ON THE EXPECTED VALUE OF THE LINEAR COMPLEXITY OF PERIODIC SEQUENCES

ÇİĞDEM ÖZAKIN

JULY 2004

ON THE EXPECTED VALUE OF THE LINEAR COMPLEXITY OF PERIODIC SEQUENCES

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF APPLIED MATHEMATICS

OF

THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

ÇİĞDEM ÖZAKIN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

THE DEPARTMENT OF CRYPTOGRAPHY

JULY 2004

Approval of the Graduate School of Applied Mathematics

_____

Prof. Dr. Aydın AYTUNA
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Prof. Dr. Ersan AKYILDIZ
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Ferruh ÖZBUDAK Supervisor

Examining Committee Members

Prof. Dr. Ersan AKYILDIZ _____

Assoc. Prof. Dr. Ali DOĞANAKSOY _____

Assoc. Prof. Dr. Yusuf İPEKOğLU _____

Assoc. Prof. Dr. Ferruh ÖZBUDAK _____

Dr. Muhiddin UĞUZ _____

Abstract

ON THE EXPECTED VALUE OF LINEAR COMPLEXITY OF PERIODIC SEQUENCES

Özakın, Çiğdem
M.Sc., Department of Cryptography
Supervisor: Assoc. Prof. Dr. Ferruh ÖZBUDAK

July 2004, 53 pages

In cryptography, periodic sequences with terms in $\mathbb{F}_2$ are used almost everywhere. These sequences should have large linear complexity to be cryptographically strong. In fact, the linear complexity of a sequence should be close to its period. In this thesis, we study the expected value for N-periodic sequences with terms in the finite field $\mathbb{F}_q$.

This study is entirely devoted to W. Meidl and Harald Niederreiter's paper which is "On the Expected Value of the Linear Complexity and the k-Error Linear Complexity of Periodic Sequences" We only expand this paper, there is no improvement. In this paper there are important theorems and results about the expected value of linear complexity of periodic sequences.

Keywords: Linear Complexity, Günther Weight, Periodic Sequences, Cyclotomic Cosets, Discrete Fourier Transform, Expected Value.

Öz

PERİYODİK DİZİLERİN BEKLENEN DOĞRUSAL KARMAŞIKLIK DEĞERİ

Özakın, Çiğdem
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi: Doç. Dr. Ferruh ÖZBUDAK

Temmuz 2004, 53 sayfa

Kriptografide terimleri $\mathbb{F}_2$ cisminden olan periyodik dizilerin kullanımı yaygındır. Bu dizilerin, kriptolojik açıdan güvenli olması için, doğrusal karmaşıklık değerlerinin büyük olması gerekir. Aslında bu değer dizinin periyoduna oldukça yakın olmalıdır. Bu tezde, terimleri $\mathbb{F}_q$ cisminden olan periyodik dizilerin beklenen doğrusal karmaşıklığı incelenmiştir.

Bu çalışmada tamamıyle W. Meidl ve Harald Niederreiter'ın "On the Expected Value of the Linear Complexity and the k-Error Linear Complexity of Periodic Sequences" makalesinden yararlanılmıştır. Bu makelede periyodik dizilerin doğrusal karmaşıklığının beklenen değerleri hakkında önemli teoremler ve sonuçlar kaydedilmiştir. Bu tezde, bu makalenin içeriği genişletilmiş, her hangi yeni bir gelişme olmamıştır.

Anahtar Kelimeler: Doğrusal karmaşıklık, Günther ağırlığı, Periyodik dizi, Fourier Dönüşümü,

to my Mum,
to my Dad
and to my Brother

Acknowledgments

I am grateful to Assoc. Prof. Dr. Ferruh Özbudak for guiding, encouraging and motivating me throughout this study.

I think, a few people can have the chance to meet such a perfect person. I have learned many things from him. I want to thank Assoc. Prof. Dr. Ali Doğanaksoy for his contribution to my education, to my life.

I want to thank my parents. They made me feel strong and confident every time, I overcame all dificulties, because they were always with me.

She has been an important part of my life. She was always with me. Not only for the last two years, but also for the time since I have met her, I want to thank Senay Yıldız, for her unique friendship.

Table of Contents

List of Tables

Chapter 1

Introduction

Let $S = (s_0, s_1, s_2, \ldots)$ be a sequence with terms in the finite field $\mathbb{F}_q$. S is said to be *N-periodic* if $s_i = s_{i+N}$ for all $i \geq 0$. Then the sequence is determined by the terms of one period, so it can be possible to use the notation $S = (s_0, s_1, \ldots, s_{N-1})^\infty$. For any *N-periodic* sequence S, $S^N(x)$ is defined to be the polynomial

$$S^N(x) = s_0 + s_1 x + s_2 x^2 + \ldots + s_{N-1} x^{N-1}.$$

Definition 1.0.1. Let $S = (s_0,\ s_1, \ldots, s_{N-1})^\infty$ be an N-periodic sequence with terms in $\mathbb{F}_q$. The *linear complexity* $L(S)$ of the sequence is the smallest non-negative integer c satisfying the equation $s_j + d_1 s_{j-1} + \ldots + d_c s_{j-c} = 0$ for some coefficients $d_1,\ d_2, \ldots,\ d_c \in \mathbb{F}_q$.

Definition 1.0.2. Let $S = (s_0, s_1, \ldots, s_{N-1})^\infty$ be an N-periodic sequence with terms in $\mathbb{F}_q$. The *minimal polynomial* of the sequence S is

$$m(x) = x^c + d_1 x^{c-1} + \ldots + d_{c-1} x + d_c \in \mathbb{F}_q[x].$$

In the minimal polynomial, the degree of the minimal polynomial, c, is the linear complexity of the sequence S. Obviously, $L(S) = 0$ if S is the zero sequence.

1.1 Generalized Discrete Fourier Transform and Discrete Fourier Transform

Definition 1.1.1. Let $g(x) = \sum_i a_i x^i$ be a polynomial in the polynomial ring $\mathbb{F}[x]$ over a field $\mathbb{F}$. For an integer $t \geq 0$, t-th *Hasse derivative* of $g(x)$ is defined as the polynomial

$$g^{[t]}(x) = \sum_i \binom{i}{t} a_i x^{i-t}.$$

Proposition 1.1.2. *For any integer $t \geq 0$, we have $g^{(t)}(x) = t! g^{[t]}(x)$ where $g^{(t)}(x)$ denotes the t-th formal derivative.*

Proof: Let

$$g(x) = \sum_i a_i x^i.$$

Note that;

$$g^{(t)}(x) = \sum_i a_i i(i-1)(i-2)\dots(i-t+1)x^{i-t}.$$

We know that

$$\begin{aligned} i(i-1)(i-2)\dots(i-t+1) &= \frac{i(i-1)\dots(i-t+1)(i-t)!t!}{(i-t)!t!} \\ &= t!\binom{i}{t}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} g^{(t)}(x) &= \sum_i a_i t! \binom{i}{t} x^{i-t} \\ &= t! g^{[t]}(x). \end{aligned}$$

□

Definition 1.1.3. Let $S^N = (s_0, s_1, \dots, s_{N-1}) \in \mathbb{F}_q^N$ be an N-tuple, such that

$N = p^v n$, where $\gcd(p, n) = 1$ and $p = char\,(\mathbb{F}_q)$. If

$$S^N(x) = s_0 + s_1 x + s_2 x^2 + \ldots + s_{N-1} x^{N-1}$$

be the polynomial corresponding to the sequence S. Then the *Generalized Discrete Fourier Transform* of S^N, which is denoted by $(GDFT)(S^N)$, is a $p^v \times n$ matrix determined as:

$$GDFT(S^N) = \begin{pmatrix} S^N(1) & S^N(\alpha) & \ldots & S^N(\alpha^{n-1}) \\ (S^N)^{[1]}(1) & (S^N)^{[1]}(\alpha) & \ldots & (S^N)^{[1]}(\alpha^{n-1}) \\ \vdots & \vdots & & \vdots \\ (S^N)^{[p^v-1]}(1) & (S^N)^{[p^v-1]}(\alpha) & \ldots & (S^N)^{[p^v-1]}(\alpha^{n-1}) \end{pmatrix}$$

where α is any primitive n-th root of unity in some extension field of $\mathbb{F}_q$.

Example 1.1.4. $S = (100101)^\infty$ is a sequence with terms in $\mathbb{F}_2$, so $p = 2$. Its period is $N = 6 = 2 \times 3$. Here $v = 1$ and $n = 3$. Hence the $GDFT(S^6)$ is a 2×3 matrix, which is determined as:

$$GDFT(S^6) = \begin{pmatrix} S^6(1) & S^6(\alpha) & S^6(\alpha^2) \\ (S^6)^{[1]}(1) & (S^6)^{[1]}(\alpha) & (S^N)^{[1]}(\alpha^2) \end{pmatrix}.$$

In this sequence $s_0 = 1,\ s_1 = 0,\ s_2 = 0,\ s_3 = 1,\ s_4 = 0,\ s_5 = 1$.
Thus, $S^6(x) = 1 + x^3 + x^5$. Let us first find the 1st Hasse Derivative of $S^6(x)$.

$$\begin{aligned} (S^6)^{[1]}(x) &= \sum_{i=0}^{5} \binom{i}{1} s_i x^{i-1} \\ &= \binom{3}{1} x^2 + \binom{5}{1} x^4 \\ &= 3x^2 + 5x^4 \\ &\equiv x^2 + x^4 \bmod 2 \end{aligned}$$

We have $n = 3$, so we choose a primitive 3rd root of unity. Let α be a primitive 3rd root of unity. Then,

$$\begin{aligned} & \alpha^3 = 1 \\ \Rightarrow \quad & \alpha^3 - 1 = 0 \\ \Rightarrow \quad & (\alpha - 1)\left(\alpha^2 + \alpha + 1\right) = 0 \end{aligned}$$

Since α is a primitive 3rd root of unity

$$\alpha - 1 \neq 0.$$

Hence we have

$$\begin{aligned} \alpha^2 + \alpha + 1 &= 0 \\ \Rightarrow \alpha^2 &= \alpha + 1. \end{aligned}$$

Thus, the entries of the GDFT are as follows:

$$\begin{aligned} S^6(1) &= 1 + 1 + 1 \\ &\equiv 1 \bmod 2 \\ S^6(\alpha) &= 1 + \alpha^3 + \alpha^5 \\ &\equiv 1 + 1 + \alpha^3\alpha^2 \mod 2 \\ &\equiv \alpha^2 \mod 2 \\ &\equiv \alpha + 1 \mod 2 \end{aligned}$$

$$
\begin{aligned}
S^6(\alpha^2) &= 1+\alpha^6+\alpha^{10} \\
&\equiv 1+(\alpha^3)^2+(\alpha^3)^3\alpha \mod 2 \\
&\equiv 1+1+\alpha \mod 2 \\
&\equiv \alpha \mod 2 \\
(S^6)^{[1]}(1) &= 1+1 \\
&\equiv 0 \mod 2 \\
(S^6)^{[1]}(\alpha) &= \alpha^2+\alpha^4 \\
&\equiv \alpha+1+\alpha^3\alpha \mod 2 \\
&\equiv \alpha+1+\alpha \mod 2 \\
&\equiv 1 \\
(S^6)^{[1]}(\alpha^2) &= \alpha^4+\alpha^8 \\
&\equiv \alpha^3\alpha+(\alpha^3)^2\alpha^2 \mod 2 \\
&\equiv \alpha+\alpha+1 \mod 2 \\
&\equiv 1 \mod 2
\end{aligned}
$$

So,

$$
GDFT(S^6) = \begin{pmatrix} 1 & \alpha+1 & \alpha \\ 0 & 1 & 1 \end{pmatrix}
$$

Remark 1.1.5. The entries of the GDFT of an N-tuple depend on the choice of the primitive n-th root of unity.

Remark 1.1.6. Let $S^N = (s_0, s_1, \ldots, s_{N-1}) \in \mathbb{F}_q^N$, such that $gcd(p, N) = 1$, where $p = char\,(\mathbb{F}_q)$. Then GDFT of S^N reduces to N-tuple, $\big(S^N(1), S^N(\alpha) \ldots, S^N(\alpha^{N-1})\big)$, which is called the Discrete Fourier Transform (DFT).

1.2 Günther Weight

Definition 1.2.1. The *Günther Weight* of a matrix is the number of its entries that are nonzero or that lie below a nonzero entry.

Example 1.2.2. Remember Example 1.1.4,

$$GDFT(S^6) = \begin{pmatrix} 1 & \alpha+1 & \alpha \\ 0 & 1 & 1 \end{pmatrix}, \quad \text{Günther weight of this matrix is 6.}$$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \quad \text{Günther weight of A is 6.}$$

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{Günther weight of B is 8.}$$

Remark 1.2.3. If the matrix has only one row then the G*ü*nther weight of the matrix is just the Hamming weight.

1.3 Cyclotomic Cosets

Definition 1.3.1. Let $q = p^m$ for some $m \geq 1$, where p is prime. If n is an integer such that $\gcd(q, n) = 1$ and d is the multiplicative order of q in the multiplicative group of $\mathbb{Z}_n^*$. Then for an integer j, where $0 \leq j \leq n-1$, the *cyclotomic coset*, C_j, of j modulo n (relative to q) is defined as the set

$$C_j = \{k : k \equiv jq^r \bmod n,\ 0 \leq r\ <\ d\}\,.$$

Theorem 1.3.2. *(Günther-Blahut Theorem)*[2] *Let* $S = (s_0, s_1, \ldots, s_N - 1)^\infty$ *be an* N*-periodic sequence with terms in* $\mathbb{F}_q$*, such that* $N = p^v n$*, where* $gcd(p, n) = 1$ *and* $p = char\,(\mathbb{F}_q)$*. Then the linear complexity of this sequence is equal to the*

Günther weight of the GDFT(S^N).

Remark 1.3.3. If $gcd(p, N) = 1$, that is $N = n$, then GDFT(S^N) is an N-tuple $(S^N(1), S^N(\alpha), \ldots, S^N(\alpha^{N-1}))$. Therefore, the linear complexity of the sequence S is the Hamming weight of the N-tuple.

Example 1.3.4. For $q = p = 3$ and $n = 7$, the cyclotomic coset of j modulo n are:

- $j = 0$: for $k \in C_0$, $k \equiv jq^r \equiv 0 \cdot 3^r \equiv 0 \bmod 7$

  $C_0 = \{0\}$

- $j = 1$: for $k \in C_1$, $k \equiv jq^r \equiv 1 \cdot 3^r \equiv 3^r \bmod 7$

  $r = 0 \Rightarrow k \equiv 3^0 \equiv 1 \bmod 7$,

  $r = 1 \Rightarrow k \equiv 3^1 \equiv 3 \bmod 7$,

  $r = 2 \Rightarrow k \equiv 3^2 \equiv 2 \bmod 7$,

  $r = 3 \Rightarrow k \equiv 3^3 \equiv 6 \bmod 7$

  $r = 4 \Rightarrow k \equiv 3^4 \equiv 4 \bmod 7$

  $r = 5 \Rightarrow k \equiv 3^5 \equiv 5 \bmod 7$

  $r = 6 \Rightarrow k \equiv 3^6 \equiv 1 \bmod 7$

  $C_1 = \{1, 2, 3, 4, 5, 6\}$

- $j = 2$: for $k \in C_2$, $k \equiv jq^r \equiv 2 \cdot 3^r \bmod 7$

  $r = 0 \Rightarrow k \equiv 2 \cdot 3^0 \equiv 2 \bmod 7$,

  $r = 1 \Rightarrow k \equiv 2 \cdot 3^1 \equiv 6 \bmod 7$,

  $r = 2 \Rightarrow k \equiv 2 \cdot 3^2 \equiv 4 \bmod 7$,

  $r = 3 \Rightarrow k \equiv 2 \cdot 3^3 \equiv 5 \bmod 7$

  $r = 4 \Rightarrow k \equiv 2 \cdot 3^4 \equiv 1 \bmod 7$

  $r = 5 \Rightarrow k \equiv 2 \cdot 3^5 \equiv 3 \bmod 7$

  $r = 6 \Rightarrow k \equiv 2 \cdot 3^6 \equiv 2 \bmod 7$

  $C_2 = \{1, 2, 3, 4, 5, 6\}$

- $j = 3$: for $k \in C_3$, $k \equiv jq^r \equiv 3 \cdot 3^r \bmod 7$

  $r = 0 \Rightarrow k \equiv 3 \cdot 3^0 \equiv 3 \bmod 7$,

  $r = 1 \Rightarrow k \equiv 3 \cdot 3^1 \equiv 2 \bmod 7$,

  $r = 2 \Rightarrow k \equiv 3 \cdot 3^2 \equiv 6 \bmod 7$,

  $r = 3 \Rightarrow k \equiv 3 \cdot 3^3 \equiv 4 \bmod 7$

  $r = 4 \Rightarrow k \equiv 3 \cdot 3^4 \equiv 5 \bmod 7$

  $r = 5 \Rightarrow k \equiv 3 \cdot 3^5 \equiv 1 \bmod 7$

  $r = 6 \Rightarrow k \equiv 3 \cdot 3^6 \equiv 3 \bmod 7$

  $C_3 = \{1, 2, 3, 4, 5, 6\}$

- $j = 4$: for $k \in C_4$, $k \equiv jq^r \equiv 4 \cdot 3^r \bmod 7$

  $r = 0 \Rightarrow k \equiv 4 \cdot 3^0 \equiv 4 \bmod 7$,

  $r = 1 \Rightarrow k \equiv 4 \cdot 3^1 \equiv 5 \bmod 7$,

  $r = 2 \Rightarrow k \equiv 4 \cdot 3^2 \equiv 1 \bmod 7$,

  $r = 3 \Rightarrow k \equiv 4 \cdot 3^3 \equiv 3 \bmod 7$

  $r = 4 \Rightarrow k \equiv 4 \cdot 3^4 \equiv 2 \bmod 7$

  $r = 5 \Rightarrow k \equiv 4 \cdot 3^5 \equiv 6 \bmod 7$

  $r = 6 \Rightarrow k \equiv 4.3^6 \equiv 4 \bmod 7$

  $C_4 = \{1, 2, 3, 4, 5, 6\}$

- $j = 5$: for $k \in C_5$, $k \equiv jq^r \equiv 5 \cdot 3^r \bmod 7$

  $r = 0 \Rightarrow k \equiv 5 \cdot 3^0 \equiv 5 \bmod 7$,

  $r = 1 \Rightarrow k \equiv 5 \cdot 3^1 \equiv 1 \bmod 7$,

  $r = 2 \Rightarrow k \equiv 5 \cdot 3^2 \equiv 3 \bmod 7$,

  $r = 3 \Rightarrow k \equiv 5 \cdot 3^3 \equiv 2 \bmod 7$

  $r = 4 \Rightarrow k \equiv 5 \cdot 3^4 \equiv 6 \bmod 7$

  $r = 5 \Rightarrow k \equiv 5 \cdot 3^5 \equiv 4 \bmod 7$

$$r = 6 \Rightarrow k \equiv 5 \cdot 3^6 \equiv 5 \bmod 7$$

$C_5 = \{1, 2, 3, 4, 5, 6\}$

- $j = 6$: for $k \in C_6$, $k \equiv jq^r \equiv 6 \cdot 3^r \bmod 7$

$$r = 0 \Rightarrow k \equiv 6 \cdot 3^0 \equiv 6 \bmod 7,$$

$$r = 1 \Rightarrow k \equiv 6 \cdot 3^1 \equiv 4 \bmod 7,$$

$$r = 2 \Rightarrow k \equiv 6 \cdot 3^2 \equiv 5 \bmod 7,$$

$$r = 3 \Rightarrow k \equiv 6 \cdot 3^3 \equiv 1 \bmod 7$$

$$r = 4 \Rightarrow k \equiv 6 \cdot 3^4 \equiv 3 \bmod 7$$

$$r = 5 \Rightarrow k \equiv 6 \cdot 3^5 \equiv 2 \bmod 7$$

$$r = 6 \Rightarrow k \equiv 6 \cdot 3^6 \equiv 6 \bmod 7$$

$C_6 = \{1, 2, 3, 4, 5, 6\}$

Note that $C_1 = C_2 = C_3 = C_4 = C_5 = C_6$ and the equality of these cyclotomic cosets also follows directly from Definition 1.3.1. However for a better understanding we prefer to illustrate the computations in this example.

This property leads us to a proposition.

Proposition 1.3.5. *Let C_j be a cyclotomic coset of j modulo n (relative to q). If $k \in C_j$, then $C_j = C_k$.*

Proof: If $k \in C_j$, then

$$k \equiv jq^r \mod n \tag{1.1}$$

for some $r \geq 0$. We have $\gcd(q, n) = 1$. Let d be the multiplicative order of q in $\mathbb{Z}_n^*$. Then the multiplicative inverse of q^r modulo n is q^{d-r}. Multiplying both sides of (1.1) with q^{d-r}, we get;

$$kq^{d-r} \equiv j \mod n$$

This implies that $j \in C_k$.
Let $a \in C_j$, then for some $r_1 \geq 0$,

$$\begin{aligned} a &\equiv jq^{r_1} \mod n \\ &\equiv kq^{d-r}q^{r_1} \mod n \\ &\equiv kq^{d-r+r_1} \mod n \end{aligned}$$

which implies that $a \in C_k$. Therefore we have $C_j \subset C_k$.
Let $b \in C_k$, then for some $r_2 \geq 0$, we have

$$\begin{aligned} b &\equiv kq^{r_2} \mod n \\ &\equiv jq^{r}q^{r_2} \mod n \\ &\equiv jq^{r+r_2} \mod n \end{aligned}$$

which implies that $b \in C_j$. Therefore,

$$C_k \subset C_j.$$

$C_j \subset C_k$ and $C_k \subset C_j$ implies that $C_k = C_j$.

□

Note that, the cyclotomic cosets are distinct sets.

Definition 1.3.6. Let C_j be a cyclotomic coset of j modulo n (relative to q). Given k_1, $k_2 \in C_j$, such that

$$k_1 \equiv jq^{r_1} \mod n \tag{1.2}$$

$$k_2 \equiv jq^{r_2} \mod n \tag{1.3}$$

the operation $\otimes$ is defined as:

$$k_1 \otimes k_2 := jq^{r_1+r_2} \mod n.$$

Note that this operation is commutative and associative.

Lemma 1.3.7. *$\langle C_j, \otimes \rangle$ is an abelian group under the operation $\otimes$.*

Proof: First we prove the well-definedness of the operation $\otimes$. Let $k_1, k_2 \in C_j$ be given as in (1.2) and (1.3). Suppose that

$$k_1 \equiv jq^{r_1} \equiv jq^{r_1^{'}} \bmod n,$$

$$k_2 \equiv jq^{r_2} \equiv jq^{r_2^{'}} \bmod n.$$

We need to check if $jq^{r_1+r_2} \equiv jq^{r_1^{'}+r_2^{'}} \bmod n$.
Note that,

$$q^{r_1+r_2} - q^{r_1^{'}+r_2^{'}} \equiv q^{r_1+r_2} - q^{r_1^{'}+r_2} + q^{r_1^{'}+r_2} - q^{r_1^{'}+r_2^{'}} \bmod n$$

$$\equiv q^{r_2}(q^{r_1} - q^{r_1^{'}}) + q^{r_1^{'}}(q^{r_2} - q^{r_2^{'}}) \bmod n. \tag{1.4}$$

Hence,

$$j(q^{r_1+r_2} - q^{r_1^{'}+r_2^{'}}) \equiv j(q^{r_1} - q^{r_1^{'}})q^{r_2} + j(q^{r_2} - q^{r_2^{'}})q^{r_1^{'}} \bmod n.$$

Since $jq^{r_1} \equiv jq^{r_1^{'}} \bmod n$, we have $n \mid j(q^{r_1} - q^{r_1^{'}})$.
Also since $jq^{r_2} \equiv jq^{r_2^{'}} \bmod n$ we have $n \mid j(q^{r_2} - q^{r_2^{'}})$. Therefore, we have

$$n \mid j(q^{r_1} - q^{r_1^{'}})q^{r_2} + j(q^{r_2} - q^{r_2^{'}})q^{r_1^{'}}$$

On the other hand, by (1.4)

$$n \mid j\left(q^{r_1+r_2} - q^{r_1^{'}+r_2^{'}}\right),$$

hence

$$j(q^{r_1+r_2}) \equiv j(q^{r_1^{'}+r_2^{'}}) \bmod n.$$

This completeness the well-definedness and it is routine to check the associativity and commutativity.

Let us prove the existence of the identity element. Let $e \in C_j$ such that $e = jq^{r_0} \bmod n$ for some $r_0 \geq 0$. We know that e is the identity element if and only if $e \otimes a = a \otimes e = a$ for any $a \in C_j$. Since $\otimes$ is commutative, it is sufficient to check if there exist an element e satisfying $e \otimes a = a$. Let $a = jq^r$ for some $r \geq 0$.

$$\begin{aligned} a \otimes e &= a \\ jq^r \otimes jq^{r_0} &\equiv jq^r \bmod n \\ jq^{r+r_0} &\equiv jq^r \bmod n \\ jq^r(q^{r_0} - 1) &\equiv 0 \bmod n \\ \Rightarrow n &\mid jq^r(q^{r_0} - 1) \end{aligned}$$

We have $\gcd(q, n) = 1$. This implies that

$$\begin{aligned} \Rightarrow n &\mid j(q^{r_0} - 1) \\ \Rightarrow j(q^{r_0} - 1) &\equiv 0 \bmod n \\ \Rightarrow jq^{r_0} &\equiv j \bmod n \\ \Rightarrow e &\equiv j \bmod n \end{aligned}$$

We have proved the existence of the identity element. Now we have to prove the uniqueness of the identity element. To do this suppose that there exists

$e' = jq^{r_1}$ satisfying $e' \otimes a = a$. Therefore we have the following:

$$\begin{aligned}
a \otimes e' &= a \otimes e \\
jq^r \otimes jq^{r_1} &= jq^r \otimes j \\
jq^{r+r_1} &\equiv jq^r \bmod n \\
jq^{r+r_1} - jq^r &\equiv 0 \bmod n \\
jq^r(q^{r_1} - 1) &\equiv 0 \bmod n \\
\Rightarrow n &\mid jq^r(q^{r_1} - 1) \\
\Rightarrow n &\mid j(q^{r_1} - 1) \\
\Rightarrow j(q^{r_1} - 1) &\equiv 0 \bmod n \\
\Rightarrow j(q^{r_1} - 1) &\equiv 0 \bmod n \\
\Rightarrow jq^{r_1} &\equiv j \bmod n \\
\Rightarrow e' &\equiv j \bmod n \\
\Rightarrow e' &\equiv e \bmod n
\end{aligned}$$

We have proved that the identity element is unique. Therefore $\langle C_j, \otimes \rangle$ is an abelian group under the operation $\otimes$.

□

Corollary 1.3.8. *Let C_j be a cyclotomic coset of j modulo n (relative to q) and $|C_j| = l_j$, then we have:*

$$jq^{l_j} \equiv j \bmod n \tag{1.5}$$

Proof: If $|C_j| = l_j$ then we know that, for any element k in C_j satisfies

$$\underbrace{k \otimes k \otimes \ldots \otimes k}_{l_j \ times} = e.$$

Therefore, for $k \equiv jq \bmod n$ we have:

$$\begin{aligned} \underbrace{jq \otimes jq \otimes \ldots \otimes jq}_{l_j \ times} &= e \\ jq^{l_j} &= j \end{aligned}$$

□

Lemma 1.3.9. *Let $S = (s_0, s_1, \ldots, s_{N-1})^\infty$ be an N-periodic sequence, such that $N = p^v n$, where $gcd(p, n) = 1$ and $p = char(\mathbb{F}_q)$. Suppose that C_j is the cyclotomic coset of j modulo n (relative to q) such that $|C_j| = l_j$. If $S^N(x)$ is the polynomial corresponding to S, then for $0 \leq t \leq p^v - 1$ we have the following:*

i) $\left(S^N\right)^{[t]}(x)(\alpha^j) \in \mathbb{F}_{q^{l_j}}$

ii) For any $k \in C_j$ where $k \equiv jq^r \bmod n$, we have

$$(S^N)^{[t]}(x)(\alpha^k) = ((S^N)^{[t]}(\alpha^j))^{q^r} \tag{1.6}$$

where α is any primitive n-th root of unity in some extension field of $\mathbb{F}_q$.

Proof: Recall that, for any $a, b \in \mathbb{F}_q$, we have

$$(a+b)^{p^m} = a^{p^m} + b^{p^m} \tag{1.7}$$

$$a^{q^r} = a \text{ for any r} \geq 0 \tag{1.8}$$

i) We have

$$(S^N)^{[t]}(\alpha^j) = \sum_i \binom{i}{t} s_i \alpha^{j(i-t)}.$$

Note that the coefficients $\binom{i}{t}s_i$ are the elements of $\mathbb{F}_q$.

$$\begin{aligned}
\left((S^N)^{[t]}(\alpha^j)\right)^{q^{l_j}} &= \left(\sum_i \binom{i}{t} s_i \alpha^{j(i-t)}\right)^{q^{l_j}} \\
&= \sum_i \left(\binom{i}{t} s_i \alpha^{j(i-t)}\right)^{q^{l_j}}, \quad \text{by (1.7).} \\
&= \sum_i \binom{i}{t} s_i \alpha^{jq^{l_j}(i-t)}, \quad \text{by (1.8).} \\
&= \sum_i \binom{i}{t} s_i \alpha^{j(i-t)}, \quad \text{by (1.5).} \\
&= (S^N)^{[t]}(\alpha^j)
\end{aligned}$$

Therefore, $(S^N)^{[t]}(\alpha^j) \in \mathbb{F}_q^{l_j}$.

$$\begin{aligned}
ii)\ (S^N)^{[t]}(\alpha^k) &= \sum_i \binom{i}{t} s_i \alpha^{k(i-t)} \\
&= \sum_i \binom{i}{t} s_i \alpha^{jq^r(i-t)} \\
&= \sum_i \left(\binom{i}{t} s_i \alpha^{j(i-t)}\right)^{q^r}, \quad \text{by (1.8).} \\
&= \left(\sum_i \binom{i}{t} s_i \alpha^{j(i-t)}\right)^{q^r}, \quad \text{by (1.7)} \\
&= \left[(S^N)^{[t]}(\alpha^j)\right]^{q^r}
\end{aligned}$$

□

Proposition 1.3.10. *Let S be an N-periodic sequence with terms in $\mathbb{F}_q$ such that $N = p^v n$ where $gcd(p, n) = 1$ and $p = char\,(\mathbb{F}_q)$. Let*

$$C_j = \left\{j = k_1, k_2, \ldots, k_{l_j}\right\}$$

be a cyclotomic coset of j modulo n (relative to q) with $|C_j| = l_j$. Suppose that

$$A_t^n = (a_{t,0}, a_{t,1}, \ldots, a_{t,n-1})$$

is any row in the GDFT(S^N), then for all $1 \leq r \leq l_j$ *either* $a_{t,k_r} = 0$ *or* $a_{t,k_r} \neq 0$

Proof: For an element $k_{r_0} \in C_j$ where $k_{r_0} = jq^{r_0}$ for some $r_0 \geq 0$.
The entry $a_{t,k_{r_0}} = (S^N)^{[t]}(\alpha^{k_{r_0}})$ and we have by (1.6)

$$(S^N)^{[t]}(\alpha^{k_{r_0}}) = ((S^N)^{[t]}(\alpha^j))^{q^{r_0}}.$$

If $a_{t,k_{r_0}} = 0$ that is $\left((S^N)^{[t]}(\alpha^j)\right)^{q^{r_0}} = 0$, then $(S^N)^{[t]}(\alpha^j) = 0$, since $(S^N)^{[t]}(\alpha^j) \in \mathbb{F}_{q^{l_j}}$ and $\mathbb{F}_{q^{l_j}}$ has no nonzero zero divisor. Therefore,
$a_{t,k_i} = (S^N)^{[t]}(\alpha^{k_i}) = \left((S^N)^{[t]}(\alpha^j)\right)^{q^{r_i}} = 0$ for all $r_i \geq 0$.
If $a_{t,k_{r_0}} \neq 0$, that is, $a_{t,k_{r_0}} = ((S^N)^{[t]}(\alpha^j))^{q^{r_0}} \neq 0$. Thus, $(S^N)^{[t]}(\alpha^j) \neq 0$. Therefore, $a_{t,k_i} = (S^N)^{[t]}(\alpha^{k_i}) = ((S^N)^{[t]}(\alpha^j))^{q^{r_i}} \neq 0$ for any $r_i \geq 0$

□

Corollary 1.3.11. *Let S be an N-periodic sequence with terms in $\mathbb{F}_q$, such that $N = p^v n$, where $p = char\,(\mathbb{F}_q)$ and $gcd(p, n) = 1$. Suppose that $C_j = \left\{j = k_1, k_2, \ldots, k_{l_j}\right\}$ is the cyclotomic coset of j modulo n (relative to q). If t_j is the least index such that in the t_j-th row, $A^n_{t_j} = (a_{t_j,0}, a_{t_j,1}, \ldots, a_{t_j,n-1})$, of the GDFT($S^N$) we have $a_{t_j,k_r} \neq 0$, provided that such a row exists, then the contribution of C_j to the Günther Weight of the GDFT(S^N) is $l_j(p^v - t_j + 1)$.*

Proof: In the t_j-th row $A^n_{t_j} = (a_{t_j,0}, a_{t_j,1}, \ldots, a_{t_j,n-1})$ we have $a_{t,k_r} \neq 0$ so by Proposition 1.3.10 we have $a_{t_j,k_i} \neq 0$ for any $k_i \in C_j$. Since there are $p^v - t_j$ entries below a non zero entry of $A^n_{t_j}$ and we have l_j nonzero entries from the cyclotomic coset C_j. Totally we have $l_j + l_j(p^v - t_j)$ entries contributing to the Günther Weight.

□

Corollary 1.3.12. *Let S be an N-periodic sequence with terms in $\mathbb{F}_q$, such that $N = p^v n$ where $gcd(p, n) = 1$ and $p = char\,(\mathbb{F}_q)$. Suppose that $C_{j_1}, C_{j_2}, \ldots, C_{j_h}$ are the different cyclotomic cosets modulo n (relative to q) and $l_{j_1}, l_{j_2}, \ldots, l_{j_h}$*

are their cardinalities respectively. Then the linear complexity of S is given by

$$L(S) = \sum_{i=1}^{h} (p^v - t_{j_i} + 1) l_{j_i}. \tag{1.9}$$

where $(p^v - t_{j_i} + 1)l_{j_i}$ is the contribution of the cyclotomic coset C_{j_i} to the Günther Weight.

Remark 1.3.13. Let h denote the number of the different cyclotomic cosets modulo n. Then any GDFT uniquely corresponds to a $p^v \times h$ matrix $\mathcal{M}$, where the entries in the i-th column are in $\mathbb{F}_{q^{l_{j_i}}}$ and $|C_{j_i}| = l_{j_i}$. The set of these matrices can be denoted as $\mathbf{M}$

Proposition 1.3.14. *The number of the different matrices in the GDFT form is Ω given by*

$$\Omega = (q^{l_{j_1}})^{p^v} (q^{l_{j_2}})^{p^v} \dots (q^{l_{j_h}})^{p^v} = q^{np^v}. \tag{1.10}$$

Proof: Since the entries of the i-th column are in $\mathbb{F}_{q^{l_{j_i}}}$, we have $q^{l_{j_i}}$ choices for just one entry. As we have p^v entries in a column, there are $(q^{l_{j_i}})^{p^v}$ choices for a column. Since we have h columns then the number of different matrices in the GDFT form is $\prod_{i=1}^{h} (q^{l_{j_i}})^{p^v}$.
Also we know that

$$\sum_{i=1}^{h} l_{j_i} = n$$

since the cyclotomic cosets are different. Then

$$\begin{aligned} \prod_{i=1}^{h} \left(q^{l_{j_i}}\right)^{p^v} &= \left((q^{l_{j_1}})(q^{l_{j_2}}) \dots (q^{l_{j_h}})\right)^{p^v} \\ &= \left(q^{l_{j_1} + l_{j_2} + \dots + l_{j_h}}\right)^{p^v} \\ &= q^{np^v} \\ &= q^N \end{aligned}$$

□

Remark 1.3.15. The number of different matrices in the GDFT form is q^N

which is also equal to the number of all N-periodic sequences with terms in $\mathbb{F}_q$.

Chapter 2

The Expected Value Of The Linear Complexity

In this chapter, we consider the expected value the linear complexity of an N-periodic sequence S with terms in $\mathbb{F}_q$, where $N = p^v n$ such that $\gcd(p, n) = 1$ and p is the characteristic of $\mathbb{F}_q$. Since S is N-periodic such that, $S = (s_0, s_1 \ldots, s_{N-1})^\infty$ it can be considered as an N-tuple of $\mathbb{F}_q^N$.

In general the expected value of the linear complexity is given by the formula:

$$\mathbf{E}_N(L(S)) = \sum_{S \in \mathbb{F}_q^N} \mathbf{p}(S) L(S) \tag{2.1}$$

where $\mathbf{p}$ is the probability measure. Here, the probability of each $S \in \mathbb{F}_q^N$ to occur is supposed to be $\frac{1}{q^N}$.

2.1 Expected Value Of The Linear Complexity

Theorem 2.1.1. *Let S be an N-periodic sequence with terms in $\mathbb{F}_q$ such that $N = p^v n$ where $gcd(p, n) = 1$ and $p = char(\mathbb{F}_q)$. If $l_1, l_2, \ldots, l_s$ are different cardinalities of the cyclotomic cosets modulo n and Φ_i, $1 \leq i \leq s$, is the number of elements belonging to cyclotomic cosets with cardinality l_i. Then the expected*

value of the linear complexity of S is:

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} \tag{2.2}$$

Proof: Let $D_1, D_2, \ldots, D_h$ be different cyclotomic cosets modulo n and

$$|D_r| = m_r$$

for $r = 1, 2, \ldots, h$. We know that the linear complexity of S is equal to the Günther Weight of the $GDFT(S^N)$. As we have said in Remark 1.3.13, every matrix in the $GDFT$ form corresponds to a $p^v \times h$ matrix $\mathcal{M}$, where the entries in the r-th column are in $\mathbb{F}_{q^{m_r}}$. Let us say that $\vec{k_1}, \vec{k_2}, \ldots, \vec{k_h}$ are the columns of the matrix $\mathcal{M}$. Suppose that $t(\vec{k_r})$ is the least positive integer such that the $t(\vec{k_r})$-th coordinate of the column $t(\vec{k_r})$ is nonzero, then the Günther Weight of $\mathcal{M}$ is:

$$g(\mathcal{M}) = \sum_{\substack{r=1 \\ \vec{k_r} \neq 0}}^{h} m_r \left(p^v - t\left(\vec{k_r}\right) + 1 \right) \tag{2.3}$$

In (2.2),

$$\mathbf{E}_N(L(S)) = \sum_{S \in \mathbb{F}_q^N} \mathbf{p}(S) L(S)$$

putting the probability and linear complexity values we get:

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= \frac{1}{q^N} \sum_{\mathcal{M} \in \mathbf{M}} \sum_{\substack{r=1 \\ \vec{k_r} \neq 0}}^{h} m_r \left(p^v - t\left(\vec{k_r}\right) + 1 \right) \\
&= \frac{1}{q^N} \sum_{r=1}^{h} \sum_{\substack{\mathcal{M} \in \mathbf{M} \\ \vec{k_r} \neq 0}} m_r \left(p^v - t\left(\vec{k_r}\right) + 1 \right) \\
&= \frac{p^v}{q^N} \sum_{r=1}^{h} m_r \sum_{\substack{\mathcal{M} \in \mathbf{M} \\ \vec{k_r} \neq 0}} 1 - \frac{1}{q^N} \sum_{r=1}^{h} \sum_{\substack{\mathcal{M} \in \mathbf{M} \\ \vec{k_r} \neq 0}} (t(\vec{k_r}) - 1) \\
&:= \mathbf{T_1} - \mathbf{T_2}
\end{aligned}$$

By above equations:

$$\begin{aligned}\mathbf{T_1} &= \frac{p^v}{q^N}\sum_{r=1}^{h} m_r \sum_{\substack{\mathcal{M}\in\mathbf{M}\\ \vec{k_r}\neq\vec{0}}} 1 \text{ and}\\ \mathbf{T_2} &= \frac{1}{q^N}\sum_{r=1}^{h} m_r \sum_{\substack{\mathcal{M}\in\mathbf{M}\\ \vec{k_r}\neq\vec{0}}} (t(\vec{k_r})-1)\end{aligned}$$

Claim 1:

$$\sum_{\substack{\mathcal{M}\in\mathbf{M}\\ \vec{k_r}\neq 0}} 1 = q^N - q^{N-p^v m_r} \Leftrightarrow \#\left\{\mathcal{M}\in\mathbf{M} : \tilde{k_r} = \tilde{0}\right\} = q^{N-p^v m_r}$$

Proof of the Claim 1:
$\vec{k_r} = \vec{0}$ is the column corresponds to the cyclotomic coset D_r. Since there are p^v components, $p^v m_r$ entries are 0 and do not lie below a nonzero entry in the matrix GDFT form. The entries of the columns $\vec{k_1}, \vec{k_2}, \ldots, \vec{k_{r-1}}, \vec{k_{r+1}}, \ldots, \vec{k_h}$ can be selected in $(q^{m_1})^{p^v}, (q^{m_2})^{p^v}, \ldots, (q^{m_{r-1}})^{p^v}, (q^{m_{r+1}})^{p^v}, \ldots, (q^{m_h})^{p^v}$ ways respectively. Thus, the number of $\mathcal{M}$ matrices with $\vec{k_r} = \vec{0}$ is :

$$(q^{m_1})^{p^v}(q^{m_2})^{p^v}\ldots(q^{m_{r-1}})^{p^v}(q^{m_{r+1}})^{p^v}\ldots(q^{m_h})^{p^v}$$

$$\begin{aligned}&= q^{(m_1+m_2+\ldots+m_{r-1}+m_{r+1}+\ldots+m_h)p^v}\\ &= q^{(m_1+m_2+\ldots+m_{r-1}+m_r+m_{r+1}+\ldots+m_h)p^v - m_r p^v}\\ &= q^{N-p^v m_r}\end{aligned}$$

and claim 1 is proved.
Recall that the number of $\mathcal{M}$ matrices as given in (1.10) is q^N. Therefore, the

number of $\mathcal{M}$ matrices in $\mathbf{M}$ with $\vec{k_r} \neq \vec{0}$ is $q^N - q^{N-p^v m_r}$. Finally;

$$\begin{aligned}
\mathbf{T_1} &= \frac{p^v}{q^N} \sum_{r=1}^{h} m_r \sum_{\substack{\mathcal{M}\in\mathbf{M} \\ \vec{k_r}\neq\vec{0}}} 1 \\
&= \frac{p^v}{q^N} \sum_{r=1}^{h} m_r \left(q^N - q^{N-p^v m_r}\right) \\
&= p^v \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{p^v m_r}}\right) \\
&= p^v \underbrace{\sum_{r=1}^{h} m_r}_{n} - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v m_r}} \\
&= N - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v m_r}}
\end{aligned}$$

Claim 2:

$$\sum_{\substack{\mathcal{M}\in\mathbf{M} \\ \vec{k_r}\neq 0}} (t(\vec{k_r}) - 1) = \sum_{t=1}^{p^v} (t-1) \sum_{\substack{\mathcal{M}\in\mathbf{M} \\ t(\vec{k_r})=t}} 1 = \sum_{t=1}^{p^v} (t-1)(q^{m_r} - 1)(q^{m_r})^{p^v - t} q^{N-p^v m_r}$$

$$\Leftrightarrow$$

For all t with $1 \leq t \leq p^v$ and for all r with $1 \leq r \leq h$;

$$\#\left\{\mathcal{M} \in \mathbf{M} : t(\tilde{k_r}) = t\right\} = (q^{m_r} - 1)(q^{m_r})^{p^v - t} q^{N-p^v m_r}$$

Proof of Claim 2:
Now, consider the $\mathcal{M}$ matrices in $\mathbf{M}$ with $\vec{k_r} \neq \vec{0}$ and the least index which is nonzero is t, that is, $t(\vec{k_r}) = t$.

First of all, let us choose the entries of the columns other than the column $\vec{k_r}$. As we have done in the proof of the claim 1, we can select them in $q^{N-p^v m_r}$. Now we have to select the entries of $\vec{k_r}$. Since t is the least index which is nonzero, the components above this entry will be zero. We can choose the t-th

entry in $q^{m_r}-1$ way (we can not choose 0). There are p^v-t entries below the t-th, so we can select these entries in $(q^{m_r})^{p^v-t}$ ways.

Combining all these things, we obtain that the number of $\mathcal{M}$ matrices satisfying the above conditions is $(q^{m_r}-1)\,(q^{m_r})^{p^v-t}\,q^{N-p^v m_r}$. And this ends the proof of the claim 2. And, by this way,

$$\begin{aligned}\sum_{t=1}^{p^v}(t-1)\sum_{\substack{\mathcal{M}\in\mathbf{M}\\ t(\vec{k_r})=t}}1 &= \sum_{t=1}^{p^v}(t-1)\,(q^{m_r}-1)\,(q^{m_r})^{p^v-t}\,q^{N-p^v m_r}\\ &= \sum_{t=1}^{p^v}(t-1)\,(q^{m_r}-1)\left(q^{p^v m_r-tm_r+N-p^v m_r}\right)\\ &= \sum_{t=1}^{p^v}(t-1)\,(q^{m_r}-1)\left(q^{N-tm_r}\right)\end{aligned}$$

By all these arguments,

$$\mathbf{T_2}=\frac{1}{q^N}\sum_{r=1}^{h}m_r\sum_{\substack{\mathcal{M}\in\mathbf{M}\\ \vec{k_r}\neq\vec{0}}}(t(\vec{k_r})-1)=\frac{1}{q^N}\sum_{r=1}^{h}m_r\sum_{t=1}^{p^v}(t-1)\,(q^{m_r}-1)\left(q^{N-tm_r}\right)$$

$$=\sum_{r=1}^{h}m_r\,(q^{m_r}-1)\sum_{t=1}^{p^v}(t-1)\,q^{-tm_r}$$

By subtracting 1 from the index t we get:

$$=\sum_{r=1}^{h}m_r\,(q^{m_r}-1)\sum_{t=0}^{p^v-1}t\left(q^{-m_r}\right)^{t+1}$$

$$=\sum_{r=1}^{h}m_r\,(q^{m_r}-1)\,q^{-m_r}\sum_{t=0}^{p^v-1}t\left(q^{-m_r}\right)^{t}$$

$$=\sum_{r=1}^{h}m_r\left(1-\frac{1}{q^{m_r}}\right)\sum_{t=0}^{p^v-1}t\left(q^{-m_r}\right)^{t}$$

Claim 3: For any real number $z \neq 0$, we have:

$$\sum_{t=0}^{k-1} tz^t = \frac{z - kz^k + (k-1)\, z^{k+1}}{(z-1)^2} \tag{2.4}$$

Proof of Claim 3:

$$\begin{aligned}
\underbrace{\sum_{t=0}^{k-1} tz^t}_{\mathbf{S}} &= \sum_{t=1}^{k-1} tz^t \\
&= \sum_{t=1}^{k} tz^t - kz^k \\
&= \sum_{t=0}^{k-1} (t+1)\, z^{t+1} - kz^k \\
&= z \underbrace{\sum_{t=0}^{k-1} tz^t}_{\mathbf{S}} + z \sum_{t=0}^{k-1} z^t - kz^k
\end{aligned}$$

$$\begin{aligned}
\mathbf{S} &= z\mathbf{S} + z \sum_{t=0}^{k-1} z^t - kz^k \\
&= z\mathbf{S} + z\frac{z^k - 1}{z-1} - kz^k \\
\mathbf{S} - z\mathbf{S} &= \frac{z^{k+1} - z}{z-1} - \frac{kz^k\,(z-1)}{z-1} \\
\mathbf{S}\,(1-z) &= \frac{z^{k+1} - z - kz^{k+1} + kz^k}{z-1} \\
\mathbf{S} &= -\frac{z^{k+1} - z - kz^{k+1} + kz^k}{(z-1)^2} \\
&= \frac{z - kz^k + (k-1)\, z^{k+1}}{(z-1)^2}.
\end{aligned}$$

The proof of this claim is ended here. Substituting $z = q^{-m_r}$ and $k = p^v$ in

(2.4) we get:

$$\begin{aligned}
\mathbf{T_2} &= \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{m_r}}\right) \sum_{t=0}^{p^v-1} t \left(q^{-m_r}\right)^t \\
&= \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{m_r}}\right) \left[\frac{q^{-m_r} - p^v q^{-m_r p^v} + (p^v - 1)\, q^{-m_r(p^v+1)}}{\left(q^{-m_r} - 1\right)^2}\right] \\
&= \sum_{r=1}^{h} m_r \frac{q^{m_r} - 1}{q^{m_r}} \left[\frac{q^{-m_r} - p^v q^{-m_r p^v} + (p^v - 1)\, q^{-m_r(p^v+1)}}{\left(\frac{1-q^{m_r}}{q^{m_r}}\right)^2}\right] \\
&= \sum_{r=1}^{h} m_r \frac{q^{m_r}}{q^{m_r} - 1} \left(q^{-m_r} - p^v q^{-m_r p^v} + (p^v - 1)\, q^{-m_r(p^v+1)}\right) \\
&= \sum_{r=1}^{h} \frac{m_r}{q^{m_r} - 1} \left(1 - p^v q^{m_r(1-p^v)} + (p^v - 1)\, q^{-p^v m_r}\right) \\
&= \sum_{r=1}^{h} \frac{m_r}{q^{m_r} - 1} \left(1 - p^v q^{m_r} q^{-m_r p^v} + p^v q^{-m_r p^v} - q^{-m_r p^v}\right) \\
&= \sum_{r=1}^{h} \frac{m_r}{q^{m_r} - 1} \left(1 - p^v q^{-m_r p^v} \left(q^{m_r} - 1\right) - q^{-m_r p^v}\right)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{r=1}^{h} \frac{m_r}{q^{m_r} - 1} \left(1 - q^{-m_r p^v}\right) - \sum_{r=1}^{h} m_r p^v q^{-m_r p^v} \\
&= \sum_{r=1}^{h} \frac{m_r \left(1 - q^{-p^v m_r}\right)}{q^{m_r} - 1} - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v m_r}}
\end{aligned}$$

Continuing from the equation $\mathbf{E}_N(L(S)) = \mathbf{T_1} - \mathbf{T_2}$

$$\begin{aligned}
\mathbf{T_1} - \mathbf{T_2} &= N - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v m_r}} - \sum_{r=1}^{h} \frac{m_r \left(1 - q^{-p^v m_r}\right)}{q^{m_r} - 1} + p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v m_r}} \\
&= N - \sum_{r=1}^{h} \frac{m_r \left(1 - q^{-p^v m_r}\right)}{q^{m_r} - 1}
\end{aligned}$$

□

Corollary 2.1.2. *If $gcd(p, N) = 1$, that is $v = 0$ and $N = n$, then the expected value of the linear complexity of S*

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \tag{2.5}$$

Proof: If $v = 0$,

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} \\
&= N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-l_i})}{q^{l_i} - 1} \\
&= N - \sum_{i=1}^{s} \frac{\Phi_i \cdot \left(q^{l_i} - 1\right)}{\left(q^{l_i} - 1\right) q^{l_i}} \\
&= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}}.
\end{aligned}$$

□

Corollary 2.1.3. *If $n = 1$, that is $N = p^v$, then the expected value of the linear complexity of S*

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q-1}\left(1 - \frac{1}{q^N}\right). \tag{2.6}$$

Proof: Since $n = 1$, the only cyclotomic coset modulo n (relative to q) is $C_0 = \{0\}$. Thus, $l_1 = 1$ and $\Phi_1 = 1$. Hence

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} \\
&= N - \frac{\Phi_1 \cdot (1 - q^{-p^v l_1})}{q^{l_1} - 1} \\
&= N - \frac{1 - q^{-p^v}}{q - 1} \\
&= N - \frac{1 - q^{-N}}{q - 1}
\end{aligned}$$

□

Corollary 2.1.4. *Let S be a random N-periodic sequence with terms in $\mathbb{F}_q$, such that $N = p^v n$ where $gcd(p, n) = 1$ and $p = char(\mathbb{F}_q)$, then the expected value of the linear complexity of S satisfies*

$$\mathbf{E}_N(L(S)) > N - \frac{n}{q-1}.$$

If $v = 0$, we have

$$\mathbf{E}_N(L(S)) \geq \left(1 - \frac{1}{q}\right) N.$$

Proof: We have from (2.2)

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1}$$

Since $l_i \geq 1$, we have $q^{l_i} \geq q$ and $(1 - q^{-p^v l_i}) < 1$. Therefore,

$$\begin{aligned} \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} &< \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q-1} \\ &< \sum_{i=1}^{s} \frac{\Phi_i}{q-1}. \end{aligned}$$

Note that:

$$\sum_{i=1}^{s} \Phi_i = n. \tag{2.7}$$

Therefore,

$$\begin{aligned} \sum_{i=1}^{s} \frac{\Phi_i}{q-1} &= \frac{1}{q-1} \sum_{i=1}^{s} \Phi_i \\ &= \frac{n}{q-1}. \end{aligned}$$

Thus, the expected value of the linear complexity:

$$\begin{aligned}\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} \\ &> N - \frac{n}{q-1}.\end{aligned}$$

If $v = 0$, then we have $N = n$ and by (2.5),

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}}.$$

Since $l_i \geq 1$, we have $q^{l_i} \geq q$ and by (2.7), we obtain:

$$\begin{aligned}\sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \leq \sum_{i=1}^{s} \frac{\Phi_i}{q} &= \frac{1}{q} \sum_{i=1}^{s} \Phi_i \\ &= \frac{N}{q}.\end{aligned}$$

Finally,

$$\begin{aligned}\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \\ &\geq N - \frac{N}{q} = N\left(1 - \frac{1}{q}\right).\end{aligned}$$

□

Corollary 2.1.5. *Let S be a random N-periodic sequence with terms in $\mathbb{F}_2$. Hence $p = char\,(\mathbb{F}_2) = 2$ and $N = 2^v n$ where $gcd(2, n) = 1$. Then the lower bound for the expected value of the linear complexity of S will be:*

$$\mathbf{E}_N(L(S)) > N - \frac{n+2}{3}.$$

If $v = 0$, we have

$$\mathbf{E}_N(L(S)) \geq \frac{3N-1}{4}.$$

Proof: We have $q = 2$. Consider singleton cyclotomic coset $C_a = \{a\}$. By

(1.5) we have

$$\begin{aligned} 2a &= a \bmod n \\ 2a - a &= 0 \bmod n \\ a &= 0 \bmod n \end{aligned}$$

Thus, the only cyclotomic coset (relative to 2) with cardinality 1 is $C_0 = \{0\}$. The expected value of linear complexity of S is

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1}.$$

Without loss of generality suppose that $l_1 = 1$, then $\Phi_1 = 1$ and $l_i \geq 2$ for any $i \geq 2$ by the observation above. Since $(1 - q^{-p^v l_i}) < 1$ and $q = 2$, we get:

$$\begin{aligned} \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1} &< \sum_{i=1}^{s} \frac{\Phi_i}{2^{l_i} - 1} = \frac{\Phi_1}{2^{l_1} - 1} + \sum_{i=2}^{s} \frac{\Phi_i}{2^{l_i} - 1} \\ &\leq \frac{1}{2 - 1} + \sum_{i=2}^{s} \frac{\Phi_i}{2^2 - 1} \\ &= 1 + \sum_{i=2}^{s} \frac{\Phi_i}{3} = 1 + \frac{n - 1}{3} = \frac{n + 2}{3}. \end{aligned}$$

Therefore,

$$\mathbf{E}_N(L(S)) > N - \frac{n + 2}{3}.$$

If $v = 0$, that is $N = n$, by (2.5)

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \\
&= N - \frac{\Phi_1}{2^{l_1}} - \sum_{i=2}^{s} \frac{\Phi_i}{2^{l_i}} \\
&= N - \frac{1}{2} - \sum_{i=2}^{s} \frac{\Phi_i}{2^{l_i}} \\
&\geq N - \frac{1}{2} - \sum_{i=2}^{s} \frac{\Phi_i}{4} = N - \frac{1}{2} - \frac{N-1}{4} = \frac{3N-1}{4}.
\end{aligned}$$

Therefore,

$$\mathbf{E}_N(L(S)) \geq \frac{3N-1}{4}.$$

□

2.2 Cyclotomic Cosets Modulo Prime Powers

Up to here, the sequence S with terms in $\mathbb{F}_q$ is N-periodic such that $N = p^v n$ where $p = char\,(\mathbb{F}_q)$ and $\gcd(p, n) = 1$. Now $N = n^k$ where n is an odd prime different from p and $k \geq 1$ is an integer. Before determining the expected value of the linear complexity of a random sequence S, we have to consider the cyclotomic cosets modulo n^k, actually the number of the cyclotomic cosets modulo n^k.

We have n is an odd prime. Thus, $\mathbb{Z}_n^*$ is a prime field. Since n is different from p, then we can consider the multiplicative order of q in $\mathbb{Z}_n^*$. Let d be the multiplicative order of q in the prime field $\mathbb{Z}_n^*$, then

$$q^d \equiv 1 \bmod n.$$

Thus, we can say

$$q^d = 1 + cn^\rho \quad \rho \geq 1 \tag{2.8}$$

for some $c, \rho \in \mathbb{Z}$ with $\gcd(c, n) = 1$.

Lemma 2.2.1. *Let d be the multiplicative order of q in $\mathbb{Z}_n^*$ and $q^d = 1 + cn^\rho$ for some $\rho \geq 1$. Then d is also the multiplicative order of q in $\mathbb{Z}_{n^j}^*$ if and only if $j \leq \rho$.*

Proof: If d is the multiplicative order of q in $\mathbb{Z}_{n^j}^*$ then

$$q^d \equiv 1 \bmod n^j \quad \Leftrightarrow \quad n^j \mid q^d - 1 = cn^\rho \quad \Leftrightarrow \quad n^j \mid cn^\rho.$$

Since $\gcd(n, c) = 1$, we have

$$n^j \mid n^\rho \quad \Leftrightarrow \quad j \leq \rho.$$

□

Lemma 2.2.2. *Let n be a prime and a be a positive integer. Let α be the nonnegative integer such that $n^\alpha \parallel a!$. Then we have*

$$\alpha = \sum_{l=1}^{\infty} \left\lfloor \frac{a}{n^l} \right\rfloor$$

Proof: Recall that $a! = a(a-1)\ldots 2.1$. Among the integers in the set $S = \{1, 2, \ldots, a\}$, there are exactly $\left\lfloor \frac{a}{n} \right\rfloor$ integers $s \in S$ with $n \mid s$. Moreover for each $l \geq 1$, there are exactly $\left\lfloor \frac{a}{n^l} \right\rfloor$ integers $s \in S$ with $n^l \mid s$. Considering all of them we complete the proof.

□

Lemma 2.2.3. *Let n be a prime, $i \geq 1$ an integer and $2 \leq b \leq n^i$. Let j be the nonnegative integer such that $n^j \parallel b$. For each $1 \leq l \leq j$, we have*

$$\left\lfloor \frac{n^i}{n^l} \right\rfloor = \left\lfloor \frac{n^i - b}{n^l} \right\rfloor + \left\lfloor \frac{b}{n^l} \right\rfloor$$

and for each $j+1 \leq l \leq i$*, we have*

$$\left\lfloor \frac{n^i}{n^l} \right\rfloor = \left\lfloor \frac{n^i - b}{n^l} \right\rfloor + \left\lfloor \frac{b}{n^l} \right\rfloor + 1$$

Proof: Assume first $1 \leq l \leq j$, we have $b = n^l u$ for a positive integer u. Hence

$$\begin{aligned} \left\lfloor \frac{n^i}{n^l} \right\rfloor &= \frac{n^i}{n^l} \\ &= n^{i-l} \\ \left\lfloor \frac{n^i - b}{n^l} \right\rfloor &= \frac{n^i - b}{n^l} \\ &= n^{i-l} - u \\ &= \left\lfloor \frac{n^i}{n^l} \right\rfloor - \left\lfloor \frac{b}{n^l} \right\rfloor \\ \Rightarrow \left\lfloor \frac{n^i}{n^l} \right\rfloor &= \left\lfloor \frac{n^i - b}{n^l} \right\rfloor + \left\lfloor \frac{b}{n^l} \right\rfloor \end{aligned}$$

Hence it remains to consider the case $j+1 \leq l \leq i$. We have uniquely determined nonnegative integers u_0 and u_1 such that $b = n^l u_0 + u_1$. Moreover $1 \leq u_1 \leq n^l - 1$. Then

$$\begin{aligned} n^i - b &= n^l(n^{i-l} - u_0) - u_1 \\ &= n^l(n^{i-l} - u_0 - 1) + (n^l - u_1) \end{aligned}$$

Hence,

$$\left\lfloor \frac{n^i - b}{n^l} \right\rfloor = n^{i-l} - u_0 - 1$$

Since $\left\lfloor \frac{b}{n^l} \right\rfloor = u_0$, we have

$$\left\lfloor \frac{n^i}{n^l} \right\rfloor = \left\lfloor \frac{n^i - b}{n^l} \right\rfloor + \left\lfloor \frac{b}{n^l} \right\rfloor + 1.$$

This completes the proof.

□

Lemma 2.2.4. *Let n be a prime, $i \geq 1$ and $2 \leq b \leq n^i$. Let n be the nonnegative integer such that $n^\alpha \parallel \binom{n^i}{b}$. Then we have*

$$\alpha \geq i - b + 2$$

Proof: Note that

$$\binom{n^i}{b} = \frac{n^i!}{(n^i - b)!b!}.$$

Using Lemma 2.2.2, we obtain that

$$\alpha = \sum_{l=1}^{i} \left\{ \left\lfloor \frac{n^i}{n^l} \right\rfloor - \left\lfloor \frac{n^i - b}{n^l} \right\rfloor + \left\lfloor \frac{b}{n^l} \right\rfloor \right\}$$

Let j be the nonnegative integer such that $n^j \parallel b$. Using Lemma 2.2.3, we obtain that $\alpha = i - j$. As $n^j \parallel b$ and n is an odd prime, we have $b \geq \max(3^j, 2)$ and hence $b - j \geq \max(3^j, 2) - j$.
As $j \geq 0$, we also have $\max(3^j, 2) - j \geq 2$. Hence $b - j \geq 2$ and therefore $\alpha = i - j \geq i - b + 2$.

□

Proposition 2.2.5. *Let d be the multiplicative order of q in $\mathbb{Z}_n^*$, c and ρ be the integers defined in (2.8). For $i \geq 1$ we have*

$$q^{dn^i} \equiv 1 + n^i c n^\rho \bmod n^{i+\rho+1}. \tag{2.9}$$

Proof: Using (2.8), for $i \geq 1$, we have

$$q^{dn^i} = (1 + cn^\rho)^{n^i} = \sum_{b=0}^{n^i} \binom{n^i}{b} (cn^\rho)^b.$$

It is enough to prove that for each $2 \leq b \leq n^i$,

$$n^{i+\rho+1} \mid \binom{n^i}{b} (cn^\rho)^b$$

Using Lemma 2.2.4, we have $n^{i-b+2} \mid \binom{n^i}{b}$. As $\rho \geq 1$, we have $n^{b-1}n^{\rho} \mid (cn^{\rho})^b$. Therefore

$$n^{i+\rho+1} = n^{i-b+2}n^{b-1}n^{\rho} \mid \binom{n^i}{b}(cn^{\rho})^b.$$

□

In addition by (2.9), we can easily say that for all $i \geq 1$, we have

$$q^{dn^i} \equiv 1 \bmod n^{\rho+i}, \tag{2.10}$$

but

$$q^{dn^i} \neq 1 \bmod n^{\rho+i+1}.$$

Lemma 2.2.6. *Let δ_i be the multiplicative order of q in $\mathbb{Z}^*_{n^{\rho+i}}$. Then*

$$\delta_i \mid dn^i \quad \text{but} \quad \delta_i \nmid dn^{i-1}. \tag{2.11}$$

Proof: Since δ_i is the multiplicative order of q in $\mathbb{Z}^*_{n^{\rho+i}}$. Then

$$q^{\delta_i} \equiv 1 \bmod n^{\rho+i}.$$

By 2.10, $\delta_i \mid dn^i$. Suppose that $\delta_i \mid dn^{i-1}$, then $dn^{i-1} = k\delta_i$ for some $k \in \mathbb{Z}$. Thus,

$$q^{dn^{i-1}} \equiv \left(q^{\delta_i}\right)^k \equiv 1 \bmod n^{\rho+i}. \tag{2.12}$$

On the other hand, by (2.9)

$$q^{dn^{i-1}} = (1 + cn^{\rho})^{n^{i-1}} \equiv 1 + n^{i-1}cn^{\rho} \bmod n^{\rho+i}.$$

This implies that from (2.12)

$$n^{\rho+1} \mid n^{i-1}cn^{\rho} \quad \Rightarrow \quad n^i \mid n^{i-1}c \Rightarrow n \mid c.$$

But this is a contradiction since $\gcd(n, c) = 1$. Therefore, $\delta_i \nmid dn^{i-1}$.

□

Lemma 2.2.7. *Let d and δ_i be the multiplicative orders of q in $\mathbb{Z}_n^*$ and $\mathbb{Z}_{n^{\rho+i}}^*$ respectively, where $q^d = 1 + cn^\rho$ for some $\rho \geq 1$ and $gcd(c, n) = 1$. Then*

$$d \mid \delta_i. \tag{2.13}$$

Proof: If d is the multiplicative order of q in $\mathbb{Z}_n^*$, then we have

$$q^d = 1 + cn^\rho.$$

This implies that

$$q^d \equiv 1 \bmod n^\rho.$$

Moreover, if δ_i is the multiplicative order of $\mathbb{Z}_{n^{\rho+i}}^*$, then we have

$$q^{\delta_i} \equiv 1 \bmod n^{\rho+i}.$$

This implies that

$$n^{\rho+i} \mid q^{\delta_i} - 1 \quad \Rightarrow \quad n^\rho \mid q^{\delta_i} - 1 \quad \Rightarrow \quad q^{\delta_i} \equiv 1 \bmod n^\rho.$$

We know that d is the multiplicative order of q in $\mathbb{Z}_{n^\rho}^*$. Therefore, $d \mid \delta_i$.

□

Proposition 2.2.8. *Let d and δ_i be the multiplicative orders of q in $\mathbb{Z}_n^*$ and $\mathbb{Z}_{n^{\rho+i}}^*$ respectively, where $q^d = 1 + cn^\rho$ for some $\rho \geq 1$ and $gcd(c, n) = 1$. Then*

$$\delta_i = dn^i.$$

Proof: If d is the multiplicative order of q in $\mathbb{Z}_n^*$, then by (2.13), $d \mid \delta_i$. Thus, for some $a \in \mathbb{Z}$,

$$\delta_i = ad \quad \Rightarrow \quad \frac{\delta_i}{d} = a.$$

In addition, if δ_i is the multiplicative order of q in $\mathbb{Z}_{n^{\rho+i}}^*$, then by (2.13), $\delta_i \mid dn^i$

and $\delta_i \nmid dn^{i-1}$. This implies that

$$\frac{\delta_i}{d} \mid n^i \quad \Rightarrow \quad a \mid n^i$$

so $a = n^k$ for some $k \leq i$ and

$$\begin{aligned} \delta_i \nmid dn^{i-1} &\Rightarrow \frac{\delta_i}{d} \nmid dn^{i-1} \\ &\Rightarrow a \nmid n^{i-1} \\ &\Rightarrow n^k \nmid n^{i-1}. \end{aligned}$$

Thus, $k = i$ and

$$\begin{aligned} \frac{\delta_i}{d} &= a \\ &= n^i \\ \Rightarrow \delta_i &= dn^i. \end{aligned}$$

□

If we summarize, the multiplicative order of q in $\mathbb{Z}_{n^j}^*$ is d for $j \leq \rho$ and dn^i in $\mathbb{Z}_{n^{\rho+i}}^*$ for $i \geq 1$.

Now, we will determine the cardinalities of the cyclotomic cosets modulo n^k for:

- $k \leq \rho$
- $k = \rho + i$ where $i \geq 1$,

Consider the case $k \leq \rho$. Then the multiplicative order of q is d in $\mathbb{Z}_{n^k}^*$. We have

$$\mathbb{Z}_{n^k} = \left\{ b \mid b \equiv an^r \bmod n^k,\ \gcd(a, n) = 1,\ 0 \leq r \leq k-1,\ a \neq 0 \right\} \cup \{0\}.$$

Obviously, $C_0 = \{0\}$.

Lemma 2.2.9. *Let d be the multiplicative order of q in $\mathbb{Z}_{n^k}^*$ where $q^d = 1 + cn^\rho$ for some $\rho \geq 1$ and $gcd(c, n) = 1$. Suppose that $k \leq \rho$. Then the elements in the set*

$$\left\{b \mid b \equiv an^r \bmod n^k,\ \gcd(a, n) = 1,\ 0 \leq r \leq k-1,\ a \neq 0\right\}$$

that is, the nonzero elements of $\mathbb{Z}_{n^k}$, are separated into cyclotomic cosets modulo n^k (relative to q) with cardinality d.

Proof: For any $b \in \mathbb{Z}_{n^k}$, in a cyclotomic coset of b modulo n^k (relative to q), the elements have the form

$$bq^m \equiv an^r q^m \bmod n^k$$

for some m such that $1 \leq m \leq d$ and $an^r q^d \equiv an^r \bmod n^k$.
Claim: $an^r q,\ an^r q^2,\ an^r q^3, \ldots, an^r q^d$ are all distinct.
Proof of Claim: Suppose $an^r q^i \equiv an^r q^j \bmod n^k$ for some $i, j \leq d$. Then we have

$$aq^i \equiv aq^j \bmod n^{k-r}.$$

Since $\gcd(a, n)$=1,

$$q^i \equiv q^j \bmod n^{k-r}.$$

Since $\gcd(q, n) = 1$,

$$q^{i-j} \equiv 1 \bmod n^{k-r}.$$

since the multiplicative order of q is d in $\mathbb{Z}_{n^k}^*$ and $i - j < d$ then $i - j = 0$ which implies that $i = j$. Thus, $an^r q,\ an^r q^2,\ an^r q^3, \ldots, an^r q^d$ are all distinct.
Therefore, each cyclotomic coset modulo n^k (relative to q) had d elements where $k \leq \rho$.

□

Corollary 2.2.10. *Let d be the multiplicative order of q in $\mathbb{Z}_{n^k}^*$ where $q^d =$*

$1 + cn^\rho$ *for some* $\rho \geq 1$ *and* $gcd(c, n) = 1$. *Suppose that* $k \leq \rho$, *then there are*

$$\frac{n^k - 1}{d}$$

cyclotomic cosets modulo n^k *(relative to* q*) with cardinality* d.

Proof: Suppose $k \leq \rho$. Since there are $n^k - 1$ nonzero elements in $\mathbb{Z}_{n^k}$ we have

$$\frac{n^k - 1}{d}$$

different cyclotomic cosets.

□

Now, consider the case $k > \rho$, that is, $k = \rho + i$ for some $i \geq 1$. We know that the multiplicative order of q is dn^i in $\mathbb{Z}_{n^k}^*$. We have

$$\mathbb{Z}_{n^k} = \mathbb{Z}_{n^k}^* \cup \left\{ b \mid b \equiv an^r \bmod n^k,\ \gcd(a, n) = 1,\ 1 \leq r \leq k - 1 \right\} \cup \{0\}.$$

Obviously, $C_0 = \{0\}$.

Lemma 2.2.11. *Let* d *and* δ_i *be the multiplicative orders of* q *in* $\mathbb{Z}_n^*$ *and* $\mathbb{Z}_{n^{\rho+i}}^*$ *respectively, where* $q^d = 1 + cn^\rho$ *for some* $\rho \geq 1$ *and* $gcd(c, n) = 1$ *for* $k > \rho$. *Then the elements in* $\mathbb{Z}_{n^k}^*$ *split up into cyclotomic cosets with cardinality* $dn^{k-\rho}$.

Proof: If $k > \rho$, then $k = \rho + i$ for some $i \geq 1$. We know that the elements of the cyclotomic cosets of b mod n^k (relative to q) have the form

$$bq^m \bmod n^k$$

for some $m \geq 1$ and $b \in \mathbb{Z}_{n^k}^*$.
Claim 1: If $b \in \mathbb{Z}_{n^k}^*$, then $bq^m \in \mathbb{Z}_{n^k}^*$.
Proof of Claim 1: If $b \in \mathbb{Z}_{n^k}^*$, then $\gcd(b, n) = 1$ and since $\gcd(q, n) = 1$, we have $\gcd(bq^m, n) = 1$, which proves the claim.
Note that dn^i is the multiplicative order of q in $\mathbb{Z}_{n^k}^*$.
Claim 2: $bq,\ bq^2, \ldots, bq^{dn^i}$ are all distinct.

Proof of Claim 2: Suppose they are not distinct. Then for some $r, s \leq dn^i$

$$bq^r \equiv bq^s \bmod n^k.$$

Since $\gcd(b, n)$=1,

$$q^r \equiv q^s \bmod n^k.$$

Since $\gcd(q, n)$=1,

$$q^{r-s} \equiv 1 \bmod n^k.$$

where $r - s < dn^i$. As we know that the multiplicative order of q is dn^i in $\mathbb{Z}^*_{n^k}$ for $k > \rho$. Thus, $bq,\ bq^2, \ldots, bq^{dn^i}$ are all distinct.

Since

$$\begin{aligned} k &= \rho + i \\ \Rightarrow i &= k - \rho. \end{aligned}$$

Therefore, the cardinality of the cyclotomic cosets is $dn^i = dn^{k-\rho}$.

□

Lemma 2.2.12. *Let $q^d = 1 + cn^\rho$ for some $\rho \geq 1$ and $gcd(c, n) = 1$ and suppose $k > \rho$. Then for any element in*

$$K = \left\{ b \mid b \equiv an^r \bmod n^k,\ \gcd(a, n) = 1,\ 1 \leq r \leq k - 1 \right\},$$

belongs to a cyclotomic coset (relative to q) of cardinality t where

$$t = d \text{ if } k - r \leq \rho, \tag{2.14}$$

$$t = dn^j \text{ if } 1 \leq j \leq k - \rho. \tag{2.15}$$

Proof: If $k > \rho$ then $k = \rho + i$ for some $i \geq 1$. Let $b \equiv an^r \in K$. We know

that $\gcd(a,n)=1$ and $\gcd(q,n)=1$ implies that $\gcd(aq^m, n^r)=1$. Therefore,

$$\begin{aligned} bq^m &= an^r q^m \\ &= aq^m n^r \in K. \end{aligned}$$

Since a cyclotomic coset has t elements where the elements are $bq,\ bq^2, \ldots, bq^t$, t is the least positive integer satisfying,

$$bq^t \equiv b \bmod n^k.$$

Since $b \equiv an^r \bmod n^k$,

$$\begin{aligned} an^r &\equiv an^r q^t \bmod n^k \\ \Rightarrow aq^t &\equiv a \bmod n^{k-r}. \end{aligned}$$

Since $\gcd(a,n)$=1,

$$q^t \equiv 1 \bmod n^{k-r}.$$

That is t is the multiplicative order of q in $\mathbb{Z}_{n^{k-r}}$. Thus,

$$t = d \ \text{ if } \ k-r \leq \rho$$

and $\quad t = dn^j \ \text{ if } \ k-r > \rho$, that is $k-r = \rho + j$ for some $j \geq 1$, so $k-r-\rho = j$. Also we have

$$\begin{aligned} & 1 \leq r \leq k-1 \\ \Rightarrow\ & 1-k \leq -r \leq -1 \\ \Rightarrow\ & 1-\rho \leq k-r-\rho \leq k-1-\rho \\ \Rightarrow\ & 1-\rho \leq j \leq k-1-\rho. \end{aligned}$$

since we have $j \geq 1$, from both inequality we obtain $1 \leq j \leq k-1-\rho$. In addition, by Lemma 2.2.11 the elements in $\mathbb{Z}_{n^k}^*$ split up into cyclotomic cosets with cardinality $dn^{k-\rho}$. Therefore, we can say that $t = dn^j$ for $1 \leq j \leq k-\rho$.

□

Corollary 2.2.13. *Let $k > \rho$, then the elements of the set*

$$K = \left\{ b \mid b \equiv an^r \bmod n^k,\ \gcd(a,n) = 1,\ 1 \le r \le k-1 \right\}$$

split up into

$$\frac{n^\rho - 1}{d}$$

cyclotomic coset with cardinality d.

Proof: By Lemma 2.2.11, the cardinality of the cyclotomic cosets is $t = d$, if $k - r \le \rho \ \Rightarrow k - \rho \le r$. We have also $r \le k-1$. Thus, there are totally

$$\sum_{r=k-\rho}^{k-1} \left(n^{k-r} - n^{k-r-1} \right)$$

elements which are relatively prime to n^{k-r} and splitting up into all cyclotomic cosets with cardinality d. Since $k - \rho \le r \le k-1$ then $1 - k \le -r \le \rho - k$. If we change the variables

$$\sum_{r=1-k}^{\rho-k} \left(n^{k+r} - n^{k+r-1} \right) = \sum_{r=0}^{\rho-1} \left(n^{k+r-k+1} - n^{k+r-k+1-1} \right)$$

$$= \sum_{r=0}^{\rho-1} \left(n^{r+1} - n^r \right)$$

$$= (n-1) \sum_{r=0}^{\rho-1} n^r$$

$$= (n-1)\, \frac{n^\rho - 1}{n-1}$$

$$= n^\rho - 1\ .$$

Since the cardinalities of the cyclotomic cosets are d then there are

$$\frac{n^\rho - 1}{d}$$

cyclotomic cosets.

□

Corollary 2.2.14. *Let $k > \rho$, then there are*

$$\frac{n^{\rho-1}(n-1)}{d}$$

cyclotomic coset with cardinality dn^j where $1 \leq j \leq k-\rho$.

Proof: By (2.15) $t = dn^j$ is the cardinality of the cyclotomic cosets mod n^k (relative to q) where $1 \leq j \leq k-\rho$. The elements of the cyclotomic cosets having cardinality dn^j are elements which are relatively prime to $n^{\rho+j}$ and the number of these elements is $n^{\rho+j} - n^{\rho+j-1}$. Therefore, there are

$$\frac{n^{\rho+j} - n^{\rho+j-1}}{dn^j} = \frac{n^{\rho-1}n^j(n-1)}{dn^j} = \frac{n^{\rho-1}(n-1)}{d}$$

different cyclotomic cosets with cardinality dn^j.

□

Theorem 2.2.15. *Let S be a random N-periodic sequence with terms in $\mathbb{F}_q$, where $N = n^k$ where n is an odd prime different from $p = char(\mathbb{F}_q)$. If d is the multiplicative order of q in $\mathbb{F}_n$ and $q^d = 1 + cn^\rho$ for some positive integers ρ, c with $gcd(n, c) = 1$. Then we have*

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q} - (n^\sigma - 1)\frac{1}{q^d} - (n-1)n^{\sigma-1}\sum_{j=1}^{k-\sigma}\frac{n^j}{q^{dn^j}} \tag{2.16}$$

where $\sigma = min(k, \rho)$.

Proof: If $N = n^k$ then $\gcd(p, N) = 1$, by Corollary 2.1.2, we have

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s}\frac{\Phi_i}{q^{l_i}}.$$

Case 1: $k \leq \rho$. $C_0 = \{0\}$ is the only cyclotomic coset mod n^k with cardinality

1. Thus,

$$\begin{aligned} \Phi_1 &= 1 \\ l_1 &= 1. \end{aligned}$$

The other cyclotomic cosets mod n^k, with non-zero elements, have cardinality d by Lemma 2.2.8 and since there are $n^k - 1$ non-zero elements we have

$$\begin{aligned} \Phi_2 &= n^k - 1 \\ l_2 &= d. \end{aligned}$$

Case 2: $k > \rho$. $C_0 = \{0\}$ is the only cyclotomic coset mod n^k with cardinality 1. Thus,

$$\begin{aligned} \Phi_1 &= 1 \\ l_1 &= 1. \end{aligned}$$

There are $n^\rho - 1$ elements in the cyclotomic cosets mod n^k with cardinality d by Corollary 2.2.12. So we have,

$$\begin{aligned} \Phi_2 &= n^\rho - 1 \\ l_2 &= d. \end{aligned}$$

Finally, there are $n^{\rho+j-1}(n-1)$ elements in the cyclotomic cosets mod n^k with cardinality dn^j where $1 \leq j \leq k - \rho$, by Corollary 2.2.14. So we have,

$$\begin{aligned} \Phi_3 &= n^{\rho+j-1}(n-1) \\ l_3 &= dn^j. \end{aligned}$$

Therefore, if $k \leq \rho$, we have:

$$\begin{aligned} \mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \\ &= N - \frac{\Phi_1}{q^{l_1}} - \frac{\Phi_2}{q^{l_2}} \\ &= N - \frac{1}{q} - \frac{n^k - 1}{q^d}, \end{aligned} \tag{2.17}$$

and for the second case if $k > \rho$, we have:

$$\begin{aligned} \mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \\ &= N - \frac{\Phi_1}{q^{l_1}} - \frac{\Phi_2}{q^{l_2}} - \sum_{j=1}^{k-\rho} \frac{\Phi_j}{q^{l_j}} \\ &= N - \frac{1}{q} - \frac{n^\rho - 1}{q^d} - \sum_{j=1}^{k-\rho} \frac{n^{\rho+j-1}(n-1)}{q^{dn^j}}. \end{aligned} \tag{2.18}$$

To combine (2.17) and (2.18) if we take $\sigma = \min(\rho, k)$ then we get

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q} - (n^\sigma - 1)\frac{1}{q^d} - (n-1)n^{\sigma-1} \sum_{j=1}^{k-\sigma} \frac{n^j}{q^{dn^j}}.$$

□

Corollary 2.2.16. *Let $\rho = 1$, then the expected value of the linear complexity is*

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q} - (n-1) \sum_{j=0}^{k-1} \frac{n^j}{q^{dn^j}}. \tag{2.19}$$

Proof: If $\rho = 1$ then $\sigma = \min(\rho, k) = 1$. Therefore,

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \frac{1}{q} - (n^\sigma - 1)\frac{1}{q^d} - (n-1)n^{\sigma-1}\sum_{j=1}^{k-\sigma}\frac{n^j}{q^{dn^j}} \\
&= N - \frac{1}{q} - \frac{n-1}{q^d} - (n-1)\sum_{j=1}^{k-1}\frac{n^j}{q^{dn^j}} \\
&= N - \frac{1}{q} - \frac{(n-1)n^0}{q^{dn^0}} - (n-1)\sum_{j=1}^{k-1}\frac{n^j}{q^{dn^j}} \\
&= N - \frac{1}{q} - \sum_{j=0}^{k-1}\frac{n^j}{q^{dn^j}}
\end{aligned}$$

□

Corollary 2.2.17. *Let $k = 1$, then the expected value of the linear complexity is*

$$\mathbf{E}_N(L(S)) = (N-1)\left(1 - \frac{1}{q^d}\right) + \frac{q-1}{q} \tag{2.20}$$

Proof: If $k = 1$ then $N = n^k = n$ and $\sigma = \min(\rho, k) = 1$. Therefore,

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \frac{1}{q} - (n^\sigma - 1)\frac{1}{q^d} - (n-1)n^{\sigma-1}\sum_{j=1}^{k-\sigma}\frac{n^j}{q^{dn^j}} \\
&= N - \frac{1}{q} - (n-1)\frac{1}{q^d} - (n-1)n^{1-1}\underbrace{\sum_{j=1}^{1-1}\frac{n^j}{q^{dn^j}}}_{0} \\
&= N - \frac{1}{q} - \frac{n-1}{q^d} \\
&= N - \frac{1}{q} - \frac{N-1}{q^d} \\
&= N - \frac{1}{q} - \frac{N}{q^d} + \frac{1}{q^d} \\
&= N\left(1 - \frac{1}{q^d}\right) + \frac{1}{q^d} + 1 - 1 - \frac{1}{q} \\
&= N\left(1 - \frac{1}{q^d}\right) - \left(1 - \frac{1}{q^d}\right) + 1 - \frac{1}{q} \\
&= (N-1)\left(1 - \frac{1}{q^d}\right) + \frac{q-1}{q}.
\end{aligned}$$

□

2.3 Counting the Number of Periodic Sequences With Given Linear Complexity

For an N-periodic sequence S with terms in $\mathbb{F}_q$, where $p = char\,(\mathbb{F}_q)$ and $N = n^k$ such that n is an odd prime different from p, the GDFT of this sequence is an N-tuple DFT. If d is the multiplicative order of q in $\mathbb{Z}_n$ and $q^d = 1 + cn$, such that $\gcd(c, n) = 1$, then the linear complexity of S is the linear combination of the cardinalities of different cyclotomic cosets modulo n^k (relative to q). Therefore, by (1.9), we have

$$L(S) = a_0 + \sum_{i=1}^{k} a_i dn^{i-1} \qquad . \tag{2.21}$$

In this equation, $a_0 \in \{0, 1\}$ represents the contribution of the singleton coset $C_0 = \{0\}$ to the Günther Weight which is the Hamming Weight of N-tuple DFT. The coefficients, a_i, are to denote the number of different cyclotomic cosets with cardinality dn^{i-1}. Here we have $q^d = 1 + cn$, so the power of n, which we denote it by ρ in the previous sections, is equal to 1. By Corollary 2.2.14, since $\rho = 1$, we have $\frac{n-1}{d}$ cyclotomic cosets with cardinality dn^{i-1} where $i = 1, \ldots, k$. Therefore, the coefficients $1 \leq a_i \leq \frac{n-1}{d}$.

So, we can choose a_i different cosets with cardinality dn^{i-1} in $\binom{n-1/d}{a_i}$ ways. In the N-tuple DFT, the entry in the column that corresponds to the cyclotomic cosets with cardinality dn^{i-1} is an element of $\mathbb{F}_{q^{dn^{i-1}}}$. If this entry contributes the Hamming weight, we have $q^{dn^{i-1}} - 1$ choices for a_i places. So there are

$$\binom{n-1/d}{a_i} \left(q^{dn^{i-1}} - 1\right)^{a_i}$$

choices. for $i \geq 1$. For $i = 0$, the entry that corresponds to the singleton coset C_0 is an element of $\mathbb{F}_q$. So there are $(q-1)^{a_0}$ possibilities. Then the number of

sequences with the linear complexity $L(S)$, $\mathcal{N}_N(L(S))$ is given by:

$$\mathcal{N}_N(L(S)) = (q-1)^{a_0} \prod_{i=1}^{k} \binom{n-1/d}{a_i} \left(q^{dn^{i-1}} - 1\right)^{a_i}$$

Remark 2.3.1. If N is an odd prime different from p, that is $N = n$, then the linear complexity can be written as $L(S) = a_0 + a_1 d$ where $a_0 \in \{0, 1\}$ and $0 \leq a_1 \leq \frac{N-1}{d}$ and the number of sequences with linear complexity $L(S)$ is

$$\mathcal{N}_N(L(S)) = (q-1)^{a_0} \binom{n-1/d}{a_1} \left(q^d - 1\right)^{a_1}$$

Lemma 2.3.2. *Let $q = 2$, $N = 2^n - 1$, where n is a prime. If the multiplicative order of $q = 2$ in $\mathbb{Z}_N^*$ is d, then $n = d$.*

Proof:

$$\begin{aligned} N = 2^n - 1 &\Leftrightarrow 2^n - 1 \equiv 0 \bmod N \\ &\Leftrightarrow 2^n \equiv 1 \bmod N. \end{aligned}$$

Since d is the multiplicative order of 2 in $\mathbb{Z}_N^*$ then $d \mid n$. On the other hand $2^d = 1 + bN^r$ for some $r > 0$ and $b \in \mathbb{Z}$ where $gcd(b, N) = 1$

$$\begin{aligned} 2^d = 1 + bN^r &\Leftrightarrow 2^d - 1 = bN^r \\ &\Leftrightarrow N = 2^n - 1 \mid bN^r = 2^d - 1 \\ &\Leftrightarrow 2^n - 1 \mid 2^d - 1 \\ &\Rightarrow n \leq d. \end{aligned}$$

Since we have $d \mid n$ and $n \leq d$, $n = d$.

□

In the case that $q = 2$, $N = 2^n - 1$, where n is a prime, the cardinality of any cyclotomic coset modulo N has to divide n, since the multiplicative order of 2 is n Since n is prime, there are only cyclotomic cosets with cardinality 1 and n.

The cyclotomic coset with cardinality 1 is $C_0 = \{0\}$. $N-1$ elements different from 0 in $\mathbb{Z}_N$ split up into $\frac{N-1}{n}$ cyclotomic cosets with cardinality n.

Theorem 2.3.3. *Suppose $q = 2$ and $N = 2^n - 1$, where n is a prime. If $L(S) = a_0 + a_1 n$, then*

$$\mathcal{N}_N(a_0 + a_1 n) = \binom{N-1/n}{a_1} N^{a_1} \text{ where } a_0 \in \{0,1\} \text{ and } 0 \leq a_1 \leq (N-1)/n$$

and

$$\mathbf{E}_N(L(S)) = (N-1)\left(1 - \frac{1}{2^n}\right) + \frac{1}{2}.$$

Proof: We have $n = d$ by Lemma 2.3.2. And we have $L(S) = a_0 + a_1 n$.

There is 1 cyclotomic coset with cardinality 1, which is $C_0 = 0$. The entry of the DFT that corresponds to this cyclotomic coset is an element of $\mathbb{F}_2$. So there are $(2-1)^{a_0} = 1$ way to choose this entry.
There are $\frac{N-1}{n}$ different cyclotomic cosets with cardinality $n = d$ and a_1 denotes the number of cyclotomic cosets that contributes to the Günther weight. We can choose these cyclotomic cosets in $\binom{(N-1)/n}{a_1}$ ways and the entries that correspond to these cyclotomic cosets can be chosen in $(2^n-1)^{a_i} = N^{a_i}$ ways. So the number of sequences having the linear complexity $L(S)$ is

$$\mathcal{N}_N(c) = \binom{N-1/d}{a_1} N^{a_1}$$

There are $\frac{N-1}{n}$ cyclotomic cosets modulo N with cardinality n and one singleton coset. Hence we have by Corollary 2.1.2,

$$\begin{aligned}
\mathbf{E}_N(L(S)) &= N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}} \\
&= N - \frac{1}{2} - \frac{N-1}{2^n} \\
&= N - 1 + 1 - \frac{1}{2} - \frac{N-1}{2^n} \\
&= (N-1)(1 - \frac{1}{2^n}) + \frac{1}{2}
\end{aligned}$$

□

Remark 2.3.4. If $N = p^v n$ and n is a prime different from p, then $\mathbb{Z}_n^*$ has $n-1$ elements and $\frac{n-1}{d}$ different cyclotomic cosets modulo n with cardinality d.

Theorem 2.3.5. *Let S be an N-periodic sequence with terms in $\mathbb{F}_q$ where $N = p^v n$, $p = char(\mathbb{F}_q)$, and let n be a prime different from p. If d is the multiplicative order of q in the prime field $\mathbb{F}_n$. Then*

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q-1}\left(1 - \frac{1}{q^{p^n}}\right) - \frac{n-1}{q^d-1}\left(1 - \frac{1}{q^{dp^v}}\right) \tag{2.22}$$

Proof: We know that,

$$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i \cdot \left(1 - q^{-p^v l_i}\right)}{q^{l_i} - 1}$$

Since $C_0 = \{0\}$ is the only singleton coset, without loss of generality $l_1 = 1$, $\Phi_1 = 1$, the other $\frac{n-1}{d}$ cosets have cardinality d. Thus, $l_2 = d$ and $\Phi_2 = n - 1$. Therefore,

$$\mathbf{E}_N(L(S)) = N - \frac{1}{q-1}\left(1 - \frac{1}{q^{-p^v}}\right) - \frac{(n-1)\left(1 - q^{-p^v d}\right)}{q^d - 1}$$

□

S is an N-periodic sequence with terms in $\mathbb{F}_q$, where $N = p^v n$ and n is a prime different from p. Suppose that the Günther weight of The GDFT(S^N), which is equal to the linear complexity of the sequence N is $L(S) = rd + s$. Then we have for this matrix:
$0 \leq s \leq p^v$: s is counting the entries in the column which corresponds to $C_0 = \{0\}$ and contributes the Günther Weight.
$0 \leq r \leq p^v \frac{n-1}{d}$: r is counting the entries in the columns which correspond to the cyclotomic cosets with cardinality d and contributes to the Günther Weight.

Proposition 2.3.6. *Let $N = p^v n$ and n be a prime. If q is a primitive element*

of the finite field $\mathbb{F}_n$ *and* $p^v < n-1$ *then*

$$\begin{aligned}
\mathcal{N}_N\left(r(n-1)\right) &= \left(q^{n-1}-1\right)q^{(n-1)(r-1)} \quad 1 \le r \le p^v \\
\mathcal{N}_N(0) &= 1 \\
\mathcal{N}_N(r(n-1)+s) &= (q-1)q^{s-1}\mathcal{N}_N(r(n-1)) \quad 0 \le r \le p^v 1 \le s \le p^v.
\end{aligned}$$

Proof: If q is a primitive element of $\mathbb{F}_n$, then the multiplicative order of q is $n-1$. Therefore the only cyclotomic cosets are $C_0 = \{0\}$ and $C_1 = \mathbb{F}_n \setminus \{0\}$. Then

$$\begin{aligned}
L(S) &= \sum_{i=1}^{h} w_i l_{j_i} \qquad 0 \le w_i \le p^v \\
&= r(n-1)+s \quad 0 \le r \le p^v \text{ and } 0 \le s \le p^v.
\end{aligned}$$

Since $p^v < n-1$ then $r < n-1$ and $s < n-1$, so the representation of the linear complexity is unique. Recall that s is the number of entries of the column that corresponds to the cyclotomic coset $C_0 = \{0\}$ and r is the number of nonzero entries of the column that corresponds to the cyclotomic coset having the cardinality $n-1$.

If $c = r(n-1)$ that is the entries of the column that corresponds to the cyclotomic coset $C_0 = \{0\}$ are zero. For the other column where the entries are elements of $\mathbb{F}_{q^{n-1}}$ to have the Günther Weight as $r(n-1)$ we have $q^{n-1}-1$ choices for the first nonzero entry. For any entry below the first nonzero entry there are q^{n-1} choices. Since there are $r-1$ entry for the rest we have $(q^{n-1})^{r-1}$ choices. so there are $(q^{n-1}-1)(q^{n-1})^{r-1}$ matrices having the Günther Weight as $r(n-1)$. Therefore,

$$\mathcal{N}_N\left(r(n-1)\right) = \left(q^{n-1}-1\right)q^{(n-1)(r-1)}.$$

If $c = 0$, since there is one zero matrix we have

$$\mathcal{N}_N(0) = 1.$$

If $L(S) = r(n-1) + s$, we have $\mathcal{N}_N\left(r(n-1)\right)$ choices for the entries of the column that corresponds to the cyclotomic coset having the cardinality $n-1$. Of the column, where the entries are elements of $\mathbb{F}_q$, that corresponds to the cyclotomic coset $C_0 = \{0\}$, we have $q-1$ choices for the first nonzero entry. Since below this entry there are $s-1$ entries, we have q^{s-1} choices. Thus, there are $(q-1)q^{s-1}\mathcal{N}_N\left(r(n-1)\right)$ different matrices having the Günther Weight as $r(n-1)+s$. Therefore,

$$\mathcal{N}_N(r(n-1)+s) = (q-1)q^{s-1}\mathcal{N}_N(r(n-1))$$

□

PERIOD(N)	**EXPECTED VALUE**
$N = p^v n^k$	$\mathbf{E}_N(L(S)) = \sum_{S \in \mathbb{F}_q^N} \mathbf{p}(S) L(S)$
$N = p^v n$	$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i \cdot (1 - q^{-p^v l_i})}{q^{l_i} - 1}$
$N = p^v n$	$\mathbf{E}_N(L(S)) > N - \frac{n}{q-1}$
$N = 2^v n,\ p = 2$	$\mathbf{E}_N(L(S)) > N - \frac{n+2}{3}$
$N = n$	$\mathbf{E}_N(L(S)) = N - \sum_{i=1}^{s} \frac{\Phi_i}{q^{l_i}}$
$N = n$	$\mathbf{E}_N(L(S)) \geq \left(1 - \frac{1}{q}\right) N$
$N = n,\ p = 2$	$\mathbf{E}_N(L(S)) \geq \frac{3N-1}{4}$
$N = p^v$	$\mathbf{E}_N(L(S)) = N - \frac{1}{q-1}\left(1 - \frac{1}{q^N}\right)$
$N = n^k$ n: prime $q^d = 1 + cn^\rho$ $n \neq p$ $\sigma = \min(k, \rho)$	$\mathbf{E}_N(L(S)) = N - \frac{1}{q} - (n^\sigma - 1)\frac{1}{q^d} - (n-1)n^{\sigma-1} \sum_{j=1}^{k-\sigma} \frac{n^j}{q^{dn^j}}$
$N = 2^n - 1$ n: prime $p = 2$	$\mathbf{E}_N(L(S)) = (N-1)\left(1 - \frac{1}{2^d}\right) + \frac{1}{2}$
$N = p^v n$ n: prime $n \neq p$	$\mathbf{E}_N(L(S)) = N - \frac{1}{q-1}\left(1 - \frac{1}{q^{p^v}}\right) - \frac{n-1}{q^d-1}\left(1 - \frac{1}{q^{dp^v}}\right)$

Table 2.1: The Expected Value of Linear Complexity for Different Cases of the Period

References

[1] W. Meidl and H. Niederreiter, *On The Expected Value Of The Linear Complexity And The k-Error Linear Complexity of Periodic Sequences*, IEEE Trans. Inform. Theory, vol. 48 pp. 2817-2825, November 2002.

[2] James L. Massey and Shilei Serconek, *Linear Complexity of Periodic Sequences: A General Theory*,in Advances in Cryptology CRYPTO'96 (Lecture Notes in Computer Science), N. Koblitz, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1109, pp.358-371