k)} = D_p(\mathbf{y_o}, \mathbf{y_1}, \ldots, \mathbf{y_{n+p-1}}) \leq \frac{k}{p}+\frac{1}{p}\sum_{\mathbf{h}\in C_k(p)}\frac{1}{r(\mathbf{h},p)}\left|\sum_{n=0}^{p-1} e(\mathbf{h}\cdot\mathbf{y_n})\right|$$

$$\begin{aligned}\sum_{n=0}^{p-1} e(\mathbf{h}\cdot\mathbf{y_n}) &= \sum_{n=0}^{p-1} e\left(\sum_{j=1}^{k} h_j\frac{x_{n+j-1}}{p}\right) = \sum_{n=0}^{p-1} e\left(\sum_{j=1}^{k} h_j\frac{\psi^{j-1}(x_n)}{p}\right)\\ &= \sum_{n=0}^{p-1}\chi\left(\sum_{j=1}^{k} h_j\psi^{j-1}(x_n)\right)\end{aligned}$$

For $\mathbf{h} = (h_1, \ldots, h_k) \in C_k(p)$

$$S(\mathbf{h}) = \sum_{n \in \mathbb{F}_p} \chi \left(\sum_{j=1}^{k} h_j \psi^{j-1}(n) \right)$$

Therefore $\{x_0, x_1, \ldots, x_{p-1}\} = \mathbb{F}_p$ implies

$$S(\mathbf{h}) = \sum_{n=0}^{p-1} \chi \left(\sum_{j=1}^{k} h_j \psi^{j-1}(x_n) \right) = \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{y_n})$$

Hence,

$$D_p^{(k)} \leq \frac{k}{p} + \frac{1}{p} \sum_{\mathbf{h} \in C_k(p)} \frac{1}{r(\mathbf{h}, p)} |S(\mathbf{h})|$$

For fixed $\mathbf{h} \in C_k(p)$ let m be the number of nonzero coordinates of $\mathbf{h}$, then $1 \leq m \leq k$. If $m = 1$, then

$$S(\mathbf{h}) = \sum_{n \in \mathbb{F}_p} \chi(h_j \psi^{j-1}(n)) = \sum_{n \in \mathbb{F}_p} \chi(h_j n) = 0 \ ,$$

since ψ^j is a permutation of $\mathbb{F}_p$ for all $j \geq 0$. If $2 \leq m \leq k$, let $1 \leq i_1 < i_2 < \cdots < i_m \leq k$ such that $h_{i_1} \neq 0, \ldots, h_{i_m} \neq 0$. Then

$$S(\mathbf{h}) = \sum_{n \in \mathbb{F}_p} \chi \left(\sum_{t=1}^{m} h_{i_t} \psi^{i_t - 1}(n) \right) = \sum_{n \in \mathbb{F}_p} \chi \left(\sum_{t=1}^{m} h_{i_t} \psi^{i_t - i_1}(n) \right) \tag{3.17}$$

since for each$j \geq 0$, ψ^j defines a permutation of $\mathbb{F}_p$, we can write $\psi^{i_1 - 1}(n)$ instead of n .

Let $c_j \in \mathbb{F}_p$ be defined by $c_0 = 0$, $c_1 = 1$ and $c_{j+2} = bc_{j+1} + ac_j$ for $j \geq 0$. Since $f(x) = x^2 - bx - a$ is primitive over $\mathbb{F}_p$, we have $c_j \neq 0$ for $1 \leq j \leq p$. In fact, (c_j) is a second order homogeneous linear recurring sequence with characteristic polynomial $f(x)$. Then by applying a similar method as in chapter 2, we can see that $c_j = \frac{(\gamma^p)^j - \gamma^j}{\gamma^p - \gamma}$ where $\gamma \in \mathbb{F}_{p^2}$ is a root of $f(x)$. Since $f(x)$ is primitive over $\mathbb{F}_p$, $c_j = 0$ when j is a multiple of $p + 1$ hence the result follows.

Now, by induction on j we will show that,

$$\psi^j(n) = \frac{nc_{j+1} + ac_j}{nc_j + ac_{j-1}}$$

for $1 \leq j \leq p$, where $n \neq ac_{i-1}c_i^{-1}$ for $1 \leq i \leq j$. For $j = 1$,

$$\frac{nc_2 + ac_1}{nc_1 + ac_0} = \frac{nb + a}{n} = an^{-1} + b = \psi^1(n)$$

where, $n \neq 0$. Suppose that

$$\psi^j(n) = \frac{nc_{j+1} + ac_j}{nc_j + ac_{j-1}}$$

for some $1 \leq j \leq p-1$, where $n \neq -ac_{i-1}c_i^{-1}$ for $1 \leq i \leq j$.

$$\begin{aligned} \psi^{j+1}(n) &= \psi(\psi^j(n)) = a(\psi^j(n))^{-1} + b \\ &= a\,\frac{nc_j + ac_{j-1}}{nc_{j+1} + ac_j} + b = \frac{n(ac_j + bc_{j+1}) + a(ac_{j-1} + bc_j)}{nc_{j+1} + ac_j} \\ &= \frac{nc_{j+2} + ac_{j+1}}{nc_{j+1} + ac_j} \end{aligned}$$

where $n \neq -ac_{j+1}c_j^{-1}$.

Define the rational function

$$\frac{Q(x)}{R(x)} = h_{i_1}x + \sum_{t=2}^{m} \frac{xc_{i_t - i_1 + 1} + ac_{i_t - i_1}}{xc_{i_t - i_1} + ac_{i_t - i_1 - 1}}$$

with

$$R(x) = \prod_{t=2}^{m} (xc_{i_t - i_1} + ac_{i_t - i_1 - 1})$$

Then, by theorem 1 in [23], we obtain

$$|S(\mathbf{h})| \leq 2(i_m - i_1) - (m-1) + \left| \sum_{\substack{n \in \mathbb{F}_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right|$$

Q/R has at most $deg(R) = m-1$ finite poles and since $deg(Q) = deg(R) + 1$, it has a pole at infinity with multiplicity 1. Since $deg(R) < deg(Q) = m \leq k < p$, we can apply lemma 3.2.20 and this implies that

$$|S(\mathbf{h})| \leq (2m-2)p^{1/2} + 2(i_m - i_1) - (m-1)$$

Finally, $i_m - i_1 \leq k-1$ yields

$$|S(\mathbf{h})| \leq (2m-2)p^{1/2} + 2k - m - 1$$

From this result we get that

$$\Sigma := \sum_{\mathbf{h}\in C_k(p)} \frac{1}{r(\mathbf{h},p)} |S(\mathbf{h})| = \sum_{m=1}^{k} \frac{1}{\prod_{t=1}^{m} r(h_{i_t},p)} |S(\mathbf{h})|$$

$$\leq \sum_{m=1}^{k} \sum_{1\leq i_1<i_2<\cdots<i_m\leq k} \left(\sum_{h\in C_1(p)} \frac{1}{r(h,p)} \right)^m |S(\mathbf{h})|$$

For $m = 1$, $|S(\mathbf{h})| = 0$ hence we can write

$$\leq \sum_{m=2}^{k} \sum_{1\leq i_1<i_2<\cdots<i_m\leq k} \left(\sum_{h\in C_1(p)} \frac{1}{r(h,p)} \right)^m |S(\mathbf{h})|$$

$$\leq \sum_{m=2}^{k} \sum_{1\leq i_1<i_2<\cdots<i_m\leq k} \left(\sum_{h\in C_1(p)} \frac{1}{r(h,p)} \right)^m ((2m-2)p^{1/2} + 2k - m - 1)$$

then applying lemma 3.2.19 yields

$$< \sum_{m=2}^{k} \sum_{1\leq i_1<i_2<\cdots<i_m\leq k} \left(\frac{2}{\pi}\log p + \frac{2}{5} \right)^m ((2m-2)p^{1/2} + 2k - m - 1)$$

$$= (2p^{1/2}-1) \sum_{m=1}^{k} m\binom{k}{m} \left(\frac{2}{\pi}\log p + \frac{2}{5} \right)^m - 2p^{1/2} \left((\frac{2}{\pi}\log p + \frac{7}{5})^k - 1 \right)$$

$$+(2k-1) \left((\frac{2}{\pi}\log p + \frac{7}{5})^k - 1 \right)$$

Let $G(z) = \sum_{m=1}^{k} \binom{k}{m} z^m$. Then

$$G(z) = (1+z)^k - 1$$

and

$$zG'(z) = \sum_{m=1}^{k} m\binom{k}{m} z^m = kz(1+z)^{k-1} .$$

Therefore

$$\sum_{m=1}^{k} m\binom{k}{m}\left(\frac{2}{\pi}\log p+\frac{2}{5}\right)^{m}=k\left(\frac{2}{\pi}\log p+\frac{2}{5}\right)\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}$$

and hence

$$\Sigma<(2p^{1/2}-1)k(\frac{2}{\pi}\log p+\frac{2}{5})(\frac{2}{\pi}\log p+\frac{2}{5})^{k-1}-2p^{1/2}\left((\frac{2}{\pi}\log p+\frac{7}{5})^{k}-1\right)+$$

$$(2k-1)\left((\frac{2}{\pi}\log p+\frac{7}{5})^{k}-1\right)$$

With simple manipulations,

$$\Sigma<2p^{1/2}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{2k-7}{5}\right)+2p^{1/2}+$$

$$\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{12k-7}{5}\right)-2k+1$$

Hence,

$$D_p^{(}k)\leq\frac{k}{p}\ +\ \frac{1}{p}\Sigma<2p^{-1/2}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{2k-7}{5}\right)+2p^{-1/2}+$$

$$\frac{1}{p}\left(\frac{2}{\pi}\log p+\frac{7}{5}\right)^{k-1}\left(\frac{2k-2}{\pi}\log p+\frac{12k-7}{5}\right)+\frac{1-k}{p}$$

Since $\frac{1-k}{p}<0$ we get the desired result.

□

3.2.2. Lower bounds

In the preceeding paragraphs it was shown that $D_p^{(k)} = O(p^{-1/2}(\log p)^k)$ for $2 \leq k < p$. In the following paragraphs, lower bounds for $D_p^{(k)}$ which was obtained in Niederreiter [24] will be given.

For a prime $p \geq 5$, choose $a, b \in \mathbb{F}_p$ in such a way that the polynomial $x^2 - bx + a$ is primitive over $\mathbb{F}_p$. Then a sequence $x_0, x_1, \ldots$ is generated by the inversive recursion

$$x_{n+1} \equiv -ax_n^{-1} + b \pmod{p}\ , for n = 0, 1, \ldots$$

The numbers $y_n = \frac{x_n}{p}$, $n = 0, 1, \ldots$ in the interval $[0, 1)$ are called the *inversive congruential PRNs*. The sequence is purely periodic with period p .

We write $e(u) = e^{2\pi i u}$ for $u \in \mathbb{R}$ and $\mathbf{u} \cdot \mathbf{v}$ denotes the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$.

Lemma 3.2.22 *Let* $\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}} \in [0, 1)^k$, $k \geq 1$ *with discrepancy*

$$D_N = D_N(\mathbf{t_0}, \mathbf{t_1}, \ldots, \mathbf{t_{N-1}})\ .$$

Then for any nonzero $\mathbf{h} = (h_1, \ldots, h_k) \in \mathbb{Z}^k$,

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) \right| \leq \frac{2}{\pi} \left(\left(\frac{\pi + 1}{2} \right)^m - \frac{1}{2^m} \right) N D_N \prod_{j=1}^{k} \max(1, 2|h_j|)\ ,$$

where m *is the number of nonzero coordinates of* $\mathbf{h}$.

Proof: Since the sum above is a complex number we can write it as:

$$\sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) = e(\theta) \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) \right|$$

for some $\theta \in \mathbb{R}$. So,

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) \right| = e(-\theta) \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) = \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n} - \theta)$$

By looking at the real parts, we get

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t_n}) \right| = \sum_{n=0}^{N-1} \cos 2\pi(\mathbf{h} \cdot \mathbf{t_n} - \theta) \leq \frac{2}{\pi} \left(\left(\frac{\pi + 1}{2} \right)^m - \frac{1}{2^m} \right) N D_N \prod_{j=1}^{k} \max(1, 2|h_j|)$$

where the last step follows from p/64, Niederreiter, [21]

□

For a nontrivial additive character χ of $\mathbb{F}_q$ and for $a \in \mathbb{F}_q^*$, we define the following character sum

$$K(\chi, a) = \sum_{c \in \mathbb{F}_q} \chi(c + ac^{-1})$$

Consider $\overline{K}(\chi, a)$ where $\overline{K}$ represents the complex conjugate of K. Then

$$\overline{K}(\chi, a) = \sum_{-c \in \mathbb{F}_q} \chi(-c + a(-c)^{-1}) = K(\chi, a)$$

since $-c$ runs through the elements of $\mathbb{F}_q$ when c runs through the elements of $\mathbb{F}_q$. Hence, $K(\chi, a)$ is always real.

Lemma 3.2.23 *For any nontrivial additive χ we have,*

$$\sum_{a \in \mathbb{F}_q^*} K(\chi, a)^2 = q^2$$

Proof:

$$\begin{aligned}
\sum_{a \in \mathbb{F}_q^*} K(\chi, a)^2 &= \sum_{a \in \mathbb{F}_q^*} \left(\sum_{c \in \mathbb{F}_q} \chi(c + ac^{-1}) \sum_{d \in \mathbb{F}_q} \chi(d + ad^{-1}) \right) \\
&= \sum_{a \in \mathbb{F}_q^*} \left(\sum_{c,d \in \mathbb{F}_q} \chi(c + ac^{-1}) \chi(d + ad^{-1}) \right) \\
&= \sum_{a \in \mathbb{F}_q^*} \left(\sum_{c,d \in \mathbb{F}_q} \chi(c + d) \chi(a(c^{-1} + d^{-1})) \right) \\
&= \sum_{c,d \in \mathbb{F}_q} \left(\chi(c + d) \sum_{a \in \mathbb{F}_q^*} \chi(a(c^{-1} + d^{-1})) \right)
\end{aligned}$$

since χ is an additive character. If $c^{-1} + d^{-1} \neq 0$, then

$$\sum_{a \in \mathbb{F}_q} \chi(a(c^{-1} + d^{-1})) = 0$$

together with $\chi(a(c^{-1} + d^{-1})) = 1$ when $a = 0$, implies that

$$\sum_{a \in \mathbb{F}_q^*} \chi(a(c^{-1} + d^{-1})) = -1$$

If $c^{-1}+d^{-1}=0$, then for all $a \in \mathbb{F}_q^*$, $\chi(a(c^{-1}+d^{-1}))=1$, hence

$$\sum_{a\in\mathbb{F}_q^*} \chi(a(c^{-1}+d^{-1})) = q-1$$

$$\begin{aligned}\sum_{a\in\mathbb{F}_q^*} K(\chi,a)^2 &= (q-1)q - \sum_{\substack{c,d\in\mathbb{F}_q \\ c^{-1}+d^{-1}\neq 0}} \chi(c+d) \\ &= (q-1)q - \sum_{c,d\in\mathbb{F}_q} \chi(c+d) + q = q^2\end{aligned}$$

since there are q pairs $(c,d) \in \mathbb{F}_q^2$ with $c^{-1}+d^{-1}=0$ and $\sum_{c,d\in\mathbb{F}_q} \chi(c+d)=0$.

□

Let ψ be a nontrivial multiplicative character of $\mathbb{F}_q$. For ψ, the Gaussian sum is defined as

$$G(\psi,\chi) = \sum_{c\in\mathbb{F}_q^*} \psi(c)\chi(c)$$

and the Jacobi sum on $\mathbb{F}_q$ is defined as

$$J(\psi) = \sum_{c_1+c_2=1} \psi(c_1)\psi(c_2) = \sum_{c\in\mathbb{F}_q} \psi(c(1-c))$$

with $J(0)=0$. The conjugate character ψ^{-1} is defined by $\psi^{-1}(c)=\psi(c^{-1})$ for $c\in\mathbb{F}_q$. $\psi(cd)=\psi(c)\psi(d)$ for all $c,d\in\mathbb{F}_q$ and $\sum_{c\in\mathbb{F}_q}\psi(c)=0$

Lemma 3.2.24 *For any nontrivial χ and ψ,*

$$\sum_{c,d\in\mathbb{F}_q} \chi(c+d)\psi^{-1}(c^{-1}+d^{-1}) = G(\psi,\chi)(J(\psi)+2)$$

Proof: Let $c,d\in\mathbb{F}_q$.

$$\psi^{-1}(c^{-1}+d^{-1}) = \psi(c)+\psi(d)$$

if $c=0$ or $d=0$ by the conventions $0^{-1}=0$ and $\psi(0)=0$. When both c and d are nonzero,

$$\psi^{-1}(c^{-1}+d^{-1}) = \psi^{-1}((c+d)(cd)^{-1}) = \psi((cd)(c+d)^{-1}) = \psi(cd)\psi^{-1}(c+d)$$

So we can write

$$\psi^{-1}(c^{-1}+d^{-1}) = \begin{cases} \psi^{-1}(c+d)\psi(cd) & \text{if } cd \neq 0 \\ \\ \psi(c)+\psi(d) & \text{if } cd = 0 \end{cases}$$

So,

$$\sum_{c,d\in\mathbb{F}_q} \chi(c+d)\psi^{-1}(c^{-1}+d^{-1})$$

$$= \sum_{c,d\in\mathbb{F}_q^*} \chi(c+d)\psi^{-1}(c+d)\psi(cd) + \sum_{c\in\mathbb{F}_q} \chi(c)\psi^{-1}(c^{-1}) + \sum_{d\in\mathbb{F}_q} \chi(d)\psi^{-1}(d^{-1})$$

$$= \sum_{c,d\in\mathbb{F}_q^*} \chi(c+d)\psi^{-1}(c+d)\psi(cd) + 2G(\psi,\chi)$$

since $\psi^{-1}(c^{-1}) = \psi(c)$ and $\psi^{-1}(d^{-1}) = \psi(d)$. Therefore,

$$\sum_{c,d\in\mathbb{F}_q} \chi(c+d)\psi^{-1}(c^{-1}+d^{-1}) = \sum_{c,d\in\mathbb{F}_q} \chi(c+d)\psi^{-1}(c+d)\psi(cd) + 2G(\psi,\chi)$$

because $\psi(0) = 0$. By substituting $c+d=f$, we get

$$\begin{aligned} \sum_{c,d\in\mathbb{F}_q} \chi(c+d)\psi^{-1}(c+d)\psi(cd) &= \sum_{c,f\in\mathbb{F}_q} \chi(f)\psi^{-1}(f)\psi(c(f-c)) \\ &= \sum_{f\in\mathbb{F}_q^*} \chi(f)\psi^{-1}(f) \sum_{c\in\mathbb{F}_q} \psi(cf(f-cf)) \\ &= \sum_{f\in\mathbb{F}_q^*} \chi(f)\psi(f) \sum_{c\in\mathbb{F}_q} \psi(c(1-c)) \\ &= G(\psi,\chi)J(\psi) \end{aligned}$$

□

The group of multiplicative characters of $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q^*$ and therefore it is cyclic of order $q-1$. Let $H_q(m)$ be the set of multiplicative characters of order m where m is a positive divisor of $q-1$. Let P_q be the set of primitive elements of $\mathbb{F}_q$.

Lemma 3.2.25 *For any nontrivial χ,*

$$\sum_{a\in P_q} K(\chi,a)^2 = \frac{\phi(q-1)}{q-1}q^2 + \frac{\phi(q-1)}{q-1}$$

$$\cdot \sum_{\substack{m|q-1\\ m>1}} \frac{\mu(m)}{\phi(m)} \sum_{\psi\in\mathbb{H}_q(m)} G(\psi,\chi)^2(J(\psi)+2)$$

where μ is the Moebius function.

Proof: By the result of problem 5.14 on page 258 of [17],

$$\frac{\phi(q-1)}{q-1}\sum_{m|q-1}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\psi(q) = \begin{cases} 1 & if a\in P_q \\ 0 & otherwise \end{cases}$$

Therefore

$$\sum_{a\in P_q} K(\chi,a)^2 = \sum_{a\in\mathbb{F}_q^*}\left(\frac{\phi(q-1)}{q-1}\sum_{m|q-1}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\psi(a)\right)K(\chi,a)^2 .$$

Let $A = \frac{\phi(q-1)}{q-1}\sum_{m|q-1}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\psi(a)$. In the above equality we were able to extend the summation from P_q to $\mathbb{F}_q^*$, since $P_q\subset\mathbb{F}_q^*$ and for elements of $\mathbb{F}_q^*$ that are not in P_q , $A=0$ and for elements of P_q , $A=1$. Hence,

$\sum_{a\in P_q} K(\chi,a)^2$

$$= \frac{\phi(q-1)}{q-1}\sum_{m|q-1}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\sum_{a\in\mathbb{F}_q^*}\psi(a)K(\chi,a)^2$$

$$= \frac{\phi(q-1)}{q-1}\sum_{\substack{m|q-1\\ m\neq 1}}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\sum_{a\in\mathbb{F}_q^*}\psi(a)K(\chi,a)^2 + \frac{\phi(q-1)}{q-1}\sum_{a\in\mathbb{F}_q^*}K(\chi,a)^2$$

since there is only one character with order 1, ψ_0 and it satisfies $\psi_0(a)=1$ for all $a\in\mathbb{F}_q^*$. Then by applying lemma 3.2.23, we get

$$\sum_{a\in P_q} K(\chi,a)^2 = q^2\frac{\phi(q-1)}{q-1} + \sum_{\substack{m|q-1\\ m>1}}\frac{\mu(m)}{\phi(m)}\sum_{\psi\in H_q(m)}\sum_{a\in\mathbb{F}_q^*}\psi(a)K(\chi,a)^2$$

For any nontrivial ψ,

$$\sum_{a\in\mathbb{F}_q^*}\psi(a)K(\chi,a)^2=\sum_{a\in\mathbb{F}_q^*}\psi(a)\sum_{c,d\in\mathbb{F}_q}\chi(c+d+a(c^{-1}+d^{-1}))\ .$$

χ is an additive character implies that

$$\chi(c+d+a(c^{-1}+d^{-1}))=\chi(c+d)\chi(a(c^{-1}+d^{-1}))$$

Hence,

$$\sum_{a\in\mathbb{F}_q^*}\psi(a)K(\chi,a)^2=\sum_{c,d\in\mathbb{F}_q}\chi(c+d)\sum_{a\in\mathbb{F}_q^*}\psi(a)\chi(a(c^{-1}+d^{-1}))$$

$$=\sum_{\substack{c,d\in\mathbb{F}_q\\ c^{-1}+d^{-1}=0}}\chi(c+d)\sum_{a\in\mathbb{F}_q^*}\psi(a)\ +\sum_{\substack{c,d\in\mathbb{F}_q\\ c^{-1}+d^{-1}\neq 0}}\chi(c+d)\sum_{a\in\mathbb{F}_q^*}\psi(a)\chi(a(c^{-1}+d^{-1}))$$

$\sum_{a\in\mathbb{F}_q^*}\psi(a)=0$, hence the above sum becomes

$$=\sum_{\substack{c,d\in\mathbb{F}_q\\ c^{-1}+d^{-1}\neq 0}}\chi(c+d)\sum_{a\in\mathbb{F}_q^*}\psi(a)\psi^{-1}(c^{-1}+d^{-1})\chi(a)$$

$$=G(\psi,\chi)\sum_{c,d\in\mathbb{F}_q}\chi(c+d)\psi^{-1}(c^{-1}+d^{-1})=G(\psi,\chi)^2(J(\psi)+2)$$

where lemma 3.2.24 is used in the last step.

□

Lemma 3.2.26 *For any nontrivial χ there exists an $a\in P_q$ with*

$$|K(\chi,a)|>q^{1/2}-2q^{2/5}\ .$$

Proof: For nontrivial ψ,χ we have $|G(\psi,\chi)|=q^{1/2}$ and $|J(\psi)|\leq q^{1/2}$ by theorems (1.1.5) and (1.1.6), respectively . Since the group of multiplicative characters of $\mathbb{F}_q$ is cyclic, $\#H_q(m)=\phi(m)$ and therefore

$$\sum_{\psi\in H_q(m)}G(\psi,\chi)^2(J(\psi)+2)\leq\phi(m)q(q^{1/2}+2)$$

By lemma 3.2.25 and the above equality,

$$\sum_{a\in P_q} K(\chi,a)^2 \geq \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2)\sum_{\substack{m|q-1\\ m>1}} |\mu(m)|$$

$$> \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2)\sum_{m|q-1} |\mu(m)|$$

since $\mu(1)=1$. Let $\omega(q-1)$ be the number of different prime factors of $q-1$ and let $q-1 = p_1^{k_1}\dots P_{\omega(q-1)}^{k_{\omega(q-1)}}$ be the prime decomposition of $q-1$. Then

$$\sum_{d|q-1} |\mu(d)| = 1 + \sum_i \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + \dots$$

$$= 1 + \binom{\omega(q-1)}{1} + \dots + \binom{\omega(q-1)}{\omega(q-1)} = 2^{\omega(q-1)} .$$

So we obtain,

$$\sum_{a\in P_q} K(\chi,a)^2 > \frac{\phi(q-1)}{q-1}q^2 - \frac{\phi(q-1)}{q-1}q(q^{1/2}+2)2^{\omega(q-1)} \tag{3.18}$$

Now, we want to show that $2^{\omega(m)} < (2.4)m^{0.357}$ for any positive integer m . For $m=1,\ \omega(m)=0$ and $2^{\omega(m)}=1<2.4$. For $m>1$, let $m = p_1^{e_1}\dots p_r^{e_r}$ be the prime factorization of m . Then

$$2^{\omega(m)} = 2^r = m^{(\log 2)/\log 7}\frac{2^r}{(p_1^{e_1}\dots p_r^{e_r})^{(\log 2)/\log 7}}$$

$$= m^{(\log 2)/\log 7}\prod_{j=1}^{r}\frac{2}{p_j^{e_j(\log 2)/log7}} < m^{0.357}\prod_{j=1}^{r}\frac{2}{p_j^{(\log 2)/log7}}$$

For $p_j \geq 7$

$$\frac{2}{p_j^{(\log 2)/\log 7}} < 1$$

so

$$m^{0,357}\prod_{j=1}^{r}\frac{2}{p_j^{(\log 2)/\log 7}} < m^{0,357}\frac{2^3}{(2\cdot 3\cdot 5)^{\log 2/\log 7}}$$

Hence,

$$2^{\omega(m)} < \frac{8}{30^{(\log 2)/\log 7}} m^{0,357} < (2,4)m^{0,357}$$

and

$$\sum_{a \in P_q} K(\chi, a)^2 > \frac{\phi(q-1)}{q-1} q(q - (2,4)q^{0,357}(q^{1/2}+2))$$

since $2^{\omega(q-1)} < (2,4)(q-1)^{0,357} < (2,4)q^{0,357}$ When $q < 2^{10}$, $q-(2,4)q^{0,357}(q^{1/2}+2) < 0$. So we can assume that $q \geq 2^{10}$. Then we have

$$4q^{1/10} - (2,4)q^{0,057}(1 + 2q^{-1/2}) \geq 4q^{1/10} - (2,55)q^{0,057}$$

$$\geq 8 - (2,55)2^{0,057} > 4$$

and we get

$$q - q^{4/5}((2,4)q^{0,057}(1 + 2q^{-1/2})) > q - q^{4/5}(4 - q^{1/10}) = (q^{1/2} - 2q^{2/5})^2$$

So,

$$\sum_{a \in P_q} K(\chi, a)^2 > \frac{\phi(q-1)q}{q-1}(q^{1/2} - 2q^{2/5})^2 > \phi(q-1)(q^{1/2} - 2q^{2/5})^2$$

Let $a_1 \in P_q$ be such that $K(\chi, a_1)^2 = \max_{a \in P_q} K(\chi, a)^2$. Then, $\#P_q = \phi(q-1)$ implies that

$$K(\chi, a_1)^2 \phi(q-1) > \sum_{a \in P_q} K(\chi, a)^2 > \phi(q-1)(q^{1/2} - 2q^{2/5})^2$$

and hence $|K(\chi, a_1)| > q^{1/2} - 2q^{2/5}$.

□

Lemma 3.2.27 *Let χ be nontrivial and let $0 < t < 1$. Then there are more than $A_q(t)\phi(q-1)$ values of $a \in P_q$ for which $|K(\chi, a)| > tq^{1/2}$, where*

$$A_q(t) = \frac{(1-t^2)q - (q^{1/2}+2)2^{\omega(q-1)}}{(4-t^2)q + 4q^{1/2} + 1}$$

Proof: We can assume that $A_q(t) \geq 0$. Suppose that $|K(\chi, a)| \leq tq^{1/2}$ holds for at most $A_q(t)\phi(q-1)$ values of $a \in P_q$. Then $|K(\chi, a)| \leq tq^{1/2}$ holds for at least $(1 - A_q(t))\phi(q-1)$ values of $a \in P_q$. For a nontrivial additive character χ and for $a, b \in \mathbb{F}_q$ a *Kloosterman sum* is defined as

$$K(\chi; a, b) = \sum_{c \in \mathbb{F}_q^*} \chi(ac + bc^{-1}) \; .$$

So our definition is equal to,

$$K(\chi, a) = K(\chi; 1, a) + \chi(0) = K(\chi; 1, a) + 1 \; .$$

From the classical bound on Kloosterman sums we obtain

$$|K(\chi, a)| \leq 2q^{1/2} + 1$$

for all $a \in \mathbb{F}_q^*$ .Therefore

$$\sum_{a \in P_q} K(\chi, a)^2 \leq (1 - A_q(t))\phi(q-1)t^2 q + A_q(t)\phi(q-1)(2q^{1/2} + 1)^2$$

$$\leq \phi(q-1)((1-t^2)q - (q^{1/2} + 2)2^{\omega(q-1)} + t^2 q)$$

$$\leq \phi(q-1)(q \; - \; (q^{1/2} + 2) \; 2^{\omega(q-1)})$$

$$\leq \frac{q}{q-1}\phi(q-1)(q - (q^{1/2} + 2)2^{\omega(q-1)}) \; .$$

Hence,

$$\sum_{a \in P_q} K(\chi, a)^2 \leq \frac{\phi(q-1)}{q-1} q^2 - \frac{\phi(q-1)}{q-1} q(q^{1/2} + 2)2^{\omega(q-1)}$$

But, this contradicts (3.18).

□

In lemma 3.2.22, let $k \geq 2$, $N = p$, $\mathbf{t_n} = \mathbf{y_n}$ for $0 \leq n \leq p-1$ with $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbb{Z}^k$ Then we get

$$\left| \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{y_n}) \right| \leq \frac{2}{\pi} \left(\left(\frac{\pi + 1}{2} \right)^2 - \frac{1}{4} \right) p D_p^{(k)} 2^2 = 2(\pi + 2) p D_p^{(k)}$$

$$pD_P^{(k)} \geq \frac{1}{2\pi+4}\left|\sum_{n=0}^{p-1} e(\mathbf{h}\cdot\mathbf{y_n})\right|$$

$$\left|\sum_{n=0}^{p-1} e(\mathbf{h}\cdot\mathbf{y_n})\right| = \left|\sum_{n=0}^{p-1} e(y_n - y_{n+1})\right| = \left|\sum_{n=0}^{p-1} e(\frac{1}{p}(x_n - x_{n+1}))\right|$$

$$= \left|\sum_{n=0}^{p-1} e(\frac{1}{p}(x_n + ax_n^{-1} - b))\right| = \left|\sum_{n=0}^{p-1} e(\frac{1}{p}(x_n + ax_n^{-1}))\right|$$

Let $\chi(c) = e(c/p)$ be the nontrivial additive character on $\mathbb{F}_p$. Then

$$\left|\sum_{n=0}^{p-1} e(\mathbf{h}\cdot\mathbf{y_n})\right| = \left|\sum_{n=0}^{p-1} \chi((x_n + ax_n^{-1}))\right| = |K(\chi, a)|$$

since $x_0, \ldots, x_{p-1}$ runs through $\mathbb{F}_p$. Thus,

$$pD_p^{(k)} \geq \frac{1}{2\pi+4}|K(\chi, a)| \tag{3.19}$$

for all $k \geq 2$.

Lemma 3.2.28 *For any primitive element $a \in \mathbb{F}_q$ there are exactly $\frac{\phi(q^2-1)}{2\phi(q-1)}$ primitive polynomials over $\mathbb{F}_q$ of the form $x^2 - bx + a$.*

Proof: If $x^2 - bx + a$ is primitive over $\mathbb{F}_q$, then for some primitive element $\alpha \in \mathbb{F}_{q^2}$, $x^2 - bx + a = (x - \alpha)(x - \alpha^q)$ which implies that $a = \alpha^{q+1}$. Let $S(a)$ be the number of primitive elements β such that $\beta^{q+1} = a$. The primitive elements α, α^q are the roots of the above polynomial and $q+1$st power of both are equal to a. Hence the number of primitive polynomials over $\mathbb{F}_q$ of the form $x^2 - bx + a$ is given by $\frac{1}{2}S(a)$. Let $\beta \in \mathbb{F}_{q^2}$ and let $ord(\beta)$ denote the order of β in $\mathbb{F}_{q^2}^*$. Then $ord(a) = q - 1$ and $a = \gamma^{q+1}$ for some $\gamma \in \mathbb{F}_{q^2}^*$. Let λ be a fixed primitive element of $\mathbb{F}_{q^2}$. Then there exists $k \in \mathbb{Z}$ such that, $\gamma = \lambda^k$.

$$q - 1 = ord(a) = ord(\lambda^{k(q+1)}) = \frac{q^2-1}{gcd(q^2-1, (q+1)k)} ,$$

hence $gcd(q^2 - 1, (q + 1)k) = q + 1$, i.e, $gcd(q - 1, k) = 1$.

Now, we are going to find $S(a)$. Let β be an element in $\mathbb{F}_{q^2}^*$. Then we have $\beta^{q+1} = a$ if and only if $(\beta\gamma^{-1})^{q+1} = 1$, i.e., if and only if $\beta\gamma^{-1} = \lambda^{(q-1)j}$ for some $j \in \mathbb{Z}$. So, the elements $\beta \in \mathbb{F}_q^*$ such that $\beta^{q+1} = a$ are of the form $\beta = \lambda^{k+(q-1)j}$ where k is fixed and $j \in \mathbb{Z}$. Suppose that β is a primitive element of $\mathbb{F}_{q^2}$, i.e, $ord(\beta) = q^2 - 1 = \frac{q^2-1}{gcd(q^2-1,k+(q-1)j)}$. So, $gcd(q^2 - 1, k + (q - 1)j) = 1$. Furthermore, $gcd(q - 1, k) = 1$ implies that $gcd(q^2 - 1, k + (q - 1)j) = 1$ if and only if $gcd(q + 1, k + (q - 1)j) = 1$. So, $S(a)$ is the number of integers $j \pmod{q+1}$ with $gcd(q + 1, k + (q - 1)j) = 1$

To find $S(a)$, we need to find the number of solutions j of the congruence

$$k + (q - 1)j \equiv m \pmod{q + 1} \tag{3.20}$$

for every $m \pmod{q+1}$ with $gcd(m, q+1) = 1$. Let q be even, then $gcd(q-1, q+1) = 1$ and hence for each $m \in \mathbb{Z}$ the congruence in (3.20) has a unique solution by [15], p/94. This means, $S(a) = \phi(q + 1) = \frac{\phi(q^2-1)}{\phi(q-1)}$.

Let q be odd, then $gcd(q - 1, q + 1) = 2$. For every integer $m \pmod{q+1}$ with $gcd(q + 1, m) = 1$, consider the congruence $k + (q - 1)j \equiv m \pmod{q+1}$,i.e, $(q - 1)j \equiv m - k \pmod{q+1}$. Then $gcd(q - 1, k) = gcd(q + 1, m) = 1$ implies that k, m are odd and the above congruence has two solutions $j \pmod{q+1}$ for every choice of m, again by [15], p/94. Hence $S(a) = 2\phi(q + 1) = \frac{\phi(q^2-1)}{\phi(q-1)}$.

Therefore $S(a) = \frac{\phi(q^2-1)}{\phi(q-1)}$ and the number of primitive polynomials over $\mathbb{F}_q$ of the form $x^2 - bx + a$ is $\frac{\phi(q^2-1)}{2\phi(q-1)}$.

□

Theorem 3.2.29 *For any prime $p \geq 5$ there are at least $\phi(p + 1)$ primitive polynomials $x^2 - bx + a$ over $\mathbb{F}_p$ such that for the corresponding inversive congruential PRNs we have*

$$D_p^{(k)} > \frac{1}{2\pi + 4}(p^{-1/2} - 2p^{-3/5})$$

for all $k \geq 2$.

Proof: From the equation (3.19) we get

$$D_p^{(k)} \geq \frac{1}{p(2\pi+4)}|K(\chi,a)| \; .$$

Now, choose $a \in \mathbb{F}_p$ in such a way that the lower bound for $|K(\chi,a)|$ in lemma 3.2.26 holds. For this a there are $\frac{\phi(p^2-1)}{2\phi(p-1)} = \phi(p+1)$ primitive polynomials $x^2 - bx + a$ over $\mathbb{F}_p$ and for the corresponding inversive congruential generators we have the lower bound

$$D_p^{(k)} > \frac{1}{p(2\pi+4)}(p^{1/2} + 2p^{2/5}) = \frac{1}{2\pi+4}(p^{-1/2} + 2p^{-2/5})$$

□

Theorem 3.2.30 *Let $p \geq 5$ be a prime and let $0 < t < 1$. Then there are more than $A_p(t)\phi(p^2-1)/2$ primitive polynomials $x^2 - bx + a$ over $\mathbb{F}_p$ such that for the corresponding inversive congruential PRNs we have*

$$D_p^{(k)} > \frac{t}{2\pi+4}p^{-1/2}$$

for all $k \geq 2$, where

$$A_p(t) = \frac{(1-t^2)p - (p^{1/2}+2)2^{\omega(p-1)}}{(4-t^2)p + 4p^{1/2} + 1} \; .$$

Proof: We have

$$D_p^{(k)} \geq \frac{1}{p(2\pi+4)}|K(\chi,a)| \; .$$

By lemma 3.2.27 we have more than $A_p(t)\phi(p-1)$ values of $a \in \mathbb{F}_p$ such that $|K(\chi,a)| > tp^{1/2}$. For each such a we have $\frac{\phi(p^2-1)}{2\phi(p-1)}$ suitable primitive polynomials. Therefore, there are more than $A_p(t)\frac{\phi(p^2-1)}{2}$ primitive polynomials such that for the corresponding inversive congruential generators we have

$$D_p^k > \frac{1}{p(2\pi+4)}tp^{1/2} = \frac{1}{(2\pi+4)}tp^{-1/2}$$

□

3.2.3. Distribution of inversive congruential pseudorandom numbers in parts of the period

For arbitrary $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$, consider the sequence generated by (3.10) and let ψ be the permutation of $\mathbb{F}_p$ defined by

$$\psi(x_n) = x_{n+1} \ , n = 0, 1, \ldots$$

The sequence is periodic with period $t \leq p$.

The first nontrivial bounds on the discrepancy of a sequence of inversive congruential PRNs in parts of the period, which we are going to describe below, are given by Niederreiter, Shparlinski in [26].

Let $x_0/p, x_1/p, \ldots, x_{N-1}/p$ be the inversive congruential PRNs with $1 \leq N \leq t$, where t is arbitrary. We define the discrepancy D_N of these numbers as

$$D_N = \sup_{J \subseteq [0,1)} \left| \frac{A(J,N)}{N} - \lambda(J) \right|$$

where $A_J(N)$ is the number of points $x_0/p, x_1/p, \ldots, x_{N-1}/p$ in the interval J and $\lambda(J)$ is the length of J . For integers $h \not\equiv 0 \pmod{p}$, let

$$S_h(N) = \sum_{n=0}^{N-1} \exp(\frac{2\pi i h x_n}{p})$$

Theorem 3.2.31 *For any prime p and any integer $h \not\equiv 0 \pmod{p}$*

$$|S_h(N)| < \left(\left(\frac{8}{3} \right)^{1/2} + 2 \right)^{1/2} N^{1/2} p^{1/4} + \left(\frac{3}{8} \right)^{1/2} p^{1/2}$$

for $1 \leq N \leq t$.

Proof: For $N \leq 2p^{1/2}$,

$$\left(\left(\frac{8}{3} \right)^{1/2} + 2 \right)^{1/2} N^{1/2} p^{1/4} + \left(\frac{3}{8} \right)^{1/2} p^{1/2} > N + N^{1/2}$$

so the upper bound for $|S_h(N)|$ is greater than N. Therefore we can assume that $N > 2p^{1/2}$. This implies that $p \geq t \geq N > 2p^{1/2}$, i.e , $p^2 > 4p$ and hence $p \geq 5$. For a fixed prime $p \geq 5$ and an integer $h \not\equiv 0 \pmod{p}$, let

$$\chi(\omega) = \exp(\frac{2\pi i h\omega}{p}) \ , \omega \in \mathbb{F}_p$$

then

$$S_h(N)) = \sum_{n=0}^{N-1} \chi(x_n)$$

Let ψ^m denote the mth iterate of the permutation ψ for any $m \in \mathbb{Z}$. Then $x_n = \psi^n(x_0)$ for any $n \geq 0$.

$$\left| S_h(N) - \sum_{n=0}^{N-1} \chi(x_{n+k}) \right| = \left| \sum_{n=0}^{N-1} (\chi(x_n) - \chi(x_{n+k})) \right| \leq 2|k| \tag{3.21}$$

Let $k \in \mathbb{Z}$ with $k \geq 1$ and define

$$\Re(K) = \begin{cases} \{k \in \mathbb{Z} \ : -(K-1)/2 \leq k \leq (K-1)/2\}, & \text{if K is odd} \\ \{k \in \mathbb{Z} \ : -K/2 + 1 \leq k \leq K/2\}, & \text{if K is even} \end{cases} \tag{3.22}$$

Note that, $|\Re(K)| = K$ and

$$\sum_{k \in \Re(K)} |k| = \frac{K^2}{4}$$

if K is even and

$$\sum_{k \in \Re(K)} |k| = \frac{K^2 - 1}{4}$$

if K is odd. Hence,

$$\sum_{k \in \Re(K)} |k| \leq \frac{K^2}{4}$$

Let

$$W = \left| \sum_{n=0}^{N-1} \sum_{k \in \Re(K)} \chi(x_{n+k}) \right| \ .$$

Then

$$W \leq \sum_{n=0}^{N-1} \left| \sum_{k \in \Re(K)} \chi(x_{n+k}) \right| = \sum_{n=0}^{N-1} \left| \sum_{k \in \Re(K)} \chi(\psi^k(x_n)) \right|$$

If we use (3.21) for all $k \in \Re(K)$ with W, we get

$$\left|\sum_{k\in Re(K)} S_h(N)\right| \leq W + 2\sum_{k\in\Re(K)} |k| \leq W + \frac{K^2}{2}$$

Now, we find a lower bound on W^2 ;

$$\begin{aligned} W^2 = \left(\sum_{n=0}^{N-1} 1\cdot\left|\sum_{k\in\Re(K)}\chi(\psi^k(x_n))\right|\right)^2 &\leq \sum_{n=o}^{N-1} 1 \sum_{n=0}^{N-1}\left|\sum_{k\in\Re(K)}\chi(\psi^k(x_n))\right|^2 \\ &= N\sum_{n=0}^{N-1}\left|\sum_{k\in\Re(K)}\chi(\psi^k(x_n))\right|^2 \end{aligned}$$

by Cauchy-Schwarz inequality.

$$\begin{aligned} W^2 &\leq N\sum_{w\in\mathbb{F}_p}\left|\sum_{k\in\Re(K)}\chi(\psi^k(w))\right|^2 \\ &\leq N\sum_{k,l\in\Re(K)}\left|\sum_{w\in\mathbb{F}_p}\chi(\psi^k(w)-\psi^l(w))\right| \\ &= N\sum_{\substack{k,l\in\Re(K)\\ k=l}}\left|\sum_{w\in\mathbb{F}_p}\chi(0)\right| + 2N\sum_{\substack{k,l\in\Re(K)\\ k>l}}\left|\sum_{w\in\mathbb{F}_p}\chi(\psi^k(w)-\psi^l(w))\right| \\ &= KNp + 2N\sum_{\substack{k,l\in\Re(K)\\ k>l}}\left|\sum_{w\in\mathbb{F}_p}\chi(\psi^k(w)-\psi^l(w))\right| \end{aligned}$$

$$\begin{aligned} \sum_{w\in\mathbb{F}_p}\chi(\psi^k(w)-\psi^l(w)) &= \sum_{w\in\mathbb{F}_p}(\psi^{k-l}(\psi^l(w))-\psi^l(w)) \\ &= \sum_{w\in\mathbb{F}_p}(\psi^{k-l}(w)-w) \end{aligned}$$

When K is odd, $\frac{-(K-1)}{2} \leq l < k \leq \frac{K-1}{2}$ implies that $1 \leq k-l = m \leq K-1$ and when K is even $\frac{-K}{2}+1 \leq l < k \leq \frac{K}{2}$ implies that $1 \leq k-l = m \leq K-1$. Therefore,

$$W^2 \leq KNp + 2N\sum_{m=1}^{K-1}(K-m)\left|\sum_{w\in\mathbb{F}_p}\chi(\psi^m(w)-w)\right|$$

Assume that $K \leq t$. For $1 \leq m \leq K-1$, there exist nonzero constant or linear polynomials $f_m, g_m \in \mathbb{F}_p[x]$ such that

$$\psi^m(w) = \frac{f_m(w)}{g_m(w)}$$

for all $w \in \mathbb{F}_p \setminus \varepsilon_m$, where ε_m consists of the roots of all polynomials g_j , $1 \leq j \leq m$. Since g_j is at most of degree 1, for $1 \leq j \leq m$, $|\varepsilon_m| \leq m$ and

$$\left| \sum_{w \in \mathbb{F}_p} \chi(\psi^m(w) - w) - \sum_{\substack{w \in \mathbb{F}_p \\ g_m(w) \neq 0}} \chi(\frac{f_m(w)}{g_m(w)} - w) \right|$$

$$\leq \left| \sum_{w \in \varepsilon_m} \chi(\psi^m(w) - w) - \sum_{\substack{w \in \varepsilon_m \\ g_m(w) \neq 0}} \chi(\frac{f_m(w)}{g_m(w)} - w) \right|$$

$$\leq 2m - 1$$

Indeed, it is easy to prove the above equality:

For $w \in \mathbb{F}_p \setminus \varepsilon_m$, we have $\psi^m(w) = \frac{f_m(w)}{g_m(w)}$ and hence we do not consider the terms with $w \in F_p \setminus \varepsilon_m$ in the above sum. If $g_m(w)$ is a nonzero constant then ε_m can contain at most $m-1$ elements, if $g_m(w)$ is a linear polynomial then it can have only one zero $w_0 \in \varepsilon_m$ and this zero is not included in the second sum. In the first case the elements of ε_m are the terms that the first and the second sum differ from each other. In the second case the elements of ε_m are the terms that the first sum differs from the second sum and the elements of $\varepsilon_m \setminus \{w_0\}$ are the elements that the second sum differs from the first sum. Therefore, the first sum can contain at most m terms which do not occur in the second sum and the second sum may contain at most $m-1$ terms which do not occur in the first sum, hence the last step of the above inequality follows.

If g_m is a nonzero constant polynomial then $\psi^m(w) = w$ for all $w \in \mathbb{F}_p \setminus \varepsilon_m$. But, $|\varepsilon_m| \leq m < t$, implies that there exists $x_n \notin \varepsilon_m$ and $\psi^m(x_n) = x_{n+m} \neq x_n$. Therefore, we assume that g_m is a linear polynomial and hence

$$\left| \sum_{\substack{w\in\mathbb{F}_p \\ g_m(w)\neq 0}} \chi(\frac{f_m(w)}{g_m(w)} - w) \right| = \left| \sum_{w\in\mathbb{F}_p^*} \chi(dw^{-1} + ew) \right|$$

for some $d \in \mathbb{F}_p$ and $e \in \mathbb{F}_p^*$. What we obtain in the last step is a Kloosterman sum in absolute value and it is bounded by $2p^{1/2}$. Hence

$$\left| \sum_{w\in\mathbb{F}_p} \chi(\psi^m(w) - w) \right| \leq 2p^{1/2} + 2m - 1$$

for $1 \leq m \leq K-1$. Therefore,

$$W^2 \leq KNp + 2N \sum_{m=1}^{K-1} (K-m)(2p^{1/2} + 2m - 1) \ .$$

$$\begin{aligned} \sum_{m=1}^{K-1} (K-m)(2p^{1/2} + 2m - 1) &= \sum_{m=1}^{K-1} K(2p^{1/2} - 1) + m(2K - 2p^{1/2} + 1) - 2m^2 \\ &= K(K-1)(p^{1/2} + \frac{2K-1}{6}) \ . \end{aligned}$$

So,

$$\begin{aligned} W^2 &\leq KNp + NK(K-1)(2p^{1/2} + \frac{2K-1}{3}) \\ &< KNp + NK(K-1)(2p^{1/2} + \frac{2K}{3}) \\ &= K^2N \left((p - 2p^{1/2})K^{-1} + 2p^{1/2} - \frac{2}{3} + \frac{2K}{3} \right) \end{aligned}$$

With this upper bound for W^2, we obtain

$$\begin{aligned} K|S_h(N)| &\leq W + \frac{K^2}{2} \\ &\leq KN^{1/2}((p - 2p^{1/2})K^{-1} + 2p^{1/2} - \frac{2}{3} + \frac{2K}{3})^{1/2} + \frac{K^2}{2} \end{aligned}$$

and

$$|S_h(N)| \leq N^{1/2}((p - 2p^{1/2})K^{-1} + 2p^{1/2} - \frac{2}{3} + \frac{2K}{3})^{1/2} + \frac{K}{2} \ .$$

Let $K = \lceil (\frac{3}{2})^{1/2}(p-2p^{1/2})^{1/2} \rceil$ and $A = (p-2p^{1/2})K^{-1} + 2p^{1/2} - \frac{2}{3} + \frac{2}{3}K$. Then $t \geq N > 2p^{1/2}$ implies that $t \geq K$ and

$$\begin{aligned} A &= (p-2p^{1/2})K^{-1} + 2p^{1/2} - \frac{2}{3} + \frac{2}{3}K \\ &\leq \left(\frac{2}{3}\right)^{1/2}(p-2p^{1/2})^{1/2} + 2p^{1/2} + \left(\frac{2}{3}\right)^{1/2}(p-2p^{1/2})^{1/2} \\ &= 2\left(\frac{2}{3}\right)^{1/2}(p-2p^{1/2})^{1/2} + 2p^{1/2} < \left(\frac{8}{3}\right)^{1/2} + 2p^{1/2} \end{aligned}$$

So,

$$|S_h(N)| < N^{1/2}\left(\left(\frac{8}{3}\right)^{1/2} + 2p^{1/2}\right)^{1/2} + \left(\frac{3}{8}\right)^{1/2}(p-2p^{1/2})^{1/2} + \frac{1}{2}$$

Since $(p-2p^{1/2}) < p^{1/2} - 1$ and $\left(\frac{3}{8}\right)^{1/2} > \frac{1}{2}$, the above inequality becomes

$$|S_h(N)| < N^{1/2}p^{1/4}\left(\left(\frac{8}{3}\right)^{1/2} + 2\right)^{1/2} + \frac{3}{8}p^{1/2}$$

□

Theorem 3.2.32 *The discrepancy D_N of the inversive congruential PRNs $x_0/p, x_1/p, \ldots, x_{N-1}/p$ satisfies*

$$D_N \leq \left(\left(\left(\frac{8}{3}\right)^{1/2} + 2\right)^{1/2} N^{-1/2}p^{1/4} + \left(\frac{3}{8}\right)^{1/2} N^{-1/2}p^{1/2}\right)\left(\frac{4}{\pi^2}\log p + \frac{2}{5}\right) + \frac{1}{p}$$

for $1 \leq N \leq t$ and primes $p \geq 31$.

Proof: Let B be a bound on $|S_h(N)|$ for all integers $h \not\equiv 0 \pmod{p}$. Then by corollary 3.11 in [25] together with an inequality of Cochrane [1] we can write

$$D_N \leq \frac{B}{N}\left(\frac{4}{\pi^2}\log p + 0,38 + \frac{0,608}{p} + \frac{0,116}{p^2}\right) + \frac{1}{p}\,.$$

For primes $p \geq 31$, we can take B as the bound on $|S_h(n)|$ in theorem 3.2.31 and we obtain the bound on D_N .

□

3.3. The Linear Complexity and The Linear Complexity Profile

The *linear complexity profile* $\mathcal{L}(S, N)$ of an infinite sequence $\mathcal{S} = (s_n)_{n\geq 0}$ of elements of $\mathbb{F}_{\text{ıı}}$ is the function which for every integer $N \geq 2$ is defined as the least order k of a linear recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n$$

which is satisfied by this sequence for $0 \leq n \leq N-k-1$. We have the convention that $\mathcal{L}(\mathcal{S}, N) = 0$ is the first N terms of $\mathcal{S}$ are zero and $\mathcal{L}(\mathcal{S}, N) = N$ if $s_0 = s_1 = \cdots = s_{N-2} = 0$ but $s_{N-1} \neq 0$.

The *linear complexity* of $\mathcal{S}$ is defined as

$$\mathcal{L}(\mathcal{S}) = \sup_{N\geq 2} \mathcal{L}(\mathcal{S}, N) \ .$$

The *nonlinear complexity profile* $\mathcal{NL}_m(\mathcal{S}, N)$ of an infinite sequence $\mathcal{S} = (s_n)_{n\geq 0}$ of elements of $\mathbb{F}_q$ is the function defined for every integer $N \geq 2$ as the least order k of a polynomial recurrence relation

$$s_{n+k} = \Psi(s_{n+k-1}, \ldots, s_n) \ , \ 0 \leq n \leq N-k-1$$

where $\Psi(\lambda_1, \ldots, \lambda_k)$ is a polynomial of total degree at most m which is satisfied by the sequence.

In general, $\mathcal{NL}_1(\mathcal{S}, N) \neq \mathcal{L}(\mathcal{S}, N)$ because in the definition of the linear complexity profile only homogeneous linear recurrence relations are used. In fact we have

$$\mathcal{L}(\mathcal{S}, N) \geq \mathcal{NL}_1(\mathcal{S}, N) \geq \mathcal{NL}_2(\mathcal{S}, N) \geq \ldots$$

In the following paragraphs, we give the lower bounds on the nonlinear complexity profile of inversive congruential generator and the linear complexity profile of quadratic exponential generator which were obtained by Gutierrez, Shparlinski, Winterhof in [14].

First, we define the inversive generator and the quadratic exponential generator:

The inversive generator giving the sequence $\mathcal{V} = (\upsilon_n)_{n\geq 0}$ is defined as

$$\psi(\upsilon) = \begin{cases} a\upsilon^{-1} + b & if \upsilon \neq 0 \\ b & if \upsilon = 0 \end{cases} \tag{3.23}$$

where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We can also write

$$\upsilon_n = \psi(\upsilon_{n-1}) \ .$$

We have the convention that $\psi^0(\upsilon) = \upsilon$ for all $\upsilon \in \mathbb{F}_q$.

Given an element $\upsilon \in \mathbb{F}_q^*$, we define the sequence generated by the *quadratic exponential generator* by $\mathcal{U} := (u_n)_{n\geq 0}$ where

$$u_n := \upsilon^{n^2} \ , n = 0, 1, \ldots \tag{3.24}$$

Now, let

$$H_0(x) = x \ , \ H_i(x) = H_{i-1}(ax^{-1} + b) \ , \ i = 1, 2, \ldots , \tag{3.25}$$

be a sequence of rational functions over $\mathbb{F}_q$ with $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. We observe that this sequence is purely periodic and we denote by T the period length.

Let $f_0(x) = x$ and $g_0(x) = 1$. Then $H_0(x) = x = f_0(x)/g_0(x)$, which is a nonconstant polynomial with $\max(deg(f_0), deg(g_0)) = 1$ and $gcd(f_0, g_0) = 1$. Now, suppose that $H_i(x) = f_i(x)/g_i(x)$ for some $f_i, g_i \in \mathbb{F}_q[x]$ which is a nonconstant polynomial with $\max(deg(f_i), deg(g_i)) = 1$ and $gcd(f_i, g_i) = 1$. Then there exist $a_i, b_i, c_i, d_i \in \mathbb{F}_q$ such that $f_i(x) = a_i x + b_i$ and $g_i(x) = c_i x + d_i$. Therefore,

$$\begin{aligned} H_{i+1}(x) &= H_i(ax^{-1} + b) = \frac{f_i(ax^{-1} + b)}{g_i(ax^{-1} + b)} \\ &= \frac{(ba_i + b_i)x + aa_i}{(bc_i + d_i)x + ac_i} = \frac{f_{i+1}(x)}{g_{i+1}(x)} \end{aligned}$$

where $\max(deg(f_{i+1}), deg(g_{i+1})) = 1$ and $gcd(f_{i+1}, g_{i+1}) = 1$ otherwise we have a contradiction to our assumptions about H_i . Since $\max(deg(f_i), deg(g_i)) = 1$ for all $i \geq 0$, H_i is always a nonconstant rational function.

Lemma 3.3.33 *For all integers i, k with $0 \leq i < k \leq T$ and all polynomials $\Psi \in \mathbb{F}_q[x_0, \ldots, x_i]$ and $G \in \mathbb{F}_q[x]$ with $gcd(G, g_k) = 1$ we have*

$$G(x)H_k(x) \neq \Psi(H_i(x), \ldots, H_0(x))$$

Proof: By induction, it can be shown that if $g_i(x) = c_i x + d_i$ then $f_i(x) = (bc_i + d_i)x + ac_i$. This is true for $f_0(x)$ since $c_0 = 0$ and $d_0 = 1$. Suppose that if $g_j(x) = c_j x + d_j$ then $f_j(x) = (bc_j + d_j)x + ac_j$ for some j . We want to show that if $g_{j+1} = c_{j+1}x + d_{j+1}$ then $f_{j+1} = (bc_{j+1} + d_{j+1})x + c_{j+1}$. Now,

$$\begin{aligned} \frac{f_{j+1}(x)}{g_{j+1}(x)} &= H_{j+1}(x) = H_j(ax^{-1} + b) \\ &= \frac{f_j(ax^{-1} + b)}{g_j(ax^{-1} + b)} \\ &= \frac{(b(bc_j + d_j) + ac_j)x + a(bc_j + d_j)}{(bc_j + d_j)x + ac_j} \end{aligned}$$

Since we assumed that $g_{j+1}(x) = c_{j+1}x + d_{j+1}$, we have $c_{j+1} = bc_j + d_j$ and $d_{j+1} = ac_j$. This implies $f_{j+1}(x) = (bc_{j+1} + d_{j+1})x + ac_{j+1}$. Note here that $g_{i+1}(x) = f_i(x)$ for all $i \geq 0$.

If $c_i = 0$ then $H_i(x) = x$ and $i = 0$ or $i \geq T$. For all integers $0 \leq j_1 < j_2 < T$,

$$gcd(g_{j_1} g_{j_2}) = 1 \ .$$

Otherwise

$$g_{j_1}(x) = k g_{j_2}(x) \text{ with } k \in \mathbb{F}_q^*$$

which yields $f_{j_1}(x) = k f_{j_2}(x)$ and thus $H_{j_1}(x) = H_{j_2}(x)$. Therefore,

$$H_{j_1+1}(x) = H_{j_1}(ax^{-1} + b) = H_{j_2}(ax^{-1} + b) = H_{j_2+1}(x)$$

and iteratively,

$$H_{j_1+T-j_2}(x) = H_{j_2+T-j_2}(x) = H_T(x) = H_0(x)$$

which is a contradiction to the definition of T .

Suppose that for $i = 0$,

$$G(x)H_k(x) = \Psi(H_0(x)) = \Psi(x) \ .$$

Then $G(x)f_k(x) = \Psi(x)g_k(x)$ and $gcd(G, g_k) = 1$ implies that $g_k(x)$ divides $f_k(x)$. Since $\max(deg(f_k), deg(g_k)) = 1$ and $H_k(x)$ is a nonconstant polynomial, we have $deg(f_k) = 1$ and $deg(g_k) = 0$. This implies that $c_k = 0$ and this yields a contradiction since $0 \leq i < k < T$. Now, suppose that for $i > 0$, we have an equation of the form

$$G(x)H_k(x) = \Psi(H_i(x), \ldots, H_0(x)) \ .$$

Then

$$G(x)f_k(x) = g_k(x)\Psi(H_i(x), \ldots, x)$$

and clearing the denominators we get

$$G(x)f_k(x)g_i(x)^{s_i} \ldots g_1(x)^{s_1} = g_k(x)\Psi(x) \ .$$

where $s_1, \ldots, s_i$ are nonnegative integers. Since $gcd(G, g_k) = 1 = gcd(f_k, g_k)$ and $gcd(g_j, g_k) = 1$ for all $1 \leq j \leq i < k < T$, g_k does not divide the left hand side of the above equality which is a contradiction. Therefore

$$G(x)H_k(x) \neq \Psi(H_i(x), \ldots, H_0(x)) \ .$$

□

Theorem 3.3.34 *The nonlinear complexity profile of a sequence $\mathcal{V} = (v_n)_{n\geq 0}$ produced by the inversive generator which is purely periodic with period t, satisfies*

$$\mathcal{NL}_m(\mathcal{V}, N) \geq \min\left\{ \left\lceil \frac{N-1}{m+2} \right\rceil, \left\lceil \frac{t-1}{m+1} \right\rceil \right\} \ .$$

Proof: Suppose that k is the least positive integer such that

$$v_{n+k} = \Psi(v_{n+k-1}, \ldots, v_n) \qquad 0 \leq n \leq N-k-1$$

with a polynomial $\Psi(\lambda_1, \ldots, \lambda_k)$ over $\mathbb{F}_q$ of total degree at most m . Then

$$\psi^k(v_n) = \Psi(\psi^{k-1}(v_n), \ldots, \Psi^0(v_n)) \qquad 0 \leq n \leq N-k-1 \ .$$

Let E_j denote the poles of the rational functions $H_0, \ldots, H_j$ for any $j \geq 0$. Since $\max\{deg(f_i), deg(g_i)\} = 1, \quad |E_j| \leq j$. For $j = 0$,

$$\psi^0(x) = x = H_0(x)$$

where $x \in \mathbb{F}_q$. Suppose that for some $i > 0$,

$$\psi^i(x) = H_i(x)$$

where $x \in \mathbb{F}_q \setminus E_i$.

For $x \in \mathbb{F}_q \setminus E_i$, we can write

$$\psi^{i+1}(x) = \psi^i(\psi(x)) = H_i(\psi(x)) = H_i(ax^{-1} + b) = H_{i+1}(x)$$

when $\psi(x) \in \mathbb{F}_q \setminus E_i$ is also true. Since $x \in \mathbb{F}_q \setminus E_i$, $\psi(x) = H(x)$ and hence the equality holds when $H(x) \in \mathbb{F}_q \setminus E_i$. This means that the condition $x \in \mathbb{F}_q \setminus E_{i+1}$ should be satisfied. Therefore, by induction, we have $\psi^j(x) = H_j(x)$ for all $j \geq 0$ and $x \in \mathbb{F}_q \setminus E_j$.

The sequence (H_i) is purely periodic. Let T be the smallest period of the sequence (H_i) . We have $T \geq t$ where t is the period of the inversive generator. In fact, for any $x \in \mathbb{F}_q \setminus E_t$, $H_t(x) = \psi^t(x) = x$ and for $x \in E_t$, we have $x = \psi^t(x) = H_{t+1}(x)$. Hence, if $E_t = \mathbb{F}_q$ then $T = t + 1$ and otherwise $T \geq t$. We can suppose that $k \leq t \leq T$. Let $G(x) = 1$. Then lemma 1 implies that $H_k(x) \neq \Psi(H_{k-1}(x), \ldots, H_0(x))$, i.e,

$$H(x) = -H_k(x) + \Psi(H_{k-1}(x), \ldots, H_0(x))$$

is a nonzero rational function. Since $H_i(x) = \frac{f_i(x)}{g_i(x)}$ are nonconstant rational functions where $f_i(x), g_i(x) \in \mathbb{F}_q[x]$ with $\max\{deg(f_i), deg(g_i)\} = 1$, $H(x) = \frac{F(x)}{G(x)}$ with $F(x), G(x) \in \mathbb{F}_q[x]$. Here $deg(F) \leq mk + 1$. When $\upsilon_n \notin E_k$, $\psi^j(\upsilon_n) = H_j(\upsilon_n)$ for all $0 \leq j \leq k$ and hence

$$\begin{aligned} H_k(\upsilon_n) = \psi^k(\upsilon_n) &= \Psi(\psi^{k-1}(\upsilon_n), \ldots, \Psi^0(\upsilon_n)) \\ &= \Psi(H_{k-1}(\upsilon_n), \ldots, H_0(\upsilon_n)) \end{aligned}$$

for $0 \leq n \leq N-k-1$, hence

$$\frac{F(x)}{G(x)} = H(x) = -H_k(x) + \Psi(H_{k-1}(x), \ldots, H_0(x))$$

is zero for all $v_n \notin E_k$ with $0 \leq n \leq N-k-1$. To determine zeros of $H(x)$, we should consider the elements $v_0, \ldots, v_{N-k-1}$ which are pairwise distinct and not contained in E_k . If $N-k-1 \leq t$ then among the $N-k$ elements $v_0, \ldots, v_{N-1}$ there are at least $N-2k$ distinct zeros of $H(x)$ and if $N-k-1 > t$ then there are at least $t-k$ distinct zeros of $H(x)$. So, the polynomial $F(x)$ has at least $\min\{N-2k, t-k\}$ zeros and hence $deg(F) \geq \min\{N-2k, t-k\}$. This implies $mk+1 \geq \min\{N-2k, t-k\}$. If $N-2k = \min\{N-2k, t-k\}$ then $k = \mathcal{NL}_m(\mathcal{V}, N) \geq \frac{N-1}{m+2}$ otherwise, $k = \mathcal{NL}_m(\mathcal{V}, N) \geq \frac{t-1}{m+1}$. Therefore,

$$\mathcal{NL}_m(\mathcal{V}, N) \geq \min\{\left\lceil \frac{N-1}{m+2} \right\rceil, \left\lceil \frac{t-1}{m+1} \right\rceil\}$$

□

Theorem 3.3.35 *The linear complexity profile of a sequence* $\mathcal{U} = (u_n)_{n\geq 0}$ *produced by the quadratic exponential generator* (3.24) *which is purely periodic with period* t *satisfies the inequality*

$$\mathcal{L}(\mathcal{U}, N) \geq \left\lceil \frac{\min\{N, t\}}{2} \right\rceil$$

Proof: Let k be the least positive integer with

$$u_{n+k} = a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \cdots + a_0 u_n$$

for $0 \leq n \leq N-k-1$. Then $\mathcal{L}(\mathcal{U}, N) = k$. For $l, n \geq 0$,

$$u_{n+l} = v^{(n+l)^2} = v^{l^2} u_n v^{2nl} .$$

Now let $a_k = -1$ and $b_l = v^{l^2} a_l$, then

$$-u_{n+k} + a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \cdots + a_0 u_n = 0$$

which implies

$$a_k v^{k^2} v^{2nk} + a_{k-1} v^{(k-1)^2} v^{2n(k-1)} + \cdots + a_1 v v^{2n} + a_0 = 0$$

and

$$b_k \upsilon^{2nk} + b_{k-1}\upsilon^{2n(k-1)} + \cdots + b_1\upsilon^{2n} + b_0 = 0$$

for $0 \leq n \leq N - K - 1$. Consider the polynomial

$$f(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0 \ .$$

Now, we are going to find out the number of zeros of $f(x)$. Let τ be the multiplicative order of υ . For even values of τ the elements $1, \upsilon^2, \upsilon^4, \ldots, \upsilon^{\tau-2}$ and for odd values of τ, the elements $1, \upsilon^2, \upsilon^4, \ldots, \upsilon^{2\tau-2}$ are distinct. If τ is even and $\tau - 2 > 2(N-k-1)$ then $f(x)$ has at least $N-k$ zeros; $1, \upsilon^2, \ldots, \upsilon^{2(N-k-1)}$, otherwise $f(x)$ has at least $\tau/2$ zeros; $1, \upsilon^2, \ldots, \upsilon^{\tau-2}$. Hence there are at least $\min\{\tau/2, N-k\}$ roots of $f(x)$. Suppose that τ is odd. If $2\tau - 2 > 2(N-k-1)$ then $f(x)$ has at least $N-k$ zeros; $1, \upsilon^2, \ldots, \upsilon^{2(N-k-1)}$, otherwise there are at least τ zeros of $f(x)$;$1, \upsilon^2, \ldots, \upsilon^{2\tau-2}$. Hence there are at least $\min\{\tau, N-k\}$ roots of $f(x)$ if τ is odd.

$$deg(f(x)) = k \geq \min\{\tau/2, N-k\}, \min\{\tau, N-k\}$$

and $t \leq \tau$ implies that $k = \mathcal{L}(\mathcal{U}, N) \geq \left\lceil \frac{\min\{N,t\}}{2} \right\rceil$.

□

There is a relation between the linear complexity of a general inversive congruential generator with modulus p and maximal period length and the degree of the permutation polynomial defining it. We explain this in the following paragraphs.

The linear complexity $\mathcal{L}(\mathcal{S})$ of an infinite sequence $\mathcal{S} = (s_n)_{n\geq 0}$ on a ring $\mathcal{R}$ can also be defined as the length L of the shortest linear recurrence relation

$$s_{n+L} = a_{L-1}s_{n+L-1} + \cdots + a_0 s_n, \quad n = 1, 2, \ldots \tag{3.26}$$

with $a_{L-1}, \ldots, a_0 \in \mathcal{R}$ which is satisfied by the sequence $(s_n)_{n\geq 0}$. With this definition in mind consider the nonlinear congruential generator of the form

$$x_{n+1} \equiv f(x_n) \pmod{p}$$

where the modulus $p \geq 5$ is a prime number, $x_0 \in \mathbb{F}_p$ and $f : \mathbb{F}_p \to \mathbb{F}_p$ denotes a function such that the generator has period length p . Then $x_{n+p} = x_n, \quad n = 0, 1, \ldots$ and we can view $\mathcal{X} = (x_n)_{n \geq 0}$ as a linear recurring sequence with a characteristic polynomial $x^p - 1 = (x-1)^p$. The minimal polynomial of this sequence is a divisor of $(x-1)^p$, hence it should be of the form $m(x) = (x-1)^t$ where $1 \leq t \leq p$. In fact, $m(x)$ is the characteristic polynomial of the linear recurrence relation of least possible order satisfied by the sequence $\mathcal{X}$. Therefore the linear complexity $\mathcal{L}(\mathcal{X}) = t$.

We have mentioned in section 3.1.1 by equation (3.4) that the terms of the above sequence can be written as

$$x_n = \sum_{j=0}^{s} \binom{n+j}{j} a_j = g(n) \ \ for \ \ all \ \ n \geq 0$$

with $g \in \mathbb{F}_p[x]$ with $deg(g) = s = t - 1$. Here, g is a permutation polynomial of $\mathbb{F}_p$ since $\{g(0), g(1), \ldots, g(p-1)\} = \mathbb{F}_p$. Therefore we can conclude that the linear complexity of the nonlinear congruential sequence with period $p \geq 5$, is equal to $deg(g) + 1$ where g is the permutation polynomial defining the sequence.

Now, we look at the linear complexity of the *power generator* which is defined in (2.11). We assume that the power generator is purely periodic with period t . For all periodic sequences (x_n) with period t , $x_{n+t} = x_n \quad$ for all $\ n \geq 0$. Hence $L \leq t$ since we assumed that the power generator is purely periodic with period t .

We give two important lemmas which will be used to prove main results about the linear complexity of the power generator in Shparlinski [27].

Lemma 3.3.36 *Let $q \geq 2$ and g be integers, and let τ be the largest positive integer for which the powers g^x , $x = 1, \ldots, \tau$ are distinct modulo q . Then for any $H \leq \tau$ and $1 \leq h \leq q$, there exists an integer a , $0 \leq a \leq q-1$, such that the congruence*

$$g^x \equiv a + y \pmod{q} \ \ 0 \leq x \leq H-1, 0 \leq y \leq h-1 \ ,$$

has

$$T_a(H,h) \geq \frac{Hh}{q}$$

solutions (x,y) .

Proof: We have

$$\sum_{a=0}^{q-1} T_a(H,h) = Hh \ .$$

Let a_0 be the integer $1 \leq a_0 \leq q-1$ such that $T_{a_0}(H,h) = \max\{T_a(H,h) |\ 0 \leq a \leq q-1\}$. Then

$$qT_{a_0}(H,h) \geq \sum_{a=0}^{q-1} T_a(H,h) = Hh$$

and hence

$$T_{a_0}(H,h) \geq \frac{Hh}{q} \ .$$

□

Lemma 3.3.37 *Let a sequence* $(s_n)_{n\geq 0}$ *satisfy a linear recurrence relation of the form* (3.26) *over a field* $\mathbb{F}$. *Then for any* $T \geq L+1$ *pairwise distinct nonnegative integers* $j_1, \ldots, j_T$ *there exist* $c_1, \ldots, c_T \in \mathbb{F}$, *not all equal to zero, such that*

$$\sum_{i=1}^{T} c_i s_{n+j_i} = 0 \quad n = 1, 2, \ldots .$$

Proof: Consider the set S of all solutions of the linear recurrence relation given in (3.26). By [17, section 8.5], S is a vector space of dimension L over $\mathbb{F}$. For $i = 1, \ldots, T$, let $\mathbf{s}_{n+j_i} = (s_{n+j_i}, s_{n+j_i+1}, \ldots, s_{n+j_i+L-1})$ where $n = 1, 2, \ldots$. Then $\mathbf{s}_{n+j_1}, \ldots, \mathbf{s}_{n+j_T}$ are solutions of (3.26) and since $T \geq L+1$, they are linearly dependent over $\mathbb{F}$. There exist $c_1, \ldots, c_T \in \mathbb{F}$, not all zero such that

$$\sum_{i=1}^{T} c_i \mathbf{s}_{n+j_i} = \mathbf{0}, \quad n = 1, 2, \ldots \ .$$

By considering the first component of this sum, we get

$$\sum_{i=1}^{T} c_i s_{n+j_i} = 0 \quad n = 1, 2, \ldots .$$

□

Now, we give the upper bound for the linear complexity of the power generator in the prime modulus case.

Theorem 3.3.38 *Let $m = p$ be a prime. Assume that the sequence $(u_n)_{n\geq 0}$, given by (2.11) with $m = p$ is purely periodic with period t . Then, for the linear complexity L of this sequence, the bound*

$$L \geq \frac{t^2}{p-1}$$

holds.

Proof: Let τ be the largest positive integer such that the powers e^x for $x = 1, \ldots, \tau$ are distinct modulo $p-1$. Suppose that $\tau < t$. Since $e^\tau \equiv 1 \pmod{p-1}$, $\vartheta^\tau \equiv \vartheta \pmod{p}$ which contradicts t being the period of the power generator with modulus p . Therefore $\tau \geq t$. Lemma 3.3.36 implies that there exists a with $0 \leq a \leq p-2$ such that for the number of solutions T of the congruence

$$e^x \equiv a + y \pmod{p-1}, 0 \leq x \leq \tau - 1, 0 \leq y \leq t-1, \tag{3.27}$$

we have

$$T \geq \frac{\tau t}{p-1} \geq \frac{t^2}{p-1} .$$

Let $(j_1, k_1), \ldots, (j_T, k_t)$ be the corresponding solutions of the congruence (3.27). Assume that $T \geq L+1$ $(L \leq T-1)$. Then

$$u_{n+j_i} \equiv \vartheta^{e^{n+j_i}} \equiv u_n e^{j_i} \equiv u_n^{a+k_i} \pmod{p}, \quad n = 1, 2, \ldots, \ i = 1, \ldots, T ,$$

and by lemma 3.3.37, there exist $c_1, \ldots, c_T \in \mathbb{F}_p$, not all equal to zero such that

$$\sum_{i=1}^{T} c_i u_n^{a+k_i} \equiv 0 \pmod{p}, \quad n = 1, 2, \ldots .$$

By the definition of the power generator $\vartheta \neq 0$ and hence $u_n \equiv \vartheta^{e^n} \not\equiv 0 \pmod{p}$, $n = 1, 2, \ldots$, and the nonzero polynomial

$$F(x) = \sum_{i=1}^{T} c_i x^{k_i} \in \mathbb{F}_p[x]$$

of degree

$$deg f \leq \max_{1\leq i\leq T} k_i \leq t-1$$

has t distinct zeros $u_1, \ldots, u_{t-1}$ which is impossible. So, we have $L \geq T \geq \frac{t^2}{p-1}$.

□

We call the numbers $m = pl$ as *Blum integers* where p, l are distinct primes. We show that the linear complexity of the power generator with modulus $m = pl$ is at least of order $t\phi(m)^{-1/2}$.

Theorem 3.3.39 *Let $m = pl$, where p and l are two distinct primes. Assume that the sequence $(u_n)_{n\geq 0}$ given by (2.11), is purely periodic with period t . Then for the linear complexity L of this sequence the bound*

$$L \geq t\phi(m)^{-1/2}$$

holds.

Proof: Let t_p be the period of the sequence (u_n) modulo p and t_l be the period of the same sequence modulo l . We have the inequality $t \leq t_p t_l$ and hence

$$\frac{t_p^2 t_l^2}{(p-1)(l-1)} \geq \frac{t^2}{\phi(m)} .$$

Suppose that $\frac{t_p^2}{p-1} \geq \frac{t_l^2}{l-1}$ .Then

$$\frac{t_p^2}{p-1} \geq t\phi(m)^{-1/2} .$$

The linear complexity L is not smaller than the linear complexity modulo p, hence by theorem 3.3.38 we have

$$L \geq t\phi(m)^{-1/2} .$$

□

Bibliography

[1] COCHRANE,T. On a trigonometric inequality of vinogradov. *J.Number Theory*, 27:9–16, 1987.

[2] EICHENAUER-HERRMANN,J. Inversive congruential pseudorandom numbers avoid the planes. *Mathematics of computation*, 56(193):297 – 301, January 1991.

[3] EICHENAUER-HERRMANN,J. On the discrepancy of quadratic congruential pseudorandom numbers with power of two modulus. *J.Comput.Appl.Math*, 53(3):371–376, 1994.

[4] EICHENAUER-HERRMANN,J. Discrepancy bounds for non overlapping pairs of quadratic congruential pseudorandom numbers. *Arch.Math.*, 65(4):362–368, 1995.

[5] EICHENAUER-HERRMANN,J. Quadratic congruential pseudorandom numbers:distribution of lagged pairs. *J.Comput.Appl.Math*, 79(1):75–85, 1997.

[6] EICHENAUER-HERRMANN,J. and HERRMANN,E. Compound cubc congruential pseudorandom numbers. *Computing*, 59(1):85–90, 1997.

[7] EICHENAUER-HERRMANN,J. and NIEDERREITER,H. On the discrepancy of quadratic congruential pseudorandom numbers. *J.Comp.Appl.Math*, 34:243–249, 1991.

[8] EICHENAUER-HERRMANN,J. and TOPUZOĞLU,A. On the period length of congruential pseudorandom number sequences generated by inversions. *Journal of computational mathematics*, 31:87–96, 1990.

[9] EICHENAUER,J., GROTHE,H., and LEHN,J. Marsaglia's lattice test and non-linear congruential pseudo random number generators. *Metrika*, 35:241 – 250, 1988.

[10] EICHENAUER,J. and LEHN,J. On the structure of quadratic congruential sequences. *Manuscripta Math.*, 58:129–140, 1987.

[11] EICHENAUER,J., LEHN,J., and TOPUZOĞLU,A. A nonlinear congruential pseudorandom number generator with power of two modulus. *Mathematics of computation*, 51:757 – 759, 1988.

[12] EICHENAUER,J. and NIEDERREITER,H. On marsaglia'a lattice test for pseudorandom numbers. *Manuscripta mathematica*, 62:245 – 248, 1988.

[13] FRIEDLANDER,J.B., POMERANCE,C., and SHPARLINSKI,I.E. Period of the power generator and small values of carmicheal's function. *Mathematics of computation*, 70(236):1591–1605, 2000.

[14] GUTIERREZ,J., SHPARLINSKI,I., and WINTERHOF,A. On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators. *IEEE Transactions on informaton theory*, to appear.

[15] HARDY,G.H. and WRIGHT,E.M. *An introduction to the theory of numbers*. Oxford University Press, fifth edition edition.

[16] KNUTH,D.E. *The Art of Computer Programming*, volume 2. Addison-Wesley,Reading,MA, 3rd ed. edition, 1998.

[17] LIDL,R. and NIEDERREITER,H. *Finite fields*. Addison-Wesley, Reading, Mass., 1983.

[18] LIDL,R. and NIEDERREITER,H. *Introduction to finite fields and their applications*. Cambridge Univ. Press, Cambridge, 1994.

[19] MARSAGLIA,G. Random numbers fall mainly in the planes. *Proc. Nat. Acad. Sci. U.S.A*, 61:25–28, 1968.

[20] NIEDERREITER,H. Pseudo-random numbers and optimal coefficients. *Adv. in Math.*, 26:99–181, 1977.

[21] NIEDERREITER,H. The serial test for pseudorandom numbers generated by the linear congruential method. *Numer. Math.*, 46:51–68, 1985.

[22] NIEDERREITER,H. Remarks on nonlinear congruential pseudorandom numbers. *Metrika*, 35:321 – 328, 1988.

[23] NIEDERREITER,H. The serial test for congruential pseudorandom numbers generated by inversions. *Mathematics of Computation*, 52(185):135–144, January 1989.

[24] NIEDERREITER,H. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Mathematics of computation*, 55(191):277–287, July 1990.

[25] NIEDERREITER,H. *Random number generation and quasi-monte carlo methods*. SIAM,Philadelphia, 1992.

[26] NIEDERREITER,H. and SHPARLINSKI,I.E. On the distribution of inversive congruential pseudorandom numbers in parts of the period. *Mathematics of computation*, 70(236):1569–1574, June 2000.

[27] SHPARLINSKI,I.E. On the linear complexity of the power generator. *Des.Codes Cryptogr.*, 23:5–10, 2001.

Bibliography

[1] COCHRANE,T. On a trigonometric inequality of vinogradov. *J.Number Theory*, 27:9–16, 1987.

[2] EICHENAUER-HERRMANN,J. Inversive congruential pseudorandom numbers avoid the planes. *Mathematics of computation*, 56(193):297 – 301, January 1991.

[3] EICHENAUER-HERRMANN,J. On the discrepancy of quadratic congruential pseudorandom numbers with power of two modulus. *J.Comput.Appl.Math*, 53(3):371–376, 1994.

[4] EICHENAUER-HERRMANN,J. Discrepancy bounds for non overlapping pairs of quadratic congruential pseudorandom numbers. *Arch.Math.*, 65(4):362–368, 1995.

[5] EICHENAUER-HERRMANN,J. Quadratic congruential pseudorandom numbers:distribution of lagged pairs. *J.Comput.Appl.Math*, 79(1):75–85, 1997.

[6] EICHENAUER-HERRMANN,J. and HERRMANN,E. Compound cubc congruential pseudorandom numbers. *Computing*, 59(1):85–90, 1997.

[7] EICHENAUER-HERRMANN,J. and NIEDERREITER,H. On the discrepancy of quadratic congruential pseudorandom numbers. *J.Comp.Appl.Math*, 34:243–249, 1991.

[8] EICHENAUER-HERRMANN,J. and TOPUZOĞLU,A. On the period length of congruential pseudorandom number sequences generated by inversions. *Journal of computational mathematics*, 31:87–96, 1990.

[9] EICHENAUER,J., GROTHE,H., and LEHN,J. Marsaglia's lattice test and non-linear congruential pseudo random number generators. *Metrika*, 35:241 – 250, 1988.

[10] EICHENAUER,J. and LEHN,J. On the structure of quadratic congruential sequences. *Manuscripta Math.*, 58:129–140, 1987.

[11] EICHENAUER,J., LEHN,J., and TOPUZOĞLU,A. A nonlinear congruential pseudorandom number generator with power of two modulus. *Mathematics of computation*, 51:757 – 759, 1988.

[12] EICHENAUER,J. and NIEDERREITER,H. On marsaglia'a lattice test for pseudorandom numbers. *Manuscripta mathematica*, 62:245 – 248, 1988.

[13] FRIEDLANDER,J.B., POMERANCE,C., and SHPARLINSKI,I.E. Period of the power generator and small values of carmicheal's function. *Mathematics of computation*, 70(236):1591–1605, 2000.

[14] GUTIERREZ,J., SHPARLINSKI,I., and WINTERHOF,A. On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators. *IEEE Transactions on informaton theory*, to appear.

[15] HARDY,G.H. and WRIGHT,E.M. *An introduction to the theory of numbers*. Oxford University Press, fifth edition edition.

[16] KNUTH,D.E. *The Art of Computer Programming*, volume 2. Addison-Wesley,Reading,MA, 3rd ed. edition, 1998.

[17] LIDL,R. and NIEDERREITER,H. *Finite fields*. Addison-Wesley, Reading, Mass., 1983.

[18] LIDL,R. and NIEDERREITER,H. *Introduction to finite fields and their applications*. Cambridge Univ. Press, Cambridge, 1994.

[19] MARSAGLIA,G. Random numbers fall mainly in the planes. *Proc. Nat. Acad. Sci. U.S.A*, 61:25–28, 1968.

[20] NIEDERREITER,H. Pseudo-random numbers and optimal coefficients. *Adv. in Math.*, 26:99–181, 1977.

[21] NIEDERREITER,H. The serial test for pseudorandom numbers generated by the linear congruential method. *Numer. Math.*, 46:51–68, 1985.

[22] NIEDERREITER,H. Remarks on nonlinear congruential pseudorandom numbers. *Metrika*, 35:321 – 328, 1988.

[23] NIEDERREITER,H. The serial test for congruential pseudorandom numbers generated by inversions. *Mathematics of Computation*, 52(185):135–144, January 1989.

[24] NIEDERREITER,H. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Mathematics of computation*, 55(191):277–287, July 1990.

[25] NIEDERREITER,H. *Random number generation and quasi-monte carlo methods*. SIAM,Philadelphia, 1992.

[26] NIEDERREITER,H. and SHPARLINSKI,I.E. On the distribution of inversive congruential pseudorandom numbers in parts of the period. *Mathematics of computation*, 70(236):1569–1574, June 2000.

[27] SHPARLINSKI,I.E. On the linear complexity of the power generator. *Des.Codes Cryptogr.*, 23:5–10, 2001.