Southern Illinois University Carbondale
**OpenSIUC**

Research Papers Graduate School

Fall 10-13-2010

# The Number of Zeros in a Linear Recurrence Sequence Over a Finite Field

Suwanda Hennedige Y. Kottegoda
*Southern Illinois university - Carbondale*, yasanthi_k@yahoo.com

# THE NUMBER OF ZEROS IN A LINEAR RECURRENCE SEQUENCE OVER A FINITE FIELD

by

Yasanthi Kottegoda

B.S., University of Colombo, Sri Lanka, 2007

A Research Report
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

Department of Mathematics
in the Graduate School
Southern Illinois University Carbondale
December, 2010

**RESEARCH REPORT APPROVAL**

THE NUMBER OF ZEROS IN A LINEAR RECCURENCE SEQUENCE OVER

A FINITE FIELD

By

Yasanthi Kottegoda

A Research Report Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Mathematics

Approved by:

Dr. R. Fitzgerald, Chair

Dr. G. Budzban

Dr. J. Yucas

Graduate School
Southern Illinois University Carbondale
13th October 2010.

**AN ABSTRACT OF THE RESEARCH PAPER OF**

YASANTHI KOTTEGODA, for the Master of Science degree in MATHEMATICS, presented on 13th October 2010, at Southern Illinois University Carbondale.

TITLE: THE NUMBER OF ZEROS IN A LINEAR RECURRENCE SEQUENCE OVER A FINITE FIELD

MAJOR PROFESSOR: Dr. Robert Fitzgerald

This paper provides basic results of finite field theory which describe the structure of finite fields, trace function, characters and Gaussian sums in order to determine the bounds on the number of zeros in a linear recurrence sequence of irreducible polynomial of given degree and order.

## TABLE OF CONTENTS

## LIST OF TABLES

# INTRODUCTION

This paper provides a basic treatment of finite field theory in order to determine the bounds on the number of zeros in a linear recurrence sequence of irreducible polynomial of given degree and order. The method discussed here is based on Gaussian sums which leads to better estimates of the bounds.

Chapter 1 deals with the basic concepts of finite field theory such as the structure of finite fields, *the trace function*, characters and Gaussian sums. Also some of the most important theorems regarding those topics and the proofs of most of the theorems are presented here.

Chapter 2 which is the most important section, describes the linear recurrence sequence in a finite field and some of its characteristics. Out of the basic theorems which involves the linear recurring sequences discussed here, the most important theorem is the one which determines the bounds on the number of zeros in a sequence of irreducible polynomial of given degree and order. This method is based on Gaussian sums and the basic results of finite field theory which are explained in the first chapter is heavily used here.

Chapter 3 provides results obtained by a MAPLE program written in order to determine the number of zeros in sequences induced by irreducible polynomials over the finite field of order 2, of degree 8 and order 85, degree 9 and order 73, degree 10 and order 93 under certain initial values.

# CHAPTER 1

# BASIC RESULTS OF FINITE FIELDS

## 1.1 STRUCTURE OF FINITE FIELDS

This chapter is adapted from [2].

**Lemma 1.1.1.** *Let $F$ be a finite field containing a subfield $K$ with $q$ elements. Then $F$ has $q^m$ elements, where $m = [F : K]$.*

*Proof.* $F$ is a vector space over $K$. Since $F$ is finite, it is finite-dimensional as a vector space over $K$. Let $[F : K] = m$. Then F has a basis say, $\{b_1, b_2, \ldots, b_m\}$ over $K$ which consists of $m$ elements. Then every element $b$ can be expressed in the form,

$$b = a_1b_1 + a_2b_2 + \ldots + a_mb_m \text{ where } a_1, a_2, \ldots, a_m \in K.$$

Since $K$ has $q$ elements, each $a_i$ can take $q$ values. So $F$ has exactly $q^m$ elements. □

**Lemma 1.1.2.** *If $F$ is a finite field with $q$ elements, then every $a \in F$ satisfies $a^q = a$.*

*Proof.* When $a = 0$, it is trivial that $a^q = a$. When $a \neq 0$, the nonzero elements in $F$ form a group of order $q - 1$ under multiplication. Then $a^{q-1} = 1$ for every $a \in F \setminus \{0\}$. If multiplied both sides by $a$ this will give the result. □

**Theorem 1.1.3.** *(Subfield Criterion) Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has an order $p^m$, where $m$ is a positive divisor of $n$. Conversely, if $m$ is a positive divisor of $n$, then there is exactly one subfield of $\mathbb{F}_q$ with $p^m$ elements.(Note that $p$ is a prime.)*

As a result of this theorem, it can be concluded that the finite field, $\mathbb{F}_q$ is a subfield of the finite field, $\mathbb{F}_{q^n}$ and from Lemma 1.1.1, $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

**Lemma 1.1.4.** *Let $f \in F[x]$ be an irreducible polynomial of degree $m$, over $\mathbb{F}_q$. Then if $f(x)$ divides $x^{q^n} - x$ then $m$ divides $n$.*

*Proof.* Suppose $f(x)$ divides $x^{q^n} - x$. Let $\alpha$ be a root of $f$ in the splitting field of $f$ over $\mathbb{F}_q$. Then $\alpha$ is a root of $x^{q^n} - x$ which implies $\alpha^{q^n} = \alpha$, so that $\alpha \in \mathbb{F}_{q^n}$. Therefore $\mathbb{F}_q(\alpha)$is a subfield of $\mathbb{F}_{q^n}$. Since $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$,

$$[\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q]$$

$$\Rightarrow n = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]m$$

$\Rightarrow m$ divides $n$. □

**Theorem 1.1.5.** *If $f$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree $m$, then $f$ has a root $\alpha$ in $\mathbb{F}_{q^m}$. Also, all the roots of $f$ are simple and given by the $m$ distinct elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.*

*Proof.* Let $\alpha$ be a root of $f$ in the splitting field of $f$ over $\mathbb{F}_q$. Since the degree of $f$ is $m$, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Also $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$. Then by Lemma 1.1.1, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. So $\alpha \in \mathbb{F}_{q^m}$. Now we will show that if $\beta \in \mathbb{F}_{q^m}$ is a root of $f$ then so is $\beta^q$. Let $f(x) = a_m x^m + \ldots + a_1 x + a_0$ where $a_i \in \mathbb{F}_q$ for $0 \leq i \leq m$. Then

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \ldots + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + \ldots + a_1^q \beta^q + a_0^q \qquad \text{(By Lemma 1.1.2)} \\ &= (a_m \beta^m + \ldots + a_1 \beta + a_0)^q \\ &= f(\beta)^q \\ &= 0 \end{aligned}$$

So $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are roots of $f$. Now we have to show that these elements are distinct. Let's assume that it is not so. That is, there exist some integers $j, k$ where

$0 \leq j \leq k \leq m-1$ such that $\alpha^{q^i} = \alpha^{q^k}$. This implies that $\left(\alpha^{q^i}\right)^{q^{m-k}} = \left(\alpha^{q^k}\right)^{q^{m-k}}$. Then $\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$. Therefore $\alpha$ is a root of the polynomial $x^{q^{m-k+j}} = x$. Since $f(x)$ is the minimal polynomial of $\alpha$, $f(x)$ divides $x^{q^{m-k+j}} = x$. Then by Lemma 1.1.4, $m$ divides $m-k+j$. But $0 < m-k+j < m$ which gives a contradiction. Hence $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are distinct. □

**Definition.** Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the *conjugates* of $\alpha$ with respect to $\mathbb{F}_q$.

**Remark.** The conjugates of $\alpha \in \mathbb{F}_{q^m}$ are distinct if and only if the minimal polynomial of $\alpha$ over $\mathbb{F}_q$ has degree $m$ (by Theorem 1.1.5). Otherwise the degree $d$ of the polynomial is a proper divisor of $m$. Then the conjugates of $\alpha$ with respect to $\mathbb{F}_q$ are the distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, each repeated $m/d$ times.

## 1.2 TRACE FUNCTION

Let us consider that the field $F$ is a finite extension of the field $K$ where $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Then $F$ has a dimension $m$ over $K$.

**Definition.** Let $\alpha \in F$. The *trace* $\mathrm{Tr}_{F/K}(\alpha)$ of $\alpha$ 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 the *absolute trace* of $\alpha$ and it is denoted by $\mathrm{Tr}_F(\alpha)$.

**Remark.** The trace of $\alpha$ over $K$ is the sum of the conjugates of $\alpha$ with respect to $K$.

**Theorem 1.2.1.** *The trace of $\alpha$ over $K$ is an element of $K$.*

*Proof.* Let $f \in K[x]$ be the minimal polynomial of $\alpha$ over $K$ where its degree is $d$. Since $K \subseteq K(\alpha) \subseteq F$, and since $[F : K] = m$, $d$ is a divisor of $m$. Then

$g(x) = f(x)^{m/d} \in K[x]$, which is of degree $m$ is called the *characteristic polynomial* of $\alpha$ over $K$. Then by Theorem 1.1.5, the roots of $f$ in $F$ are given by $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$. Then (by the remark given below the definition of conjugates), the roots of $g$ in $F$ are the conjugates of $\alpha$ with respect to $K$. Therefore

$$g(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0 \tag{1.1}$$

$$= (x-\alpha)(x-\alpha^q)\dots(x-\alpha^{q^{m-1}}) \tag{1.2}$$

By comparing the coefficients of $x^{m-1}$ in (1.1) and (1.2) gives that

$$\mathrm{Tr}_{F/K}(\alpha) = -a_{m-1} \in K \qquad \text{(Since } g(x) \in K[x]\text{)}.$$

$\square$

**Theorem 1.2.2.** *Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then the trace function $Tr_{F/K}$ satisfies the following properties:*

*(a) $Tr_{F/K}(\alpha+\beta)=Tr_{F/K}(\alpha)+Tr_{F/K}(\beta)$ for all $\alpha, \beta \in F$;*

*(b) $Tr_{F/K}(c\alpha) = c\,Tr_{F/K}(\alpha)$ for all $c \in K$, $\alpha \in F$;*

*(c) $Tr_{F/K}$ is a linear transformation from $F$ onto $K$, where both $F$ and $K$ are viewed as vector spaces over $K$;*

*(d) $Tr_{F/K}(a) = ma$ for all $a \in K$;*

*(e) $Tr_{F/K}(\alpha^q)=Tr_{F/K}(\alpha)$ for all $\alpha \in F$.*

*Proof.* *(a)* Let $\alpha, \beta \in F$. Then,

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q + \dots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\dots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= \alpha+\dots+\alpha^{q^{m-1}}+\beta+\dots+\beta^{q^{m-1}} \\ &= \mathrm{Tr}_{F/K}(\alpha)+\mathrm{Tr}_{F/K}(\beta).\end{aligned}$$

*(b)* Let $c \in K$. By Lemma 1.1.2, $c^{q^r} = c$ for every $r \geq 0$. Therfore for any $\alpha \in F$,

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

*(c)* By the properties *(a)* and *(b)* and by Theorem 1.2.1, it can be concluded that $\mathrm{Tr}_{F/K}(\alpha)$ is a linear transformation from $F$ into $K$. To prove that this mapping is onto, we will prove that there exist an $\alpha \in F$ such that $\mathrm{Tr}_{F/K}(\alpha) \neq 0$.

[If we can prove this existence of $\alpha \in F$, then $\mathrm{Tr}_{F/K}(\alpha) = c \neq 0$. Then for any $k \in K$,

$$\begin{aligned}\mathrm{Tr}_{F/K}\left(kc^{-1}\alpha\right) &= kc^{-1}\mathrm{Tr}_{F/K}(\alpha) \qquad \text{(By property } \textit{(b)}\text{)} \\ &= kc^{-1}c \\ &= k.\end{aligned}$$

Then $\mathrm{Tr}_{F/K}$ will be onto $K$.]

Now $\mathrm{Tr}_{F/K}(\alpha) = 0$ if and only if $\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} = 0$ which is possible if and only if $\alpha$ is a root of the polynomial $x + x^q + \ldots + x^{q^{m-1}} \in K[x]$ in $F$. But this polynomial can have only $q^{m-1}$ roots in $F$ and $F$ has $q^m$ elements and this concludes that there exist an element $\alpha \in F$ such that $\mathrm{Tr}_{F/K}(\alpha) \neq 0$. This proves that the mapping is onto $K$.

*(d)* Let $a \in K$. Then

$$\begin{aligned}\mathrm{Tr}_{F/K}(a) &= a + a^q + \ldots + a^{q^{m-1}} \\ &= a + a + \ldots + a \qquad \text{(By Lemma 1.1.2)} \\ &= ma.\end{aligned}$$

*(e)* Since $F$ has $q^m$ number of elements, by Lemma 1.1.2, $\alpha^{q^m} = \alpha$, for every $\alpha \in F$. So $\mathrm{Tr}_{F/K}(\alpha^q) = \alpha^q + \alpha^{q^2} \ldots + \alpha^{q^m} = \alpha^q + \alpha^{q^2} \ldots + \alpha = \mathrm{Tr}_{F/K}(\alpha)$. □

**Theorem 1.2.3.** *Let $F$ be a finite field extension of the finite field $K$, both considered as vector spaces over $K$. Then the linear transformations from $F$ into $K$ are exactly the mappings $L_\beta, \beta \in F$, where $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ for all $\alpha \in F$. Furthermore, $L_\beta \neq L_\gamma$ whenever $\beta$ and $\gamma$ are distinct elements of $F$.*

*Proof.* By the properties of the trace function (property *(c)*), $\mathrm{Tr}_{F/K}(\beta\alpha)$ is a linear transformation from $F$ into $K$ and hence $L_\beta$ is a linear transformation from $F$ into $K$. Since $\mathrm{Tr}_{F/K}$ maps $F$ onto $K$, for every $\beta, \gamma \in F$ where $\beta \neq \gamma$, there is a suitable $\alpha \in F$ there exist an $\alpha \in F$ such that

$$L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) = \mathrm{Tr}_{F/K}((\beta - \gamma)\alpha) \neq 0.$$

So the mappings $L_\beta$ and $L_\gamma$ are distinct. If $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$, $F$ has $q^m$ distinct elements and hence there are $q^m$ different $L_\beta$ linear transformtions from $F$ into $K$. On the other hand, let $L$ be an arbitrary linear transformation from $F$ into $K$. Let $\alpha \in F$. Since$[F : K] = m$ (Since $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$) the basis of $F$ over $K$ has $m$ elements. Let $\{a_1, a_2, \ldots, a_m\}$ be a basis for $F$ over $K$. Then

$$\alpha = c_1a_1 + c_2a_2 + \ldots + c_ma_m \text{ for some } c_1, c_2, \ldots, c_m \in K.$$

Then

$$L(\alpha) = L(c_1a_1 + c_2a_2 + \ldots + c_ma_m) = c_1L(a_1) + c_2L(a_2) + \ldots + c_mL(a_m)$$

and for each $L(a_i)$ where $i = 1, 2, \ldots, m$, it can take $q$ values (Since $K$ has $q$ elements) and hence $L(\alpha)$ can have $q^m$ distinct values. Therefore there are only $q^m$ number of linear transformations from $F$ into $K$. So the set of all $L_\beta$ mappings will be the only linear transformations from $F$ into $K$. □

**Theorem 1.2.4.** *(Transitivity of Trace) Let $K$ be a finite field, and let $F$ be a finite extension of $K$ and $E$ a finite extension of $F$. Then,*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$$

*for all $\alpha \in E$.*

*Proof.* Let $K = \mathbb{F}_q$, let $[F : K] = m$ and $[E : F] = n$. Then $[E : K] = mn$. For $\alpha \in E$,

$$\begin{aligned}
\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} \mathrm{Tr}_{E/F}(\alpha)^{q^i} \\
&= \sum_{i=0}^{m-1} \left( \sum_{j=0}^{n-1} \alpha^{q^{jm}} \right)^{q^i} \\
&= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \\
&= \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha)
\end{aligned}$$

□

## 1.3 CHARACTERS

**Definition.** Let $G$ be a finite abelian group (written multiplicatively) of order $|G|$ with the identity element $1_G$. A *character* $\chi$ of $G$ is a homomorphism from $G$ into the multiplicative group $U$ of complex numbers of absolute value 1. That is, a mapping from $G$ into $U$ with $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.

Note that:

1. Since $\chi(1_G) = \chi(1_G)\chi(1_G)$, then $\chi(1_G) = 1$.

2. $(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$ for every $g \in G$ and therefore the values of $\chi$ are the $|G|$th roots of unity.

3. $\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$ and so, $(\chi(g))^{-1} = \overline{\chi(g)}$ for every $g \in G$ where the bar denotes the complex conjugation.

4. The *trivial* character denoted by $\chi_0$ is defined by $\chi_0(g) = 1$ for all $g \in G$. (All the other characters $G$ are called *nontrivial*).

5. With each character $\chi$ of $G$, there is associated the *conjugate* character $\overline{\chi}$ defined by $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$.

6. If there are finitely many characters $\chi_1, \chi_2, \ldots, \chi_n$ of $G$, then the product character $\chi_1\chi_2 \ldots \chi_n$ can be obtained by $(\chi_1\chi_2 \ldots \chi_n)(g) = \chi_1(g)\chi_2(g) \ldots \chi_n(g)$ for all $g \in G$.

7. If $\chi_1 = \chi_2 = \ldots = \chi_n = \chi$, then the product $\chi_1\chi_2 \ldots \chi_n$ can be written as $\chi^n$.

The set of characters of a group $G$ forms an abelian group under the above defined multiplication of characters and the group is denoted by $G^\wedge$. Since the characters of $G$ can only be the $|G|$th roots of unity, $G^\wedge$ is finite.

**Remark.** Let $G$ be a finite cyclic group of order $n$ and let $g$ be a generator of $G$. Then for a fixed integer $j$ such that $0 \leq j \leq n-1$, the function,

$$\chi_j(g^k) = e^{2\pi ijk/n}, \qquad \text{where} \quad k = 0, 1, \ldots, n-1$$

defines a character of $G$. (Since $\chi_j(g^k g^l) = (\chi_j(g^k)(\chi_j(g^l)$ and $e^{2\pi ijk/n}$ is a $n$th root of unity) Also, if $\chi$ is any character of $G$, then $\chi(g)$ must be an $n$th root of unity and it will be of the form $\chi(g) = e^{2\pi ij/n}$ for some $j$ such that $0 \leq j \leq n-1$. Therefore, $\chi = \chi_j$. Hence $G^\wedge$ consists exactly of the characters $\chi_0, \chi_1, \ldots, \chi_{n-1}$.

**Theorem 1.3.1.** *Let $H$ be a subgroup of the finite abelian group $G$ and let $\psi$ be a character of $H$. Then $\psi$ can be extended to a character of $G$; i.e. there exists a character of $\chi$ of $G$ with $\chi(h) = \psi(h)$ for all $h \in H$.*

*Proof.* Suppose $H$ is a proper subgroup of $G$. Let $\psi$ be a character of $H$. Choose $a \in G$ with $a \notin H$ and let $H_1$ be the subgroup of $G$ generated by $H$ and $a$. Let $m$ be the least positive integer for which $a^m \in H$. Then every element $g \in H_1$ can be written uniquely in the form $g = a^j h$ with $0 \leq j < m$ and $h \in H$. Define a function $\psi_1$ on $H_1$ by $\psi_1(g) = \omega^j \psi(h)$, where $\omega$ is a fixed complex number satisfying $\omega^m = \psi(a^m)$. Let's check whether $\psi_1$ is indeed a character of $H_1$. Let $g_1 = a^k h_1, 0 \leq k < m, h_1 \in H$, be another element of $H_1$. If $j + k < m$, then

$$\begin{aligned}
\psi_1(gg_1) &= \psi_1(a^j h a^k h_1) \\
&= \psi_1(a^{j+k} h h_1) \\
&= \omega^{j+k} \psi(h h_1) \\
&= \omega^{j+k} \psi(h) \psi(h_1) \\
&= \omega^j \psi(h) \omega^k \psi(h_1) = \psi_1(g)\psi_1(g_1)
\end{aligned}$$

If $j + k \geq m$, , then $gg_1 = a^{j+k-m}(a^m h h_1)$ and so

$$\begin{aligned}
\psi_1(gg_1) &= \omega^{j+k-m} \psi(a^m h h_1) \\
&= \omega^{j+k-m} \psi(a^m) \psi(h h_1) \\
&= \omega^{j+k} \psi(h h_1) = \psi_1(g)\psi_1(g_1)
\end{aligned}$$

For $h \in H$, $\psi_1(h) = \psi(h)$. If $H_1 = G$ then we are done. Otherwise, this process can be continued until an extension of $\psi$ to $G$ is obtained. Since $G$ is finite, this can be done in finite number of steps. □

**Theorem 1.3.2.** *For any two distinct elements $g_1, g_2 \in G$ there exists a character $\chi$ of $G$ with $\chi(g_1) \neq \chi(g_2)$.*

*Proof.* Let $h = g_1 g_2^{-1}$. So $h \neq 1_G$. Let $H$ be the cyclic subgroup of order $r$ generated by $h$. Let $j \neq 0$. Then by the above remark, $\psi_j(h) = e^{2\pi i j/r} \neq 1$ where $\psi_j$ is a character of $H$. Then by the Theorem 1.3.1, there exists a character $\chi$ of $G$ such that $\chi(h) = \psi_j(h)$ for all $h \in H$. So $\chi(h) \neq 1$. So $\chi(g_1 g_2^{-1}) \neq 1$ and hence $\chi(g_1) \neq \chi(g_2)$. □

**Theorem 1.3.3.** *If $\chi$ is a nontrivial character of the finite abelian group $G$, then*

$$\sum_{g \in G} \chi(g) = 0 \tag{1.3}$$

*If $g \in G$ with $g \neq 1_G$ then,*

$$\sum_{\chi \in G^\wedge} \chi(g) = 0 \tag{1.4}$$

*Proof.* For the first part of the theorem, $\chi$ is nontrivial. Then there exists $h \in G$ with $\chi(h) \neq 1$. Then

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(g) \qquad \text{(Since if } g \text{ runs through } G, \text{ so does } hg).$$

Then we have

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0.$$

Hence (1.3).

For the second part, define the function $g^{'}$ such that $g^{'}(\chi) = \chi(g)$ for $\chi \in G^\wedge$. This is a character of the finite abelian group $G^\wedge$ since

$$g^{'}(\chi_1\chi_2) = \chi_1\chi_2(g) = \chi_1(g)\chi_2(g) = g^{'}(\chi_1)g^{'}(\chi_2).$$

So for $g \in G$ such that $g \neq 1_G$, by Theorem 1.3.2, there exists $\chi \in G^\wedge$ such that $\chi(g) \neq \chi(1_G) = 1$. So $g^{'}$ is non trivial. So by the first part of this theorem applied to $G^\wedge$,

$$\sum_{\chi \in G^\wedge} g^{'}(\chi) = 0$$

Since $g^{'}(\chi) = \chi(g)$,

$$\Rightarrow \sum_{\chi \in G^\wedge} \chi(g) = 0$$

. □

**Theorem 1.3.4.** *The number of characters of a finite abelian group $G$ is equal to $|G|$.*

*Proof.* By Theorem 1.3.3, (1.4),

$$\sum_{g\in G}\sum_{\chi\in G^\wedge}\chi(g)=\sum_{\chi\in G^\wedge}\chi(1_G)=|G^\wedge| \quad (\text{Since } \chi(1_G)=1, \text{ this gives the count of } G^\wedge) \tag{1.5}$$

$$\sum_{g\in G}\sum_{\chi\in G^\wedge}\chi(g)=\sum_{\chi\in G^\wedge}\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi_0(g) \quad (\text{By (1.3) in Theorem 1.3.3})$$
$$=|G|$$

Then by (1.5), $|G^\wedge|=|G|$. □

**Definition.** The set of all characters of $G$ which annihilate a given subgroup $H$ (i.e characters $\chi$ of $G$ such that $\chi(h)=1$ for all $h\in H$) is called the *annihilator of $H$ in $G^\wedge$*.

**Definition.** Let $\mathbb{F}_q$ be the finite field with $q$ elements. Let $p$ be the characteristic of $\mathbb{F}_q$. Let Tr: $\mathbb{F}_q\to\mathbb{F}_p$ be the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Then the function $\chi_1$ defined by

$$\chi_1(c)=e^{2\pi i \mathrm{Tr}(c)/p} \qquad \text{for all} \quad c\in\mathbb{F}_q$$

is a character of the additive group of $\mathbb{F}_q$. The character $\chi_1$ is called the *canonical additive character* of $\mathbb{F}_q$.

**Theorem 1.3.5.** *For $b\in\mathbb{F}_q$, the function $\chi_b$ with $\chi_b(c)=\chi_1(bc)$ for all $c\in\mathbb{F}_q$ is an additive character of $\mathbb{F}_q$, and every additive character of $\mathbb{F}_q$ is obtained this way.*

*Proof.* For $c_1,c_2\in\mathbb{F}_q$,

$$\chi_b(c_1+c_2)=\chi_1(bc_1+bc_2)$$
$$=\chi_1(bc_1)\chi_1(bc_2)$$
$$=\chi_b(c_1)\chi_b(c_2)$$

So the first part is proved. For the second part, by Theorem 1.2.2 *(c)*, Tr maps $\mathbb{F}_q$ onto $\mathbb{F}_p$. Hence $\chi_1$ is a nontrivial character. Therefore, for $a, b \in \mathbb{F}_q$ where $a \neq b$,

$$\frac{\chi_a(c)}{\chi_b(c)} = \frac{\chi_1(ac)}{\chi_1(bc)} = \chi_1((a-b)c) \neq 1.$$

for suitable $c \in \mathbb{F}_q$. So $\chi_a$ and $\chi_b$ are distinct characters. Therefore if $b$ runs through $\mathbb{F}_q$, we can get $q$ distinct additive characters in the form of $\chi_b$. Also by Theorem 1.3.4, $\mathbb{F}_q$ has exactly $q$ additive characters. So it can be concluded that all the additive characters of $\mathbb{F}_q$ can be obtained on this way. □

**Remark.** Let $E$ be a finite extension field of $\mathbb{F}_q$ and let $\chi_1$ be the canonical additive character of $\mathbb{F}_q$. Let $\mu_1$ be the canonical additive character of $E$ where the Tr is replaced by the absolute trace function $\mathrm{Tr}_E$ from $E$ to $\mathbb{F}_p$. Let $\beta \in E$. Then by the Theorem 1.2.4,

$$\mathrm{Tr}_E(\beta) = \mathrm{Tr}_{\mathbb{F}_q}(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)) \quad \text{for all} \quad \beta \in E.$$

Then,

$$\begin{aligned}
\chi_1\left(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)\right) &= e^{2\pi i \mathrm{Tr}_{\mathbb{F}_q}\left(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)\right)/p} \\
&= e^{2\pi i \mathrm{Tr}_E(\beta)/p} \\
&= \mu_1(\beta)
\end{aligned}$$

Therefore,

$$\chi_1\left(\mathrm{Tr}_{E/\mathbb{F}_q}(\beta)\right) = \mu_1(\beta) \tag{1.6}$$

**Definition.** Characters of the *multiplicative group* $\mathbb{F}_q^*$ of $\mathbb{F}_q$ are called *multiplicative characters* of $\mathbb{F}_q$.

## 1.4 ORTHOGONALITY RELATIONS FOR CHARACTERS

**Proposition 1.4.1.** *Let $\chi$ and $\psi$ be characters of $G$. Then*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} 0 & \textit{for } \chi \neq \psi \\ 1 & \textit{for } \chi = \psi \end{cases} \tag{1.7}$$

*Proof.* Let $\chi$ and $\psi$ be characters of $G$. When $\chi = \psi$,

$$\begin{aligned}\chi(g)\overline{\psi(g)} &= \chi(g)\psi(g)^{-1} \\ &= \chi(g)\chi(g)^{-1} = \chi(1_G) = 1.\end{aligned}$$

So $\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \frac{1}{|G|}\sum_{g\in G} 1 = \frac{1}{|G|}|G| = 1.$

If $\chi \neq \psi$,

$$\begin{aligned}\chi(g)\overline{\psi(g)} &= \chi(g)\overline{\psi}(g) \\ &= \chi\overline{\psi}(g)\end{aligned}$$

We check that $\chi\overline{\psi}$ is non-trivial. Suppose otherwise. Then

$$\begin{aligned}\chi\overline{\psi}(g) = 1 &\Rightarrow \chi(g)\psi(g)^{-1} = 1 \\ &\Rightarrow \chi(g) = \psi(g) \qquad \text{for every} \quad g \in G\end{aligned}$$

which contradicts with the fact that $\chi \neq \psi$. Therefore $\chi\overline{\psi}$ is non trivial. So by applying (1.3) in Theorem 1.3.3,

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

and hence $\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = 0$. Therefore it can be concluded that,

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} 0 & \text{for } \chi \neq \psi \\ 1 & \text{for } \chi = \psi \end{cases}$$

□

**Proposition 1.4.2.** *Let $g$ and $h$ be elements of $G$. Then*

$$\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)} = \begin{cases} 0 & \textit{for } g \neq h \\ 1 & \textit{for } g = h \end{cases} \tag{1.8}$$

*Proof.* Let $g$ and $h$ be elements of $G$. If $g = h$ then

$$\chi(g)\overline{\chi(h)} = \chi(g)\chi(g)^{-1} = 1$$

This imples that $\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)} = 1$. If $g \neq h$, then

$$\chi(g)\overline{\chi(h)} = \chi(g)\chi(h)^{-1} = \chi(g)\chi(h^{-1}) = \chi(gh^{-1})$$

Since $g \neq h$, $gh^{-1} \neq 1_G$. Then by (1.4) in Theorem 1.3.3,

$$\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)} = \frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(gh^{-1}) = 0$$

Therefore,

$$\frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{for } g \neq h \\ 1 & \text{for } g = h \end{cases}$$

□

Applying the orthogonality relations in Proposition 1.4.1 and Proposition 1.4.2 to additive and multiplicative characters of $\mathbb{F}_q$, the following fundamental identities can be obtained. Let $\chi_a$ and $\chi_b$ be additive characters of $\mathbb{F}_q$. If $a \neq b$, then $\chi_a \neq \chi_b$ and if $a = b$ then $\chi_a = \chi_b$. Then by (1.7),

$$\sum_{c\in\mathbb{F}_q}\chi_a(c)\overline{\chi_b(c)} = \begin{cases} 0 & \text{for } a \neq b \\ q & \text{for } a = b \end{cases} \tag{1.9}$$

If $a \neq 0$, since $\chi_0 = 1$ and hence by (1.9),

$$\sum_{c\in\mathbb{F}_q}\chi_a(c) = 0. \tag{1.10}$$

Furthermore, for elements $c, d \in \mathbb{F}_q$ we obtain

$$\sum_{b \in \mathbb{F}_q} \chi_b(c)\overline{\chi_b(d)} = \begin{cases} 0 & \text{for } c \neq d \\ q & \text{for } c = d \end{cases} \tag{1.11}$$

Similarly, for multiplicative characters $\psi$ and $\tau$ of $\mathbb{F}_q$,

$$\sum_{c \in \mathbb{F}_q^*} \psi(c)\overline{\tau(c)} = \begin{cases} 0 & \text{for } \psi \neq \tau \\ q-1 & \text{for } \psi = \tau \end{cases} \tag{1.12}$$

Also

$$\sum_{c \in \mathbb{F}_q^*} \psi(c) = 0 \qquad \text{for } \psi \neq \psi_0. \tag{1.13}$$

If $c, d \in \mathbb{F}_q^*$ then

$$\sum_{\psi} \psi(c)\overline{\psi(d)} = \begin{cases} 0 & \text{for } c \neq d \\ q-1 & \text{for } c = d \end{cases} \tag{1.14}$$

where the sum is extended over all multiplicative characters $\psi$ of $\mathbb{F}_q$.

## 1.5 GAUSSIAN SUMS

**Definition.** Let $\psi$ be a multipliactive character and $\chi$ an additive character of $\mathbb{F}_q$. Then the *Gaussian Sum* $G(\psi, \chi)$ is defined by

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

Before we discuss some properties of the Gaussian Sums, let's assume that $\psi_0$ and $\chi_0$ are the trivial multiplicative character and trivial additive character of $\mathbb{F}_q$ respectively.

**Theorem 1.5.1.** *Let $\psi$ be a multiplicative and $\chi$ an additive character of $\mathbb{F}_q$. Then* *the Gaussian Sum* $G(\psi, \chi)$ *satisfies*

$$G(\psi, \chi) = \begin{cases} q-1 & \textit{for } \psi = \psi_0, \chi = \chi_0 \\ -1 & \textit{for } \psi = \psi_0, \chi \neq \chi_0 \\ 0 & \textit{for } \psi \neq \psi_0, \chi = \chi_0 \end{cases} \tag{1.15}$$

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

$$|G(\psi, \chi)| = q^{1/2} \tag{1.16}$$

*Proof.* If $\psi = \psi_0, \chi = \chi_0$ then $G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c) = \sum_{c \in \mathbb{F}_q^*} 1 = q - 1$. If $\psi \neq \psi_0, \chi = \chi_0$ then $G(\psi, \chi) = \sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c)$. Then by (1.13), $\sum_{c \in \mathbb{F}_q^*} \psi(c) = 0$. If $\psi = \psi_0, \chi \neq \chi_0$, then

$$G(\psi_0, \chi) = \sum_{c \in \mathbb{F}_q^*} \chi(c) = \sum_{c \in \mathbb{F}_q} \chi(c) - \chi(0) = -1$$

(Since $\psi_0 = 1$ and by (1.10)). If $\psi \neq \psi_0, \chi \neq \chi_0$ then

$$\begin{aligned} |G(\psi, \chi)|^2 &= \overline{G(\psi, \chi)} G(\psi, \chi) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \overline{\psi(c)\chi(c)} \psi(c_1)\chi(c_1) \\ &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \psi(c^{-1}c_1)\chi(c_1 - c) \end{aligned}$$

If we substitute $c^{-1}c_1 = d$, then

$$\begin{aligned} |G(\psi, \chi)|^2 &= \sum_{c \in \mathbb{F}_q^*} \sum_{c_1 \in \mathbb{F}_q^*} \psi(d)\chi(c(d-1)) \\ &= \sum_{c \in \mathbb{F}_q^*} \psi(d) \left( \sum_{c \in \mathbb{F}_q} \chi(c(d-1)) - \chi(0) \right) \\ &= \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{c \in \mathbb{F}_q} \chi(c(d-1)) - \sum_{d \in \mathbb{F}_q^*} \psi(d) \\ &= \sum_{d \in \mathbb{F}_q^*} \psi(d) \sum_{c \in \mathbb{F}_q} \chi(c(d-1)) \qquad \text{(By (1.13))} \end{aligned}$$

If $d \neq 1$, then by (1.10) (note that $\chi$ is non trivial), $\sum_{c \in \mathbb{F}_q} \chi(c(d-1)) = 0$. If $d = 1$ then $\sum_{c \in \mathbb{F}_q} \chi(c(d-1)) = q$. Therefore, $|G(\psi, \chi)|^2 = \psi(1)q = q$ and hence the result. □

**Theorem 1.5.2.** *Gaussian sums for the finite field $\mathbb{F}_q$ satisfy the following properties:*

*(a)* $G(\psi, \chi_{ab}) = \overline{\psi(a)} G(\psi, \chi_b)$ *for* $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$;

*(b)* $G(\psi, \overline{\chi}) = \psi(-1) G(\psi, \chi)$;

*(c)* $G(\overline{\psi}, \chi) = \psi(-1) \overline{G(\psi, \chi)}$;

*(d)* $G(\psi, \chi) G(\overline{\psi}, \chi) = \psi(-1) q$ *for* $\psi \neq \psi_0, \chi \neq \chi_0$

*(e)* $G(\psi^p, \chi_b) = G(\psi, \chi_{\sigma(b)})$ *for* $b \in \mathbb{F}_q$*, where* $p$ *is the characteristic of* $\mathbb{F}_q$ *and* $\sigma(b) = b^p$.

*Proof.* *(a)* Let $c \in \mathbb{F}_q$. Then by the definition in Theorem 1.3.5,

$$\chi_{ab}(c) = \chi_1(abc) = \chi_b(ac)$$

and hence

$$G(\psi, \chi_{ab}) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi_{ab}(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c) \chi_b(ac)$$

Now set $ac = d$. Then

$$\begin{aligned} G(\psi, \chi_{ab}) &= \sum_{d \in \mathbb{F}_q^*} \psi(a^{-1} d) \chi_b(d) \\ &= \psi(a^{-1}) \sum_{d \in \mathbb{F}_q^*} \psi(d) \chi_b(d) \\ &= \overline{\psi(a)} G(\psi, \chi_b). \end{aligned}$$

*(b)* Since $\chi$ is an additive character of $\mathbb{F}_q$, by the Theorem 1.3.5, $\chi = \chi_b$ for a suitable $b \in \mathbb{F}_q$. So since $\chi$ is additive, $\overline{\chi}(c) = \chi_b(-c) = \chi_1(-bc) = \chi_{-b}(c)$ for $c \in \mathbb{F}_q$. So $\overline{\chi} = \chi_{-b}$. Then by using $a = -1$ in *(a)*,

$$G(\psi, \overline{\chi}) = G(\psi, \chi_{-b}) = \overline{\psi}(-1)G(\psi, \chi_b) = \psi(-1)G(\psi, \chi).$$

(Since $\psi(-1)\psi(-1) = \psi(1) = 1 \Rightarrow \overline{\psi}(-1) = \psi(-1)$)

*(c)* By *(b)*, $G(\overline{\psi}, \chi) = \overline{\psi}(-1)G(\overline{\psi}, \overline{\chi})$. Since $\overline{\psi}(-1) = \overline{\psi(-1)} = \psi(-1)$ and $G(\overline{\psi}, \overline{\chi}) = \sum_{c \in \mathbb{F}_q^*} \overline{\psi}(c)\overline{\chi}(c) = \overline{\sum_{c \in \mathbb{F}_q^*} \psi(c)\chi(c)} = \overline{G(\psi, \chi)}$,

$$G(\overline{\psi}, \chi) = \psi(-1)\overline{G(\psi, \chi)}.$$

*(d)* By *(c)*,

$$\begin{aligned} G(\psi, \chi)G(\overline{\psi}, \chi) &= \psi(-1)G(\psi, \chi)\overline{G(\psi, \chi)} \\ &= \psi(-1)\left|G(\psi, \chi)\right|^2 \\ &= \psi(-1)q \qquad \text{(By 1.16)} \end{aligned}$$

*(e)* By Theorem 1.2.2, *(e)*, Tr$(a)$=Tr$(a^p)$ for $a \in \mathbb{F}_q$. So we have $\chi_1(a) = \chi_1(a^p)$. (By the definition of the cannonical additive character). Let $\sigma(b) = b^p$. Then we have $\chi_b(c) = \chi_1(bc) = \chi_1((bc)^p) = \chi_1(b^p c^p) = \chi_{\sigma(b)}(c^p)$. Then

$$G(\psi^p, \chi_b) = \sum_{c \in \mathbb{F}_q^*} \psi^p(c)\chi_b(c) = \sum_{c \in \mathbb{F}_q^*} \psi(c^p)\chi_{\sigma(b)}(c^p).$$

But $c^p$ runs through $\mathbb{F}_q^*$ as $c$ runs through $\mathbb{F}_q^*$, and hence

$$G(\psi^p, \chi_b) = \sum_{c^p \in \mathbb{F}_q^*} \psi(c^p)\chi_{\sigma(b)}(c^p) = G(\psi, \chi_{\sigma(b)}).$$

□

Gaussian sums occur in a variety of contexts. This can be clearly seen from the following propositions.

**Proposition 1.5.3.** *Let $\chi$ be a additive character of $\mathbb{F}_q$ and $\psi$ be a multiplicative character of $\mathbb{F}_q$. Then,*

$$\psi(c) = \frac{1}{q} \sum_{\chi} G(\psi, \overline{\chi}) \chi(c) \qquad \textit{for } c \in \mathbb{F}_q^*. \tag{1.17}$$

*Proof.* If $c, d \in \mathbb{F}_q$, and if $c = d$, then by (1.11), $\sum_{b \in \mathbb{F}_q} \chi_b(c)\overline{\chi_b(d)} = q$. So,

$$\begin{aligned}\psi(c) &= \frac{1}{q} \sum_{c \in \mathbb{F}_q^*} \psi(d) \sum_{b \in \mathbb{F}_q} \chi_b(c)\overline{\chi_b(d)} \\ &= \frac{1}{q} \sum_{b \in \mathbb{F}_q} \chi_b(c) \sum_{c \in \mathbb{F}_q^*} \psi(d)\overline{\chi}_b(d)\end{aligned}$$

for any $c \in \mathbb{F}_q^*$. By Theorem 1.3.5, every additive character of $\mathbb{F}_q$ is of the form $\chi_b$ where $b \in \mathbb{F}_q$ and so $\sum_{b \in \mathbb{F}_q} \chi_b(c) = \sum_{\chi} \chi(c)$. Therefore

$$\psi(c) = \frac{1}{q} \sum_{\chi} G(\psi, \overline{\chi}) \chi(c) \qquad \text{for } c \in \mathbb{F}_q^*.$$

where the sum is extended over all additive characters $\chi$ of $\mathbb{F}_q$. □

**Proposition 1.5.4.** *Let $\psi$ be a multiplicative character of $\mathbb{F}_q$ and let $\chi$ be a additive character of $\mathbb{F}_q$. Then*

$$\chi(c) = \frac{1}{q-1} \sum_{\psi} G(\overline{\psi}, \chi) \psi(c) \qquad \textit{for } c \in \mathbb{F}_q^*. \tag{1.18}$$

*Proof.* If $c, d \in \mathbb{F}_q$, and if $c = d$, then by (1.14), $\sum_{\psi} \psi(c)\overline{\psi(d)} = q - 1$. So,

$$\begin{aligned}\chi(c) &= \frac{1}{q-1} \sum_{d \in \mathbb{F}_q^*} \chi(d) \sum_{\psi} \psi(c)\overline{\psi(d)} \\ &= \frac{1}{q-1} \sum_{\psi} \psi(c) \sum_{d \in \mathbb{F}_q^*} \overline{\psi}(d)\chi(d) \qquad \text{for } c \in \mathbb{F}_q^*.\end{aligned}$$

Then we obtain,

$$\chi(c) = \frac{1}{q-1} \sum_{\psi} G(\overline{\psi}, \chi) \psi(c) \qquad \text{for } c \in \mathbb{F}_q^*.$$

□

# CHAPTER 2

# BOUNDS ON THE NUMBER OF ZEROS IN A LINEAR RECURRENCE SEQUENCE

Here we will discuss a method to determine the bounds on the number of zeros in a linear reccurence sequence of an irreducible polynomial of given degree and order, which is based on Gaussian sums. This material is adapted from [2].

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

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n + a \qquad \text{for } n = 0, 1, \ldots \tag{2.1}$$

is called a (*kth-order*) *linear recurring sequence* in $\mathbb{F}_q$. The terms $s_0, s_1, \ldots s_{k-1}$, which determine the rest of the sequence uniquely, are refered to as the *initial values*. A relation of the form (2.1) is called a *(kth-order) linear recurrence relation*. We speak of a *homogeneous* linear recurrence relation if $a = 0$. Otherwise it is *inhomogeneous*.

**Definition.** Let $S$ be an arbitrary nonempty set and let $s_0, s_1, \ldots$ be a sequence of elements of $S$. If there exist integers $r > 0$ and $n_0 \geq 0$ such that $s_{n+r} = s_n$ for all $n \geq n_0$, then the sequence is called *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.** Let $s_0, s_1, \ldots$ be a $k$th order homogeneous linear recurring sequence in $\mathbb{F}_q$ satisfying the linear recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \ldots + a_0 s_n \qquad \text{for } n = 0, 1, \ldots \tag{2.2}$$

where $a_j \in \mathbb{F}_q$ for $0 \leq j \leq k-1$. The polynomial

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

is called the *characteristic polynomial* of the linear recurring sequence.

**Definition.** Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$. $m(x) \in \mathbb{F}_q[x]$ is said to be the *minimal polynomial* of the sequence if it has the following property: a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of positive degree is a characteristic polynomial of $s_0, s_1, \ldots$ if and only if $m(x)$ divides $f(x)$.

**Definition.** Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer $e$ for which $f(x)$ divides $x^e - 1$ is called the *order* of $f$ and it is denoted by $ord(f)$.

**Theorem 2.0.5.** *Let $s_0, s_1, \ldots$ be a $k$th-order homogeneous linear recurring sequence in $K = \mathbb{F}_q$ whose characteristic polynomial $f(x)$ is irreducible over $K$. Let $\alpha$ be a root of $f(x)$ in the extension field $F = \mathbb{F}_{q^k}$. Then there exists a uniquely determined $\theta \in F$ such that*

$$s_n = Tr_{F/K}(\theta\alpha^n) \qquad \text{for} \quad n = 0, 1, \ldots$$

*Proof.* Let $s_0, s_1, \ldots$be a $k$th-order homogeneous linear recurring sequence in $K = \mathbb{F}_q$ and let $F = \mathbb{F}_{q^k}$. $\alpha$ is a root of the irreducible polynomial $f(x)$ of degree $k$, in $F$. Therefore

$$[K(\alpha) : K] = k$$

and

$$[F : K] = k \qquad\qquad \text{(By Lemma 1.1.1)}.$$

Then since $K \subseteq K(\alpha) \subseteq F$,

$$[F : K(\alpha)][K(\alpha) : K] = k$$

$$\Rightarrow [F : K(\alpha)] = 1$$

$$\Rightarrow F = K(\alpha)$$

So $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$ constitutes a basis of $F$ over $K$. Define $L : F \to K$ such that

$$L(\alpha^n) = s_n, \qquad n = 0, 1, \ldots, k-1$$

Then by the Theorem 1.2.3, there exist a uniquely determined $\theta \in F$ such that $L_\theta(\gamma) = \mathrm{Tr}_{F/K}(\theta\gamma)$ for all $\gamma \in F$. In particular,

$$s_n = \mathrm{Tr}_{F/K}(\theta\alpha^n)$$

Now we have to show that the elements $\mathrm{Tr}_{F/K}(\theta\alpha^n)$, $n = 0, 1, \ldots,$ form a homogeneous linear recurring sequence with characteristic polynomial $f(x)$. If $f(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_0 \in K[x]$, then by the properties of the trace function,

$$\mathrm{Tr}_{F/K}\left(\theta\alpha^{n+k}\right) - a_{k-1}\mathrm{Tr}_{F/K}\left(\theta\alpha^{n+k-1}\right) - \ldots - a_0\mathrm{Tr}_{F/K}(\theta\alpha^n)$$

$$= \mathrm{Tr}_{F/K}\left(\theta\alpha^{n+k} - a_{k-1}\theta\alpha^{n+k-1} - \ldots - a_0\theta\alpha^n\right)$$

$$= \mathrm{Tr}_{F/K}(\theta\alpha^n f(\alpha))$$

$$= 0$$

for all $n \geq 0$. □

**Theorem 2.0.6.** *Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$ with minimal polynomial $m(x) \in \mathbb{F}_q[x]$. Then the least period of the sequence is equal to ord($m(x)$).*

**Theorem 2.0.7.** *Let $s_0, s_1, \ldots$ be a homogeneous linear recurring sequence in $\mathbb{F}_q$ with least period $r$. Suppose the minimal polynomial $m(x)$ of the sequence is irreducible over $\mathbb{F}_q$, has degree $k \geq 1$, and satisfies $m(0) \neq 0$. Let $h$ be the least common multiple of $r$ and $q-1$. Then,*

$$\left| Z(0) - \frac{(q^{k-1}-1)r}{q^k - 1} \right| \leq \left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^k-1}\right) q^{k/2}$$

*and*

$$\left| Z(b) - \frac{q^{k-1}r}{q^k - 1} \right| \leq \left(\frac{r}{h} - \frac{r}{q^k-1} + \frac{h-r}{h} q^{1/2}\right) q^{(k/2)-1}$$

*for $b \neq 0$.*

*Proof.* Set $K = \mathbb{F}_q$. Let $F$ be the splitting field of $m(x)$ over $K$. I.e

$$m(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k), \alpha_i \in F \tag{2.3}$$

Since $[F : K] = k$, by Lemma 1.1.1, $F$ has $q^k$ elements and hence $F = \mathbb{F}_{q^k}$. Let $\alpha$ be a fixed root of $m(x)$ in $F$. I.e there exist a $i'$ such that $\alpha_{i'} = \alpha$ in (2.3). Since $m(0) \neq 0$, $\alpha \neq 0$. Then by Theorem 2.0.5, there exist a $\theta \in F$ such that

$$s_n = \mathrm{Tr}_{F/K}(\theta\alpha^n) \text{ for } n = 0, 1, \ldots \tag{2.4}$$

If $\theta = 0$ then $\mathrm{Tr}_{F/K}$= 0 =$s_n$ for every $n$. This implies that the sequence is 0 where the least period $r = 1$ which implies that degree of $m(x)$ is 0. This contradicts the hypothesis. Therefore $\theta \neq 0$. Let $\lambda'$ be the canonical additive character of $K$. [I.e $\chi_1(c) = \lambda'(c) = e^{2\pi i \mathrm{Tr}(c)/p}$, for every $c \in \mathbb{F}_q$ where $p = \mathrm{char}(K)$]. Let $b \in K$. Consider

$$\frac{1}{q}\sum_{c \in K} \lambda'(c(b - s_n))$$

Since $\lambda'(0) = 1$, if $b = s_n$ then

$$\frac{1}{q}\sum \lambda'(0) = \frac{1}{q}(q) = 1.$$

If $b \neq s_n$ then

$$\frac{1}{q}\sum_{c\in K}\lambda'(c(b-s_n) = \frac{1}{q}\sum_{c\in K}\chi_1(c(b-s_n)$$

$$= \frac{1}{q}\sum_{c\in K}\chi_{b-s_n}(c)$$

$$= 0 \qquad \text{(by the relation 1.10)}$$

For each $n = 0, 1, \ldots,$

$$\frac{1}{q}\sum_{c\in K}\lambda'(c(b-s_n)) = \frac{1}{q}\sum_{c\in K}\Big(\lambda'(cb-cs_n)\Big)$$

$$= \frac{1}{q}\sum_{c\in K}\Big(\lambda'(cb)\lambda'(-cs_n)\Big)$$

$$= \frac{1}{q}\sum_{c\in K}\Big(\lambda'(bc)\lambda'\left(-c\mathrm{Tr}_{F/K}\left(\theta\alpha^n\right)\right)\Big)$$

(By (2.4))

$$= \frac{1}{q}\sum_{c\in K}\Big(\lambda'(bc)\lambda'\left(\mathrm{Tr}\left(-c\theta\alpha^n\right)\right)\Big) \tag{2.5}$$

(By the properties of Tr in Theorem 1.2.2)

$Z(b)$ is the number of occurrences of $b$ in a full period of the linear recurring sequence. So by (2.5),(by considering a period)

$$Z(b) = \frac{1}{q}\sum_{n=0}^{r-1}\sum_{c\in K}\lambda'\left(bc\right)\lambda'\left(\mathrm{Tr}_{F/K}\left(-c\theta\alpha^n\right)\right) \tag{2.6}$$

Let $\lambda$ be the canonical additive character of $F$. Then

$$\lambda'\left(\mathrm{Tr}_{F/K}\left(\beta\right)\right) = \lambda\left(\beta\right)$$

for every $\beta \in F$ (By the relation (1.6))

Then by (2.6),

$$
\begin{aligned}
Z(b) &= \frac{1}{q}\sum_{n=0}^{r-1}\sum_{c\in K}\lambda^{'}(bc)\,\lambda\left(-c\theta\alpha^{n}\right) \\
&= \frac{1}{q}\sum_{n=0}^{r-1}\sum_{c\in K}\lambda^{'}(bc)\,\overline{\lambda\left(c\theta\alpha^{n-1}\right)} \\
&= \frac{1}{q}\sum_{n=0}^{r-1}\sum_{c\in K}\lambda^{'}(bc)\,\overline{\lambda}\left(c\theta\alpha^{n}\right) \qquad \left(\text{Since}\overline{\lambda}\left(c\theta\alpha^{n}\right)=\overline{\lambda\left(c\theta\alpha^{n}\right)}\right) \\
&= \frac{1}{q}\sum_{c\in K}\lambda^{'}(bc)\sum_{n=0}^{r-1}\overline{\lambda}\left(c\theta\alpha^{n}\right) \\
&= \frac{1}{q}\left[\lambda^{'}(0)\left(\sum_{n=0}^{r-1}\overline{\lambda}(0)\right)+\sum_{c\in K^{*}}\lambda^{'}(bc)\sum_{n=0}^{r-1}\overline{\lambda}\left(c\theta\alpha^{n}\right)\right] \\
&= \frac{1}{q}\left[r+\sum_{c\in K^{*}}\lambda^{'}(bc)\sum_{n=0}^{r-1}\overline{\lambda}\left(c\theta\alpha^{n}\right)\right] \quad (\text{Since } \lambda \text{ is a group homomorphism, } \lambda(0)=1)
\end{aligned}
$$

So

$$
Z(b)=\frac{1}{q}\left[r+\sum_{c\in K^{*}}\lambda^{'}(bc)\sum_{n=0}^{r-1}\overline{\lambda}\left(c\theta\alpha^{n}\right)\right] \tag{2.7}
$$

$\overline{\lambda}$ is a additive character of $F=\mathbb{F}_{q^k}$. Then

$$
\overline{\lambda}(\beta)=\frac{1}{q^{k}-1}\sum_{\psi}G\left(\overline{\psi},\overline{\lambda}\right)\psi(\beta)\,,\text{for every}\beta\in F^{*} \qquad (\text{By the relation (1.18)})
$$

where the sum is extended over all multiplicative characters $\psi$ of $F$. Then

$$
\overline{\lambda}\left(c\theta\alpha^{n}\right)=\frac{1}{q^{k}-1}\sum_{\psi}G\left(\overline{\psi},\overline{\lambda}\right)\psi\left(c\theta\alpha^{n}\right)
$$

$\Longrightarrow$

$$
\begin{aligned}
\sum_{n=0}^{r-1}\overline{\lambda}\left(c\theta\alpha^{n}\right) &= \frac{1}{q^{k}-1}\sum_{n=0}^{r-1}\sum_{\psi}G\left(\overline{\psi},\overline{\lambda}\right)\psi\left(c\theta\alpha^{n}\right) \\
&= \frac{1}{q^{k}-1}\sum_{n=0}^{r-1}\sum_{\psi}G\left(\overline{\psi},\overline{\lambda}\right)\psi(c\theta)\,\psi(\alpha)^{n} \\
&= \frac{1}{q^{k}-1}\sum_{\psi}\psi(c\theta)\,G\left(\overline{\psi},\overline{\lambda}\right)\sum_{n=0}^{r-1}\psi(\alpha)^{n}
\end{aligned}
$$

Then

$$\sum_{n=0}^{r-1} \overline{\lambda}\left(c\theta\alpha^n\right) = \frac{1}{q^k-1} \sum_{\psi} \psi\left(c\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right) \sum_{n=0}^{r-1} \psi\left(\alpha\right)^n \tag{2.8}$$

$\sum_{n=0}^{r-1} \psi\left(\alpha\right)^n$ is a finite geometric series, where

$$\sum_{n=0}^{r-1} \psi\left(\alpha\right)^n = r \quad \text{when} \quad \psi\left(\alpha\right) = 1$$

and

$$\sum_{n=0}^{r-1} \psi\left(\alpha\right)^n = \frac{1-\psi\left(\alpha\right)^r}{1-\psi\left(\alpha\right)} \quad \text{when} \quad \psi\left(\alpha\right) \neq 1$$

But $\psi\left(\alpha\right)^r = \psi\left(\alpha^r\right) = \psi(1) = 1$ [Since the order of $m(x) = r$ (which is explained later), order of $\alpha$ is $r$].

$$\text{Then} \quad \sum_{n=0}^{r-1} \psi\left(\alpha\right)^n \quad \text{vanishes for } \psi\left(\alpha\right) \neq 1 \tag{2.9}$$

Take $J$ to be the set of all characters $\psi$ for which $\psi\left(\alpha\right) = 1$.

$\Longrightarrow \sum_{n=0}^{r-1} \psi\left(\alpha\right)^n = r$ for every $\psi \in J$.

Then by (2.8),

$$\sum_{n=0}^{r-1} \overline{\lambda}\left(c\theta\alpha^n\right) = \frac{r}{q^k-1} \sum_{\psi \in J} \psi\left(c\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right)$$

Substituting this in (2.7)

$$\begin{aligned} Z(b) &= \frac{r}{q} + \frac{r}{q\left(q^k-1\right)} \sum_{c \in K^*} \lambda^{'}(bc) \sum_{\psi \in J} \psi\left(c\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right) \\ &= \frac{r}{q} + \frac{r}{q\left(q^k-1\right)} \sum_{\psi \in J} \psi(c)\psi\left(\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right) \sum_{c \in K^*} \lambda^{'}(bc) \\ &= \frac{r}{q} + \frac{r}{q\left(q^k-1\right)} \sum_{\psi \in J} \psi\left(\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right) \sum_{c \in K^*} \lambda^{'}(bc)\psi(c) \end{aligned}$$

Let $\psi^{'}$ be the restriction of $\psi$ to $K^*$.

Then

$$\begin{aligned} \sum_{c \in K^*} \psi(c)\lambda^{'}(bc) &= \sum_{c \in K^*} \psi^{'}(c)\lambda^{'}(bc) \\ &= \sum_{c \in K^*} \psi^{'}(c)\lambda_b^{'}(c) \qquad \left(\text{Since } \lambda^{'}(bc) = \lambda_b^{'}(c)\right) \end{aligned}$$

Since $\lambda^{'}$ is the cannonical additive character, $\sum_{c \in K^*} \psi^{'}(c)\lambda_b^{'}(c)$ is the Gaussian sum in $K$. Then

$$Z(b) = \frac{r}{q} + \frac{r}{q\left(q^k - 1\right)} \sum_{\psi \in J} \psi\left(\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right) G\left(\psi^{'}, \lambda_b^{'}\right) \tag{2.10}$$

Now let us consider the case where $b = 0$. Then $\lambda_0^{'}(c) = 1$ is the trivial additive character of $K$. Then if $\psi^{'}$ is trivial,

$$G\left(\psi^{'}, \lambda_b^{'}\right) = \sum_{c \in K^*} \psi^{'}(c)\lambda_b^{'}(c) = q - 1$$

If $\psi^{'}$ is nontrivial,

$$G\left(\psi^{'}, \lambda_b^{'}\right) = \sum_{c \in K^*} \psi^{'}(c) = 0 \qquad \text{(By the relation (1.13))}$$

So let $A \subseteq J$ such that for $\psi \in A$, $\psi^{'}$ is trivial. Then for every $\psi \in A$
$G\left(\psi^{'}, \lambda_b^{'}\right) = q - 1$ and for every $\psi \in J \setminus A$, $G\left(\psi^{'}, \lambda_b^{'}\right) = 0$
Then $Z(0) = \frac{r}{q} + \frac{(q-1)r}{q\left(q^k-1\right)} \sum_{\psi \in A} \psi\left(\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right)$ (By (2.10))

$$Z(0) = \frac{r}{q} + \frac{(q-1)\,r}{q\left(q^k - 1\right)} \left[\psi^*\left(\theta\right) G\left(\overline{\psi^*}, \overline{\lambda}\right) + \sum_{\psi \in A}^{*} \psi\left(\theta\right) G\left(\overline{\psi}, \overline{\lambda}\right)\right] \tag{2.11}$$

[Note: $\psi^*$ is the trivial multiplicative character and the asterix on the summation symbol indicates that the trivial multiplicative character is deleted from the range of summation.]

$$\begin{aligned}
G\left(\overline{\psi^*}, \overline{\lambda}\right) &= \sum_{c \in F^*} \overline{\psi^*}(c)\overline{\lambda}(c) \\
&= \sum_{c \in F^*} \overline{\lambda}(c) \\
&= \sum_{c \in F} \overline{\lambda}(c) - \overline{\lambda}(0) \\
&= \sum_{c \in F} \overline{\lambda}(c) - 1 \\
&= -1 \qquad \left(\text{Since} \sum_{c \in F} \overline{\lambda}(c) = 0\right)
\end{aligned}$$

Then by (2.11),

$$Z(0)=\frac{r}{q}+\frac{(q-1)\,r}{q\,(q^k-1)}\left[-1+\sum_{\psi\in A}^{*}\psi\,(\theta)\,G\left(\overline{\psi},\overline{\lambda}\right)\right]$$

Then

$$Z(0)-\frac{\left(q^{k-1}-1\right)r}{q^k-1}=\frac{(q-1)\,r}{q\,(q^k-1)}\sum_{\psi\in A}^{*}\psi\,(\theta)\,G\left(\overline{\psi},\overline{\lambda}\right)$$

$$\begin{aligned}\left|Z(0)-\frac{\left(q^{k-1}-1\right)r}{q^k-1}\right| &= \left|\frac{(q-1)\,r}{q\,(q^k-1)}\sum_{\psi\in A}^{*}\psi\,(\theta)\,G\left(\overline{\psi},\overline{\lambda}\right)\right| \qquad (2.12)\\ &\le \frac{(q-1)\,r}{q\,(q^k-1)}\sum_{\psi\in A}^{*}|\psi\,(\theta)|\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|\\ &= \frac{(q-1)\,r}{q\,(q^k-1)}\,(|A|-1)\,q^{k/2}\end{aligned}$$

(By Theorem 1.5.1, $\psi_0\notin A^*$ and $\lambda\neq\lambda_0\Rightarrow|G\,(\psi,\lambda)|=q^{k/2}$ )

Let $H$ be the smallest subgroup of $F^*$ which contains $\alpha$ and $K^*$.

O($\alpha$)=$r$ in $F^*$

[Since $\text{ord}(m(x))=r$, then $x^r-1=p(x)m(x)$ for some $p(x)\in K[x]$. Then $\alpha^r-1=0$ (Since $m(\alpha)=0$).Then $\alpha^r=1$. If O($\alpha$)=$r_1<r$. Then $\alpha^{r_1}=1\Rightarrow\alpha^{r_1}-1=0$. Then $\alpha$ is a root of $x^{r_1}-1$. Therefore $m(x)/x^{r_1-1}$. Therefore $\text{ord}(m(x))=r_1$, which is a contradiction.]

The multiplicative group $F^*$ is cyclic. Then $|H|=h=l.c.m(r,q-1)$.

[Note: $H$ is the subgroup generated by $K^*$ and $\alpha$]

Furthermore, if $\psi\in A$ iff $\psi\,(\beta)$ for every $\beta\in H$.

[ Proof: $\Rightarrow$ Let $\psi\in A$. Then $\psi_{/_{K^*}}=1$ and $\psi(\alpha)=1$. Let $\beta\in H$. Then $\beta=\alpha_1^{\epsilon_1},\alpha_2^{\epsilon_2}\ldots,\alpha_k^{\epsilon_k},\alpha_i\in K^*\cup\{\alpha\}$

$\Rightarrow\psi\,(\beta)=\psi\,(\alpha_1)^{\epsilon_1}\,\psi\,(\alpha_2)^{\epsilon_2}\ldots\psi\,(\alpha_k)^{\epsilon_k}=1\Leftarrow$ Suppose $\psi(\beta)=1$ for every $\beta\in H$. Then for every $k\in K^*$, $\psi(k)=1$ and $\psi(\alpha)=1$. Hence $\psi\in A$.]

So $A$ is the annihilator of $H$ in $(F^*)^\wedge$.

$$\Rightarrow \qquad |A| = \frac{|F^*|}{|H|} = \frac{q^k-1}{h}$$

By (2.12),

$$\left|Z(0) - \frac{\left(q^{k-1}\right) r}{q^k}\right| \leq \frac{(q-1)\, r}{q\,(q^k-1)} \left(\frac{q^k-1}{h} - 1\right) q^{k/2}$$
$$= \frac{(q-1)\, r}{q} \left(\frac{1}{h} - \frac{1}{q^k-1}\right) q^{k/2}$$
$$= \left(1 - \frac{1}{q}\right) \left(\frac{r}{h} - \frac{r}{q^k-1}\right) q^{k/2}.$$

Now suppose $b \neq 0$.

By (2.10),

$$Z(b) = \frac{r}{q} + \frac{r}{q\,(q^k-1)} \sum_{\psi \in J} \psi\,(\theta)\, G\left(\overline{\psi}, \overline{\lambda}\right) G\left(\psi' \lambda_b'\right) \quad \text{where } \lambda_b' \text{ is a nontrivial.}$$
$$= \frac{r}{q} + \frac{r}{q\,(q^k-1)} \left(\psi^*\,(\theta)\, G\left(\overline{\psi^*}, \overline{\lambda}\right) G\left(\psi'^*, \lambda_b'\right) + \sum_{\psi \in J}^{*} \psi\,(\theta)\, G\left(\overline{\psi}, \overline{\lambda}\right) G\left(\psi', \lambda_b'\right)\right)$$

[Previously, $G\left(\overline{\psi^*}, \overline{\lambda}\right) = -1$

$$G\left(\psi^{*'}, \lambda_b'\right) = \sum_{c \in K^*} \psi^{*'}(c) \lambda_b'(c)$$
$$= \sum_{c \in K^*} \lambda_b'(c)$$
$$= \sum_{c \in K} \lambda_b'(c) - \lambda_b(0)$$
$$= -1$$

$$\Rightarrow \psi^*\,(\theta)\, G\left(\overline{\psi^*}, \overline{\lambda}\right) G\left(\psi'^*, \lambda_b'\right) = 1 \qquad ]$$

So

$$Z(b)=\frac{r}{q}+\frac{r}{q\left(q^{k}-1\right)}+\frac{r}{q\left(q^{k}-1\right)}\sum_{\psi\in J}^{*}\psi\left(\theta\right)G\left(\overline{\psi},\overline{\lambda}\right)G\left(\psi^{'},\lambda_{b}^{'}\right)$$

$$\Rightarrow Z(b)-\frac{q^{k-1}r}{q^{k}-1}=\frac{r}{q\left(q^{k}-1\right)}\sum_{\psi\in J}^{*}\psi\left(\theta\right)G\left(\overline{\psi},\overline{\lambda}\right)G\left(\psi^{'},\lambda_{b}^{'}\right)$$

It was found earlier that if $\psi^{'}$ is trivial then $G\left(\psi^{'},\lambda_{b}^{'}\right)=-1$ and $\left|G\left(\psi^{'},\lambda_{b}^{'}\right)\right|=q^{1/2}$ if $\psi^{'}$ is non trivial.

$$\begin{aligned}\left|Z(b)-\frac{q^{k-1}r}{q^{k}-1}\right| &\leq \frac{r}{q\left(q^{k}-1\right)}\sum_{\psi\in J}^{*}\left|\psi\left(\theta\right)\right|\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|\left|G\left(\psi^{'},\lambda_{b}^{'}\right)\right|\\ &=\frac{r}{q\left(q^{k}-1\right)}\left[\sum_{\psi\in A}^{*}\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|\left|G\left(\psi^{'},\lambda_{b}^{'}\right)\right|+\sum_{\psi\in J\setminus A}^{*}\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|\left|G\left(\psi^{'},\lambda_{b}^{'}\right)\right|\right]\\ &=\frac{r}{q\left(q^{k}-1\right)}\left[\sum_{\psi\in A}^{*}\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|+\sum_{\psi\in J\setminus A}^{*}\left|G\left(\overline{\psi},\overline{\lambda}\right)\right|\left(q^{1/2}\right)\right]\\ &=\frac{r}{q\left(q^{k}-1\right)}\left[\left(\left|A\right|-1\right)q^{k/2}+\left(\left|J\right|-\left|A\right|\right)q^{1/2}q^{k/2}\right]\\ &=\frac{r}{\left(q^{k}-1\right)}\left[\left|A\right|-1+\left(\left|J\right|-\left|A\right|\right)q^{1/2}\right]q^{k/2-1}\end{aligned}$$

$J$ is the annihilator of the subgroup generated by $\alpha$ (in $F^{*}$) in $\left(F^{*}\right)^{\wedge}$. Then

$$\left|J\right|=\frac{\left(q^{k}-1\right)}{r}=\frac{\left|F^{*}\right|}{\left|\alpha\right|}.$$

Then

$$\begin{aligned}\left|Z(b)-\frac{q^{k-1}r}{q^{k}-1}\right| &\leq \frac{r}{\left(q^{k}-1\right)}\left[\left(\frac{q^{k}-1}{h}-1\right)+\left(\frac{q^{k}-1}{r}-\frac{\left(q^{k}-1\right)}{h}\right)q^{1/2}\right]q^{k/2-1}\\ &=\left[\frac{r}{h}-\frac{r}{q^{k}-1}+\frac{h-r}{h}q^{1/2}\right]q^{k/2-1}.\end{aligned}$$

□

These bounds are only useful for large $r$. For instance, if $q=2$ , $k=10$ and the least period $r=33$, we get

$$\left|Z(0)-16.48\right|\leq 15.48$$

$\Rightarrow 1 \leq Z(0) \leq 31$

In this case, the sequence has atleast one 0 and atleast two 1's which is trivially true. By other means (see [1]) one can show $11 \leq Z(0) \leq 21$.

# CHAPTER 3

# THE NUMBER OF ZEROS OF SOME LINEAR RECCURENCE SEQUENCES

Here we present some results obtained by a Maple program written to determine the number of zeros which occur in a full period of a linear recurrence sequence based on an irreducible polynomial. We will discuss the monic irreducible polynomials of degree 8 and order 85, degree 9 and order 73 and finally, degree 10 and order 93. (Refer to the Appendix for the MAPLE codes). All the polynomials considered here are over the finite field of order 2.

First we do the monic irreducible polynomials of degree 8 and order 85. The list of all monic irreducible polynomials of degree 8 which are of order 85 are as follows:

P1=$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$

P2=$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$

P3=$x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$

P4=$x^8 + x^7 + x^3 + x + 1$

P5=$x^8 + x^7 + x^5 + x + 1$

P6=$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$

P7=$x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$

P8=$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$

We computed the number of zeros in the sequences based on the polynomials P1, P2, P3, P4, P5, P6, P7 and P8 for every possible initial sequence. (See Appendix I-VIII). We obtained only two values for $Z(0)$, namely 37 and 45. According to Theorem 2.0.7, $Z(0)$ should satisfy the following condition.

$$\left| Z(0) - \frac{(q^{k-1}-1)r}{q^k - 1} \right| \leq \left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^k - 1}\right) q^{k/2}.$$

Since all the irreducible polynomials considereded here are over $\mathbb{F}_2$, the $q$ in Theorem 2.0.7, is equal to 2. Also by Theorem 2.0.6, $r$ is equal to the order of the irreducible polynomial, which is 85 in this case. The least common multiple of $r$ and $q-1$ is equal to $r$ since $q=2$. Hence $h$ in this case will be equal to 85. Since the degree of the irreducible polynomials is 8, $k=8$. Therefore $\frac{(q^{k-1}-1)r}{q^k-1} = 42.3333.....$ Also $\left(1-\frac{1}{q}\right)\left(\frac{r}{h}-\frac{r}{q^k-1}\right)q^{k/2} = 5.3333.....$

So

$$|Z(0) - 42.333...| \leq 5.333...$$

$$\Rightarrow 37 \leq Z(0) \leq 48.$$

Since all the $Z(0)$s are within these bounds, this verifies the Theorem 2.0.7.

The other main observation of these results is for every monic irreducible polynomial of degree 8 and order 85, $Z(0)$ can take only two values for every possible initial sequence. That is for each one of the $2^8-1=255$ initial sequences $s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7$, the only possible values for $Z(0)$ are 37 and 45. As a partial explanation we will prove that all 8th order linear recurrences of least period 85 can have at most 3 values for $Z(0)$. (See [1])

Let $f$ be an irreducible polynomial (over $\mathbb{Z}_2$) of degree 8 and order 85. By the Theorem 2.0.5, a linear recurrence sequence based on $f$ has the form,

$$s_n = \mathrm{Tr}(\theta\beta^n) \qquad n = 1, 2, ..., 85$$

where $\beta$ is a root of $f$ and $\theta \in \mathbb{F}_{2^8}^*$. There are $2^8-1=255$ many initial sequences $s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7$, where $(s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7,) \neq (0,0,0,0,0,0,0,0)$ and 255 many $\theta$. Then there exist a bijection between the initial values and $\theta$s. Let this sequence of $s_n$ be called *S($\theta, f$)*. Fix a primitive element $\alpha$ in $\mathbb{F}_{2^8}^*$. Since $\beta$ has order 85 in the cyclic group $\mathbb{F}_{2^8}^*$, we can write $\beta = \alpha^{3k}$ for some $k$ relatively prime to 85. Also $\theta = \alpha^t$ for some $t$ such that $1 \leq t \leq 255$. Then *S($\theta, f$)* consists of the traces of

$$T(\theta, f) = \{\alpha^t \alpha^{3kn} : n = 1, 2, ..., 85\}.$$

To determine the $Z(0)$s, the order of the terms in the sequence is not important. We only need to know the number of elements in $T(\theta, f)$ that have the trace equal to zero.

**Theorem 3.0.8.** *Let $f, g \in \mathbb{Z}_2[x]$ be irreducible polnomials of degree 8 and order 85. Let $\theta_1 = \alpha^t$ and $\theta_2 = \alpha^s$. If $t \equiv s \pmod 3$ then $T(\theta_1, f)$= $T(\theta_2, g)$ and so*

$$Z_{S(\theta_1,f)}(0) = Z_{S(\theta_2,g)}(0).$$

*Proof.* Let $\beta_1 = \alpha^{3k}$ be a root of $f$ and $\beta_2 = \alpha^{3l}$ be a root of $g$. Note that ($k$, 85)=1 and ($l$, 85)=1. Pick $n$ such that $1 \leq n \leq 85$. Set $r = (t - s)/3$. Set $m = l^{-1}(r + kn)$ (mod 85). ($l^{-1}$ exists as ($l$, 85)=1.)

Then

$$ml \equiv r + kn \pmod{85}$$

$$3ml \equiv 3r + 3kn \pmod{255}$$

$$3ml \equiv t - s + 3kn \pmod{255}$$

$$s + 3ml \equiv t + 3kn \pmod{255}$$

$$\alpha^{s+3ml} = \alpha^{t+3kn}$$

$$\theta_2\beta_2^m = \theta_1\beta_1^n.$$

Therefore $T(\theta_1, f) \subset T(\theta_2, g)$. The reverse inclusion can also be proved by a similar argument. This completes the proof. □

**Corollary** *Over all 8th order linear recurrences $S$ of least period 85, there are at most 3 values for $Z(0)$.*

*Proof.* Let $f$ be a irreducible polynomial of degree 8 and order 85. For $i$ = 0, 1, 2, set $S_i = S(\alpha^i, f)$. Let $S = S(\theta, g)$ be any sequence. Let $\theta = \alpha^t$. Then there exist an $i$ such that $i = 0, 1, 2$ such that $t \equiv i \pmod 3$. Then by Theorem 3.0.8, $Z_S(0) = Z_{S_i}(0)$. □

Now we will discuss the monic irreducible polynomials of degree 9 and order 93. The list of all monic irreducible polynomials of degree 9 which are of order 73 are as follows:

Q1=$x^9 + x + 1$

Q2=$x^9 + x^4 + x^2 + x + 1$

Q3=$x^9 + x^6 + x^3 + x + 1$

Q4=$x^9 + x^6 + x^5 + x^2 + 1$

Q5=$x^9 + x^7 + x^4 + x^3 + 1$

Q6=$x^9 + x^8 + 1$

Q7=$x^9 + x^8 + x^6 + x^3 + 1$

Q8=$x^9 + x^8 + x^7 + x^5 + 1$

Table 3.1 presents all the above given monic irreducible polynomials of degree 9 and order 73 and the last five columns give the corresponding values of the number of zeros for each different initial sequence. (Note that each initial sequence given here represents the order of $s_0\ s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8$.)

| polynomial | 111000000 | 111111111 | 101010101 | 100000000 | 100000011 |
|---|---|---|---|---|---|
| Q1 | 45 | 45 | 45 | 45 | 37 |
| Q2 | 37 | 33 | 37 | 33 | 33 |
| Q3 | 45 | 33 | 33 | 45 | 33 |
| Q4 | 33 | 33 | 33 | 37 | 37 |
| Q5 | 37 | 33 | 33 | 37 | 37 |
| Q6 | 37 | 45 | 45 | 45 | 45 |
| Q7 | 33 | 33 | 33 | 45 | 37 |
| Q8 | 33 | 33 | 37 | 33 | 37 |

Table 3.1.

Table 3.1 shows that the number of zeros for every polynomial considered here have taken only three values, which are 33, 37 and 45, in all cases of initial sequences that are taken into consideration. According to Theorem 2.0.7, $Z(0)$ should satisfy the following condition.

$$\left|Z(0) - \frac{(q^{k-1}-1)r}{q^k-1}\right| \leq \left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^k-1}\right) q^{k/2}.$$

Since all the irreducible polynomials considereded here are over $\mathbb{F}_2$, the $q$ in Theorem 2.0.7, is equal to 2. Also by Theorem 2.0.6, $r$ is equal to the order of the irreducible polynomial, which is 73 in this case. The least common multiple of $r$ and $q-1$ is equal to $r$ since $q = 2$. Hence $h$ in this case will be equal to 73. Since the degree of the irreducible polynomials in Table 3.2 is 9, $k = 9$. Therefore $\frac{(q^{k-1}-1)r}{q^k-1} = 36.428571.....$ Also $\left(1 - \frac{1}{q}\right)\left(\frac{r}{h} - \frac{r}{q^k-1}\right) q^{k/2} = 9.6975.$

So

$$|Z(0) - 36.428571...| \leq 9.6975$$

$$\Rightarrow 26.73107... \leq Z(0) \leq 46.12607....$$

Since the $Z(0)$s in Table 3.1 are within these bounds, this verifies the Theorem 2.0.7.

Finally, we will consider the set of all the monic irreducible polynomials of degree 10 and order 93 which are given as follows:

R1=$x^{10} + x^5 + x^4 + x^2 + 1$

R2=$x^{10} + x^8 + x^3 + x + 1$

R3=$x^{10} + x^8 + x^6 + x^5 + 1$

R4=$x^{10} + x^9 + x^7 + x^2 + 1$

R5=$x^{10} + x^9 + x^7 + x^5 + x^2 + x + 1$

R6=$x^{10} + x^9 + x^8 + x^5 + x^3 + x + 1$

Table 3.2 gives all the above given monic irreducible polynomials of degree 10 and order 93 and the last five columns give the corresponding values of the number of zeros for each different initial sequence. (Note that each initial sequence given here represents the order of $s_0\ s_1\ s_2\ s_3\ s_4\ s_5\ s_6\ s_7\ s_8\ s_9$.)

| polynomial | 1101000001 | 1111111111 | 1010101010 | 1000000000 | 1000000111 |
|---|---|---|---|---|---|
| R1 | 45 | 45 | 45 | 61 | 45 |
| R2 | 61 | 45 | 45 | 45 | 45 |
| R3 | 45 | 45 | 45 | 61 | 45 |
| R4 | 61 | 45 | 45 | 45 | 45 |
| R5 | 45 | 45 | 45 | 45 | 45 |
| R6 | 61 | 45 | 45 | 45 | 45 |

Table 3.2.

Table 3.2 shows that the number of zeros for every polynomial considered here have taken two values, which are 45 and 61, in all cases of initial sequences that are taken into consideration. According to Theorem 2.0.7, $Z(0)$ should satisfy the following condition.

$$\left|Z(0) - \frac{(q^{k-1}-1)r}{q^k-1}\right| \leq \left(1-\frac{1}{q}\right)\left(\frac{r}{h}-\frac{r}{q^k-1}\right)q^{k/2}.$$

Since all the irreducible polynomials considereded here are over $\mathbb{F}_2$, the $q$ in Theorem 2.0.7, is equal to 2. Also by Theorem 2.0.6, $r$ is equal to the order of the irreducible polynomial, which is 93 in this case. The least common multiple of $r$ and $q-1$ is equal to $r$ since $q = 2$. Hence $h$ in this case will be equal to 93. Since the degree of the irreducible polynomials in Table 3.2 is 10, $k = 10$. Therefore $\frac{(q^{k-1}-1)r}{q^k-1} = 46.4545.....$ Also $\left(1-\frac{1}{q}\right)\left(\frac{r}{h}-\frac{r}{q^k-1}\right)q^{k/2} = 14.5454....$

So

$$|Z(0) - 46.4545...| \leq 14.5454...$$

$$\Rightarrow 32 \leq Z(0) \leq 61.$$

Since the $Z(0)$s in Table 3.2 are within these bounds, this verifies the Theorem 2.0.7.

## REFERENCES

[1] Fitzgerald, R. Notes on Finite fields, Unpublished.

[2] Lidl, R. and Niederreiter, H. , *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1994.

# APPENDICES

APPENDIX I

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P1 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-3]+s[m-4]+s[m-5]+s[m-6]+s[m-7]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
        [0, 1, 0, 0, 0, 0, 0, 0, 45]
        [1, 1, 0, 0, 0, 0, 0, 0, 45]
        [0, 0, 1, 0, 0, 0, 0, 0, 45]
        [1, 0, 1, 0, 0, 0, 0, 0, 45]
        [0, 1, 1, 0, 0, 0, 0, 0, 45]
        [1, 1, 1, 0, 0, 0, 0, 0, 37]
        [0, 0, 0, 1, 0, 0, 0, 0, 45]
        [1, 0, 0, 1, 0, 0, 0, 0, 45]
        [0, 1, 0, 1, 0, 0, 0, 0, 45]
        [1, 1, 0, 1, 0, 0, 0, 0, 37]
        [0, 0, 1, 1, 0, 0, 0, 0, 45]
        [1, 0, 1, 1, 0, 0, 0, 0, 37]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 37]

[0, 0, 0, 0, 1, 0, 0, 0, 37]

[1, 0, 0, 0, 1, 0, 0, 0, 45]

[0, 1, 0, 0, 1, 0, 0, 0, 45]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 37]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 37]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 45]

[0, 1, 1, 1, 1, 0, 0, 0, 37]

[1, 1, 1, 1, 1, 0, 0, 0, 37]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 37]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 45]

[0, 0, 1, 0, 0, 1, 0, 0, 45]

[1, 0, 1, 0, 0, 1, 0, 0, 45]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 37]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 45]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 37]

[1, 1, 1, 1, 0, 1, 0, 0, 45]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 37]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 37]

[1, 1, 1, 0, 1, 1, 0, 0, 37]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 45]

[1, 1, 0, 1, 1, 1, 0, 0, 45]

[0, 0, 1, 1, 1, 1, 0, 0, 37]

[1, 0, 1, 1, 1, 1, 0, 0, 45]

[0, 1, 1, 1, 1, 1, 0, 0, 45]

[1, 1, 1, 1, 1, 1, 0, 0, 37]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 37]

[0, 1, 0, 0, 0, 0, 1, 0, 37]

[1, 1, 0, 0, 0, 0, 1, 0, 37]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 45]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 45]

[1, 0, 0, 1, 0, 0, 1, 0, 45]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 37]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 37]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 45]

[0, 0, 1, 0, 1, 0, 1, 0, 37]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 45]

[0, 0, 1, 1, 1, 0, 1, 0, 45]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 45]

[1, 1, 1, 1, 1, 0, 1, 0, 45]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 45]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 37]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 37]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 45]

[1, 0, 1, 1, 0, 1, 1, 0, 37]

[0, 1, 1, 1, 0, 1, 1, 0, 37]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 37]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 45]

[0, 0, 1, 0, 1, 1, 1, 0, 37]

[1, 0, 1, 0, 1, 1, 1, 0, 45]

[0, 1, 1, 0, 1, 1, 1, 0, 45]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 45]

[1, 0, 0, 1, 1, 1, 1, 0, 37]

[0, 1, 0, 1, 1, 1, 1, 0, 45]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 45]

[1, 0, 1, 1, 1, 1, 1, 0, 37]

[0, 1, 1, 1, 1, 1, 1, 0, 45]

[1, 1, 1, 1, 1, 1, 1, 0, 37]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 37]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 37]

[0, 1, 1, 0, 0, 0, 0, 1, 37]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 37]

[1, 0, 0, 1, 0, 0, 0, 1, 45]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 45]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 45]

[0, 1, 1, 1, 0, 0, 0, 1, 45]

[1, 1, 1, 1, 0, 0, 0, 1, 37]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 45]

[0, 1, 0, 0, 1, 0, 0, 1, 45]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 37]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 45]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 37]

[1, 1, 0, 1, 1, 0, 0, 1, 37]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 45]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 45]

[0, 0, 0, 0, 0, 1, 0, 1, 37]

[1, 0, 0, 0, 0, 1, 0, 1, 37]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 37]

[0, 0, 1, 0, 0, 1, 0, 1, 45]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 37]

[1, 1, 1, 0, 0, 1, 0, 1, 45]

[0, 0, 0, 1, 0, 1, 0, 1, 37]

[1, 0, 0, 1, 0, 1, 0, 1, 45]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 45]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 45]

[0, 1, 0, 0, 1, 1, 0, 1, 37]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 45]

[1, 1, 1, 0, 1, 1, 0, 1, 37]

[0, 0, 0, 1, 1, 1, 0, 1, 37]

[1, 0, 0, 1, 1, 1, 0, 1, 45]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 37]

[0, 0, 1, 1, 1, 1, 0, 1, 45]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 37]

[1, 1, 1, 1, 1, 1, 0, 1, 45]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 45]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 37]

[1, 0, 1, 0, 0, 0, 1, 1, 45]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 37]

[1, 1, 0, 1, 0, 0, 1, 1, 45]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 37]

[0, 1, 1, 1, 0, 0, 1, 1, 45]

[1, 1, 1, 1, 0, 0, 1, 1, 45]

[0, 0, 0, 0, 1, 0, 1, 1, 37]

[1, 0, 0, 0, 1, 0, 1, 1, 37]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 37]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 45]

[0, 0, 0, 1, 1, 0, 1, 1, 45]

[1, 0, 0, 1, 1, 0, 1, 1, 37]

[0, 1, 0, 1, 1, 0, 1, 1, 45]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 37]

[1, 0, 1, 1, 1, 0, 1, 1, 37]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 37]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 45]

[0, 1, 1, 0, 0, 1, 1, 1, 37]

[1, 1, 1, 0, 0, 1, 1, 1, 45]

[0, 0, 0, 1, 0, 1, 1, 1, 37]

[1, 0, 0, 1, 0, 1, 1, 1, 37]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 45]

[0, 0, 1, 1, 0, 1, 1, 1, 37]

[1, 0, 1, 1, 0, 1, 1, 1, 45]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 45]

[1, 0, 0, 0, 1, 1, 1, 1, 45]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 37]

[0, 0, 1, 0, 1, 1, 1, 1, 37]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 45]

[1, 0, 0, 1, 1, 1, 1, 1, 45]

[0, 1, 0, 1, 1, 1, 1, 1, 37]

[1, 1, 0, 1, 1, 1, 1, 1, 37]

[0, 0, 1, 1, 1, 1, 1, 1, 45]

[1, 0, 1, 1, 1, 1, 1, 1, 37]

[0, 1, 1, 1, 1, 1, 1, 1, 37]

[1, 1, 1, 1, 1, 1, 1, 1, 37]

APPENDIX II

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P2 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-2]+s[m-3]+s[m-4]+s[m-6]+s[m-7]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 37]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 37]
    [0, 1, 1, 0, 0, 0, 0, 0, 45]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 37]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 37]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 45]

[0, 1, 0, 0, 1, 0, 0, 0, 45]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 37]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 37]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 37]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 37]

[0, 1, 1, 1, 1, 0, 0, 0, 45]

[1, 1, 1, 1, 1, 0, 0, 0, 37]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 37]

[0, 0, 1, 0, 0, 1, 0, 0, 45]

[1, 0, 1, 0, 0, 1, 0, 0, 45]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 37]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 45]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 45]

[1, 1, 1, 1, 0, 1, 0, 0, 37]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 45]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 37]

[1, 1, 1, 0, 1, 1, 0, 0, 37]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 37]

[1, 1, 0, 1, 1, 1, 0, 0, 37]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 45]

[0, 1, 1, 1, 1, 1, 0, 0, 37]

[1, 1, 1, 1, 1, 1, 0, 0, 45]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 37]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 37]

[1, 0, 0, 1, 0, 0, 1, 0, 45]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 45]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 37]

[1, 1, 0, 0, 1, 0, 1, 0, 45]

[0, 0, 1, 0, 1, 0, 1, 0, 37]

[1, 0, 1, 0, 1, 0, 1, 0, 37]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 45]

[0, 0, 1, 1, 1, 0, 1, 0, 37]

[1, 0, 1, 1, 1, 0, 1, 0, 45]

[0, 1, 1, 1, 1, 0, 1, 0, 37]

[1, 1, 1, 1, 1, 0, 1, 0, 45]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 45]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 45]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 45]

[1, 0, 1, 1, 0, 1, 1, 0, 37]

[0, 1, 1, 1, 0, 1, 1, 0, 37]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 37]

[1, 0, 0, 0, 1, 1, 1, 0, 45]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 37]

[0, 0, 1, 0, 1, 1, 1, 0, 37]

[1, 0, 1, 0, 1, 1, 1, 0, 37]

[0, 1, 1, 0, 1, 1, 1, 0, 45]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 37]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 45]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 37]

[1, 0, 1, 1, 1, 1, 1, 0, 45]

[0, 1, 1, 1, 1, 1, 1, 0, 37]

[1, 1, 1, 1, 1, 1, 1, 0, 45]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 37]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 45]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 37]

[0, 0, 0, 1, 0, 0, 0, 1, 45]

[1, 0, 0, 1, 0, 0, 0, 1, 45]

[0, 1, 0, 1, 0, 0, 0, 1, 37]

[1, 1, 0, 1, 0, 0, 0, 1, 45]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 37]

[0, 1, 1, 1, 0, 0, 0, 1, 37]

[1, 1, 1, 1, 0, 0, 0, 1, 45]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 37]

[0, 1, 0, 0, 1, 0, 0, 1, 45]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 45]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 45]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 37]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 37]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 45]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 37]

[0, 0, 1, 0, 0, 1, 0, 1, 37]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 45]

[1, 1, 1, 0, 0, 1, 0, 1, 45]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 37]

[0, 1, 0, 1, 0, 1, 0, 1, 37]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 37]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 45]

[0, 1, 0, 0, 1, 1, 0, 1, 45]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 45]

[1, 1, 1, 0, 1, 1, 0, 1, 37]

[0, 0, 0, 1, 1, 1, 0, 1, 37]

[1, 0, 0, 1, 1, 1, 0, 1, 37]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 45]

[0, 0, 1, 1, 1, 1, 0, 1, 37]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 45]

[1, 1, 1, 1, 1, 1, 0, 1, 37]

[0, 0, 0, 0, 0, 0, 1, 1, 37]

[1, 0, 0, 0, 0, 0, 1, 1, 45]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 37]

[0, 0, 1, 0, 0, 0, 1, 1, 45]

[1, 0, 1, 0, 0, 0, 1, 1, 37]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 45]

[1, 1, 0, 1, 0, 0, 1, 1, 45]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 37]

[0, 1, 1, 1, 0, 0, 1, 1, 37]

[1, 1, 1, 1, 0, 0, 1, 1, 45]

[0, 0, 0, 0, 1, 0, 1, 1, 45]

[1, 0, 0, 0, 1, 0, 1, 1, 37]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 45]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 45]

[1, 0, 0, 1, 1, 0, 1, 1, 45]

[0, 1, 0, 1, 1, 0, 1, 1, 45]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 37]

[1, 0, 1, 1, 1, 0, 1, 1, 37]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 37]

[0, 0, 0, 0, 0, 1, 1, 1, 37]

[1, 0, 0, 0, 0, 1, 1, 1, 37]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 45]

[0, 1, 1, 0, 0, 1, 1, 1, 37]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 37]

[1, 0, 0, 1, 0, 1, 1, 1, 45]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 45]

[1, 0, 1, 1, 0, 1, 1, 1, 45]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 37]

[1, 0, 0, 0, 1, 1, 1, 1, 37]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 37]

[0, 0, 1, 0, 1, 1, 1, 1, 45]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 45]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 37]

[1, 0, 0, 1, 1, 1, 1, 1, 37]

[0, 1, 0, 1, 1, 1, 1, 1, 45]

[1, 1, 0, 1, 1, 1, 1, 1, 45]

[0, 0, 1, 1, 1, 1, 1, 1, 37]

[1, 0, 1, 1, 1, 1, 1, 1, 45]

[0, 1, 1, 1, 1, 1, 1, 1, 45]

[1, 1, 1, 1, 1, 1, 1, 1, 45]

APPENDIX III

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P3 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-2]+s[m-3]+s[m-4]+s[m-5]+s[m-7]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 45]
    [0, 1, 1, 0, 0, 0, 0, 0, 45]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 45]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 45]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 45]

[0, 1, 0, 0, 1, 0, 0, 0, 45]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 37]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 37]

[1, 1, 0, 1, 1, 0, 0, 0, 45]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 45]

[0, 1, 1, 1, 1, 0, 0, 0, 37]

[1, 1, 1, 1, 1, 0, 0, 0, 45]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 37]

[0, 0, 1, 0, 0, 1, 0, 0, 37]

[1, 0, 1, 0, 0, 1, 0, 0, 45]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 37]

[0, 1, 0, 1, 0, 1, 0, 0, 45]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 45]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 37]

[1, 1, 1, 1, 0, 1, 0, 0, 37]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 37]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 37]

[1, 1, 1, 0, 1, 1, 0, 0, 45]

[0, 0, 0, 1, 1, 1, 0, 0, 37]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 45]

[1, 1, 0, 1, 1, 1, 0, 0, 37]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 37]

[0, 1, 1, 1, 1, 1, 0, 0, 45]

[1, 1, 1, 1, 1, 1, 0, 0, 45]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 37]

[1, 1, 1, 0, 0, 0, 1, 0, 45]

[0, 0, 0, 1, 0, 0, 1, 0, 37]

[1, 0, 0, 1, 0, 0, 1, 0, 37]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 37]

[0, 1, 1, 1, 0, 0, 1, 0, 37]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 37]

[0, 0, 1, 0, 1, 0, 1, 0, 45]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 37]

[0, 0, 1, 1, 1, 0, 1, 0, 37]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 37]

[1, 1, 1, 1, 1, 0, 1, 0, 45]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 37]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 37]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 37]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 37]

[0, 0, 1, 1, 0, 1, 1, 0, 37]

[1, 0, 1, 1, 0, 1, 1, 0, 37]

[0, 1, 1, 1, 0, 1, 1, 0, 45]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 37]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 37]

[0, 0, 1, 0, 1, 1, 1, 0, 37]

[1, 0, 1, 0, 1, 1, 1, 0, 45]

[0, 1, 1, 0, 1, 1, 1, 0, 37]

[1, 1, 1, 0, 1, 1, 1, 0, 45]

[0, 0, 0, 1, 1, 1, 1, 0, 45]

[1, 0, 0, 1, 1, 1, 1, 0, 37]

[0, 1, 0, 1, 1, 1, 1, 0, 37]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 45]

[1, 0, 1, 1, 1, 1, 1, 0, 45]

[0, 1, 1, 1, 1, 1, 1, 0, 45]

[1, 1, 1, 1, 1, 1, 1, 0, 45]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 45]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 45]

[1, 0, 0, 1, 0, 0, 0, 1, 45]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 37]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 37]

[0, 1, 1, 1, 0, 0, 0, 1, 45]

[1, 1, 1, 1, 0, 0, 0, 1, 37]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 37]

[0, 1, 0, 0, 1, 0, 0, 1, 37]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 37]

[1, 0, 1, 0, 1, 0, 0, 1, 45]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 37]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 37]

[0, 0, 1, 1, 1, 0, 0, 1, 37]

[1, 0, 1, 1, 1, 0, 0, 1, 37]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 45]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 45]

[0, 0, 1, 0, 0, 1, 0, 1, 37]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 37]

[1, 1, 1, 0, 0, 1, 0, 1, 37]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 45]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 37]

[0, 1, 1, 1, 0, 1, 0, 1, 37]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 37]

[0, 1, 0, 0, 1, 1, 0, 1, 37]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 37]

[0, 1, 1, 0, 1, 1, 0, 1, 37]

[1, 1, 1, 0, 1, 1, 0, 1, 37]

[0, 0, 0, 1, 1, 1, 0, 1, 45]

[1, 0, 0, 1, 1, 1, 0, 1, 37]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 45]

[0, 0, 1, 1, 1, 1, 0, 1, 37]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 45]

[1, 1, 1, 1, 1, 1, 0, 1, 45]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 45]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 45]

[1, 0, 1, 0, 0, 0, 1, 1, 37]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 37]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 37]

[1, 1, 0, 1, 0, 0, 1, 1, 37]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 37]

[1, 1, 1, 1, 0, 0, 1, 1, 45]

[0, 0, 0, 0, 1, 0, 1, 1, 45]

[1, 0, 0, 0, 1, 0, 1, 1, 45]

[0, 1, 0, 0, 1, 0, 1, 1, 37]

[1, 1, 0, 0, 1, 0, 1, 1, 37]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 37]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 37]

[1, 0, 0, 1, 1, 0, 1, 1, 37]

[0, 1, 0, 1, 1, 0, 1, 1, 37]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 45]

[1, 0, 1, 1, 1, 0, 1, 1, 45]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 45]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 45]

[1, 1, 0, 0, 0, 1, 1, 1, 37]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 37]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 45]

[1, 0, 0, 1, 0, 1, 1, 1, 37]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 37]

[1, 0, 1, 1, 0, 1, 1, 1, 37]

[0, 1, 1, 1, 0, 1, 1, 1, 45]

[1, 1, 1, 1, 0, 1, 1, 1, 45]

[0, 0, 0, 0, 1, 1, 1, 1, 45]

[1, 0, 0, 0, 1, 1, 1, 1, 45]

[0, 1, 0, 0, 1, 1, 1, 1, 37]

[1, 1, 0, 0, 1, 1, 1, 1, 45]

[0, 0, 1, 0, 1, 1, 1, 1, 45]

[1, 0, 1, 0, 1, 1, 1, 1, 37]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 45]

[0, 0, 0, 1, 1, 1, 1, 1, 45]

[1, 0, 0, 1, 1, 1, 1, 1, 45]

[0, 1, 0, 1, 1, 1, 1, 1, 45]

[1, 1, 0, 1, 1, 1, 1, 1, 45]

[0, 0, 1, 1, 1, 1, 1, 1, 45]

[1, 0, 1, 1, 1, 1, 1, 1, 45]

[0, 1, 1, 1, 1, 1, 1, 1, 45]

[1, 1, 1, 1, 1, 1, 1, 1, 45]

APPENDIX IV

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P4 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-1]+s[m-5]+s[m-7]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 45]
    [0, 1, 1, 0, 0, 0, 0, 0, 37]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 45]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 37]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 45]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 37]

[0, 1, 0, 0, 1, 0, 0, 0, 37]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 45]

[0, 0, 0, 1, 1, 0, 0, 0, 37]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 37]

[1, 1, 0, 1, 1, 0, 0, 0, 45]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 45]

[0, 1, 1, 1, 1, 0, 0, 0, 45]

[1, 1, 1, 1, 1, 0, 0, 0, 37]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 37]

[1, 1, 0, 0, 0, 1, 0, 0, 37]

[0, 0, 1, 0, 0, 1, 0, 0, 37]

[1, 0, 1, 0, 0, 1, 0, 0, 37]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 45]

[1, 1, 0, 1, 0, 1, 0, 0, 37]

[0, 0, 1, 1, 0, 1, 0, 0, 45]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 45]

[1, 1, 1, 1, 0, 1, 0, 0, 45]

[0, 0, 0, 0, 1, 1, 0, 0, 37]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 37]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 45]

[1, 1, 1, 0, 1, 1, 0, 0, 45]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 45]

[1, 1, 0, 1, 1, 1, 0, 0, 37]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 45]

[0, 1, 1, 1, 1, 1, 0, 0, 37]

[1, 1, 1, 1, 1, 1, 0, 0, 37]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 37]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 37]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 37]

[1, 0, 0, 1, 0, 0, 1, 0, 37]

[0, 1, 0, 1, 0, 0, 1, 0, 37]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 45]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 37]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 45]

[0, 0, 1, 0, 1, 0, 1, 0, 45]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 37]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 45]

[0, 0, 1, 1, 1, 0, 1, 0, 37]

[1, 0, 1, 1, 1, 0, 1, 0, 45]

[0, 1, 1, 1, 1, 0, 1, 0, 45]

[1, 1, 1, 1, 1, 0, 1, 0, 37]

[0, 0, 0, 0, 0, 1, 1, 0, 37]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 45]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 45]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 37]

[1, 0, 0, 1, 0, 1, 1, 0, 37]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 45]

[1, 0, 1, 1, 0, 1, 1, 0, 45]

[0, 1, 1, 1, 0, 1, 1, 0, 45]

[1, 1, 1, 1, 0, 1, 1, 0, 45]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 37]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 45]

[0, 0, 1, 0, 1, 1, 1, 0, 45]

[1, 0, 1, 0, 1, 1, 1, 0, 37]

[0, 1, 1, 0, 1, 1, 1, 0, 45]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 45]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 45]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 45]

[1, 0, 1, 1, 1, 1, 1, 0, 37]

[0, 1, 1, 1, 1, 1, 1, 0, 37]

[1, 1, 1, 1, 1, 1, 1, 0, 37]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 37]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 37]

[1, 0, 0, 1, 0, 0, 0, 1, 37]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 45]

[0, 0, 1, 1, 0, 0, 0, 1, 37]

[1, 0, 1, 1, 0, 0, 0, 1, 45]

[0, 1, 1, 1, 0, 0, 0, 1, 45]

[1, 1, 1, 1, 0, 0, 0, 1, 37]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 37]

[0, 1, 0, 0, 1, 0, 0, 1, 37]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 37]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 45]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 45]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 37]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 37]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 37]

[0, 0, 1, 0, 0, 1, 0, 1, 37]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 45]

[1, 1, 1, 0, 0, 1, 0, 1, 37]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 45]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 37]

[1, 1, 1, 1, 0, 1, 0, 1, 37]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 45]

[0, 1, 0, 0, 1, 1, 0, 1, 45]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 37]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 45]

[1, 1, 1, 0, 1, 1, 0, 1, 45]

[0, 0, 0, 1, 1, 1, 0, 1, 37]

[1, 0, 0, 1, 1, 1, 0, 1, 45]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 45]

[0, 0, 1, 1, 1, 1, 0, 1, 45]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 45]

[1, 1, 1, 1, 1, 1, 0, 1, 37]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 37]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 37]

[1, 0, 1, 0, 0, 0, 1, 1, 45]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 45]

[1, 1, 0, 1, 0, 0, 1, 1, 45]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 37]

[1, 1, 1, 1, 0, 0, 1, 1, 45]

[0, 0, 0, 0, 1, 0, 1, 1, 45]

[1, 0, 0, 0, 1, 0, 1, 1, 37]

[0, 1, 0, 0, 1, 0, 1, 1, 37]

[1, 1, 0, 0, 1, 0, 1, 1, 37]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 45]

[1, 0, 0, 1, 1, 0, 1, 1, 45]

[0, 1, 0, 1, 1, 0, 1, 1, 37]

[1, 1, 0, 1, 1, 0, 1, 1, 45]

[0, 0, 1, 1, 1, 0, 1, 1, 45]

[1, 0, 1, 1, 1, 0, 1, 1, 37]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 45]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 45]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 45]

[1, 0, 0, 1, 0, 1, 1, 1, 37]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 45]

[1, 0, 1, 1, 0, 1, 1, 1, 37]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 45]

[1, 0, 0, 0, 1, 1, 1, 1, 45]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 37]

[0, 0, 1, 0, 1, 1, 1, 1, 37]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 45]

[1, 0, 0, 1, 1, 1, 1, 1, 37]

[0, 1, 0, 1, 1, 1, 1, 1, 37]

[1, 1, 0, 1, 1, 1, 1, 1, 37]

[0, 0, 1, 1, 1, 1, 1, 1, 37]

[1, 0, 1, 1, 1, 1, 1, 1, 37]

[0, 1, 1, 1, 1, 1, 1, 1, 37]

[1, 1, 1, 1, 1, 1, 1, 1, 37]

APPENDIX V

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P5 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-1]+s[m-3]+s[m-7]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 45]
    [0, 1, 1, 0, 0, 0, 0, 0, 37]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 45]
    [0, 0, 1, 1, 0, 0, 0, 0, 37]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 45]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 37]

[0, 1, 0, 0, 1, 0, 0, 0, 37]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 37]

[1, 1, 1, 0, 1, 0, 0, 0, 45]

[0, 0, 0, 1, 1, 0, 0, 0, 37]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 45]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 37]

[0, 1, 1, 1, 1, 0, 0, 0, 45]

[1, 1, 1, 1, 1, 0, 0, 0, 45]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 37]

[1, 1, 0, 0, 0, 1, 0, 0, 37]

[0, 0, 1, 0, 0, 1, 0, 0, 37]

[1, 0, 1, 0, 0, 1, 0, 0, 37]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 45]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 37]

[1, 0, 1, 1, 0, 1, 0, 0, 37]

[0, 1, 1, 1, 0, 1, 0, 0, 45]

[1, 1, 1, 1, 0, 1, 0, 0, 37]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 37]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 45]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 45]

[1, 1, 1, 0, 1, 1, 0, 0, 45]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 37]

[1, 1, 0, 1, 1, 1, 0, 0, 45]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 45]

[0, 1, 1, 1, 1, 1, 0, 0, 45]

[1, 1, 1, 1, 1, 1, 0, 0, 37]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 37]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 45]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 37]

[1, 0, 0, 1, 0, 0, 1, 0, 37]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 37]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 45]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 37]

[1, 1, 0, 0, 1, 0, 1, 0, 45]

[0, 0, 1, 0, 1, 0, 1, 0, 45]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 37]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 37]

[0, 0, 1, 1, 1, 0, 1, 0, 45]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 45]

[1, 1, 1, 1, 1, 0, 1, 0, 37]

[0, 0, 0, 0, 0, 1, 1, 0, 37]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 37]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 45]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 45]

[1, 0, 1, 1, 0, 1, 1, 0, 45]

[0, 1, 1, 1, 0, 1, 1, 0, 45]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 45]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 37]

[0, 0, 1, 0, 1, 1, 1, 0, 45]

[1, 0, 1, 0, 1, 1, 1, 0, 37]

[0, 1, 1, 0, 1, 1, 1, 0, 45]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 45]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 45]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 37]

[1, 0, 1, 1, 1, 1, 1, 0, 45]

[0, 1, 1, 1, 1, 1, 1, 0, 37]

[1, 1, 1, 1, 1, 1, 1, 0, 37]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 37]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 37]

[1, 0, 0, 1, 0, 0, 0, 1, 37]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 37]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 45]

[0, 1, 1, 1, 0, 0, 0, 1, 37]

[1, 1, 1, 1, 0, 0, 0, 1, 45]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 37]

[0, 1, 0, 0, 1, 0, 0, 1, 37]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 45]

[0, 1, 1, 0, 1, 0, 0, 1, 37]

[1, 1, 1, 0, 1, 0, 0, 1, 37]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 45]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 45]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 37]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 45]

[0, 0, 1, 0, 0, 1, 0, 1, 37]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 45]

[1, 1, 1, 0, 0, 1, 0, 1, 45]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 37]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 37]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 37]

[1, 0, 0, 0, 1, 1, 0, 1, 45]

[0, 1, 0, 0, 1, 1, 0, 1, 45]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 45]

[1, 1, 1, 0, 1, 1, 0, 1, 37]

[0, 0, 0, 1, 1, 1, 0, 1, 45]

[1, 0, 0, 1, 1, 1, 0, 1, 37]

[0, 1, 0, 1, 1, 1, 0, 1, 45]

[1, 1, 0, 1, 1, 1, 0, 1, 37]

[0, 0, 1, 1, 1, 1, 0, 1, 45]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 37]

[1, 1, 1, 1, 1, 1, 0, 1, 37]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 37]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 37]

[1, 0, 1, 0, 0, 0, 1, 1, 37]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 45]

[1, 1, 0, 1, 0, 0, 1, 1, 37]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 45]

[1, 1, 1, 1, 0, 0, 1, 1, 37]

[0, 0, 0, 0, 1, 0, 1, 1, 45]

[1, 0, 0, 0, 1, 0, 1, 1, 45]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 45]

[0, 0, 1, 0, 1, 0, 1, 1, 37]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 45]

[1, 0, 0, 1, 1, 0, 1, 1, 45]

[0, 1, 0, 1, 1, 0, 1, 1, 45]

[1, 1, 0, 1, 1, 0, 1, 1, 45]

[0, 0, 1, 1, 1, 0, 1, 1, 37]

[1, 0, 1, 1, 1, 0, 1, 1, 45]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 37]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 37]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 45]

[1, 0, 0, 1, 0, 1, 1, 1, 45]

[0, 1, 0, 1, 0, 1, 1, 1, 37]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 45]

[1, 0, 1, 1, 0, 1, 1, 1, 45]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 45]

[1, 0, 0, 0, 1, 1, 1, 1, 37]

[0, 1, 0, 0, 1, 1, 1, 1, 37]

[1, 1, 0, 0, 1, 1, 1, 1, 45]

[0, 0, 1, 0, 1, 1, 1, 1, 45]

[1, 0, 1, 0, 1, 1, 1, 1, 37]

[0, 1, 1, 0, 1, 1, 1, 1, 45]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 37]

[1, 0, 0, 1, 1, 1, 1, 1, 37]

[0, 1, 0, 1, 1, 1, 1, 1, 37]

[1, 1, 0, 1, 1, 1, 1, 1, 45]

[0, 0, 1, 1, 1, 1, 1, 1, 37]

[1, 0, 1, 1, 1, 1, 1, 1, 37]

[0, 1, 1, 1, 1, 1, 1, 1, 37]

[1, 1, 1, 1, 1, 1, 1, 1, 37]

APPENDIX VI

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P6 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-1]+s[m-3]+s[m-4]+s[m-5]+s[m-6]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union m fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 45]
    [0, 1, 1, 0, 0, 0, 0, 0, 45]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 45]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 45]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 45]

[0, 1, 0, 0, 1, 0, 0, 0, 37]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 45]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 37]

[0, 0, 1, 1, 1, 0, 0, 0, 37]

[1, 0, 1, 1, 1, 0, 0, 0, 45]

[0, 1, 1, 1, 1, 0, 0, 0, 45]

[1, 1, 1, 1, 1, 0, 0, 0, 45]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 45]

[0, 0, 1, 0, 0, 1, 0, 0, 37]

[1, 0, 1, 0, 0, 1, 0, 0, 37]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 37]

[0, 1, 0, 1, 0, 1, 0, 0, 45]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 37]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 37]

[1, 1, 1, 1, 0, 1, 0, 0, 45]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 45]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 37]

[1, 1, 1, 0, 1, 1, 0, 0, 37]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 37]

[0, 1, 0, 1, 1, 1, 0, 0, 37]

[1, 1, 0, 1, 1, 1, 0, 0, 45]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 37]

[0, 1, 1, 1, 1, 1, 0, 0, 45]

[1, 1, 1, 1, 1, 1, 0, 0, 45]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 37]

[1, 1, 1, 0, 0, 0, 1, 0, 45]

[0, 0, 0, 1, 0, 0, 1, 0, 45]

[1, 0, 0, 1, 0, 0, 1, 0, 37]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 37]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 37]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 37]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 37]

[0, 0, 1, 0, 1, 0, 1, 0, 45]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 37]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 37]

[0, 0, 1, 1, 1, 0, 1, 0, 45]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 37]

[1, 1, 1, 1, 1, 0, 1, 0, 45]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 37]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 37]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 45]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 37]

[0, 0, 1, 1, 0, 1, 1, 0, 37]

[1, 0, 1, 1, 0, 1, 1, 0, 37]

[0, 1, 1, 1, 0, 1, 1, 0, 37]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 45]

[0, 1, 0, 0, 1, 1, 1, 0, 37]

[1, 1, 0, 0, 1, 1, 1, 0, 37]

[0, 0, 1, 0, 1, 1, 1, 0, 37]

[1, 0, 1, 0, 1, 1, 1, 0, 37]

[0, 1, 1, 0, 1, 1, 1, 0, 45]

[1, 1, 1, 0, 1, 1, 1, 0, 45]

[0, 0, 0, 1, 1, 1, 1, 0, 37]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 37]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 45]

[1, 0, 1, 1, 1, 1, 1, 0, 45]

[0, 1, 1, 1, 1, 1, 1, 0, 45]

[1, 1, 1, 1, 1, 1, 1, 0, 45]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 45]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 45]

[1, 0, 0, 1, 0, 0, 0, 1, 37]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 45]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 37]

[0, 1, 1, 1, 0, 0, 0, 1, 37]

[1, 1, 1, 1, 0, 0, 0, 1, 45]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 45]

[0, 1, 0, 0, 1, 0, 0, 1, 37]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 37]

[1, 0, 1, 0, 1, 0, 0, 1, 45]

[0, 1, 1, 0, 1, 0, 0, 1, 37]

[1, 1, 1, 0, 1, 0, 0, 1, 37]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 37]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 37]

[0, 1, 1, 1, 1, 0, 0, 1, 37]

[1, 1, 1, 1, 1, 0, 0, 1, 45]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 37]

[0, 0, 1, 0, 0, 1, 0, 1, 45]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 37]

[1, 1, 1, 0, 0, 1, 0, 1, 37]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 45]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 37]

[0, 1, 1, 1, 0, 1, 0, 1, 45]

[1, 1, 1, 1, 0, 1, 0, 1, 37]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 37]

[0, 1, 0, 0, 1, 1, 0, 1, 37]

[1, 1, 0, 0, 1, 1, 0, 1, 45]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 37]

[0, 1, 1, 0, 1, 1, 0, 1, 37]

[1, 1, 1, 0, 1, 1, 0, 1, 37]

[0, 0, 0, 1, 1, 1, 0, 1, 45]

[1, 0, 0, 1, 1, 1, 0, 1, 37]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 45]

[0, 0, 1, 1, 1, 1, 0, 1, 37]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 45]

[1, 1, 1, 1, 1, 1, 0, 1, 45]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 45]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 37]

[1, 0, 1, 0, 0, 0, 1, 1, 45]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 37]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 37]

[1, 1, 0, 1, 0, 0, 1, 1, 37]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 37]

[1, 1, 1, 1, 0, 0, 1, 1, 45]

[0, 0, 0, 0, 1, 0, 1, 1, 45]

[1, 0, 0, 0, 1, 0, 1, 1, 37]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 37]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 37]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 45]

[1, 0, 0, 1, 1, 0, 1, 1, 37]

[0, 1, 0, 1, 1, 0, 1, 1, 37]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 37]

[1, 0, 1, 1, 1, 0, 1, 1, 45]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 45]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 45]

[1, 1, 0, 0, 0, 1, 1, 1, 37]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 37]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 37]

[1, 0, 0, 1, 0, 1, 1, 1, 37]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 45]

[1, 0, 1, 1, 0, 1, 1, 1, 37]

[0, 1, 1, 1, 0, 1, 1, 1, 45]

[1, 1, 1, 1, 0, 1, 1, 1, 45]

[0, 0, 0, 0, 1, 1, 1, 1, 45]

[1, 0, 0, 0, 1, 1, 1, 1, 37]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 45]

[0, 0, 1, 0, 1, 1, 1, 1, 37]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 45]

[0, 0, 0, 1, 1, 1, 1, 1, 45]

[1, 0, 0, 1, 1, 1, 1, 1, 45]

[0, 1, 0, 1, 1, 1, 1, 1, 45]

[1, 1, 0, 1, 1, 1, 1, 1, 45]

[0, 0, 1, 1, 1, 1, 1, 1, 45]

[1, 0, 1, 1, 1, 1, 1, 1, 45]

[0, 1, 1, 1, 1, 1, 1, 1, 45]

[1, 1, 1, 1, 1, 1, 1, 1, 45]

APPENDIX VII

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P7 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-1]+s[m-2]+s[m-4]+s[m-5]+s[m-6]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 37]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 45]
    [0, 1, 1, 0, 0, 0, 0, 0, 45]
    [1, 1, 1, 0, 0, 0, 0, 0, 37]
    [0, 0, 0, 1, 0, 0, 0, 0, 45]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 45]
    [1, 1, 0, 1, 0, 0, 0, 0, 45]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 37]

[1, 1, 1, 1, 0, 0, 0, 0, 37]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 45]

[0, 1, 0, 0, 1, 0, 0, 0, 37]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 45]

[0, 1, 1, 0, 1, 0, 0, 0, 45]

[1, 1, 1, 0, 1, 0, 0, 0, 37]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 45]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 37]

[0, 1, 1, 1, 1, 0, 0, 0, 37]

[1, 1, 1, 1, 1, 0, 0, 0, 37]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 45]

[0, 0, 1, 0, 0, 1, 0, 0, 45]

[1, 0, 1, 0, 0, 1, 0, 0, 37]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 37]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 45]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 37]

[1, 1, 1, 1, 0, 1, 0, 0, 45]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 45]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 45]

[1, 1, 1, 0, 1, 1, 0, 0, 45]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 37]

[1, 1, 0, 1, 1, 1, 0, 0, 37]

[0, 0, 1, 1, 1, 1, 0, 0, 45]

[1, 0, 1, 1, 1, 1, 0, 0, 37]

[0, 1, 1, 1, 1, 1, 0, 0, 37]

[1, 1, 1, 1, 1, 1, 0, 0, 37]

[0, 0, 0, 0, 0, 0, 1, 0, 37]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 45]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 45]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 45]

[1, 0, 0, 1, 0, 0, 1, 0, 45]

[0, 1, 0, 1, 0, 0, 1, 0, 37]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 45]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 37]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 45]

[0, 0, 1, 0, 1, 0, 1, 0, 37]

[1, 0, 1, 0, 1, 0, 1, 0, 37]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 45]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 45]

[0, 0, 1, 1, 1, 0, 1, 0, 37]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 45]

[1, 1, 1, 1, 1, 0, 1, 0, 45]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 45]

[0, 1, 0, 0, 0, 1, 1, 0, 37]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 45]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 37]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 37]

[1, 0, 1, 1, 0, 1, 1, 0, 45]

[0, 1, 1, 1, 0, 1, 1, 0, 45]

[1, 1, 1, 1, 0, 1, 1, 0, 45]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 37]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 37]

[0, 0, 1, 0, 1, 1, 1, 0, 45]

[1, 0, 1, 0, 1, 1, 1, 0, 37]

[0, 1, 1, 0, 1, 1, 1, 0, 37]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 45]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 37]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 37]

[1, 0, 1, 1, 1, 1, 1, 0, 45]

[0, 1, 1, 1, 1, 1, 1, 0, 37]

[1, 1, 1, 1, 1, 1, 1, 0, 45]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 37]

[0, 1, 0, 0, 0, 0, 0, 1, 45]

[1, 1, 0, 0, 0, 0, 0, 1, 45]

[0, 0, 1, 0, 0, 0, 0, 1, 45]

[1, 0, 1, 0, 0, 0, 0, 1, 45]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 37]

[0, 0, 0, 1, 0, 0, 0, 1, 45]

[1, 0, 0, 1, 0, 0, 0, 1, 37]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 37]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 45]

[0, 1, 1, 1, 0, 0, 0, 1, 45]

[1, 1, 1, 1, 0, 0, 0, 1, 37]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 45]

[0, 1, 0, 0, 1, 0, 0, 1, 45]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 37]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 45]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 45]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 37]

[0, 1, 1, 1, 1, 0, 0, 1, 45]

[1, 1, 1, 1, 1, 0, 0, 1, 37]

[0, 0, 0, 0, 0, 1, 0, 1, 37]

[1, 0, 0, 0, 0, 1, 0, 1, 45]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 37]

[0, 0, 1, 0, 0, 1, 0, 1, 45]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 45]

[1, 1, 1, 0, 0, 1, 0, 1, 45]

[0, 0, 0, 1, 0, 1, 0, 1, 37]

[1, 0, 0, 1, 0, 1, 0, 1, 45]

[0, 1, 0, 1, 0, 1, 0, 1, 37]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 37]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 45]

[1, 0, 0, 0, 1, 1, 0, 1, 37]

[0, 1, 0, 0, 1, 1, 0, 1, 45]

[1, 1, 0, 0, 1, 1, 0, 1, 37]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 37]

[1, 1, 1, 0, 1, 1, 0, 1, 45]

[0, 0, 0, 1, 1, 1, 0, 1, 37]

[1, 0, 0, 1, 1, 1, 0, 1, 37]

[0, 1, 0, 1, 1, 1, 0, 1, 45]

[1, 1, 0, 1, 1, 1, 0, 1, 37]

[0, 0, 1, 1, 1, 1, 0, 1, 45]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 45]

[1, 1, 1, 1, 1, 1, 0, 1, 45]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 45]

[0, 1, 0, 0, 0, 0, 1, 1, 45]

[1, 1, 0, 0, 0, 0, 1, 1, 37]

[0, 0, 1, 0, 0, 0, 1, 1, 37]

[1, 0, 1, 0, 0, 0, 1, 1, 37]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 45]

[1, 1, 0, 1, 0, 0, 1, 1, 45]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 37]

[1, 1, 1, 1, 0, 0, 1, 1, 37]

[0, 0, 0, 0, 1, 0, 1, 1, 37]

[1, 0, 0, 0, 1, 0, 1, 1, 45]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 45]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 37]

[0, 0, 0, 1, 1, 0, 1, 1, 37]

[1, 0, 0, 1, 1, 0, 1, 1, 37]

[0, 1, 0, 1, 1, 0, 1, 1, 45]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 37]

[1, 0, 1, 1, 1, 0, 1, 1, 45]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 45]

[0, 0, 0, 0, 0, 1, 1, 1, 45]

[1, 0, 0, 0, 0, 1, 1, 1, 37]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 45]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 37]

[0, 0, 0, 1, 0, 1, 1, 1, 37]

[1, 0, 0, 1, 0, 1, 1, 1, 45]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 37]

[0, 0, 1, 1, 0, 1, 1, 1, 37]

[1, 0, 1, 1, 0, 1, 1, 1, 37]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 37]

[1, 0, 0, 0, 1, 1, 1, 1, 45]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 45]

[0, 0, 1, 0, 1, 1, 1, 1, 37]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 37]

[1, 0, 0, 1, 1, 1, 1, 1, 45]

[0, 1, 0, 1, 1, 1, 1, 1, 45]

[1, 1, 0, 1, 1, 1, 1, 1, 37]

[0, 0, 1, 1, 1, 1, 1, 1, 45]

[1, 0, 1, 1, 1, 1, 1, 1, 37]

[0, 1, 1, 1, 1, 1, 1, 1, 45]

[1, 1, 1, 1, 1, 1, 1, 1, 45]

APPENDIX VIII

MAPLE codes to determine the number of zeros based on the monic irreducible polynomial P8 of degree 8 and order 85 in chapter 3, for every possible initial sequence.

```
for k from 257 to 511 do
for n from 1 to 8 do
s[n] :=convert(k,base,2)[n];od:
for m from 9 to 85 do
s[m] :=s[m-1]+s[m-2]+s[m-3]+s[m-4]+s[m-5]+s[m-8] mod 2;
t :={};od:
for m from 1 to 85 do
if s[m]=0 then t :=t union {m} fi;od:
[s[1],s[2],s[3],s[4],s[5],s[6],s[7],s[8],nops(t)];od;
[1, 0, 0, 0, 0, 0, 0, 0, 45]
    [0, 1, 0, 0, 0, 0, 0, 0, 45]
    [1, 1, 0, 0, 0, 0, 0, 0, 45]
    [0, 0, 1, 0, 0, 0, 0, 0, 45]
    [1, 0, 1, 0, 0, 0, 0, 0, 37]
    [0, 1, 1, 0, 0, 0, 0, 0, 45]
    [1, 1, 1, 0, 0, 0, 0, 0, 45]
    [0, 0, 0, 1, 0, 0, 0, 0, 37]
    [1, 0, 0, 1, 0, 0, 0, 0, 45]
    [0, 1, 0, 1, 0, 0, 0, 0, 37]
    [1, 1, 0, 1, 0, 0, 0, 0, 37]
    [0, 0, 1, 1, 0, 0, 0, 0, 45]
    [1, 0, 1, 1, 0, 0, 0, 0, 45]
```

[0, 1, 1, 1, 0, 0, 0, 0, 45]

[1, 1, 1, 1, 0, 0, 0, 0, 45]

[0, 0, 0, 0, 1, 0, 0, 0, 45]

[1, 0, 0, 0, 1, 0, 0, 0, 37]

[0, 1, 0, 0, 1, 0, 0, 0, 45]

[1, 1, 0, 0, 1, 0, 0, 0, 45]

[0, 0, 1, 0, 1, 0, 0, 0, 45]

[1, 0, 1, 0, 1, 0, 0, 0, 37]

[0, 1, 1, 0, 1, 0, 0, 0, 37]

[1, 1, 1, 0, 1, 0, 0, 0, 37]

[0, 0, 0, 1, 1, 0, 0, 0, 45]

[1, 0, 0, 1, 1, 0, 0, 0, 45]

[0, 1, 0, 1, 1, 0, 0, 0, 45]

[1, 1, 0, 1, 1, 0, 0, 0, 45]

[0, 0, 1, 1, 1, 0, 0, 0, 45]

[1, 0, 1, 1, 1, 0, 0, 0, 37]

[0, 1, 1, 1, 1, 0, 0, 0, 45]

[1, 1, 1, 1, 1, 0, 0, 0, 45]

[0, 0, 0, 0, 0, 1, 0, 0, 45]

[1, 0, 0, 0, 0, 1, 0, 0, 45]

[0, 1, 0, 0, 0, 1, 0, 0, 45]

[1, 1, 0, 0, 0, 1, 0, 0, 37]

[0, 0, 1, 0, 0, 1, 0, 0, 45]

[1, 0, 1, 0, 0, 1, 0, 0, 45]

[0, 1, 1, 0, 0, 1, 0, 0, 45]

[1, 1, 1, 0, 0, 1, 0, 0, 45]

[0, 0, 0, 1, 0, 1, 0, 0, 45]

[1, 0, 0, 1, 0, 1, 0, 0, 45]

[0, 1, 0, 1, 0, 1, 0, 0, 37]

[1, 1, 0, 1, 0, 1, 0, 0, 45]

[0, 0, 1, 1, 0, 1, 0, 0, 37]

[1, 0, 1, 1, 0, 1, 0, 0, 45]

[0, 1, 1, 1, 0, 1, 0, 0, 37]

[1, 1, 1, 1, 0, 1, 0, 0, 37]

[0, 0, 0, 0, 1, 1, 0, 0, 45]

[1, 0, 0, 0, 1, 1, 0, 0, 45]

[0, 1, 0, 0, 1, 1, 0, 0, 45]

[1, 1, 0, 0, 1, 1, 0, 0, 45]

[0, 0, 1, 0, 1, 1, 0, 0, 45]

[1, 0, 1, 0, 1, 1, 0, 0, 45]

[0, 1, 1, 0, 1, 1, 0, 0, 45]

[1, 1, 1, 0, 1, 1, 0, 0, 37]

[0, 0, 0, 1, 1, 1, 0, 0, 45]

[1, 0, 0, 1, 1, 1, 0, 0, 45]

[0, 1, 0, 1, 1, 1, 0, 0, 45]

[1, 1, 0, 1, 1, 1, 0, 0, 37]

[0, 0, 1, 1, 1, 1, 0, 0, 37]

[1, 0, 1, 1, 1, 1, 0, 0, 45]

[0, 1, 1, 1, 1, 1, 0, 0, 45]

[1, 1, 1, 1, 1, 1, 0, 0, 45]

[0, 0, 0, 0, 0, 0, 1, 0, 45]

[1, 0, 0, 0, 0, 0, 1, 0, 45]

[0, 1, 0, 0, 0, 0, 1, 0, 37]

[1, 1, 0, 0, 0, 0, 1, 0, 45]

[0, 0, 1, 0, 0, 0, 1, 0, 45]

[1, 0, 1, 0, 0, 0, 1, 0, 45]

[0, 1, 1, 0, 0, 0, 1, 0, 45]

[1, 1, 1, 0, 0, 0, 1, 0, 37]

[0, 0, 0, 1, 0, 0, 1, 0, 45]

[1, 0, 0, 1, 0, 0, 1, 0, 45]

[0, 1, 0, 1, 0, 0, 1, 0, 45]

[1, 1, 0, 1, 0, 0, 1, 0, 45]

[0, 0, 1, 1, 0, 0, 1, 0, 45]

[1, 0, 1, 1, 0, 0, 1, 0, 37]

[0, 1, 1, 1, 0, 0, 1, 0, 45]

[1, 1, 1, 1, 0, 0, 1, 0, 45]

[0, 0, 0, 0, 1, 0, 1, 0, 45]

[1, 0, 0, 0, 1, 0, 1, 0, 45]

[0, 1, 0, 0, 1, 0, 1, 0, 45]

[1, 1, 0, 0, 1, 0, 1, 0, 37]

[0, 0, 1, 0, 1, 0, 1, 0, 37]

[1, 0, 1, 0, 1, 0, 1, 0, 45]

[0, 1, 1, 0, 1, 0, 1, 0, 45]

[1, 1, 1, 0, 1, 0, 1, 0, 45]

[0, 0, 0, 1, 1, 0, 1, 0, 45]

[1, 0, 0, 1, 1, 0, 1, 0, 37]

[0, 1, 0, 1, 1, 0, 1, 0, 45]

[1, 1, 0, 1, 1, 0, 1, 0, 45]

[0, 0, 1, 1, 1, 0, 1, 0, 45]

[1, 0, 1, 1, 1, 0, 1, 0, 37]

[0, 1, 1, 1, 1, 0, 1, 0, 45]

[1, 1, 1, 1, 1, 0, 1, 0, 37]

[0, 0, 0, 0, 0, 1, 1, 0, 45]

[1, 0, 0, 0, 0, 1, 1, 0, 37]

[0, 1, 0, 0, 0, 1, 1, 0, 45]

[1, 1, 0, 0, 0, 1, 1, 0, 45]

[0, 0, 1, 0, 0, 1, 1, 0, 45]

[1, 0, 1, 0, 0, 1, 1, 0, 37]

[0, 1, 1, 0, 0, 1, 1, 0, 45]

[1, 1, 1, 0, 0, 1, 1, 0, 37]

[0, 0, 0, 1, 0, 1, 1, 0, 45]

[1, 0, 0, 1, 0, 1, 1, 0, 45]

[0, 1, 0, 1, 0, 1, 1, 0, 45]

[1, 1, 0, 1, 0, 1, 1, 0, 45]

[0, 0, 1, 1, 0, 1, 1, 0, 37]

[1, 0, 1, 1, 0, 1, 1, 0, 45]

[0, 1, 1, 1, 0, 1, 1, 0, 45]

[1, 1, 1, 1, 0, 1, 1, 0, 37]

[0, 0, 0, 0, 1, 1, 1, 0, 45]

[1, 0, 0, 0, 1, 1, 1, 0, 45]

[0, 1, 0, 0, 1, 1, 1, 0, 45]

[1, 1, 0, 0, 1, 1, 1, 0, 45]

[0, 0, 1, 0, 1, 1, 1, 0, 37]

[1, 0, 1, 0, 1, 1, 1, 0, 45]

[0, 1, 1, 0, 1, 1, 1, 0, 37]

[1, 1, 1, 0, 1, 1, 1, 0, 37]

[0, 0, 0, 1, 1, 1, 1, 0, 37]

[1, 0, 0, 1, 1, 1, 1, 0, 45]

[0, 1, 0, 1, 1, 1, 1, 0, 45]

[1, 1, 0, 1, 1, 1, 1, 0, 37]

[0, 0, 1, 1, 1, 1, 1, 0, 45]

[1, 0, 1, 1, 1, 1, 1, 0, 37]

[0, 1, 1, 1, 1, 1, 1, 0, 45]

[1, 1, 1, 1, 1, 1, 1, 0, 37]

[0, 0, 0, 0, 0, 0, 0, 1, 45]

[1, 0, 0, 0, 0, 0, 0, 1, 45]

[0, 1, 0, 0, 0, 0, 0, 1, 37]

[1, 1, 0, 0, 0, 0, 0, 1, 45]

[0, 0, 1, 0, 0, 0, 0, 1, 37]

[1, 0, 1, 0, 0, 0, 0, 1, 37]

[0, 1, 1, 0, 0, 0, 0, 1, 45]

[1, 1, 1, 0, 0, 0, 0, 1, 45]

[0, 0, 0, 1, 0, 0, 0, 1, 45]

[1, 0, 0, 1, 0, 0, 0, 1, 45]

[0, 1, 0, 1, 0, 0, 0, 1, 45]

[1, 1, 0, 1, 0, 0, 0, 1, 37]

[0, 0, 1, 1, 0, 0, 0, 1, 45]

[1, 0, 1, 1, 0, 0, 0, 1, 45]

[0, 1, 1, 1, 0, 0, 0, 1, 37]

[1, 1, 1, 1, 0, 0, 0, 1, 45]

[0, 0, 0, 0, 1, 0, 0, 1, 45]

[1, 0, 0, 0, 1, 0, 0, 1, 45]

[0, 1, 0, 0, 1, 0, 0, 1, 45]

[1, 1, 0, 0, 1, 0, 0, 1, 45]

[0, 0, 1, 0, 1, 0, 0, 1, 45]

[1, 0, 1, 0, 1, 0, 0, 1, 45]

[0, 1, 1, 0, 1, 0, 0, 1, 45]

[1, 1, 1, 0, 1, 0, 0, 1, 37]

[0, 0, 0, 1, 1, 0, 0, 1, 45]

[1, 0, 0, 1, 1, 0, 0, 1, 45]

[0, 1, 0, 1, 1, 0, 0, 1, 45]

[1, 1, 0, 1, 1, 0, 0, 1, 37]

[0, 0, 1, 1, 1, 0, 0, 1, 45]

[1, 0, 1, 1, 1, 0, 0, 1, 45]

[0, 1, 1, 1, 1, 0, 0, 1, 37]

[1, 1, 1, 1, 1, 0, 0, 1, 45]

[0, 0, 0, 0, 0, 1, 0, 1, 45]

[1, 0, 0, 0, 0, 1, 0, 1, 37]

[0, 1, 0, 0, 0, 1, 0, 1, 45]

[1, 1, 0, 0, 0, 1, 0, 1, 45]

[0, 0, 1, 0, 0, 1, 0, 1, 45]

[1, 0, 1, 0, 0, 1, 0, 1, 45]

[0, 1, 1, 0, 0, 1, 0, 1, 37]

[1, 1, 1, 0, 0, 1, 0, 1, 45]

[0, 0, 0, 1, 0, 1, 0, 1, 45]

[1, 0, 0, 1, 0, 1, 0, 1, 37]

[0, 1, 0, 1, 0, 1, 0, 1, 45]

[1, 1, 0, 1, 0, 1, 0, 1, 45]

[0, 0, 1, 1, 0, 1, 0, 1, 45]

[1, 0, 1, 1, 0, 1, 0, 1, 45]

[0, 1, 1, 1, 0, 1, 0, 1, 45]

[1, 1, 1, 1, 0, 1, 0, 1, 45]

[0, 0, 0, 0, 1, 1, 0, 1, 37]

[1, 0, 0, 0, 1, 1, 0, 1, 45]

[0, 1, 0, 0, 1, 1, 0, 1, 37]

[1, 1, 0, 0, 1, 1, 0, 1, 37]

[0, 0, 1, 0, 1, 1, 0, 1, 45]

[1, 0, 1, 0, 1, 1, 0, 1, 45]

[0, 1, 1, 0, 1, 1, 0, 1, 37]

[1, 1, 1, 0, 1, 1, 0, 1, 45]

[0, 0, 0, 1, 1, 1, 0, 1, 45]

[1, 0, 0, 1, 1, 1, 0, 1, 45]

[0, 1, 0, 1, 1, 1, 0, 1, 37]

[1, 1, 0, 1, 1, 1, 0, 1, 37]

[0, 0, 1, 1, 1, 1, 0, 1, 45]

[1, 0, 1, 1, 1, 1, 0, 1, 37]

[0, 1, 1, 1, 1, 1, 0, 1, 37]

[1, 1, 1, 1, 1, 1, 0, 1, 37]

[0, 0, 0, 0, 0, 0, 1, 1, 45]

[1, 0, 0, 0, 0, 0, 1, 1, 37]

[0, 1, 0, 0, 0, 0, 1, 1, 37]

[1, 1, 0, 0, 0, 0, 1, 1, 45]

[0, 0, 1, 0, 0, 0, 1, 1, 45]

[1, 0, 1, 0, 0, 0, 1, 1, 37]

[0, 1, 1, 0, 0, 0, 1, 1, 45]

[1, 1, 1, 0, 0, 0, 1, 1, 45]

[0, 0, 0, 1, 0, 0, 1, 1, 45]

[1, 0, 0, 1, 0, 0, 1, 1, 45]

[0, 1, 0, 1, 0, 0, 1, 1, 45]

[1, 1, 0, 1, 0, 0, 1, 1, 37]

[0, 0, 1, 1, 0, 0, 1, 1, 45]

[1, 0, 1, 1, 0, 0, 1, 1, 45]

[0, 1, 1, 1, 0, 0, 1, 1, 45]

[1, 1, 1, 1, 0, 0, 1, 1, 37]

[0, 0, 0, 0, 1, 0, 1, 1, 37]

[1, 0, 0, 0, 1, 0, 1, 1, 45]

[0, 1, 0, 0, 1, 0, 1, 1, 45]

[1, 1, 0, 0, 1, 0, 1, 1, 45]

[0, 0, 1, 0, 1, 0, 1, 1, 45]

[1, 0, 1, 0, 1, 0, 1, 1, 45]

[0, 1, 1, 0, 1, 0, 1, 1, 45]

[1, 1, 1, 0, 1, 0, 1, 1, 45]

[0, 0, 0, 1, 1, 0, 1, 1, 37]

[1, 0, 0, 1, 1, 0, 1, 1, 37]

[0, 1, 0, 1, 1, 0, 1, 1, 45]

[1, 1, 0, 1, 1, 0, 1, 1, 37]

[0, 0, 1, 1, 1, 0, 1, 1, 45]

[1, 0, 1, 1, 1, 0, 1, 1, 37]

[0, 1, 1, 1, 1, 0, 1, 1, 37]

[1, 1, 1, 1, 1, 0, 1, 1, 37]

[0, 0, 0, 0, 0, 1, 1, 1, 37]

[1, 0, 0, 0, 0, 1, 1, 1, 45]

[0, 1, 0, 0, 0, 1, 1, 1, 37]

[1, 1, 0, 0, 0, 1, 1, 1, 45]

[0, 0, 1, 0, 0, 1, 1, 1, 45]

[1, 0, 1, 0, 0, 1, 1, 1, 45]

[0, 1, 1, 0, 0, 1, 1, 1, 45]

[1, 1, 1, 0, 0, 1, 1, 1, 45]

[0, 0, 0, 1, 0, 1, 1, 1, 37]

[1, 0, 0, 1, 0, 1, 1, 1, 45]

[0, 1, 0, 1, 0, 1, 1, 1, 45]

[1, 1, 0, 1, 0, 1, 1, 1, 45]

[0, 0, 1, 1, 0, 1, 1, 1, 37]

[1, 0, 1, 1, 0, 1, 1, 1, 37]

[0, 1, 1, 1, 0, 1, 1, 1, 37]

[1, 1, 1, 1, 0, 1, 1, 1, 37]

[0, 0, 0, 0, 1, 1, 1, 1, 37]

[1, 0, 0, 0, 1, 1, 1, 1, 37]

[0, 1, 0, 0, 1, 1, 1, 1, 45]

[1, 1, 0, 0, 1, 1, 1, 1, 45]

[0, 0, 1, 0, 1, 1, 1, 1, 45]

[1, 0, 1, 0, 1, 1, 1, 1, 45]

[0, 1, 1, 0, 1, 1, 1, 1, 37]

[1, 1, 1, 0, 1, 1, 1, 1, 37]

[0, 0, 0, 1, 1, 1, 1, 1, 37]

[1, 0, 0, 1, 1, 1, 1, 1, 45]

[0, 1, 0, 1, 1, 1, 1, 1, 45]

[1, 1, 0, 1, 1, 1, 1, 1, 37]

[0, 0, 1, 1, 1, 1, 1, 1, 37]

[1, 0, 1, 1, 1, 1, 1, 1, 45]

[0, 1, 1, 1, 1, 1, 1, 1, 37]

[1, 1, 1, 1, 1, 1, 1, 1, 37]

APPENDIX IX

MAPLE codes to determine the number of zeros of the sequence of irreducible polynomials of degree 9 and order 73.

exp1:=$x^9 + x + 1$ :

exp2:=$x^9 + x^4 + x^2 + x + 1$ :

exp3:=$x^9 + x^6 + x^3 + x + 1$ :

exp4:=$x^9 + x^6 + x^5 + x^2 + 1$ :

exp5:=$x^9 + x^7 + x^4 + x^3 + 1$ :

exp6:=$x^9 + x^8 + 1$ :

exp7:=$x^9 + x^8 + x^6 + x^3 + x^2 + x + 1$ :

exp8:=$x^9 + x^8 + x^7 + x^5 + 1$ :

a1:=[exp1, exp2, exp3, exp4, exp5, exp6, exp7, exp8]:

s[0]:=1: s[1]:=1: s[2]:=1: s[3]:=0: s[4]:=0: s[5]:=0: s[6]:=0: s[7]:=0: s[8]:=0:

i:=8;

i := 8

a1[i];

$x^9 + x^8 + x^7 + x^5 + 1$

for n from 0 to 63 do

s[n+9]:=coeff(a1[i],x,8)*s[n+8]+coeff(a1[i],x,7)*s[n+7]+coeff(a1[i],x,6)*s[n+6] +coeff(a1[i],x,5)*s[n+5]+coeff(a1[i],x,4)*s[n+4]+coeff(a1[i],x,3)*s[n+3] +coeff(a1[i],x,2)*s[n+2]+coeff(a1[i],x,1)*s[n+1]+s[n] mod 2;od:

t :={};

t := {}

for n from 0 to 72 do

if s[n]=0 then t :=t union n fi;od;

t;

$\{3, 4, 5, 6, 7, 8, 10, 11, 12, 15, 17, 21, 27, 32, 35, 38, 39, 40,$
$42, 43, 44, 45, 48, 52, 53, 57, 60, 62, 64, 67, 68, 71, 72\}$

nops(t);

33

APPENDIX X

MAPLE codes to determine the number of zeros of the sequence of irreducible polynomials of degree 10 and order 93.

exp1:=$x^{10}+x^5+x^4+x^2+1:$

exp2:=$x^{10}+x^8+x^3+x+1:$

exp3:=$x^{10}+x^8+x^6+x^5+1:$

exp4:=$x^{10}+x^9+x^7+x^2+1:$

exp5:=$x^{10}+x^9+x^7+x^5+x^2+x+1:$

exp6:=$x^{10}+x^9+x^8+x^5+x^3+x+1:$

a1:=[exp1, exp2, exp3, exp4, exp5, exp6]:

s[0]:=1: s[1]:=1: s[2]:=0: s[3]:=1: s[4]:=0: s[5]:=0: s[6]:=0: s[7]:=0: s[8]:=0: s[9]:=1:

i:=6;

i := 6

a1[i];

$x^{10}+x^9+x^8+x^5+x^3+x+1$

for n from 0 to 82 do

s[n+10] :=coeff(a1[i],x,9)*s[n+9]+coeff(a1[i],x,8)*s[n+8]+coeff(a1[i],x,7)*s[n+7] +coeff(a1[i],x,6)*s[n+6]+coeff(a1[i],x,5)*s[n+5]+coeff(a1[i],x,4)*s[n+4] +coeff(a1[i],x,3)*s[n+3]+coeff(a1[i],x,2)*s[n+2]+coeff(a1[i],x,1)*s[n+1] +s[n] mod 2;od:

t :={};

t := {}

for n from 0 to 92 do

if s[n]=0 then t :=t union n fi;od;

t;

{2, 4, 5, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18, 19, 20, 21, 23, 25,
26, 29, 32, 35, 37, 38, 39, 41, 42, 44, 46, 47, 49, 50, 51,
52, 53, 56, 57, 59, 60, 62, 65, 66, 68, 69, 70, 71, 72, 73,
74, 75, 77, 80, 81, 82, 83, 86, 87, 88, 89, 91, 92}

nops(t);

61

# VITA

Graduate School
Southern Illinois University

Yasanthi Kottegoda Date of Birth: December 05, 1983

E-mail: yasanthi_k@yahoo.com

501, East College Street, Apt 46, Carbondale, Illinois 62901

61/1, Abeyrathna Mawatha, Boralesgamuwa, Sri Lanka

University of Colombo, Sri Lanka
Bachelor of Science, Mathematics, November 2007

Research Paper Title:
The Number of Zeros in a Linear Recurrence Sequence over a Finite Field.

Major Professor: Dr. R. Fitzgerald