ON THE LINEAR COMPLEXITY AND LINEAR COMPLEXITY PROFILE OF SEQUENCES IN FINITE FIELDS

by
İHSAN H. AKIN

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

ON THE LINEAR COMPLEXITY AND THE LINEAR COMPLEXITY PROFILE OF SEQUENCES IN FINITE FIELDS

APPROVED BY:

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

Assist. Prof. Cem GÜNERİ ....

Assist. Prof. Berrin YANIKOĞLU ....

DATE OF APPROVAL: September 18th, 2002

O' na. O kendini bilir

ABSTRACT

Pseudo random sequences, that are used for stream ciphers, are required to have the properties of unpredictability and randomness. An important tool for measuring these features is the linear complexity profile of the sequence in use.

In this thesis we present a survey of some recent results obtained on linear complexity and linear complexity profile of pseudo random sequences. The relation between the polynomial degree and the linear complexity of a function over a finite field is given, bounds for linear complexity of the "power generator" and "the self-shrinking generator" are presented and a new method of construction of sequences of high linear complexity profile is illustrated.

Key words : Linear recurrence sequences, linear complexity, linear complexity profile

ÖZET

Dizi şifreleyicilerde kullanılan yarı rasgele dizilerin rasgelelik ve öngörülememezlik özelliklerine sahip olmaları gerekir. Doğrusal karmaşıklık profili bu özellikleri ölçmede kullanılan önemli bir araçtır.

Bu tezde dizilerin doğrusal karmaşıklığı ve doğrusal karmaşıklık profili üzerinde son yıllarda elde edilen bazı önemli sonuçlar sunulmaktadır. Özellike, Bir sonlu cisim üzerinde verilen bir fonksiyonun polinomsal derecesiyle doğrusal karmaşıklığı arasındaki bağlantı, "üstsel" ve "kendini küçülten" üreteçlerin doğrusal karmaşıklık sınırları ve doğrusal karmaşıklığı yüksek dizilerin oluşturulma yöntemleri üzerindeki çalışmalar incelenmiştir.

Anahtar kelimeler: Doğrusal indirgemeli diziler, doğrusal karmaşıklık, doğrusal karmaşıklık profili.

ACKNOWLEDGEMENTS

It is genuine appreciation that I here express my gratitude to Prof. Dr. İsmail GÜLOĞLU and Assist. Prof. Cem GÜNERİ to their guide in this thesis and, of course, to Alev TOPUZOĞLU, my thesis advisor.

I would like to thank my family for their unfailing support and influence in my life.

I would like to thank to my colleagues at UEKAE (National Electronic and Cryptography Research Institute) and also thanks to my manager Alparslan BABAOĞLU for his patience and supports.

Finally, I would like to gratitude to him to for the unlimited patience, the mercy and the compassion.

TABLE OF CONTENTS

Page

1 INTRODUCTION **1**
1.1 Preliminaries 1
1.2 Sequences and Linear Complexity 3
1.3 Algebraic Function Fields 10

2 POLYNOMIAL DEGREE AND LINEAR COMPLEXITY **19**
2.1 The Main Result 19
2.2 Consequences 29

3 BOUNDS FOR LINEAR COMPLEXITY **32**
3.1 The Power Generator 32
3.2 The Self-Shrinking Generator 36

4 CONSTRUCTION OF D-PERFECT SEQUENCES USING FUNCTION FIELDS **48**
4.1 The Main Construction 48
4.2 The Extensions of the Main Construction 54
4.3 Consequences of The Constructions 56

Bibliography **58**

ON THE LINEAR COMPLEXITY AND LINEAR COMPLEXITY PROFILE OF SEQUENCES IN FINITE FIELDS

by

İHSAN H. AKIN

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

ON THE LINEAR COMPLEXITY AND THE LINEAR COMPLEXITY PROFILE OF SEQUENCES IN FINITE FIELDS

APPROVED BY:

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

Assist. Prof. Cem GÜNERİ ....

Assist. Prof. Berrin YANIKOĞLU ....

DATE OF APPROVAL: September 18th, 2002

O' na. O kendini bilir

ABSTRACT

Pseudo random sequences, that are used for stream ciphers, are required to have the properties of unpredictability and randomness. An important tool for measuring these features is the linear complexity profile of the sequence in use.

In this thesis we present a survey of some recent results obtained on linear complexity and linear complexity profile of pseudo random sequences. The relation between the polynomial degree and the linear complexity of a function over a finite field is given, bounds for linear complexity of the "power generator" and "the self-shrinking generator" are presented and a new method of construction of sequences of high linear complexity profile is illustrated.
Key words : Linear recurrence sequences, linear complexity, linear complexity profile

ÖZET

Dizi şifreleyicilerde kullanılan yarı rasgele dizilerin rasgelelik ve öngörülememezlik özelliklerine sahip olmaları gerekir. Doğrusal karmaşıklık profili bu özellikleri ölçmede kullanılan önemli bir araçtır.

Bu tezde dizilerin doğrusal karmaşıklığı ve doğrusal karmaşıklık profili üzerinde son yıllarda elde edilen bazı önemli sonuçlar sunulmaktadır. Özellike, Bir sonlu cisim üzerinde verilen bir fonksiyonun polinomsal derecesiyle doğrusal karmaşıklığı arasındaki bağlantı, “üstsel” ve “kendini küçülten” üreteçlerin doğrusal karmaşıklık sınırları ve doğrusal karmaşıklığı yüksek dizilerin oluşturulma yöntemleri üzerindeki çalışmalar incelenmiştir.

Anahtar kelimeler: Doğrusal indirgemeli diziler, doğrusal karmaşıklık, doğrusal karmaşıklık profili.

ACKNOWLEDGEMENTS

It is genuine appreciation that I here express my gratitude to Prof. Dr. İsmail GÜLOĞLU and Assist. Prof. Cem GÜNERİ to their guide in this thesis and, of course, to Alev TOPUZOĞLU, my thesis advisor.

I would like to thank my family for their unfailing support and influence in my life.

I would like to thank to my colleagues at UEKAE (National Electronic and Cryptography Research Institute) and also thanks to my manager Alparslan BABAOĞLU for his patience and supports.

Finally, I would like to gratitude to him to for the unlimited patience, the mercy and the compassion.

TABLE OF CONTENTS

Page

1 INTRODUCTION **1**
1.1 Preliminaries 1
1.2 Sequences and Linear Complexity 3
1.3 Algebraic Function Fields 10

2 POLYNOMIAL DEGREE AND LINEAR COMPLEXITY **19**
2.1 The Main Result 19
2.2 Consequences 29

3 BOUNDS FOR LINEAR COMPLEXITY **32**
3.1 The Power Generator 32
3.2 The Self-Shrinking Generator 36

4 CONSTRUCTION OF D-PERFECT SEQUENCES USING FUNCTION FIELDS **48**
4.1 The Main Construction 48
4.2 The Extensions of the Main Construction 54
4.3 Consequences of The Constructions 56

Bibliography **58**

CHAPTER 1

INTRODUCTION

Main methods used in conventional cryptography are "block ciphers" and "stream ciphers". In general, while block ciphers encrypt blocks of data at a time, stream ciphers encrypt one bit a time via XOR operation. In stream ciphers, the security of the encryption is based on the key stream, which is XORed with the plain text to produce encrypted text.

To achieve secure transmission, the first aim is to protect the original key. Once the key is unveiled, the original message is easily obtained. Second aim, especially for stream ciphers, is to protect the key stream, or formally making the key stream unpredictable from the known part of it. This can be achieved by using sequences of high linear complexity. In other words, controlling the linear complexity enables controlling the security of the stream cipher. Linear complexity profile goes one step further, gives the behavior of the linear complexity of the key stream, or equivalently, of the sequence which is generated by the encryption algorithm with the relevant encryption key.

These concepts will be made precise in section 1.2.

1.1 Preliminaries

Throughout this thesis we will basically follow the famaous book of Lidl and Neiderreiter [8] for notation and terminology. Now we give definitions and theorems which will be used in the rest of the thesis.

F_q denotes a *finite field* with q elements where q is a prime or a prime power. F_q^* is the *multiplicative group* of $F_q - \{0\}$. As it well known F_q^* is *cyclic* and has order $q-1$.

Definition 1.1. A generator of the cyclic group F_q^* is called a *primitive element* of F_q.

Firstly, we recall some facts from the theory of finite fields. We refer to the books of Lidl and Neiderreiter [8], D. Jungnickel [7] and T.W Cusick, C. Ding and A. Renvall [4] for the proof of the results we list in the first two sections of this chapter.

Theorem 1.2. *(Lagrange Interpolation Formula) For* $n \geq 0$ *, let* $a_0, a_1, \ldots, a_n$ *be* $n+1$ *distinct elements of* F*. Let* $b_0, b_1, \ldots, b_n$ *arbitrary elements of* F*. Then there exists exactly one polynomial* $f \in F[x]$ *of degree* $\geq n$ *such that* $f(a_i) = b_i$*, for* $i = 1, \ldots, n$*. This polynomial given by*

$$f(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k\neq i}^{n} (a_i - a_k)^{-1}(x - a_k). \tag{1.1}$$

Proof. See [8, Theoren 1.71]. □

Proposition 1.3. *Let* k *be a non-negative integer. Then*

$$\sum_{c \in F_q} c^k = \begin{cases} 0 & if\ k = 0 \text{ or } k \text{ is not divisible by } q-1, \\ -1 & if\ k \text{ is divisible by } q-1. \end{cases}$$

Proof. See [8, Theorem 6.3]. □

Definition 1.4. For $\alpha \in F = F_{q^m}$ and $K = F_q$ then the *trace* $\mathrm{Tr}_{F/K}(\alpha)$ of α over K is defined by

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

If K is the prime subfield of F, then $\mathrm{Tr}_{F/K}(\alpha)$ is called *absolute trace* of α and it is simply denoted by $\mathrm{Tr}_F(\alpha)$.

Theorem 1.5. *Let* $K = F_q$ *and* $F = F_{q^m}$*. Then the trace function* $\mathrm{Tr}_{F/K}$ *satisfies the following properties:*

1. $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ *for all* $\alpha, \beta \in F$*,*

2. $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ *for all* $\alpha \in F$*,* $c \in K$*,*

3. $\mathrm{Tr}_{F/K}$ *is a linear transformation from* F *onto* K*, where both* F *and* K *are viewed as a vector spaces over* K*,*

4. $\mathrm{Tr}_{F/K}(a) = ma$ *for all* $a \in K$*,*

5. $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ *for all* $\alpha \in F$ *.*

Proof. See [8, Theorem 2.23]. □

If $F = F_{2^n}$ and $K = F_2$ then the trace map satisfies the following identity, which is a special form of the Theorem 1.5, property (5) when $m = 2$,

$$\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{F/K}(\alpha^2),\ \ for\ all\ x \in F. \tag{1.2}$$

For this special case we say that trace is *invariant under the squaring automorphisms.*

Theorem 1.6. *Let* F *be a finite extension of the field* K*. If* $T : F \to K$ *is any* K*-linear function, then there exists a unique* $c \in F$ *with the property that* $T(x) = \mathrm{Tr}(cx)$ *for all* $x \in F$*. In particular the element* c *is non-zero if and only if* T *is onto.*

Proof. See [8]. □

Definition 1.7. Let K be a finite field and F be a finite extension of K. Let $\{\delta_1, \ldots, \delta_r\}$ be a basis of F over K. The basis $\{\beta_1, \ldots, \beta_r\}$ of F over K is called the *dual basis* of $\{\delta_1, \ldots, \delta_r\}$ if for $1 \le i, j \le r$ we have

$$\mathrm{Tr}_{F/K}(\delta_i \beta_j) = \begin{cases} 0 & for\ i \neq j, \\ 1 & for\ i = j \end{cases} \tag{1.3}$$

If not otherwise stated, in this thesis K is always the prime subfield of F. Thus, we will simply use $\mathrm{Tr}(\alpha)$ instead of $\mathrm{Tr}_F(\alpha)$.

1.2 Sequences and Linear Complexity

Let k be a positive integer and $a, a_0, a_1, \ldots, a_{k-1}$ be elements of a finite field F_q. A sequence $\sigma_0, \sigma_1, \ldots$ of elements of F_q satisfying the relation

$$\sigma_{n+k} = a_{k-1}\sigma_{n+k-1} + a_{k-2}\sigma_{n+k-2} + \cdots + a_0\sigma_n + a\ \ for\ n = 0, 1, \ldots \tag{1.4}$$

is called a $(kth - order)$ *linear recurrence sequence* in F_q. The terms $\sigma_0, \ldots, \sigma_{k-1}$, which determine the rest of the sequence are called *initial values.* The vector formed by initial values $(\sigma_0, \sigma_1, \ldots, \sigma_{k-1})$ is called the *initial vector.* A relation of the form (1.4) is called $(kth - order)$ *linear recurrence relation.* If $a = 0$ then the we call the relation *homogeneous* linear recurrence relation otherwise we call it *inhomogeneous* linear recurrence relation. The coefficients a_i are called *feedback coefficients.*

For the homogenous case of the linear recurrence relation (1.4), it can be written as

$$\sigma_n = \sum_{i=1}^{k} a_{k-i}\sigma_{n-i} \quad for\ n \geq k,$$

with the convention $a_k = -1$ we have,

$$0 = \sum_{i=0}^{k} a_{k-i}\sigma_{n-i} \quad for\ n \geq k.$$

The well known property of linear recurrence relations is that they can be implemented in hardware with almost no cost. This implementation is called $LFSR$ (*Linear Feedback Shift Register*).

If not otherwise stated we always consider the homogeneous case of the linear recurrence relations.

There are several mathematical objects that can serve for the description of linear recurrence relations (or, equivalently, LFSR's). For instance, one defines the *feedback polynomial* of the linear recurrence relation (1.4) by

$$f(x) := -a_k - a_{k-1}x - \ldots - a_0 x^k; \tag{1.5}$$

we note that f is a polynomial of degree $\leq k$ with constant term $+1$. Let us call the vector $\sigma^{(t)} := (\sigma_t, \sigma_{t+1}, \ldots, \sigma_{n+k-1})$ the t^{th} *state vector* of the linear recurrence relation $(t \geq 0)$. Then we may rewrite the Equation (1.4) as

$$\sigma^{(t+1)} = \sigma^{(t)} A \quad for\ t \geq 0,$$

where the *feedback matrix* A is defined by

$$A := \begin{pmatrix} 0 & 0 & & & 0 & a_0 \\ 1 & 0 & & & 0 & a_1 \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & & \ddots & 0 & a_{k-2} \\ 0 & 0 & & & 1 & a_{k-1} \end{pmatrix}_{\text{kxk}}.$$

In general, we have

$$\sigma^{(t)} = \sigma^{(0)} A^t \quad for \;\; t \geq 1.$$

Here we note that A is the companion matrix of the reciprocal polynomial

$$f^*(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_1 x - a_0$$

of f, the feedback polynomial. In the view of the following lemma, f^* is usually called the *characteristic polynomial* of the linear recurrence relation (1.4).

Lemma 1.8. *Let f be the feedback polynomial of an LFSR of length n over the field F. Then the feedback matrix A satisfies*

$$\chi_A = f^*,$$

where χ_A denotes the characteristic polynomial of A.

Proof. See Hoffman and Kunze [6]. □

A linear recurrence relation (or equally, LFSR) can therefore be described in terms of each of the three objects f, f^* and A. We emphasize that the initial values has no effect on the feedback polynomial f and hence there is always a family of shift register sequences correspond to the same f, f^* and A.

Definition 1.9. Let S be an arbitrary non-empty set, and let $\sigma_0, \sigma_1, \ldots$ be a sequence of elements of S. If there exist integers $r > 0$ and $n_0 \geq 0$ such that $\sigma_{n+r} = \sigma_n$ for all $n \geq n_0$, then the sequence is called *ultimately periodic* and r is called a *period* of the sequence. The smallest number among all the possible periods of an ultimately periodic sequence is called the *least period* of the sequence.

Definition 1.10. An ultimately periodic sequence $\sigma_0, \sigma_1, \ldots$ with least period r is called purely periodic if $\sigma_{n+r} = \sigma_n$ holds for all $n = 0, 1, \ldots$.

When the set S is a finite field it turns out that every kth-order linear recurrence relation is ultimately periodic, which is given in the next theorem.

Theorem 1.11. *Let F_q be any finite field and k any positive integer. Then every kth-order linear recurrence sequence in F_q is ultimately periodic with least period r satisfying $r \leq q^k$, and $r \leq q^k - 1$ if the sequence is homogeneous.*

Proof. See [8, Theorem 8.7]. □

If a homogeneous linear recurrence relation of order k generates a *maximal periodic sequence* of period q^{k-1} over the field F_q, then the corresponding sequence is called an *m-sequence.*

We note here that there is a family of linear recurrence relations that produce the same sequence. Hence, we have a family of characteristic polynomials related to each of the linear recurrence relation that produces the same sequence. It can be easily shown that the set of all characteristic polynomials of a given linear recurrence sequence σ, together with the zero polynomial forms an non-zero ideal I in $F[x]$ (see [7]). Since $F[x]$ is a principal ideal domain the following definition makes sense.

Definition 1.12. The unique monic generator m of I, the ideal of the characteristic polynomials of a linear recurrence sequence σ is called the *minimal polynomial* of σ.

Theorem 1.13. *Let σ be a sequence in F_q satisfying a kth-order homogeneous linear recurrence relation with characteristic polynomial $f(x) \in F_q[x]$. Then $f(x)$ is the minimal polynomial of the sequence if and only if the state vectors $\sigma^0, \sigma^1, \ldots, \sigma^{k-1}$ are linearly independent over F_q.*

Proof. See [8, Theorem 8.51]. □

Since the minimal polynomial is unique then the following definition make sense.

Definition 1.14. The linear complexity L_σ of a sequence σ is defined to be the degree of the minimal polynomial m of σ.

When a sequence σ is purely periodic with period t then $x^t + 1$ is a characteristic polynomial for this sequence. Hence the linear complexity of a σ does not exceed t.

One can also define the linear complexity of a linear recurrence sequence σ as the order of the linear recurrence relation of least order or equivalently, as the length of the shortest linear feedback shift register generating the sequence σ.

Alternatively, we can take a finite sequence $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ and consider consider the homogeneous linear recurrence relation of order k

$$\sigma_{n+k} = a_{k-1}\sigma_{n+k-1} + a_{k-2}\sigma_{n+k-2} + \cdots + a_0\sigma_n + a \tag{1.6}$$

for $n = 0, 1, \ldots, n-k$, and $a_0, \ldots, a_k \in F_q$. The linear complexity of the sequence $\sigma_1, \ldots, \sigma_n$ is defined as the least k for which equation (1.6) holds for some $a_0, \ldots, a_{k-1} \in F_q$.

Definition 1.15. Let $L_\sigma(i)$ be the linear complexity of the first i terms of the sequence σ, for $i = 1, 2, \ldots$. Then the sequence $(L_\sigma(i)) = (L_\sigma(1), L_\sigma(2), \ldots)$ is called the *linear complexity profile* of σ.

The following algorithm is the basic tool for calculating the linear complexity profile of arbitrary sequences.

Algorithm 1.16. *(The Berlekamp-Massey Algorithm) Let σ be a sequence of finite length n over F_q. The following algorithm computes integers L_k and polynomials*

$$f_k(x) = 1 - c_1^{(k)}x - c_2^{(k)}x^2 - \ldots - c_{L_k}^{(k)}x^{L_k} \tag{1.7}$$

for all $k \geq n$.

$L_0 := 0, L_1 := -1, f_0 := 1, f_1 := 1 + x.$

for $k = 1$ ***to*** $N - 1$ ***do***

  $\delta_k := -a_k + \sum_{i=1}^{L_k} c_i^{(k)} a_{k-i}$

  if $\delta_k = 0$ ***then***

    $f_{k+1} := f_k,\ L_{k+1} := L_k$

  else $m := \max\{i : \ L_i < L_{i+1}\},$

    $L_{k+1} := \max(L_k, k + 1 - L_k),$

    $f_{k+1} := f_k - \delta_k\delta_m^{-1}x^{k-m}f_m(x).$

Proof. See [7, Algorithm 6.7.5]. □

Theorem 1.17. *Let* $\sigma = (\sigma_1, \ldots, \sigma_n)$ *be a sequence of finite length* n *over* F_q. *Then the Berklamp-Massey algorithm computes the linear complexity profile* $(L_\sigma(1), \ldots, L_\sigma(n))$ *of* σ *and feedback polynomials* $f_1, \ldots, f_n$ *for LFSR's* l_k *of length* $L_\sigma(k)$ *generating the first* k *elements of* σ *(for all* $k = 1, \ldots, n$*).*

Proof. See [7, Theorem 6.7.6]. □

We remark here that the polynomials f_k appearing in the above algorithm are the feedback polynomials corresponding to each sequence $(\sigma_1, \ldots, \sigma_k)$.

Theorem 1.18. *If* $\sigma = \sigma_0, \sigma_1, \ldots$ *is a maximal periodic sequence, with period* $2^n - 1$, *in* F_2 *with minimal polynomial* m. *Let* ζ *be a root of* m *in the extension field* F_{2^n}. *Then there exists a uniquely determined* $c \in F_2$ *such that*

$$\sigma_i = \mathrm{Tr}(c\zeta^i),$$

for all non-negative integers i.

Proof. See [8, Theorem 8.24]. □

Definition 1.19. The *formal power series* or the *generating function* of an infinite sequence σ is defined by

$$\sigma_n(x) = \sum_{i=0}^{\infty} \sigma_i x^i. \tag{1.8}$$

Proposition 1.20. *The generating function of each periodic sequence* σ *can be expressed as*

$$\sigma(x) = \frac{g(x)}{f(x)}$$

with $f(0) \neq 0$ *and* $deg(g(x)) < deg(f(x))$.

Proof. First we assume that r is a period for σ, say $\sigma_{k+r} = \sigma_k$ for all $k \geq N$. Using this we can write the formal power series $\sigma(x)$ of σ as follows

$$\sigma(x) = (\sigma_0 + \ldots + \sigma_{N-1}x^{N-1}) + x^N(\sigma_N + \sigma_{N+1}x + \ldots + \sigma_{N+r-1}x^{N+r-1})(1 + x^r + x^{2r} + \ldots)$$

Using the identity

$$1 + x^r + x^{2r} + \ldots = (1 - x^r)^{-1},$$

we get

$$(1 - x^r)\sigma(x) = (\sigma_0 + \ldots + \sigma_{N-1}x^{N-1})(1 - x^r) + (\sigma_N + \sigma_{N+1}x + \ldots + \sigma_{N+r-1}x^{N+r-1}).$$

Thus $(1 - x^r)\sigma(x) \in F[x]$. Call this g. Then $\sigma(x) = g(x)/(1 - x^r)$ which proves the proposition. □

Proposition 1.21. *Let σ be a periodic sequence over F_q and*

$$\sigma(x) = r(x)/f(x), \; f(0) = 1,$$

a rational form of the generating function of σ. Then $f(x)$ is the minimal polynomial of the sequence if and only if $gcd(f(x), r(x)) = 1$.

Proof. See [4, Propostion 2.3.2]. □

With the help of the linear complexity profile we can categorize sequences using the following definition.

Definition 1.22. If d is a positive integer, than a sequence σ of elements in F_q is called d-*perfect* if

$$|2L_\sigma(i) - i| \leq d \quad \text{for all } i \geq 1.$$

Where $L_\sigma(i)$ denotes the linear complexity of the first i elements of σ

A 1-perfect sequence is also called *perfect.* A sequence is called almost perfect if it is d-perfect for some d.

Theorem 1.23. *In order to establish that a sequence σ, with irrational generating function, is d-perfect, it is suffices to prove that*

$$L_\sigma(i) \leq \frac{i + d}{2} \;\text{ for all } i \geq 1,$$

or, similarly

$$L_\sigma(i) \geq \frac{i + 1 - d}{2} \;\text{ for all } i \geq 1.$$

Proof. See [13, Chapter 7]. □

1.3 Algebraic Function Fields

Here we give the basic facts about algebraic function fields. The reader is referred to the book of Stichtenoth [16] for proofs and further results on function fields.

Definition 1.24. An *algebraic function field* F/K of one variable over an arbitrary field K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$, which is transcendental over K. Elements of F/K are called *functions*.

We'll simply refer to F/K as a function field.

Definition 1.25. The set $\tilde{K} := \{z \in F \mid z \text{ is algebraic over } K\}$ is called the *constant field* of F/K. If $\tilde{K} = K$, then K is called the *full constant field* of F/K. Elements of F/K that are in $\tilde{K}$ are called *constants functions.* We note that, in general, $\tilde{K}$ is a finite, hence algebraic extension of K.

Definition 1.26. A *valuation ring* of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties :

1. $K \subsetneq \mathcal{O} \subsetneq F$ and
2. for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Proposition 1.27. *Let $\mathcal{O}$ be a valuation ring of the function field F/K. Then*

1. *$\mathcal{O}$ is local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $P = \mathcal{O} \backslash \mathcal{O}^*$, where $\mathcal{O}^*$ is the group of units of $\mathcal{O}$.*
2. *For $0 \neq x \in F$, $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$.*

Proof. See [16, Theorem I.1.5] □

Theorem 1.28. *Let $\mathcal{O}$ be a valuation ring of the function field F/K and P be its unique maximal ideal. Then*

1. *P is a principal ideal.*

2. *If $P = t\mathcal{O}$ then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$, $u \in \mathcal{O}^*$.*

Proof. See [16, Theorem I.1.6] □

Definition 1.29. A *place* P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. An element $t \in P$ such that $P = t\mathcal{O}$ is called a *local parameter.*

We denote the valuation ring containing the place P by $\mathcal{O}_P$. The set of places of F/K is denoted by $\mathbb{P}_F$. It can be shown that $\mathbb{P}_F$ is a non-empty set, in fact, $\mathbb{P}_F$ is an infinite set, i.e. any function field F/K has has infinitely many places (see [16, Corollary I.1.19] and [16, Corollary I.3.2]).

Definition 1.30. A *discrete valuation* of F/K is a function $v : F \leftarrow \mathbb{Z} \cup \{\infty\}$ with the following properties :

1. $v(x) = \infty \Leftrightarrow x = 0$.
2. $v(xy) = v(x) + v(y)$ for any $x, y \in F$.
3. $v(x + y) \geq \min \{v(x), v(y)\}$ for any $x, y \in F$.
4. There exist an element $z \in F$ with $v(z) = 1$.
5. $v(a) = 0$ for any $0 \neq a \in K$.

Property (3) is called *The Triangle Inequality.*

Lemma 1.31. ***(Strict Triangle Inequality)*** *Let v be a discrete valuation of F/K and $x, y \in F$ with $v(x) \neq v(y)$. Then $v(x + y) = \min\{v(x), v(y)\}$.*

Proof. See [16, Lemma I.1.10]. □

To any place P of F/K, we can associate a function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ as follows : let t be a local parameter of P. For any $0 \neq z \in F$, write $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P^*$. Then define $v_P(z)$ to be n. If $z = 0$, then we set $v_P(0) = \infty$. It can be shown that v_P is independent of the choice of the local parameter t and it is a discrete valuation of F/K.

Theorem 1.32. *1. Let P be a place of F/K, and v_P be the corresponding discrete valuation. Then*

$$\mathcal{O}_P = \{z \in F |\ v_P(z) \geq 0\}$$
$$P = \{z \in F |\ v_P(z) > 0\}$$
$$\mathcal{O}_P^* = \{z \in F |\ v_P(z) = 0\}$$

An element $t \in F$ is a local parameter of P if and only if $v_P(t) = 1$.

2. Let v be discrete valuation of F/K. Then $\mathcal{O} = \{z \in F|\ v(z) \geq 0\}$ is a valuation ring of F/K with the associated place $P = \{z \in F|\ v(z) > 0\}$

Proof. See [16, Theorem I.1.12]. □

Since P is a maximal ideal in $\mathcal{O}_P$, $\mathcal{O}_P/P$ is a field which is denoted by F_P. F_P is called the *residue class field* of P. When $z \in \mathcal{O}_P$, we denote $z + P$ in F_P by $z(P)$. If $z \notin \mathcal{O}_P$, then $z(P)$ is defined to be ∞ (note that the symbol ∞ is used in a different sense here, compared to Definition 1.30). The map

$$z : \begin{cases} F & \rightarrow & F_P \cup \{\infty\} \\ z & \mapsto & z(P). \end{cases} \tag{1.9}$$

is called the *residue class map* with respect to P. Note that $\tilde{K}$, and K, are embedded into F_P under this map, since $\tilde{K} \cap P = \{0\}$. Hence, we can view F_P/K as a field extension.

Definition 1.33. For $P \in \mathbb{P}_F$, define the degree of P as $degP = [F_P : K]$

It can be shown that $degP$ is a finite number. Hence, one knows why $\tilde{K}$ is a finite extension of K as $K \subset \tilde{K} \subset F_P$ and $degP = [F_P : K] < \infty$.

Remark 1.34. *Degree one places of a function field F/K are of special interest. They are called the rational places of F/K. Note that if F/K has a rational place then $\tilde{K} = K$, i.e. the full constant field of F/K is K. Furthermore, the residue class map with respect to a rational place takes values in $K \cup \{\infty\}$. In particular,* *if K is algebraically closed field so that all places of F/K are of degree 1, then one can view elements of F as functions as follows*

$$z : \begin{cases} \mathbb{P}_F & \rightarrow & K \cup \{\infty\} \\ P & \mapsto & z(P). \end{cases}$$

Note that, this is the case when $K = \mathbb{C}$ for instance. This is why we call F/K a function field and elements a function.

Definition 1.35. Let $z \in F$ and $P \in \mathbb{P}_F$. P is a *zero* of z if $v_P(z) > 0$ and P is a *pole* of z if $v_P(z) < 0$. If $v_P(z) = m > 0$, P is called a *zero of order* m; if $v_P(z) = -m < 0$, P is a *pole of order* m.

Theorem 1.36. *Let F/K be a function field, $z \in F$ be transcendental over K. Then z has at least one zero and one pole. For any $z \in F$, the number of zeroes and poles is finite.*

Proof. See [16, Corollary I.1.19 and Corollary I.3.4] □

The simplest of all function fields is $K(x)/K$, the *rational function field*. We know investigate its places (or equivalently valuation rings or discrete valuations).

Given an arbitrary monic, irreducible polynomial $p(x) \in K[x]$ consider the valuation ring,

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\} \tag{1.10}$$

of $K(x)/K$ with the maximal ideal

$$P_{P(x)} := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ p(x)|f(x),\ p(x) \nmid g(x) \right\} \tag{1.11}$$

In particular case when $p(x)$ is linear, i.e. $p(x) = x - \alpha$ with $\alpha \in K$, we abbreviate and write

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}. \tag{1.12}$$

There is another valuation ring of $K(x)/K$

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ deg(f(x)) \leq deg(g(x)) \right\} \tag{1.13}$$

with the maximal ideal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ deg(f(x)) < deg(g(x)) \right\}. \tag{1.14}$$

P_∞ is called the *infinite place* of $K(x)/K$.

Proposition 1.37. *Let $F/K(x)$ be the rational function field.*

1. *Let $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ be the place defined by Equation (1.11), where $p(x) \in K[x]$ is an irreducible polynomial. Then $p(x)$ is local parameter for P, and the corresponding discrete valuation v_P can be described as follows: if $z \in K(x)\backslash 0$ is written in the form $z = p(x)^n \cdot (f(x)/g(x))$ with $n \in \mathbb{Z}$ and $f(x) \not| g(x)$, $p(x) \not| g(x)$, then $v_P(x) = n$. The residue class field $K(x)_P = \mathcal{O}_P/P$ is isomorphic to $K[x]/(p(x))$; an isomorphism is give by*

$$\phi : \begin{cases} K[x]/(p(x)) & \rightarrow \quad K[x]_P, \\ f(x)\ mod\ p(x) & \mapsto \quad f(x)(P). \end{cases}$$

   Consequently, $degP = deg(p(x))$.

2. *In special case $p(x) = x - \alpha$ with $\alpha \in K$, the degree of $P = P_\alpha$ is one, and the residue class map is given by*

$$z(P) = z(\alpha)\ for\ z \in K(x),$$

   where $z(\alpha)$ is defined as follows: write $z = f(x)/g(x)$ with relatively prime polynomials $f(x), g(x) \in K[x]$. Then

$$z(\alpha) = \begin{cases} f(\alpha)/g(\alpha) & if \quad g(\alpha) \neq 0, \\ \infty & if \quad g(\alpha) = 0. \end{cases}$$

3. *Finally, $P = P_\infty$ be the infinite place of $K(x)/K$ defined by Equation (1.13). Then $degP = 1$. A local parameter for P_∞ is $t = 1/x$. The corresponding discrete valuation v_∞ is given by*

$$v_\infty(f(x)/g(x)) = deg(g(x)) - deg(f(x)),$$

where $f(x), g(x) \in K(x)$. The residue class map corresponding to P_∞ is determined by $z(P_\infty) = z(\infty)$ for $z \in K[x]$, where $z(\infty)$ is defined as usual: if

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \text{ with } a_n, b_m \neq 0,$$

then

$$z(\infty) = \begin{cases} a_n/b_n & if \quad n = m, \\ 0 & if \quad n < m. \\ \infty & if \quad n > m. \end{cases}$$

4. *K is the full constant field of $K(x)/K$.*

Proof. See [16, Theorem I.2.2.] □

From here on F/K will always denote an algebraic function field of one variable such that K is the full constant field of F.

Definition 1.38. The (additively written) free abelian group $\mathcal{D}_F$, which is generated by the places of F/K is called the *divisor group* of F/K. The elements of $\mathcal{D}_F$ are called *divisors* of F/K. In other words a divisor is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P, where\ n_P \in \mathbb{Z},\ and\ n_P = 0\ for\ almost\ all\ P \in \mathbb{P}_F.$$

For $Q \in \mathbb{P}_F$ and $D = \sum n_P P \in \mathcal{D}_F$ we define $v_Q(D) := n_Q$.

The set $Supp(D) := \{P \in \mathbb{P}_F \ ; \ n_p \neq 0\}$ is called the *support* of $D \in \mathcal{D}_F$.

Definition 1.39. The degree of a divisor is defined by

$$deg(D) := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot degP. \tag{1.15}$$

A partial ordering on $\mathcal{D}_F$ is given by

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}_F.$$

A divisor $D \in \mathcal{D}_F$ which satisfies $D \geq 0$ is called a positive (effective) divisor. It is easy see that for two divisors E and D with $E \geq D$, we have $deg(E) \geq deg(D)$. Since any $x \in F$ has finitely many zeroes or poles (Theorem (1.36)) the following definition makes sense.

Definition 1.40. Let $0 \neq x \in F$ and denote by Z (respectively N) the set of zeros (respectively poles) of x in $\mathbb{P}_F$. Then define

$$(x)_0 := \sum_{P \in Z} v_P(x)P : \text{ the zero divisor of} x,$$

$$(x)_\infty := \sum_{P \in Z} -v_P(x)P : \text{ the pole divisor of } x,$$

$$(x) := (x)_0 - (x)_\infty : \text{ the principal divisor of } x.$$

Remark 1.41. *The zero (respectively pole) divisor of any $0 \neq x \in$ is an effective divisor. One can represent the principal divisor of x as*

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P.$$

Non-zero elements of K are characterized by

$$x \in K \Leftrightarrow (x) = 0.$$

Theorem 1.42. *Any principal divisor has degree 0. More precisely, for $x \in F \backslash K$, we have*

$$deg(x)_0 = deg(x)_0 = [F : K(x)] < \infty.$$

Proof. See [16, Theorem I.4.11] □

Note that the above Theorem essentially says that there are as many zeros as poles for any $z \in F$ provided that they are counted properly, i.e. taking the orders of zeros and poles into account.

Let F/K be a function field and P be a degree 1 place of F/K with local parameter t. Then for $f \in F$ we can find an integer v such that $v_P(f) \geq v$. Hence

$$v_P\left(\frac{f}{t^v}\right) = v_P(f) - v_P(t^v) \geq 0.$$

Put

$$a_v := \left(\frac{f}{t^v}\right)(P) \in F_P.$$

Since $degP = 1$, $a_v \in K$. Calculate

$$\left(\frac{f}{t^v} - a_v\right)(P) = \left(\frac{f}{t^v}\right)(P) - a_v(P) = a_v - a_v = 0.$$

Then $f/t_v - a_v$ has zero at $P_{\mathbb{P}_F}$ which implies that

$$v_P\left(\frac{f}{t^v} - a_v\right) \geq 1 \text{ or } v_P(f - t^v a_v) \geq v + 1.$$

Then

$$v_P\left(\frac{f - a_v t^v}{t^{v+1}}\right) = v_P(f - a_v t^v) - v_P(t^v) \geq 0$$

Let

$$a_{v+1} := \left(\frac{f - a_v t^v}{t^{v+1}}\right)(P) \in F_P = K.$$

Then

$$\left(\frac{f - a_v t^v}{t^{v+1}} - a_{v+1}\right)(P) = \left(\frac{f - a_v t^v}{t^{v+1}}\right)(P) - a_{v+1}(P) = a_{v+1} - a_{v+1} = 0.$$

Hence, P is a zero of $\left(\frac{f - a_v t^v}{t^{v+1}} - a_{v+1}\right)$. This, again, means that

$$v_P\left(\frac{f - a_v t^v}{t^{v+1}} - a_{v+1}\right) \geq 1$$

or equivalently

$$v_P(f - a_v t^v - a_{v+1} t^{v+1}) \geq v + 2.$$

Continuing this way one gets a sequence $(a_n)_{n=v}^{\infty}$ of elements of K such that

$$v_P\left(f - \sum_{n=v}^{m} a_n t^n\right) \geq m + 1$$

for all $m \geq v$.

We summarize this construction in the formal expansion

$$f = \sum_{n=v}^{\infty} a_n t^n.$$

This is called the *local expansion* of f at P with respect to t. One can show that this representation of f is unique, i.e. a_i's are uniquely determined (see [16, Thereom IV.2.6]).

Example 1.43. Consider the rational function field $F_2(x)/F_2$. The rational places are P_1, P_0 and P_∞, which are zeroes of $x, x+1$ and $1/x$, respectively. Denote the corresponding discrete valuations by v_0, v_1 and v_∞. Let $t = x^2 + x = x(x+1) \in F_2(x)$.

Then t is a local parameter at P_0, since $v_(t) = 1$. Note that $v_1(t) = 1,\ v_\infty(t) = -2$ and $v_Q(t) = 0$ for any $Q \in \mathcal{P}_{F_2(x)} - \{P_0, P_1, P_\infty\}$. Hence, the principal divisor of t

$$(t) = P_0 + P_1 - 2P_\infty.$$

Now we look at the local expansion of some elements of $F_2(x)/F_2$ at P_0 with respect to the local parameter t.

1. $x = (x^2 + x) + (x^4 + x^2) + (x^8 + x^4) + (x^{16} + x^8) + \ldots = t + t^2 + t^4 + t^8 + \ldots$
$$= \sum_{i=0}^{\infty} t^{2^i} = \sum_{m=1}^{\infty} t^{2^{m-1}}.$$
2. $x^2 = (x^4 + x^2) + (x^8 + x^4) + (x^{16} + x^8) + \ldots = t^2 + t^4 + t^8 + \ldots$
$$= \sum_{m=1}^{\infty} t^{2^m}.$$
3. $$\frac{x}{x+1} = x\left(\frac{1}{x+1}\right) = \frac{1}{t}x^2 = \frac{1}{t}\sum_{m=1}^{\infty} t^{2^m} = \sum_{m=1}^{\infty} t^{2^m-1}.$$
4. Using (3),
$$\left(\frac{x}{x+1}\right)^2 = \sum_{m=1}^{\infty} t^{2^{m+1}-2}.$$
5. $$x^3 = (x^2+x)x^2+x^4 = tx^2+x^4 = t = \sum_{m=1}^{\infty} t^{2^m}+\sum_{m=1}^{\infty} t^{2^{m+1}} = \sum_{m=1}^{\infty} t^{2^m+1}+\sum_{m=1}^{\infty} t^{2^{m+1}},$$
where the expansion of x^4 at P_0 with respect to t obtained in an obvious way.

Theorem 1.44. *Let $P \in \mathbb{P}_F$ be a rational place and $t \in F$ be a local parameter at P. Then any element $z \in F$ has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i \text{ with } n \in \mathbb{Z} \text{ and } a_i \in K. \tag{1.16}$$

Furthermore we have

$$v_P(z) = v_P\left(\sum_{i=n}^{\infty} a_i t^i\right) = min\{i |\ a_i \neq 0\}.$$

Proof. See [16, Theorem IV.2.6] □

CHAPTER 2

POLYNOMIAL DEGREE AND LINEAR COMPLEXITY

In this chapter we will compare the complexities of the polynomial representation and the periodic sequence representation of a function over a finite field in the complexity measures degree and linear complexity, based on the joint work of A. Winterhof and W. Meidel [10].

2.1 The Main Result

Here we fix an ordering $F_q = \{\xi_0, \xi_1, \ldots, \xi_{q-1}\}$ of the elements of the finite field F_q where q is a prime power. Let σ be a q-periodic sequence of elements of F_q. We can identify each σ by a polynomial $f \in F_q[x]$ in the light of the following lemma.

Lemma 2.1. *Every q-periodic sequence σ of elements of F_q can be represented by a uniquely determined polynomial $f(x) \in F_q[x]$ of degree at most $q-1$. Conversely, every polynomial $f(x) \in F_q[x]$ of degree at most $q-1$ defines a unique q-periodic sequence over F_q. In other words, we have*

$$\sigma = f(\xi_n) \in F_q \;\; for \;\; 0 \le n < q \;\; and \;\; \sigma_{n+q} = \sigma_n \;\; for \;\; n \ge 0. \tag{2.1}$$

Proof. Apply the Lagrange Interpolation formula (Theorem 1.2) for $f(\xi_i) = \sigma_i$, where $i = 0, 1, \ldots, q-1$. This results in unique $f \in F_q[x]$. Conversely,let $f, g \in F[x]$ be any to polynomials of degree $\le q-1$. Assume that produce same sequence. That is $f(\xi) = g(\xi)$ for every $\xi \in F_q$. On the other hand the Lagrange Interpolation Formula produce a unique polynomial from inputs, which contradicts our assumptions. Therefore, every $f \in F_q[x]$ produces a unique sequence. □

When $q = p$ where p is a prime we have a simple relation between the linear complexity of σ and the degree of its representing polynomial $f \in F_q[x]$, which is given by next theorem.

Theorem 2.2. *If q=p is a prime, $F_p = \{0, 1, \ldots, p-1\}$ and $deg(f) < p$ then we have*

$$L_\sigma = deg(f) + 1. \tag{2.2}$$

Proof. Let $deg(f) = k$. We define $g_1(x), \ldots, g_{k+1}(x) \in F_q[x]$ such that

$$\begin{aligned}
g_1(x) = f(x+1) - f(x) &\Longrightarrow deg(g_1) = deg(f) - 1 \\
g_2(x) = g_1(x+1) - g_1(x) &\Longrightarrow deg(g_2) = deg(g_1) - 1 \\
&\vdots \\
g_k(x) = g_{k-1}(x+1) - g_{k-1}(x) &\Longrightarrow deg(g_k) = deg(g_{k-1}) - 1 \\
g_{k+1} &= 0.
\end{aligned}$$

Using the functions we get

$$\begin{aligned}
0 = g_{k+1} = &\ g_k(n+1) - g_k(n) \\
= &\ g_{k-1}(n+2) - g_{k-1}(n+1) - g_{k-1}(n+1) - g_{k-1}(n) \\
\vdots & \\
= &\sum_{j=0}^{i+1} (-1)^j \binom{i-1}{j} g_{k-i}(n+j).
\end{aligned}$$

When we put $i = k-1$ we get a relation between σ_i's of order $k+1 = deg(f) + 1$. The smallest degree comes from Lemma 2.1. □

When $q = p^r,\ r > 0$, power of a prime p the situation is different. For example we consider the case $F_4 = F_2(\rho) = \{0, 1, \rho, \rho+1\}$ where ρ is the zero of the polynomial $g(x) = x^2 + x + 1 \in F_2[x]$. Let σ be the sequence $\sigma = (0, \rho+1, 0, \rho+1, 0, \ldots)$ defined by the polynomial $f(x) = \rho x + x^2 \in F_4[x]$. This sequence satisfies the linear recurrence relation $\sigma_{n-2} = \sigma_n$ for $n \geq 2$. And this is the linear relation of the smallest order. Therefore we have $L_\sigma = deg(f)$. On the other hand the sequence $\sigma = (0, 1, \rho, \rho+1, 0, \ldots)$ defined by the polynomial $f(x) = x$ does not satisfy any linear recurrence relation of order ≤ 2 and we have $L_\sigma \geq 3 = deg(f) + 2$. Indeed the sequence σ satisfies relation $\sigma_n = \sigma_{n-1} + \sigma_{n-2} + \sigma_{n-3}$ for $n \geq 3$, implying $L_\sigma = deg(f) + 2$.

For the rest of the this chapter we study the relation between L_σ and $deg(f)$ in the case $q = p^r$. We consider a fixed basis $\{\beta_1, \ldots, \beta_r\}$ of F_q over F_p. Then for $0 \leq n < q$, the element $\xi_i \in F_q$ is defined by

$$\xi_n = n_1\beta_1 + n_2\beta_2 + \ldots + n_r\beta_r, \tag{2.3}$$

where

$$n = n_1 + n_2 p + \ldots + n_r p^r \; with \; 0 \leq n_k < q \; for \; 1 \leq k \leq r.$$

It is clear that $F_q = \{\xi_0, \xi_1, \ldots, \xi_{q-1}\}$.

Let us define the polynomial $S^q(x) \in F_q[x]$ by

$$S^q(x) := \sum_{n=0}^{q-1} \sigma_n x^n. \tag{2.4}$$

Lemma 2.3. *The linear complexity of L_σ of σ is given by*

$$L_\sigma = q - deg(gcd(x^q - 1, S^q(x))) = q - v, \tag{2.5}$$

where v denotes the multiplicity of 1 as zero of $S^q(x)$ and v is defined to be 0 if $s^q(1) \neq 0$.

Proof. Let $r(x) \in F_q[x]$ and defined as $r(x) := (x^n - 1)/S^q(x)$. By Proposition 1.20 we can write the generating function $\sigma(x)$ of σ as

$$\sigma(x) = \frac{r(x)}{f(x)}, \; where \; f(x) = (x^n - 1)/gcd(x^n - 1, S^q(x)).$$

Since $f(1) = 1$ and $gcd(f(x), r(x)) = 1$ then by Proposition 1.21 implies $f(x)$ is the minimal polynomial of σ. Since the linear complexity of sequence is defined to the degree of the its minimal polynomial then the result follows. □

Remark 2.4. *Using the Lemma 2.3 one can easily verify the following*

$$L_\sigma = q \quad if \; and \; only \; if \quad S^q(1) \neq 0.$$

Lemma 2.5. *Let f be in the form*

$$f(x) = \sum_{j=0}^{q-1} \alpha_j x^j. \tag{2.6}$$

Then we have

$$S^q(1) = -\alpha_{q-1}$$

and in particular

$$L\sigma = q \; if \; and \; only \; if \; deg(f) = q - 1. \tag{2.7}$$

Proof. By the construction of σ, we have

$$S^q(1) = \sum_{n=0}^{q-1} \sigma_n = \sum_{\xi \in F_q} f(\xi).$$

Using the definition of f, we get

$$\sum_{\xi \in F_q} f(\xi) = \sum_{\xi \in F_q} \sum_{j=0}^{q-1} \alpha_j \xi^j,$$

and by changing the order of summation, we have

$$\sum_{j=0}^{q-1} \sum_{\xi \in F_q} \alpha_j \xi^j = \sum_{j=0}^{q-1} \alpha_j \sum_{\xi \in F_q} \xi^j.$$

Proposition 1.3 yields that when $j = q - 1$ inner sum is equal to -1 or otherwise it is zero. With the help of this, we have

$$\sum_{j=0}^{q-1} \alpha_j \sum_{\xi \in F_q} \xi^j = -\alpha_{q-1}.$$

Now if $L_\sigma = q$ then $v = 0$ that is $S^q(1) \neq 0$ and we found that $S^q(1) = -\alpha_{q-1}$ this implies $deg(f) = q - 1$. Conversely, if $deg(f) = q - 1$ then $S^q(1) \neq 0$. By Remark 2.4 we have $L_\sigma = q$, which completes the proof. □

Theorem 2.6. *(Lucas Congruence) For every prime p,*

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2} \cdots \binom{n_r}{kr}, \tag{2.8}$$

where base p expansion of n and k are $n = n_0 + n_1 p + \ldots + n_r p^r$, $n_i \leq p - 1$, *and* $k = k_0 + k_1 p + \ldots + k_r p^r$, $k_i \leq p - 1$ *respectively.*

Proof. See [9]. □

Remark 2.7. *To estimate the multiplicity v of 1 we will use the following expression,*

$$S^q(x)^{(t)} = \sum_{n=0}^{q-1} \binom{n}{t} \sigma_n x^{n-t}, \tag{2.9}$$

evaluated at x=1.

Let $\{\delta_1, \ldots, \delta_r\}$ be the *dual basis* of the basis $\{\beta_1, \ldots, \beta_r\}$, i.e.

$$\mathrm{Tr}(\delta_i \beta_j) = \begin{cases} 0, & for \quad i \neq j, \\ 1 & for \quad i = j. \end{cases}$$

Using the trace map and equation (2.3) we can calculate n_i's, that is

$$n_i = \mathrm{Tr}(\delta_i \xi_n), \text{ for } i = 1, \ldots, r, \tag{2.10}$$

therefore, for $0 \leq n < q$ we have

$$n = \sum_{k=1}^{r} \mathrm{Tr}(\delta_k \xi_n) p^{k-1}. \tag{2.11}$$

Applying Lucas's Congruence (Theorem 2.6) to the equation (2.11), where $t = t_1 + \ldots + t_r p^{r-1}$, $0 \leq t_i < p$, we get

$$\binom{n}{t} \equiv \binom{\mathrm{Tr}(\delta_1 \xi_n)}{t_1} \cdots \binom{\mathrm{Tr}(\delta_r \xi_n)}{t_r} \; mod \; p. \tag{2.12}$$

Now we can calculate $S^q(1)^{(t)}$

$$\begin{aligned} S^q(1)^{(t)} &= \sum_{n=0}^{q-1} \binom{n}{t} \sigma_n \\ &= \sum_{n=0}^{q-1} \binom{\mathrm{Tr}(\delta_1 \xi_n)}{t_1} \cdots \binom{\mathrm{Tr}(\delta_r \xi_n)}{t_r} \sigma_n \\ &= \sum_{n=0}^{q-1} \binom{\mathrm{Tr}(\delta_1 \xi_n)}{t_1} \cdots \binom{\mathrm{Tr}(\delta_r \xi_n)}{t_r} f(\xi_n), \end{aligned}$$

thus we get get

$$S^q(1)^{(t)} = \sum_{\xi \in F_q} \binom{\mathrm{Tr}(\delta_1 \xi)}{t_1} \cdots \binom{\mathrm{Tr}(\delta_r \xi)}{t_r} f(\xi) \tag{2.13}$$

We will use equation (2.13) in our estimation of $S^q(1)^{(t)}$.

Proposition 2.8. *Let* $p_0(x), p_1(x), \ldots, p_s(x) \in F_q[x]$ *and be defined as* $p_0(x) = 1$ *and*

$$p_t(x) = \frac{1}{t!}x(x-1)\cdots(x-t-1) \in F_q[x],\ 1 \leq t \leq s < p.$$

Then $p_0(x), \ldots, p_s(x)$ *forms a basis of the linear space of polynomials of degree at most* s.

Proof. Let $a_0, \ldots, a_s \in F_q$ such that

$$a_0p_0(x) + a_1p_1(x) + \ldots + a_sp_s(x) = 0. \tag{2.14}$$

Note that $deg(p_s) > deg(p_{s-1}) > \cdots > deg(p_0)$ with $deg(p_i(x)) = i$ for $0 \leq i \leq s$. Expanding equation (2.14) one has a_s as the coefficient $p_s(x)/s!$, implying $a_s = 0$. Similarly the rest of a_i's, $0 \leq i \leq s-1$ becomes 0, which proves the assertion. □

Lemma 2.9. *let* $f(x) = \sum_{j=0}^{q-2} \alpha_j x^j \in F_q[x]$. *If* $L_\sigma = q - s$ *with* $0 \leq s < p$ *then some coefficients* $\alpha_{q-1-p^{m_1}-p^{m_2}-\cdots-p^{m_s}}$ *of* $f(x)$ *with* $0 \leq m_1, \ldots, m_s < r$ *are non-zero*

Proof. For $0 \leq t < s$ we have $S^q(1)^{(t)} = 0$ and $S^q(1)^{(s)} \neq 1$ by Lemma 2.3. By the Proposition 2.8 the polynomials $p_0(x)$ and

$$p_t(x) = \frac{1}{t!}x(x-1)\cdots(x-t-1) \in F_q[x],\ 1 \leq t \leq s < p$$

form a basis of the linear space of the polynomials of degree at most s, then one can write $x^s/s!$ as a linear combination of the polynomials $p_0(x), \ldots, p_s(x)$, namely

$$\frac{x^s}{s!} = \sum_{t=0}^{s} c_t p_t(x) \text{ with } c_s = 1. \tag{2.15}$$

Using our estimation on $S^q(1)^{(t)}$ (Equation (2.13)), where $t = s$, we have

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} \binom{\mathrm{Tr}(\delta_1\xi)}{s_1} \cdots \binom{\mathrm{Tr}(\delta_r\xi)}{s_r} f(\xi).$$

Since $s < p$ then $s = s_1$ and $s_i = 0$ for $1 < i \leq r$. So we can write $S^q(1)^{(s)}$ as

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} \binom{\mathrm{Tr}(\delta_1\xi)}{s_1} f(\xi). \tag{2.16}$$

Using the properties of $p_t(x)$ we have

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} p_s(\mathrm{Tr}(\delta_1 \xi)) f(\xi).$$

We can write the equation (2.16) by calculating $p_s(x)$ from the equation (2.15), that is

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} \left(\frac{(\mathrm{Tr}(\delta_i \xi))^s}{s!} - \sum_{t=0}^{s-1} c_t p_t(\mathrm{Tr}(\delta_1 \xi)) \right) f(\xi).$$

our estimation on $S^q(1)^{(t)}$ (equation (2.13)) implies

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} \frac{(\mathrm{Tr}(\delta_i \xi))^s}{s!} f(\xi) - \sum_{t=0}^{s-1} c_t S^q(1)^{(t)}.$$

In the beginning of the proof we stated that $S^q(1)^{(t)} = 0$ for $1 \le t \le s-1$, then we have

$$S^q(1)^{(s)} = \sum_{\xi \in F_q} \frac{(\mathrm{Tr}(\delta_i \xi))^s}{s!} f(\xi)$$

In this equation we replace f by its expression

$$S^q(1)^{(s)} = \frac{1}{s!} \sum_{j=0}^{q-2} \alpha_j \sum_{\xi \in F_q} (\mathrm{Tr}(\delta_1 \xi))^s \xi^j,$$

and by writing the trace function explicitly we get

$$S^q(1)^{(s)} = \frac{1}{s!} \sum_{j=0}^{q-2} \alpha_j \sum_{\xi \in F_q} \left(\sum_{m=0}^{r-1} (\delta_1 \xi)^{p^m} \right)^s \xi^j$$

Expanding the power s, we have

$$S^q(1)^{(s)} = \frac{1}{s!} \sum_{m_1, \ldots, m_s = 0}^{r-1} \delta^{p^{m_1} + \ldots + p^{m_s}} \sum_{j=0}^{q-2} \alpha_j \sum_{\xi \in F_q} \xi^{p^{m_1} + \ldots + p^{m_s} + j},$$

using Proposition 1.3 on the inner sum we get

$$S^q(1)^{(s)} = -\frac{1}{s!} \sum_{m_1, \ldots, m_s = 0}^{r-1} \delta^{p^{m_1} + \ldots + p^{m_s}} \alpha_{q-1-(p^{m_1} + \ldots + p^{m_s})} \neq 0 \tag{2.17}$$

which proves the lemma. □

Lemma 2.10. *Let* $0 \leq s < p$ *and* $f(x) = \sum_{j=0}^{q-2} \alpha_j x^j \in F_q[x]$ *with*

$$\alpha_{q-1-(p^{m_1}+\ldots+p^{m_s})} \neq 0, \; \textit{for some } 0 \leq m_i < r, \; 1 \leq i \leq s.$$

Then

$$L_\sigma \geq q - sq/p.$$

Proof. Assume that $L_\sigma < q - sq/p$. By Lemma 2.3 we have $S^q(1)^{(t)} = 0$ for $0 \leq t \leq sq/p$.

Now as in the proof of pervious lemma we will calculate $S^q(1)^{(t)}$. By equation (2.13), where $t = t_1 + \ldots + t_r p^{r-1}$ with $0 \leq t_i < p$ for $0 \leq i < r$, we have

$$S^q(1)^{(t)} = \sum_{\xi \in F_q} \binom{\mathrm{Tr}(\delta_1 \xi)}{t_1} \cdots \binom{\mathrm{Tr}(\delta_r \xi)}{t_r} f(\xi),$$

using properties of $p_t(x)$ we rewrite as

$$S^q(1)^{(t)} = \sum_{\xi \in F_q} p_{t_1}(\mathrm{Tr}(\delta_1 \xi)) \cdots p_{t_r}(\mathrm{Tr}(\delta_r \xi)) f(\xi). \tag{2.18}$$

Now for each p_{t_i}, $1 \leq i \leq r$, write $x^{t_i}/t_i!$ as a linear combination of p_i's as in the previous lemma, that is

$$\frac{\mathrm{Tr}(\delta_1 \xi)^{t_i}}{t_i!} = \sum_{t=0}^{t_i} c_t p_t(\mathrm{Tr}(\delta_i \xi)), \; \textit{with } c_{t_i} = 1,$$

calculating $p_{t_i}(\mathrm{Tr}(\delta_i \xi))$'s we have

$$p_{t_i}(\mathrm{Tr}(\delta_i \xi)) = \frac{\mathrm{Tr}(\delta_1 \xi)^{t_i}}{t_i!} - \sum_{t=0}^{t_i - 1} c_t p_t(\mathrm{Tr}(\delta_t \xi))$$

using $p_{t_i}(\mathrm{Tr}(\delta_i \xi))$'s we rewrite Equation (2.18) as

$$S^q(1)^{(t)} = \sum_{\xi \in F_q} \left(\frac{\mathrm{Tr}(\delta_1 \xi)^{t_1}}{t_1!} - \sum_{t=0}^{t_1 - 1} c_t p_t(\mathrm{Tr}(\delta_t \xi)) \right) \cdots \left(\frac{\mathrm{Tr}(\delta_1 \xi)^{t_r}}{t_r!} - \sum_{t=0}^{t_r - 1} c_t p_t(\mathrm{Tr}(\delta_t \xi)) \right) f(\xi),$$

by distributing all parenthesis and then multiplying by f then using using properties of $p_t(x)$ and our estimate on $S^q(1)^{(t)}$ we get

$$\begin{aligned} S^q(1)^{(t)} &= \sum_{\xi \in F_q} \left[\left(\frac{\mathrm{Tr}(\delta_1 \xi)^{t_r}}{t_r!} \right) \cdots \left(\frac{\mathrm{Tr}(\delta_r \xi)^{t_r}}{t_r!} \right) \right] f(\xi) - \cdots - \\ & \left[\cdots \left(\sum_{t=0}^{t_i - 1} c_t S^q(1)^{(t)} \right) \cdots \right] f(\xi) - \cdots - \\ & \left[\left(\sum_{t=0}^{t_1 - 1} c_t S^q(1)^{(t)} \right) \cdots \left(\sum_{t=0}^{t_r - 1} c_t S^q(1)^{(t)} \right) \right] f(\xi), \end{aligned} \tag{2.19}$$

by the assumption that we made in the beginning of lemma all $S^q(1)^{(t)}$'s are zero, whose appear as a term element in the above equation. Then we have

$$S^q(1)^{(t)} = \sum_{\xi \in F_q} \left(\frac{\mathrm{Tr}(\delta_1 \xi)^{t_r}}{t_r!} \right) \cdots \left(\frac{\mathrm{Tr}(\delta_r \xi)^{t_r}}{t_r!} \right) f(\xi) = 0 \tag{2.20}$$

For every $\alpha \in F_q$ we have $\alpha = \sum_{k=1}^{r} \alpha_k \delta_k$ where $\alpha_k \in F_p$. Now we want to calculate $\sum_{\xi \in F_q} \mathrm{Tr}(\alpha\xi)^s f(\xi)$. By linearity of the trace map (Theorem 1.5) we have,

$$\sum_{\xi \in F_q} \mathrm{Tr}(\delta\xi)^s f(\xi) = \sum_{\xi \in F_q} \left(\sum_{k=1}^{r} \alpha_k \mathrm{Tr}(\delta_k \xi) \right)^s f(\xi),$$

expanding the inner sum, we have,

$$\sum_{\xi \in F_q} \mathrm{Tr}(\delta\xi)^s f(\xi) = \sum_{\xi \in F_q} \sum_{k_1,\ldots,k_s=1}^{r} \alpha_{k_1} \cdots \alpha_{k_s} \mathrm{Tr}(\delta_{k_1}\xi) \cdots \mathrm{Tr}(\delta_{k_s}\xi) f(\xi) =$$

$$= \sum_{k_1,\ldots,k_s=1}^{r} \alpha_{k_1} \cdots \alpha_{k_s} \sum_{\xi \in F_q} \mathrm{Tr}(\delta_{k_1}\xi) \cdots \mathrm{Tr}(\delta_{k_s}\xi) f(\xi) \tag{2.21}$$

Now we define a polynomial

$$H_s(x) := \sum_{\xi \in F_q} \mathrm{Tr}(\xi x)^s f(\xi) \tag{2.22}$$

By equation (2.20) and $1 < k_i \leq r$, $H_s(x)$ has q zeroes, namely all $\alpha \in F_q$. Since $deg(H_s(x)) \leq sq/p < q$ we have $H_s(x) \equiv 0$. On the other hand analogously to the proof of previous lemma we get

$$\begin{aligned}
H_s(x) &= \sum_{j=0}^{q-2} \sum_{\xi \in F_q} \mathrm{Tr}(\xi x)^j \xi^s, \\
&= \sum_{j=0}^{q-2} \sum_{\xi \in F_q} \left(\sum_{m=0}^{r-1} (\xi x)^{p^m} \right)^s \xi^j, \\
&= \sum_{m_1,\ldots,m_s=0}^{r-1} \sum_{j=0}^{q-2} \alpha_j \sum_{\xi \in F_q} \xi^{p^{m_1}+\ldots+p^{m_s}+j} x^{p^{m_1}+\ldots+p^{m_s}}, \\
&= -\sum_{m_1,\ldots,m_s=0}^{r-1} \alpha_{q-1-(p^{m_1}+\ldots+p^{m_s})} x^{p^{m_1}+\ldots+p^{m_s}}, \\
&= -\sum_{j=0}^{q-1} k_{q-1-j} \alpha_j x^j \equiv 0
\end{aligned}$$

with

$$k_j = \begin{cases} 0 & if \quad j_1 + \ldots + j_r \neq s, \\ \binom{s}{j_1}\binom{s-j_1}{j_2}\cdots\binom{s-j_1-\ldots-j_{r-1}}{j_r} & if \quad j_1 + \ldots + j_r = s, \end{cases}$$

where $j = j_1 + \ldots + j_r p^{r-1}$ with $0 \leq j_i < p$ for $0 \leq i \leq r$. Since $k_j \neq 0$ if and only if $j_1 + \ldots + j_r = s$ we get $\alpha_{q-1-(p^{m_1}+\ldots+p^{m_s})} = 0$ for all $0 \leq m_1, \ldots, m_s < r$ which contradicts our assumption. Then result follows. □

Theorem 2.11. *Let $f(x) \in F_q[x]$ be a polynomial of degree at most $q-1$ and σ be a sequence defined by (2.1) and (2.3). Then we have*

$$(deg(f(x) + 1 + p - q)\frac{q}{p} \leq L_\sigma \leq (deg(f(x) + 1)\frac{p}{q} + q - p$$

or equivalently,

$$(L_\sigma + p - q)\frac{p}{q} - 1 \leq deg(f(x)) \leq L_\sigma \frac{p}{q} + q - p - 1.$$

Proof. If the linear complexity $L_\sigma \leq q - p$ then the upper bound is satisfied. Then we may suppose that

$$L_\sigma \leq q - s, \ with \ 0 \leq s < p.$$

By calculating the smallest possible degree of f by Lemma 2.9, that is m_i's are equal to $r-1$, we have

$$deg(f) \geq q - 1 - s\frac{q}{p},$$

and then we can calculate

$$\begin{aligned} q - 1 - \frac{sq}{p} &\leq deg(f) \\ pq - sq &\leq (deg(f) + 1)p \\ p - s + q - q &\leq (deg(f) + 1)\frac{p}{q} \\ L_\sigma &\leq (deg(f) + 1)\frac{p}{q} + q - s. \end{aligned}$$

If $deg(f) \leq q - 1 - p$ the lower bound is satisfied. Then we may suppose that

$$deg(f) = q - 1 - s, \ 0 \leq s < p.$$

By Lemma 2.10 we have

$$L_\sigma \geq q - s\frac{q}{p}$$

and then

$$L_\sigma \geq (deg(f) + 1 + p - q)\frac{q}{p}.$$

To prove the second inequality we will use the first one. To prove the upper bound we will calculate

$$\begin{aligned} L_\sigma &\leq (deg(f)+1)\frac{p}{q} + q - p \\ L_\sigma - p + q &\leq (deg(f)+1)\frac{p}{q} \\ (L_\sigma - p + q)\frac{q}{p} &\leq deg(f) + 1 \\ (L_\sigma - p + q)\frac{q}{p} - 1 &\leq deg(f) \end{aligned}$$

to prove the upper bound we calculate

$$\begin{aligned} (deg(f) + 1 + p - q)\frac{q}{p} &\leq L_\sigma \\ (deg(f) + 1 + p - q) &\leq L_\sigma\frac{p}{q} \\ feg(f) &\leq L_\sigma\frac{p}{q} + q - p - 1, \end{aligned}$$

which prove the theorem. □

2.2 Consequences

Corollary 2.12. *If $deg(f) \geq q - 2p + 1$ then we have*

$$L_\sigma \geq \frac{q}{p}.$$

Proof. Using the upper bound for $f(x)$, which is proved in previous theorem (Theorem 2.11), we have

$$\begin{aligned} q - 2p + 1 \leq deg(f) &\leq L_\sigma\frac{p}{q} + q - p - 1 \\ \frac{2q - qp}{p} &\leq L_\sigma \\ \frac{q}{p} &\leq L_\sigma. \end{aligned}$$

□

Example 2.13. Consider $F_9 = F_3(\alpha)$ with $\alpha^2 + 1 = 0$ and the basis $\{\beta_1, \beta_2\} = \{1, \alpha\}$. The sequence σ defined by the polynomial $f(x) = x^3 + x$ satisfies $\sigma_n = -\sigma_{n-1} - \sigma_{n-2},\ n \geq 2$, and we have $L_\sigma = 2$.

Corollary 2.14. *$L_\sigma = q - sq/p$ with $0 \leq s \leq 1$ then we have*

$$L_\sigma = (deg(f) + 1 + p - q)\frac{q}{p}.$$

Proof. For $s = 0$ the result equivalent to Remark 2.4. For $s = 1$ Remark 2.4 yields that $deg(f) \leq q - 2$. Since the Equation (2.20) is valid for $0 \leq t < q$, from Equation (2.20) and Equation (2.20) we know that

$$H_1(x) = -\sum_{m=0}^{r-1} \alpha_{q-1-p^m} x^{p^m}$$

has q/p distinct zeroes, namely all the elements of the form $\alpha = \sum_{k=1}^{r} \alpha_k \delta^k$ with $\alpha_r = 0$. Since $deg(f) \leq q/p$ all the zeroes have multiplicity 1. Hence the first derivative of $H_1(x)$ is not zero polynomial, i.e.

$$H_1(x)^{(1)} = -\sum_{m=0}^{r-1} \alpha_{q-1-p^m} p^m x^{p^m - 1} = -\alpha_{q-2} \neq 0$$

and this simply imply $deg(f) \geq q - 2$, therefore $deg(f) = q - 1$. Now we have

$$deg(f(x)) = q - 2 = L_\sigma \frac{q}{p} + q - p - 1.$$

□

Corollary 2.15. *If $deg(f) = q - 1 - sq/p$ with $0 \leq s < p$ then we have*

$$L_\sigma = (deg(f) + 1)\frac{p}{q} + q - p.$$

Proof. For s $= 0$ the result equivalent to Remark 2.4. For $s \geq 1$ the assumption $L_\sigma = q - s^t$ with $0 \leq s < p$ would imply $deg(f) \geq q - 1 - s^t q/p > q - 1 - sq/p$, as in the proof of Theorem 2.11 and by Lemma 2.9. Applying the bounds on the Theorem 2.11 to $deg(f)$ we have $L_\sigma \leq q - s$. By equation (2.17) with degree of f we have

$$S^q(1)^{(s)} = -\frac{1}{s!}\, \delta^{s/p}\, \alpha_{q-1-sq/p} \neq 0.$$

□

The two corollaries above show that the upper and lower bounds on the Theorem 2.11 are sharp.

CHAPTER 3

BOUNDS FOR LINEAR COMPLEXITY

3.1 The Power Generator

In this section we will deal with the linear complexity of the Power Generator. The exposition in this section follows the work of Igor Shparlinski (see [15]).

Let v,m and e be integers with $gcd(v, m) = 1$. Then one can define a sequence σ by the recurrence relation

$$\sigma_n \equiv \sigma_{n-1}^e \ (mod\, m), \ 0 \leq \sigma_n \leq m-1, \ n = 1, 2, \dots\ , \tag{3.1}$$

with the *initial value* $\sigma_0 = v$.

Definition 3.1. The sequence defined by equation (3.1) is called the *power generator*. In the special cases, $gcd(e, \varphi(m)) = 1$, where $\varphi(m)$ is the Euler function, and $e = 2$, this sequence is called the *RSA generator* and as the *Blum-Blum-Shub generator* (see [3]), respectively.

m is called a *Blum integer* if $m = pl$, for some distinct primes p, l.

Lemma 3.2. *The sequence given by* (3.1) *is ultimately periodic with some period* $t \leq \varphi(\varphi(m))$. *In particular, if* $gcd(e, \varphi(m)) = 1$ *then the sequence is purely periodic.*

Proof. Eventually, we will have $\sigma_n \equiv \sigma_k \ (mod\, m)$ for some n, k since all the powers of v cannot have different values to modulo m. Then we have

$$\begin{aligned} v^{e^n} &\equiv \ v^{e^k} \ (mod\, m) \ \Rightarrow \\ e^n &\equiv \ v^{e^k} \ (mod\, \varphi(m)) \ \Rightarrow \\ n &\leq \ k \ (mod\, \varphi(\varphi(m))) \end{aligned}$$

then the sequence will be ultimately periodic with period $t \leq \varphi(\varphi(m)))$. If $gcd(e, \varphi(m)) = 1$ then we have a generator of the multiplicative group $\mathbb{Z}_{\varphi(m)}$, that e have order $\varphi(m)$ and so σ has zero length pre-period this implies sequence is periodic. □

Throughout this section we assume that the sequence given by (3.1) is *purely periodic*, that is $\sigma_n = \sigma_{n+t}$ beginning with $n = 0$, otherwise one can consider a shift of the original sequence.

Lemma 3.3. *Let $q \geq 2$ and g be integers, 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*

$$g^x \equiv a + y \ (mod\ q),\ 0 \leq x \leq H-1,\ 0 \leq y \leq h-1$$

has

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

solutions (x, y).

Proof. Proof can be found in [12]. □

Lemma 3.4. *Let σ be a homogeneous linear recurrence sequence over a finite field F with linear complexity L_σ. Then for any $T > L_\sigma + 1$ pairwise distinct non negative integers $j_1, \ldots, j_T$ there exist $c_1, \ldots, c_T \in F$, not all are equal to zero, such that*

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

Proof. If any two of the σ_{n+j_i}'s are equal then the results follows due to periodicity. So we assume that all σ_{n+j_i}'s are distinct.
Since σ has linear complexity L_σ then it satisfies a linear recurrence relation of order L_σ, i.e.

$$0 = \sum_{m=0}^{L_\sigma} b_m \sigma_{k-m},\ for\ k \leq L_\sigma.$$

Note that using this relation one can write as $\sigma_j,\ j \geq L_\sigma$ as a linear combination of the first L_σ terms. That is

$$\sigma_{n+j_i} = \sum_{m=0}^{L_\sigma - 1} a_{m_{j_i}} \sigma_{k-m}.$$

Now we want to look at

$$\begin{aligned} 0 &= \sum_{i=1}^{T} c_i \sigma_{n+j_i} \\ &= \sum_{i=1}^{T} c_i \sum_{m=0}^{L_\sigma - 1} a_{m_{j_i}} \sigma_{k-m} \\ &= \sum_{m=0}^{L_\sigma - 1} \sigma_{k-m} \sum_{i=1}^{T} c_i a_{m_{j_i}}. \end{aligned}$$

Since $\{\sigma_0, \dots, \sigma_{T-1}\}$ are linearly independent (Theorem 1.13), the inner sums are equal to zero. Since we have $T > L_\sigma$ the system

$$\sum_{i=1}^{T} c_i a_{m_{j_i}} = 0$$

for $m = 0, 1, \dots, L_\sigma - 1$, has a non-trivial solution, which proves the lemma. □

Theorem 3.5. *Let $m = p$ be a prime. Assume that the sequence σ, given by* (3.1) *with $m = p$, is purely periodic with period t. Then, for the linear complexity L_σ of this sequence the bound*

$$L_\sigma \geq \frac{t^2}{p-1} \tag{3.2}$$

holds.

Proof. Let τ be the largest positive integer for which the powers e^x for $x = 1, \dots, \tau$, are pairwise distinct modulo $p - 1$. Since the sequence can also be written as $\sigma = (v, v^e, v^{e^2}, v^{e^3}, \dots, v^{e^n}, \dots)$ the number of distinct powers of e is less then or equal to the period of the sequence, i.e. $\tau \geq t$. From Lemma 3.3 there exists a, $0 \leq a \leq p - 1$, such that the number of solutions of T of the congruence

$$e^x \equiv \ a + y \ (mod\, p-1), 0 \leq x \leq \tau, \ 0 \leq y \leq t - 1$$

satisfies

$$T \geq \frac{t\tau}{p-1} \geq \frac{t^2}{p-1} \tag{3.3}$$

Let $(j_1, k_1), \dots, (j_r, k_r)$ be the corresponding solutions.
Now assume that $L_\sigma \leq T - 1$. Since

$$\sigma_{n+j_i} \equiv v^{e^n + j_i} \equiv \sigma_n^{e^{j_i}} \equiv \sigma_n^{a+k_i} \ (mod\, p), \ n = 1, 2, \dots, \ \ i = 1, \dots, T,$$

by using Lemma 3.4 on $\sigma_n^{a+k_i}$ (where $L_\sigma < T$) we have integers $c_1, \ldots, c_T$, not all zero modulo p, such that

$$\sum_{i=1}^{T} c_i \sigma_n^{a+k_i} \equiv \sigma^a \sum_{i=1}^{T} c_i \sigma_n^{k_i} \equiv 0 \ (mod\ p), \ n = 1, 2, \ldots.$$

$\sigma_n \not\equiv 0 \ (mod\ p)$ for $n = 1, 2, \ldots$ since v, the initial value, is not zero. Then we can conclude that the non zero polynomial

$$f(x) = \sum_{i=1}^{T} c_i x^{k_i}$$

has t distinct zeroes, namely $u_n, \ n = 1, \ldots, t$ modulo p, which is impossible since

$$deg(f) \leq \max\{k_i \mid 1 \leq i \leq T\} \leq t - 1.$$

Hence our assumption is false. So $L_\sigma \geq T$. □

Theorem 3.6. *Let $m = pl$, where p and l are two distinct primes. Assume that the sequence σ, given by* (3.1)*, is purely periodic with period t. Then for the linear complexity L_σ of this sequence the bound*

$$L_\sigma \geq t\varphi(m)^{-1/2} \tag{3.4}$$

holds.

Proof. Let t_p be the period of the sequence σ modulo p and let t_l be the period of the sequence σ modulo l. We have the inequality $t \leq t_p t_l$. Therefore

$$\frac{t_p^2 t_l^2}{(p-1)(l-1)} \geq \frac{t^2}{\varphi(m)}.$$

Without loss of generality we may assume that

$$\frac{t_p^2}{p-1} \geq t\varphi(m)^{-1/2}.$$

Using the fact that L_σ is not smaller than the linear complexity modulo p from previous theorem we derive the desired result. □

3.2 The Self-Shrinking Generator

In 1994, Meier and Staffbelbach proposed the "*self-shrinking generator*" ([11]), a stream cipher based on irregular decimation of the output of a maximal periodic sequence.

Let $(s_n) = (s_0, s_1, \ldots)$ be the output of a maximal periodic sequence of period $2^n - 1$. At time k, consider the pairs (s_{2k}, s_{2k+1}) of the terms of (s_n). If $(s_{2k}) = 1$, then the next term (s_{2k+1}) is the output of the self-shrinking generator. If $(s_{2k}) = 0$, no term is output.

One can define the self-shrinking generator in a different way, for all non-negative integers i let $\tau(i)$ be the unique non-negative integers with the property that $s_{\tau(i)} = 1$ and that there are precisely $i+1$ ones in the sequence $s_0, s_2, \ldots, s_{2\tau(i)}$. Then output of the self-shrinking generator is the binary sequence $(z) = (s_{2\tau(0)+1}, s_{2\tau(1)+1}, \ldots)$.

To understand better we look the following example, suppose that (s_n)

$$100000100001100010100111101000111001001011011101100110101011111\ldots$$

is a maximal periodic sequence of period $2^6 - 1$. Then the self-shrinking generator bases on this maximal periodic sequence will be the output sequence

$$(z) = 00000100100110000111111100101111\ldots$$

of period 2^5.

Meier and Staffbelbach showed that the linear complexity $L_{(z)}$ of (z) is always such that $2^{\lfloor n/2 \rfloor - 1} \leq L_{(z)} \leq 2^{n-1} - 1$. Meier and Staffbelbach also remarked that, in their experiments, the linear complexity of (z) never exceeds $2^{n-1} - (n-2)$. In this section we prove that the experiments of Meier and Staffbelbach is correct and this is the work of Simon R. Blackburn (see [2]). Moreover, the expected value of the linear complexity of randomly chosen binary sequence of period 2^{n-1} is greater than $2^{n-1} - 1$ (see [14, Proposition 4.6]). Hence the output of a self-shrinking generator exhibits non-random behavior with respect to linear complexity.

If σ is a sequence of period dividing 2^{n-1} over a finite field F of characteristic 2, Then $(x^{2^{n-1}} + 1) = (x+1)^{2^{n-1}}$ is a characteristic polynomial for σ. Moreover, since the minimal polynomial m is the generator of the ideal of characteristic polynomials of σ then $m = (x+1)^{L_\sigma}$, $0 \leq L_\sigma \leq 2^{n-1}$, where L_σ is the linear complexity of σ. And also note that, $L_\sigma \leq 2^{n-1} - (n-2)$ if and only if $(x+1)^{2^{n-1}-(n-2)}$ is a characteristic polynomial for σ. This condition is equivalent to the statement

$$\sum_{i=0}^{2^{n-1}-(n-2)} \binom{2^{n-1} - (n-2)}{i} \sigma_{i+e} = 0$$

for all non-negative integers e. Since $\binom{2^{n-1}-(n-2)}{i}$ is defined to be the zero for all i such that $2^{n-1} - (n-2) < i < 2^{n-1}$, we may rephrase this condition as

$$\sum_{i=0}^{2^{n-1}-1} \binom{2^{n-1} - (n-2)}{i} \sigma_{i+e} = 0 \tag{3.5}$$

for all non-negative integers e.

Lemma 3.7. *Let σ be a sequence of period dividing $2^n - 1$ over a finite field F of characteristic 2, where n is a fixed integer such that $n \geq 3$. Then σ has linear complexity $L_\sigma \leq 2^{n-1} - (n-2)$ if and only if*

$$\sum_{i} \sigma_{i+e} = 0, \tag{3.6}$$

for all non-negative integers e, where sum is taken over all integers $i \in \{0, 1, \ldots, 2^{n-1} - 1\}$ such that the binary expansion of i contains a zero as digit whenever the corresponding digits of $n - 3$ is a one.

Before the proof we look at the integers i, for example take $n = 5$ then i is in the set $\{0, 1, \ldots, 15\}$. Now we will compare this set and $n - 3 = 2$ in their binary representations.

$$\begin{array}{rlrl} i = 0 = 0000 & 0010 \quad * & i = 1 = 0001 & 0010 \quad * \\ 2 = 0010 & 0010 & 3 = 0011 & 0010 \\ 4 = 0100 & 0010 \quad * & 5 = 0101 & 0010 \quad * \\ 6 = 0110 & 0010 & 7 = 0111 & 0010 \\ 8 = 1000 & 0010 \quad * & 9 = 1001 & 0010 \quad * \\ 10 = 1010 & 0010 & 11 = 1011 & 0010 \\ 12 = 1100 & 0010 \quad * & 13 = 1101 & 0010 \quad * \\ 14 = 1110 & 0010 & 15 = 1111 & 0010, \end{array}$$

so i ranges over $\{0, 1, 4, 5, 8, 9, 12, 13\}$. Here we also note that, one can easily find the sets by j is in the set if $j \ \wedge \ (n-3) = 0$, where $\wedge$ is the binary *and* operator. With similar calculations, one can see that, i ranges over the sets

$$\begin{gathered} \{0,1,2,3\}, \\ \{0,2,4,6\}, \\ \{0,1,4,5,8,9,12,13\}, \\ \{0,4,8,12,16,20,24,28\}, \end{gathered}$$

when $n = 3, 4, 5$ *and* 6 respectively.

Proof. (*of Lemma* 3.7) By the Equation (3.5), to prove the lemma it is sufficient to prove that for all $i \in \{0, 1, \ldots, 2^{n-1} - 1\}$, we have $\binom{2^{n-1}-(n-2)}{i} = 1$ if and only if the binary digits of i are zero whenever the corresponding digits of $n - 3$ are one.

Now Lucas's theorem states (see [1, Theorem 4.71])that for all $b_0, b_1, \ldots, b_{n-2}$ and $c_0, c_1, \ldots, c_{n-2}$ in $\{0, 1\}$,

$$\binom{\sum_{j=0}^{n-2} b_i 2^i}{\sum_{j=0}^{n-2} c_i 2^i} = 1 \text{ if and only if } c_i \leq b_i \text{ for all } i.$$

Moreover, when $n > 3$, $(2^{n-1} - (n-2)) + (n-3) = 2^{n-1} - 1 = (111 \ldots 111)_2$, where the result has $n-1$ digits (in binary representation). Since $2^{n-1} - (n-2)$ is a $n-1$

digit binary integer then the least $n-1$ significant binary digits of $2^{n-1}-(n-2)$ are the complement of the $n-1$ least significant binary digits of $n-3$. Hence, whenever $n-3$ has a one in a digit then i has a zero in that digit. Hence lemma follows. $\square$

Let R be the ring $F_{2^n}[x]/(x^{2^n}-x)$. Every element of R may be written uniquely in the form

$$\sum_{i=0}^{2^n-1} a_i x^i, \ \textit{where}\ a_0, a_1, \ldots, a_{2^n-1} \in F_{2^n}. \tag{3.7}$$

Since all the elements $\beta \in F_{2^n}$ are roots of $(x^{2^n}-x)$, the evaluation $f(\beta)$ of an element $f \in R$ at point $\beta \in F_{2^n}$ is well defined, so every $f \in R$ induces a function ϕ from $F_{2^n} \longrightarrow F_{2^n}$, and we say that *f represents* ϕ. Indeed, every function $\phi : F_{2^n} \longrightarrow F_{2^n}$ is represented by a unique element of R.

With the *weight* $wt(i)$ of a positive integer i we define the number of ones in its binary representation. For example $wt(5) = wt((101)_2) = 2$ and $wt(63) = wt((111111)_2) = 6$. Also ,this weight is called the *Hamming weight.* This weight wt has some favorable properties, namely $wt(i) = 0$ if and only if $i = 0$ and $wt(i+j) \leq w(i) + wt(j)$ where $i, j \in \mathbb{Z}$.

For all non-negative integers k, let P_k and $P_k^* \subseteq R$ be defined by

$$P_k = \left\{ \sum_{i=0}^{2^n-1} a_i x^i \in R :\ a_i = 0 \text{ for all } i \text{ such that } wt(i) > k \right\}, \tag{3.8}$$

$$P_k^* = \left\{ \sum_{i=0}^{2^n-1} a_i x^i \in P_k :\ a_0 = 0 \right\}. \tag{3.9}$$

One can easily verify that $P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n = P_{n+1} = \cdots = R$. And also we note that P_k^* consists of those elements of P_k that represents functions that map 0 to 0. Now we want to investigate some properties of P_k and P_k^*.

Lemma 3.8. *Let* $T : F_{2^n} \to F_2$ *be any* $F_2-linear\ function$*. Then* T *is represented by an element in* P_1^**.*

Proof. There exist $c \in F_{2^n}$ such that $T(x) = \mathrm{Tr}(cx)$ for all $x \in F_{2^n}$ by Theorem 1.18, where $c \geq 0$. Then T is represented by the polynomial

$$f(x) = \sum_{j=0}^{n-1} c^{2^j} x^{2^j} = \sum_{i=0}^{2^{n-1}} a_i x^i,$$

where $a_i = 0$ if $wt(i) > 1$. Hence $f(x)$ is an element of P_1^*. □

Lemma 3.9. *Let $f \in P_{k_1}$, and $g \in P_{k_2}$. Then $fg \in P_{k_1+k_2}$. If in addition $f \in P_{k_1}^*$ then $fg \in P_{k_1+k_2}^*$*

Proof. Let $i_1, i_2 \in \{0, 1, \ldots, 2^n - 1\}$ be integers such that $wt(i_1) \leq k_1$ and $wt(i_2) \leq k_2$. Then in the ring R we have that

$$x^{i_1}x^{i_2} = \begin{cases} x^{i_1+i_2} & if\ i_1 + i_2 < 2^n\ and, \\ x^{i_1+i_2-2^n+1} & if\ i_1 + i_2 \geq 2^n. \end{cases}$$

In the first case $wt(i_1 + i_2) \leq wt(i_1) + wt(i_2) = k_1 + k_2$. In the second case, since the binary digit corresponding to 2^n in the binary representation of $i_1 + i_2$ is one, then we have $wt(i_1 + i_2 - 2^n + 1) \leq wt(i_1 + i_2 - 2^n) + 1 = wt(i_1 + i_2) - 1 + 1 \leq wt(i_1) + wt(i_2) = k_1 + k_2$. So in either case we have that $x^{i_1}x^{i_2} \in P_{k_1+k_2}$. Since the product of two arbitrary polynomial $f \in P_{k_1}$ and $g \in P_{k_2}$ is a linear combinations of the terms of the form $x^{i_1}x^{i_2}$, we have the first result of the lemma holds.

The second statement of the lemma follows from the first statement together with the fact that $fg(0) = f(0)g(0) = 0 \cdot g(0) = 0$. □

Lemma 3.10. *Let $\zeta \in F_{2^n}$ be a primitive element. Let $f \in P_k^*$. Then there exists an element $g \in P_k$ such that for all $i \in \{0, 1, \ldots, 2^n - 2\}$,*

$$g(\zeta^i) = \sum_{j=0}^{i} f(\zeta^i).$$

Proof. When $k \geq n$, $P_k = R$ and the Lagrange Interpolation Formula (Theorem 1.2) gives the solution. Now assume that $k < n$. We know the following identity

$$\sum_{j=0}^{i} x^j = \frac{x^{i+1} - 1}{x - 1},$$

now by putting ζ^r, $1 \leq r \leq 2^n - 2$ instead of x, we get the following identity which holds for all $i \in \{0, 1, \ldots 2^{n-2}\}$

$$1 + \zeta^r + \ldots + \zeta^{ir} = \frac{\zeta^r}{\zeta^r - 1}\zeta^{ir} - \frac{1}{\zeta^r - 1}.$$

Suppose that f is in the form $f = \sum_{r=0}^{2^n-1} a_r x^r$ for some elements $a_0, a_1, \ldots, a_{2^n-1} \in F_{2^n}$. Since $f \in P_k^*$ we have $a_0 = 0$ and $k < n$ then $a_{2^n-1} = 0$ too. Let g be the polynomial defined by

$$g = \left(\sum_{r=1}^{2^n-2} a_r \frac{\zeta^r}{\zeta^r - 1} x^r \right) - \sum_{r=1}^{2^n-2} a_r \frac{1}{\zeta^r - 1}.$$

Since g is formed by using the coefficients of f, which is in P_k^* then $g \in P_k$ (indeed $g \in P_k^*$, since $g(0) = 0$). Moreover, for all $i \in \{0, 1, \ldots 2^n - 2\}$ we have that

$$\begin{aligned} g(\zeta^i) &= \sum_{r=1}^{2^n-2} a_r \left(\frac{\zeta^r}{\zeta^r - 1} \zeta^{ir} - \frac{1}{\zeta^r - 1} \right) \\ &= \sum_{r=1}^{2^n-2} a_r \sum_{j=0}^{i} (\zeta^j)^r \\ &= \sum_{j=0}^{i} \sum_{r=1}^{2^n-2} a_r (\zeta^j)^r \\ &= \sum_{j=0}^{i} f(\zeta^j). \end{aligned}$$

Hence the lemma follows. □

Lemma 3.11. *Let $f \in P_k^*$, where $k < n$. Then*

$$\sum_{x \in F_{2^n} \setminus \{0\}} f(x) = 0. \tag{3.10}$$

Proof. Since $f \in P_k^*$ then $f(0) = 0$. So we have

$$\sum_{x \in F_{2^n} \setminus \{0\}} f(x) = \sum_{x \in F_{2^n}} f(x). \tag{3.11}$$

Since $wt(2^n - 1) = n$ and $k < n$ then we can write f in the form

$$f = \sum_{r=1}^{2^n-2} a_r x^r \tag{3.12}$$

for some elements $a_r \in F_{2^n}$. By Lemma 1.3 we have

$$\sum_{x \in F_{2^n}} x^r = 0 \text{ where } 1 \le r \le 2^n - 2 \tag{3.13}$$

Hence

$$\begin{aligned}\sum_{x\in F_{2^n}} f(x) =& \sum_{x\in F_{2^n}} \sum_{r=1}^{2^n-2} a_r x^r \\ =& \sum_{r=1}^{2^n-2} a_r \sum_{x\in F_{2^n}} x^r \\ =& 0,\end{aligned}$$

as required. □

Let n be a positive integer and let $\zeta \in F_{2^n}$ be a primitive root. Let $T : F_{2^n} \to F_2$ be a non-zero $F_2 - linear\ map$. We define a sequence $\sigma = (\sigma_0, \sigma_2, \ldots)$ of period 2^{n-1} with elements in F_{2^n} by setting σ_i to be the $(i+1)st$ element x in the sequence $1, \zeta, \zeta^2, \ldots$ having the property that $T(x) = 1$.

To understand this construction let us look at the following example:

Example 3.12. Suppose $n = 6$, and let $\zeta \in F_{2^n}$ be a primitive root of $x^6 + x + 1$. Let T be map taking $\sum_{i=0}^{5} a_i\zeta^i$ to a_0. The sequence $1, \zeta, \zeta^2, \ldots$ has period $2^6 - 1$; writing the field element $\sum_{i=0}^{5} a_i\zeta^i$ as the binary string $a_5a_4a_3a_2a_1a_0$, the first $2^6 - 1$ elements of this sequence are (reading left to right):

000001	000010	000100	001000	010000	100000	000011	000110
001100	011000	110000	100011	000101	001010	010100	101000
010011	100110	001111	011110	111100	111011	110101	101001
010001	100010	000111	001110	011100	111000	110011	100101
001001	010010	100100	001011	010110	101100	011011	110110
101111	011101	111010	110111	101101	011001	110010	100111
001101	011010	110100	101011	010101	101010	010111	101110
011111	111110	111111	111101	111001	110001	100001	

The sequence σ is then formed by removing all the terms x of the sequence such that $T(x) = 0$:

000001	000011	100011	000101	010011	001111	111011	110101
101001	010001	000111	110011	100101	001001	001011	011011
101111	011101	110111	101101	011001	100111	001101	101011
010101	010111	011111	111111	111101	111001	110001	100001

Here we note that σ has always period precisely 2^{n-1} as it consists of 2^{n-1} distinct elements $x \in F_{2^n}$ such that $T(x) = 1$ written in some order.

Let define the *kth clocking function* $\kappa_k : F_{2^n} \longrightarrow F_2$ for all $k \in \{0, 1, \ldots, n-2\}$ by

$$\kappa_k(x) = \begin{cases} 1 & \text{if } x = \sigma_i \text{ where } 2^k \text{ divides } i, \\ 0 & \text{otherwise,} \end{cases} \tag{3.14}$$

where σ is constructed as above via T.

Lemma 3.13. *$\kappa_k(\zeta^i) = 1$ if and only if $\kappa_{k-1}(\zeta^i) = 1$ and there are an even number of ones in the sequence $\kappa_{k-1}(1), \kappa_{k-1}(\zeta^0), \ldots, \kappa_{k-1}(\zeta^i)$.*

Proof. If $\kappa_k(\zeta^i) = 1$ then $\zeta^i = \sigma_i$ such that $2^k | i$. Hence, $\kappa_{k-1}(\zeta^i) = 1$ since $2^{k-1} \mid 2^k \mid i$, where $\zeta^i = \sigma_i$. Since $2^k = 2 \cdot 2^{k-1}$ there are even number of ones in the sequence $\kappa_{k-1}(1), \kappa_{k-1}(\zeta^0), \ldots, \kappa_{k-1}(\zeta^i)$.

Conversely, since we have even number of ones in the sequence $\kappa_{k-1}(1), ..., \kappa_{k-1}(\zeta^i)$ then $2^k | i$ also and hence, $\kappa(\zeta^i) = 1$ as required. □

Lemma 3.14. *κ_k can be represented by an element $f \in P^*_{2^k}$*

Proof. We will show this assertion by induction on k. If $k = 0$, then $\kappa_0 = T$ since, $\kappa_0(x) = 1$ only if $x = \sigma_i$ (and because 1 divides every number), result follows by Lemma 3.8. Now suppose that $k > 0$ and that κ_{k-1} may be represented by an element $f_{k-1} \in P^*_{k-1}$. Let $g \in P_{2^{k-1}}$ be an element such that $g(\zeta^i) = \sum_{j=0}^{i} f_{k-1}(\zeta^j)$ for all $i \in \{0, 1, \ldots, 2^2 - 2\}$; such an element exist by Lemma 3.10. Now we define $f_k = f_{k-1}(1 + g)$. By Lemma 3.9, $f_k \in P^*_k$. Consider $f_k(\zeta^i) = f_{k-1}(\zeta^i)(1 + g(\zeta^i))$, if $f_{k-1}(\zeta^i) = 0$ then $f_k(\zeta^i) = 0$ as required. If $f_{k-1}(\zeta^i) = 1$ then $f_k(\zeta) = 1$ if there is even number of ones in the sequence $\kappa_{k-1}(1), \kappa_{k-1}(\zeta^0), \ldots, \kappa_{k-1}(\zeta^i)$ by Lemma 3.13. Moreover $\kappa_k(0) = f_k(0) = 0$ hence f_k represents κ_k. □

Let $D : F_{2^n}\backslash\{0\} \to \mathbb{Z}/2^{n-1}\mathbb{Z}$ be defined by setting $D(\zeta^j)$ to be one less than the number of elements x such that $T(x) = 1$ in the sequence $1, \zeta, \zeta^2, \ldots, \zeta^j$. Hence, if $\zeta^j = \sigma_e$ for some $e \in \{0, 1, \ldots, 2^{n-1}\}$ then $D(\zeta^i) = e$. For $k \in \{0, 1, \ldots, n-2\}$ we define the *kth digit function* $\delta_k : F_{2^n}\backslash\{0\} \to F_2$ to be the function mapping x to the digit corresponding to 2^k in the binary expansion of $D(x)$. So if $D(x) = \sum_{j=0}^{n-2} d_j 2^j \bmod 2^{n-1}$ where $d_j \in \{0, 1\}$ then $\delta_k(x) = d_k$.

Lemma 3.15. *The digit functions δ_k can be expressed in terms of clocking functions by*

$$\delta_k(\zeta^i) = 1 + \sum_{j=0}^{i} \kappa_k(\zeta^j), \tag{3.15}$$

where $k \in \{0, 1, \ldots, n-2\}$ and $i \in \{0, 1, \ldots, 2^n - 2\}$.

Proof. Note that the digit of $D(\zeta^i)$ corresponding to 2^k differs from the corresponding digit in $D(\zeta^{i-1})$ if and only if $\zeta^i = \sigma_e$ where 2^k divides e. Hence, by Lemma 3.10, there is an element $h_k \in P_{2^k}$ that represents a function that agrees with δ_k on $F_{2^n}\backslash\{0\}$. □

Theorem 3.16. *Let n be a positive integer, let $\zeta \in F_{2^n}$ be a primitive element and let $T : F_{2^n} \to F_2$ be a non-zero F_2-linear map. Let σ be the sequence over F_{2^n} of period 2^{n-1} defined above. Then $L_\sigma \leq 2^{n-1} - (n-2)$.*

Proof. The theorem is trivial when $n = 1$ or $n = 2$, so from now on we assume that $n \geq 3$.

By Lemma 3.7, it is sufficient to show that for all $j \in \{0, 1, \ldots, 2^{n-1} - 1\}$ we have that

$$\sum_i \sigma_{i+j} = 0, \tag{3.16}$$

where sum is over all $i \in \{0, 1, \ldots, 2^{n-1} - 1\}$ such that the kth binary digit of i is zero whenever the kth binary digit of $n-3$ is one.

Firstly, we will show that it is sufficient to consider case $j = 0$ only. For this, Let $J \in \{0, 1, \ldots, 2^{n-1} - 1\}$ be given. Let $\beta \in F_{2^n}$ be the $(J+1)$st element x in the sequence $1, \zeta, \zeta^2, \ldots$ such that $T(x) = 1$. We define another linear map

$T' : F_{2^n} \longrightarrow F_2$ to be composition of the map $x \mapsto \beta x$ and the map T. Define another sequence $\sigma'_n = (\sigma'_0, \sigma'_1, \ldots)$ using the map T' instead of map T. The new sequence is nothing but the rotated version of the original sequence σ in its period intervals. This implies $\sigma'_i = \sigma_{i+J}$ for all non-negative integers i. Hence the Equation (3.16) in the case $j = 0$ for (σ'_n) implies the equation (3.16) in the case $j = J$ for σ. Thus to prove the theorem it is sufficient to establish the identity

$$\sum_i \sigma_i = 0 \tag{3.17}$$

where the sum is over all $i \in \{0, 1, \ldots, 2^{n-1} - 1\}$ such that the kth binary digit of i is zero whenever the kth binary digit of $n - 3$ is one.

We may rephrase this problem slightly, as follows. Let $\phi : F_{2^n} \longrightarrow F_{2^n}$ be the function that

$$\phi(x) = \begin{cases} x & \text{if } x \text{ occurs as a summand in equation (3.17)} \\ 0 & \text{otherwise.} \end{cases}$$

Then equation (3.17) is equivalent to asserting that

$$\sum_{x \in F_{2^n} \setminus \{0\}} \phi(x) = 0. \tag{3.18}$$

We claim that ϕ may be represented by an element in P^*_{n-1}. By Lemma 3.11, this claim is sufficient to prove the identity (3.18). Now we prove this with the following lines.

Define elements $b_0, b_1, \ldots, b_{n-2} \in \{0, 1\}$ by $n - 3 = \sum_{j=0}^{n-2} b_j 2^j$ (here we note that $n - 3 < 2^{n-1}$ when $n \geq 3$, and so this definition makes sense). let p be the element defined by

$$p = x f_0 \prod (h_k + 1),$$

where the product is over those integers k such that $0 \leq k \leq n - 2, b_k = 1$, f_0 is the function that represent κ_0 (by lemma 3.14)and h_k the function that represents δ_n (by lemma 3.15). Since $x, f_0 \in P^*_1$ and $h_k + 1 \in P_{2^k}$, we have that $p \in P_{2+\sum_{k=0}^{n-2} b_k 2^k} = P^*_{n-1}$ by Lemma 3.9. We claim that p represents the function ϕ. Clearly, $p(0) = \phi(0) = 0$. Let $\zeta^i \in F_{2^n}$. Now, since the polynomial f_0 and $h_k + 1$ take their values in F_2, either $p(\zeta^i) = \zeta^i$ or $p(\zeta^i) = 0$.Furthermore, $p(\zeta^i) = \zeta^i$ if and only if $f_0(\zeta^i) = 1$ and $h_k(\zeta^j) = 0$ for all k such that $b_k = 1$. But, using the definitions of f_0 and the element h_k, this is exactly the same as the condition $T(\zeta^i) = 1$ and that a binary digit of $D(\zeta^i)$ is zero whenever the corresponding digits of $n - 3$ are one. Hence, $p \in P^*_{n-1}$ represents ϕ as required.

This establishes the identity (3.18), and hence the theorem follows. □

Now are ready to establish that fact that the linear complexity of the output sequence of a self-shrinking generator based on a is a maximal periodic sequence of period $2^n - 1$ is at most $2^{n-1} - (n - 2)$

Let $s_0, s_1, \ldots$ be the output of a maximal periodic sequence of period $2^n - 1$. Then by Theorem 1.18 there exists a primitive element $\zeta \in F_{2^n}$ and an element $c \in F_{2^n}$ such that

$$(z) = \mathrm{Tr}(c\zeta^i)$$

for all non-negative integers i.

Let $z_0, z_1, \ldots$ be the output of the self-shrinking generator based on the sequence $s_0, s_1, \ldots$. So

$$\sigma_i = s_{2\tau(i)+1}$$

where $\tau(i)$ is the unique non-negative integers such that $s_{2\tau(i)} = 1$ and there are precisely $i + 1$ ones in the sequence $s_0, s_2, \ldots, s_{2\tau(i)}$. We may rewrite this condition in terms of the trace map and the sequence σ defined previously, as follows. Let $T : F_{2^n} \to F_2$ be defined by $T(x) = \mathrm{Tr}(c^{2^{n-1}}x)$. Here we note that

$$T(\zeta^i) = \mathrm{Tr}(c\zeta^{2i}) = s_{2j},$$

as the trace map is invariant under the squaring automorphism. Define $T' : F_{2^n} \to F_2$ by $T'(x) = \mathrm{Tr}((c\zeta)^{2^{n-1}}x)$. Then

$$T'(\zeta) = \mathrm{Tr}(c\zeta\zeta^{2i}) = s_{2j+1}.$$

Now, for all non-negative integers i,

$$z_i = T'(\sigma_i)$$

where $\sigma_0, \sigma_1, \ldots$ is the sequence defined using ζ and T as in previously.

By Theorem 3.16 the sequence $\sigma_0, \sigma_1, \ldots$ satisfies a linear recurrence relation

$$\sum_{i=0}^{2^{n-1}-(n-2)} c_i \sigma_{i+j}$$

for all non-negative integers j, where the coefficients are all binomial coefficients in F_2. But by the F_2-linearity of T' we have that

$$\sum_{i=0}^{2^{n-1}-(n-2)} c_i z_{i+j} = \sum_{i=0}^{2^{n-1}-(n-2)} c_i T'(\sigma_{i+j}) = T'\left(\sum_{i=0}^{2^{n-1}-(n-2)} c_i \sigma_{i+j} \right) = T'(0) = 0.$$

Hence the linear complexity of the sequence $z_0, z_1, \ldots$ of the self-shrinking generator is at most $2^{n-1} - (n-2)$, as required.

CHAPTER 4

CONSTRUCTION OF D-PERFECT SEQUENCES USING FUNCTION FIELDS

In this chapter we present constructions of d-$perfect$ sequences based on algebraic function field. More on this approach can be found in [17] and [18].

Let F/F_q be an algebraic function field . The following notations will be used throughout the chapter: let $P \in \mathbb{P}_F$ be a rational (degree 1) place and t be a local parameter of P. Suppose that the principal divisor (t) of t satisfies

$$(t) = P + Q - D \tag{4.1}$$

where Q is a rational place other than P and D is a positive divisor of degree two. The divisor D with its degree will play an important role in constructions. Note that $(t)_\infty = D$ and hence $deg((t)_\infty) = degD = 2$.

4.1 The Main Construction

Lemma 4.1. *Let f be an element in $F - F_q(t)$ and suppose that it has*

$$f = \sum_{j=0}^{\infty} a_j t^j, \;\; a_j \in F_q$$

as its local expansion at P with respect to t. Suppose there exist $\lambda_0, \lambda_1, \ldots, \lambda_s \in F_q$, where $\lambda_s \neq 0$, such that

$$\lambda_s a_{i+s} + \lambda_{s-1} a_{i+s-1} + \cdots + \lambda_1 a_{i+1} + \lambda_0 a_i = 0, \; i = 1, 2, 3, \ldots, n-s. \tag{4.2}$$

If L is defined as

$$\begin{aligned} L :=& (\lambda_0 t^s + \lambda_1 t^{s-1} + \cdots + \lambda_s) f \\ &- [\lambda_s a_0 + (\lambda_s a_1 + \lambda_{s-1} a_0) t \\ &+ \cdots + (\lambda_s a_s + \ldots + \lambda_0 a_0) t^s] \end{aligned}$$

then $v_P(L) \geq n + 1$.

Proof. Being a local parameter at P, hence transcendental over F_q, $\{1, t, \dots, t^s\}$ are linearly independent over F_q. If we use the assumption $\lambda_s \neq 0$, then the coefficient of f in L is non-zero. If $L = 0$, then f is a rational function of t which contradicts the assumption $f \in F - F_q(t)$. Hence $L \neq 0$.

Use the local expansion of f to write L as follows:

$$\begin{aligned} L =& (\lambda_s a_0 - \lambda_s a_0) + (\lambda_s a_1 + \lambda_{s-1} a_0 - \lambda_s a_1 - \lambda_{s-1} a_0)t + \dots \\ &+ (\lambda_0 a_0 + \lambda_1 a_1 + \dots + \lambda_s a_s - \lambda_0 a_0 - \lambda_1 a_1 - \dots - \lambda_s a_s)t^s + \\ &+ (\lambda_s a_{s+1} + \lambda_{s-1} a_s + \dots + \lambda_0 a_1)t^{s+1} + (\lambda_s a_{s+2} + \lambda_{s-1} a_{s+1} + \dots + \lambda_0 a_2)t^{s+2} + \\ &+ \dots (\lambda_s a_n + \lambda_{s-1} a_{n-1} + \dots + \lambda_0 a_{n-s})t^n + \\ &+ \sum_{j=n+1}^{\infty} b_j t^j, \end{aligned}$$

where $b_j \in F_q$. The coefficients of $t^0, t^1, \dots, t^s$ are zero obviously by cancellations and the coefficients of $t^{s+1}, t^{s+2}, \dots, t^n$ are zero by the relation between λ_i's and a_i's (4.2). Hence

$$L = \sum_{j=n+1}^{\infty} b_j t^j$$

and by Theorem 1.44, $v_P(L) \geq n + 1$. $\square$

Lemma 4.2. *Let f and L be as in Lemma 4.1 then*

$$(L)_\infty \leq (f)_\infty + (t^s)_\infty \tag{4.3}$$

Proof. We start by defining two functions $g_1, g_2 \in F$ defined as

$$g_1 := (\lambda_s a_s + (\lambda_s a_1 + \lambda_{s-1} a_0)t + \cdots + (\lambda_s a_s + \dots + \lambda_0 a_0)t^s),$$

$$g_2 := \lambda_0 t^s + \lambda_1 t^{s-1} + \cdots + \lambda_s.$$

Note that $L = g_2 f - g_1$. Also note that $g_2 f \neq 0$ since $\lambda_s \neq 0$ and $\{1, t, \dots, t^s\}$ are linearly independent over F_q. Let $R \in \mathbb{P}_F$ be a pole of L, i.e. $v_R(L) = -r < 0$ and hence $v_R((L)_\infty) = r$. We claim that $v_R((L)_\infty) = r \leq v_R((f)_\infty + (t^s)_\infty)$. We will prove this claim in two cases;

Case 1: $R \notin supp(D)$

This means t doesn't have a pole at R, hence $v_R(t) \geq 0$ and $v_R((t^s)_\infty) = 0$. By the triangle inequality, we have $v_R(g_1) \geq 0$ and hence

$$-r = v_R(L) \geq \min\{v_R(g_2 f), v_R(g_1)\} = v_R(g_2 f) = v_R(g_2) + v_R(f). \tag{4.4}$$

If $g_1 = 0$ then $v_R(g_1) = \infty$ and since $g_2 f \neq 0$ then $\min\{v_R(g_2 f), v_R(g_1)\} = v_R(g_2) + v_R(f)$

Since $v_R(t) \geq 0$, then we have $v_R(g_2) = i \geq 0$, by triangle inequality. By equation (4.4) $-r \geq i + v_R(f) \Rightarrow v_R(f) \leq -r - i \leq r$. Hence $r = v_R((L)_\infty) \leq v_R((f)_\infty)$. Remembering that $v_R((t^s)_\infty) = 0$, one gets

$$v_R((L)_\infty) \leq v_R((f)_\infty) + v_R((t^s)_\infty).$$

Now suppose that $g_1 \neq 0$. Then $v_R(g_1) \geq \{v_R(\lambda_s a_0), v_R(\lambda_s a_1 + \lambda_{s-1} a_0)t, \dots\} \geq 0$. By equation (4.4),

$$-r \geq min\{v_R(g_2) + v_R(f), v_R(g_1)\},\ v_R(f) \leq -r - i,$$

where $i = v_R(g_1)$ as in above. Hence,

$$\begin{aligned} v_R((L)_\infty) = r \leq & v_R((f)_\infty) \\ = & v_R((f)_\infty) + v_R((g_2)_\infty) \\ = & v_R((f)_\infty) + v_R((t^s)_\infty). \end{aligned}$$

Combining $g_1 = 0$ and $g_1 \neq 0$ we have $v_R((L)_\infty) \leq v_R((f)_\infty) + v_R((t^s)_\infty)$ and this is true for any R with $R \in \mathbb{P}_F$ where R is a pole of L and $R \notin supp(D)$. So in case one we have $(L)_\infty \leq (f)_\infty + (t^s)_\infty$.

Case 2: $R \in supp(D)$.

This means t has a pole at R and $v_R(t) < 0$. Then we have $-r \geq min\{v_R(g_2) + v_R(f), v_R(g_1)\}$

If $g_1 = 0$ we have

$$min\{v_R(g_2) + v_R(f), v_R(g_1)\} = v_R(g_2) + v_R(f)$$

$$v_R(g_2) = v_R(t^i) \geq v_R(t^s), \text{ for the largest } i \in \{0, 1, \ldots, s\} \text{ with } \lambda_i \neq 0$$

then

$$-r \geq v_R(t^s) + v_R(f) \Rightarrow v_R((L)_\infty) \leq v_R((f)_\infty) + v_R((t^s)_\infty).$$

If $g_1 \neq 0$

1. If $\min\{v_R(g_2) + v_R(f), v_R(g_1)\} = v_R(g_2) + v_R(f)$ then follows as above.

2. If $\min\{v_R(g_2) + v_R(f), v_R(g_1)\} = v_R(g_1)$ then

$$v_R(g_1) = v_R(t^i) \geq v_R(t^s),$$

for the largest $i \in \{0, 1, \ldots, s\}$with coefficients of $t^i \neq 0$. Then

$$-r \geq v_R(t^s) \Rightarrow v_R((L)_\infty) \leq v_R((t^s)_\infty) \leq v_R((t^s)_\infty) + v_R((f)_\infty).$$

Combining $g_1 = 0$ and $g_1 \neq 0$ we have $v_R((L)_\infty) \leq v_R((f)_\infty) + v_R((t^s)_\infty)$ and this is true for any R with $R \notin \mathbb{P}_F$ where R is a pole of L and $R \notin supp(D)$. So in case two we have $(L)_\infty \leq (f)_\infty + (t^s)_\infty$.

Combining Case 1 and Case 2, the inequality holds. □

Theorem 4.3. ***(Construction 1)*** *Let P and Q be two distinct rational places of the function field F/F_q. Suppose t is a local parameter at P such that $(t) = P + Q - D$, where D is a positive divisor of degree 2. Let $f \in F - F_q(t)$ with $d \geq deg((f)_0) = deg((f)_\infty)$ and $v_P(f) \geq 0$. Suppose f has the local expansion*

$$f = \sum_{j=0}^{\infty} a_j t^j, \ a_j \in F_q, \ at \ P. \tag{4.5}$$

Define a sequence

$$\boldsymbol{a}_1(f) = (a_1, a_2, a_3, \ldots).$$

Then $\boldsymbol{a}_1(f)$ is $d-perfect$, i.e.

$$\frac{n+1-d}{n} \leq L_{\boldsymbol{a}_1(f)}(n) \leq \frac{n+d}{2}, \ for \ all \ n \geq 1.$$

Proof. Since $f \notin F - F_q(t)$ we have $d \geq deg((f)_0) \geq 1$. The Berklam-Massey Algorithm (Algorithm 1.16) for $n = 1$ results $l_{\mathbf{a}(f)}(1) = 1$. Hence

$$\frac{2-d}{2} \leq 1 \leq \frac{d+1}{2}$$

and the result holds for $n = 1$.

For $n > 1$, it is sufficient to prove that the linear complexity s of $a_1, a_2, a_3, \ldots$ is at least $\frac{n+1-d}{2}$. By the Berlekamp-Massey Algorithm (Algorithm 1.16) we can find $s+1$ elements $\lambda_0, \lambda_1, \ldots, \lambda_s$ of F_q with $\lambda_s \neq 0$ such that

$$\lambda_s a_{i+s} + \lambda_{s-1} a_{i+s-1} + \cdots + \lambda_1 a_{i+1} + \lambda_0 a_i = 0 \tag{4.6}$$

for $i = 1, 2, \ldots, n-s$.

Consider the function

$$\begin{aligned} L :=& (\lambda_0 t^s + \lambda_1 t^{s-1} + \cdots + \lambda_s) f \\ & - (\lambda_s a_0 + (\lambda_s a_1 + \lambda_{s-1} a_0) t \\ & + \cdots + (\lambda_s a_s + \ldots + \lambda_0 a_0) t^s) \end{aligned}$$

Then by Lemma 4.1 and 4.2, we have

$$v_P(L) \geq n+1,$$

and

$$(L)_\infty \leq (f)_\infty + (t^s)_\infty.$$

Since $(t)_\infty = D$, we have $(t^s)_\infty = sD$.
Since $0 < n+1 \leq v_P(L)$, L has a zero at P and $v_P(L) \leq deg((L)_0)$. Combining these observations together, we get

$$n+1 \leq v_P(L) \leq deg((L)_0) = deg((L)_\infty) \leq deg((f)_\infty + sD) = d + 2s.$$

Therefore

$$s \geq \frac{n+1-d}{2},$$

and $\mathbf{a}_1(f)$ is d-perfect. □

Remarks 4.4.

1. The most important condition for this construction is the existence of the local parameter t at P with pole divisor of degree 2. After successfully finding such t, d-perfect sequences can be constructed for any given d by choosing function f with pole divisor of degree d.

2. There can be some curves that doesn't contain such a local parameter t. For instance, elliptic curves of divisor class number one have only one rational point over the finite base field (see [16, Proposition VI.1.6]). Hence one cannot find such a local parameter t.

Example 4.5. We will consider the local expansions of the functions from the Example 1.43. Namely, the function field is the rational function field $F_2(x)/F_2$ and the local parameter is $t = x^2 + x$ for the place P_0 of $F_(x)/F_2$. Note that $(t) = P_0 + P_1 - 2P_\infty$ hence the hypothesis of the Theorem are satisfied.

1. Consider the local expansion of x at P_0.

$$x = \sum_{m=1}^{\infty} t^{2^{m-1}}.$$

Now construct a sequence $\mathbf{a}_t(x) = (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \ldots)$ using the coefficients of the local expansion of x, expect the first coefficient. Since $x \notin F_2(t) = F_2(x^2 + x)$ and $deg((x)_\infty) = 1$, the sequence $\mathbf{a}_t(x)$ is 1-perfect by Theorem 4.3.

2. Consider the local expansion of x^2 at P_0.

$$x^2 = \sum_{m=1}^{\infty} t^{2^m}.$$

Now construct a sequence $\mathbf{a}_t(x^2) = (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, \ldots)$ using the coefficients of the local expansion of x^2, expect the first coefficient. Since $x^2 \notin F_2(t) = F_2(x^2 + x)$ and $deg((x^2)_\infty) = 2$, the sequence $\mathbf{a}_t(x^2)$ is 2-perfect by Theorem 4.3

3. Consider the local expansion of $x/(x+1)$ at P_0.

$$\frac{x}{x+1} = \sum_{m=1}^{\infty} t^{2^m-1}.$$

Now construct a sequence $\mathbf{a}_t(x/(x+1)) = (1,0,1,0,0,0,1,0,0,0,0,0,0,\ldots)$ using the coefficients of the local expansion of $x/(x+1)$, expect the first coefficient. Since $x/(x+1) \notin F_2(t) = F_2(x^2+x)$ and $deg((x/(x+1))_\infty) = 1$, the sequence $\mathbf{a}_t(x/(x+1))$ is 1-perfect by Theorem 4.3

4.2 The Extensions of the Main Construction

We list some further constructions of d-perfect sequences. The proofs, are with minor changes, similar to that Theorem 4.3. Therefore we omit them and refer the reader to the related source; namely [18].

The following theorem $v_P(f) < 0$, that is the reverse case of Theorem 4.3.

Theorem 4.6. ***(Construction 2)*** *Let P and Q be two distinct rational places of the function field F/F_q. Suppose t is a local parameter at P such that $(t) = P + Q - D$, where D is a positive divisor of degree 2. Let $f \in F - F_q(t)$ with $d \geq deg((f)_0) = deg((f)_\infty)$ and $v_P(f) < 0$. Let $v = -v_P(f) > 0$. Suppose f has the local expansion*

$$f = t^{-v} \sum_{j=0}^{\infty} a_j t^j, \ a_j \in F_q, \ at\ P. \tag{4.7}$$

Define a sequence

$$\boldsymbol{a}_2(f) = (a_0, a_1, a_2, \ldots).$$

Then $\boldsymbol{a}_2(f)$ is (d+v)$-perfect$,

From now on, constructions does not omit the first element in the local expansion to construct the sequence.

The following construction deals with the case $v_P(f) = v > 0$.

Theorem 4.7. ***(Construction 3)*** *Let P and Q be two distinct rational places of the function field F/F_q. Suppose t is a local parameter at P such that $(t) =$*

$P+Q-D$, where D is a positive divisor of degree 2. Let $f \in F - F_q(t)$ with $d \geq deg((f)_0) = deg((f)_\infty)$ and $v_P(f) = v \geq 0$. Suppose f has the local expansion

$$f = t^v \sum_{j=0}^{\infty} a_j t^j, \ a_j \in F_q, \ at\ P. \tag{4.8}$$

Define a sequence

$$\boldsymbol{a}_3(f) = (a_0, a_1, a_2, \ldots).$$

Then $\boldsymbol{a}_3(f)$ is (d+v-1)−$perfect$.

Example 4.8. Let $q = 3$, F be the rational function field $F_3(x)/F_3$, and P be the zero of x. We choose $t = x^2 - x$ and $f = x$. Then we have the local expansion

$$x = -t + t^2 + t^3 - t^4 + t^5 + 0 \cdot t^6 + \ldots.$$

Then the sequence $\mathbf{a}_t(x) = (-1, 1, 1, -1, 1, 0, \ldots)$ is *perfect* by Theorem 4.7.

The following construction deals with the case $v_P(f) = -v \leq 0$.

Theorem 4.9. ***(Construction 4)*** *Let P and Q be two distinct rational places of the function field F/F_q. Suppose t is a local parameter at P such that $(t) = P+Q-D$, where D is a positive divisor of degree 2. Let $f \in F - F_q(t)$ with $d \geq deg((f)_0) = deg((f)_\infty)$ and $v_P(f) = -v \leq 0$. Suppose f has the local expansion*

$$f = t^{-v} \sum_{j=0}^{\infty} a_j t^j, \ a_j \in F_q, \ at\ P. \tag{4.9}$$

Define a sequence

$$\boldsymbol{a}_4(f) = (a_0, a_1, a_2, \ldots).$$

Then $\boldsymbol{a}_4(f)$ is (d+v+1)−$perfect$.

Theorem 4.10. ***(Construction 5)*** *Let P and Q be two distinct rational places of the function field F/F_q. Suppose t is a local parameter at P such that $(t) = P+Q-D$, where D is a positive divisor of degree 2. Let $f \in F - F_q(t)$ with $d \geq deg((f)_0) = deg((f)_\infty)$ and $v_P(f) = -v \leq 0$. Suppose f has the local expansion*

$$f = \sum_{j=1}^{v} b_j t^{j-v-1} + \sum_{n=0}^{\infty} a_n t^n, \ \ b_j, a_n \in F_q. \tag{4.10}$$

Define a sequence

$$\boldsymbol{a}_5(f) = (a_0, a_1, a_2, \ldots).$$

Then $\boldsymbol{a}_5(f)$ *is* $d{-}perfect$.

Example 4.11. Let $q = 3$, F be the rational function field $F_3(x)/F_3$, and P be the zero of x. We choose $t = x^2 - x$ and $f = 1/x$. Then we have the local expansion

$$1/x = -t^{-1} - 1 + t + t^2 - t^3 + t^4 +) \cdot t^5 + 0 \cdot t^6 + \ldots.$$

Then the sequence $\mathbf{a}_t(1/x) = (1, 1, -1, 1, 0, 0, 0, 0, \ldots)$ is *perfect* by Theorem 4.10.

4.3 Consequences of The Constructions

In this section we will give some consequences of the constructions.

For two sequence $a = (a_1, a_2, a_3, \ldots)$ and $b = (b_1, b_2, b_3, \ldots)$ of elements of F_q, we define

$$a + b := (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$$

and

$$a * b := (0, a_1 b_1, a_1 b_2 + a_2 b_1, a_1 b_3 + a_2 b_2 + a_3 b_1, \ldots).$$

Proposition 4.12. *Let* $f, g \in F/K$ *with* $v_P(f) \geq 0$ *and* $v_P(g) \geq 0$. *Construct two sequences* $a_1(f)$ *and* $b_1(f)$ *as in the statement of the Theorem 4.3, then* $a_1(f) + b_1(f)$ *is d-perfect or ultimately periodic, where* $d = deg((f+g)_\infty) \leq deg((f)_\infty) + deg((g)_\infty)$.

Proof. If $a_1(f)$ and $b_1(g)$ in special form, that is

$$a_n + b_n = a_{n+k} + b_{n+k}$$

for some $k \in \mathbb{Z}$ and $\forall n > m$ for some $m > 0$ then $a_1(f) + b_1(g)$ will be ultimately periodic with period k. Assume that the sequence $a_1(f) + b_1(g)$ is not ultimately periodic. Now, observe that $a_1(f+g)$ is nothing but $a_1(f) + b_1(g)$. Then Theorem 4.3 implies that $a_1(f) + b_1(f)$ is d-perfect. $\square$

Proposition 4.13. *Let* $f, g \in F/K$ *with* $v_P(f) \geq 0$ *and* $v_P(g) \geq 0$. *Construct two sequences* $a_1(f)$ *and* $b_1(f)$ *as in the statement of the Theorem 4.3, then* $a_1(f) * b_1(f)$ *is d-perfect or ultimately periodic, where* $d = deg((fg)_\infty) \leq deg((f)_\infty) + deg((g)_\infty)$.

Proof. If $a_1(f)$ and $b_1(g)$ in special form then $a_1(f)*b_1(g)$ will be ultimately periodic with period k. Assume that the sequence $a_1(f) * b_1(g)$ is not ultimately periodic. Now, observe that $a_1(f * g)$ is nothing but $a_1(f) * b_1(g)$. Then Theorem 4.3 implies that $a_1(f) * b_1(f)$ is d-perfect. □

Bibliography

[1] Berlekamp,E.R., *Algebraic Coding Theory*, McGraw-Hill, 1968.

[2] Blackburn,S.R., *The Linear Complexity Of The Self-Shrinking Generator*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2073–2077.

[3] Blum,L., Blum,M., and Shub,M., *A Simple Unpredictable Pseudorandom Number Generator*, SIAM J. Comp. (1986), no. 15, 364–383.

[4] Cusick,T.W., Ding,C., and Renvall,A., *Stream Ciphers And Number Theory*, North-Holland, 1998.

[5] Hardy,G.H. and Wright,E.M., *An Introduction To The Theory Of Numbers*, 5 ed., Oxford Science Publications, 1998.

[6] Hoffman,K. and Kunze,R., *Linear Algebra*, 2 ed., Prentice-Hall, 1971.

[7] Jungnikel,D., *Finite Fields, Structure and Arithmetics*, Wissenschaftsverlag, 1993.

[8] Lidl,R. and Niederreiter,H., *Finite Fields*, Addison-Wesley, 1983.

[9] McIntosh,R.J., *A Generalization Of Congruential Property Of Lucas*, Amer. Math. Monthly (1992), no. 3, 231–238.

[10] Meidel,W. and Winterhof,A., *Linear Complexity And Polynomial Degree Of A Function Over A Finite Field*, Proc. of the Conference on Finite Fields and Applications, Oxaca, Mexico (2001, to appear).

[11] Meier,W. and Staffbelbach,O., *The Linear Complexity Of The Self-Shrinking Generator*, Advences in Cryptography - EUROCRYPT'94 (1994), 205–214.

[12] Montgomery,H.L., *Distribution Of Small Powers Of A Primitive Root*, Advance In Number Theory (1993), 137–149.

[13] Niederreiter,H. and Xing,C., *Rational Points On Curves Over Finite Fields*, Cambridge University Press, 2001.

[14] Rueppel,R.A., *Analysis And Design Of Stream Chipers*, Springer-Verlag, 1986.

[15] Shparlinski,I., *On The Linear Complexity Of The Power Generator*, Des. Codes And Cryptogr. **23** (2001), no. 1, 5–10.

[16] Stichtenoth,H., *Algebraic Function Field and Codes*, Springer, 1993.

[17] Xing,C. and Ding,C., *Sequences With Perfect Linear Complexity Profiles And Curves Over Finite Fields*, IEEE Transaction on Information Theory **45** (May 1999), no. 4, 1267–1270.

[18] Xing,C., Niederreiter,H., Lam,K.Y., and Ding,C., *Construction Of Sequences with Almost Perfect Linear Complexity Profiles From Curves Over Finite Fields*, Finite Fields and Their Applications **17** (1999), 301–313.

Bibliography

[1] Berlekamp,E.R., *Algebraic Coding Theory*, McGraw-Hill, 1968.

[2] Blackburn,S.R., *The Linear Complexity Of The Self-Shrinking Generator*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2073–2077.

[3] Blum,L., Blum,M., and Shub,M., *A Simple Unpredictable Pseudorandom Number Generator*, SIAM J. Comp. (1986), no. 15, 364–383.

[4] Cusick,T.W., Ding,C., and Renvall,A., *Stream Ciphers And Number Theory*, North-Holland, 1998.

[5] Hardy,G.H. and Wright,E.M., *An Introduction To The Theory Of Numbers*, 5 ed., Oxford Science Publications, 1998.

[6] Hoffman,K. and Kunze,R., *Linear Algebra*, 2 ed., Prentice-Hall, 1971.

[7] Jungnikel,D., *Finite Fields, Structure and Arithmetics*, Wissenschaftsverlag, 1993.

[8] Lidl,R. and Niederreiter,H., *Finite Fields*, Addison-Wesley, 1983.

[9] McIntosh,R.J., *A Generalization Of Congruential Property Of Lucas*, Amer. Math. Monthly (1992), no. 3, 231–238.

[10] Meidel,W. and Winterhof,A., *Linear Complexity And Polynomial Degree Of A Function Over A Finite Field*, Proc. of the Conference on Finite Fields and Applications, Oxaca, Mexico (2001, to appear).

[11] Meier,W. and Staffbelbach,O., *The Linear Complexity Of The Self-Shrinking Generator*, Advences in Cryptography - EUROCRYPT'94 (1994), 205–214.

[12] Montgomery,H.L., *Distribution Of Small Powers Of A Primitive Root*, Advance In Number Theory (1993), 137–149.

[13] Niederreiter,H. and Xing,C., *Rational Points On Curves Over Finite Fields*, Cambridge University Press, 2001.

[14] Rueppel,R.A., *Analysis And Design Of Stream Chipers*, Springer-Verlag, 1986.

[15] Shparlinski,I., *On The Linear Complexity Of The Power Generator*, Des. Codes And Cryptogr. **23** (2001), no. 1, 5–10.

[16] Stichtenoth,H., *Algebraic Function Field and Codes*, Springer, 1993.

[17] Xing,C. and Ding,C., *Sequences With Perfect Linear Complexity Profiles And Curves Over Finite Fields*, IEEE Transaction on Information Theory **45** (May 1999), no. 4, 1267–1270.

[18] Xing,C., Niederreiter,H., Lam,K.Y., and Ding,C., *Construction Of Sequences with Almost Perfect Linear Complexity Profiles From Curves Over Finite Fields*, Finite Fields and Their Applications **17** (1999), 301–313.